FNGi DHCPatriot™
Version 4.1.x CALEA Edition
Operations Manual

By: Darren L. Ankney

Editing: Cory P. Lykins

Cover Design: Cory P. Lykins

Manual Figures: Darren L. Ankney
Cory P. Lykins

First Network Group Inc.
http://www.network1.net
4-6 Perry St.
P.O. Box 1662
Wapakoneta, OH 45895

Thank you for purchasing the DHCPatriot™ from FNGi. In this well done solution, you have received the very best broadband authentication solution that the industry has to offer, as well as FNGi's renowned attention to detail. With your purchase, you also receive a free year of our maintenance contract that includes premium access to a full year of our legendary product support, as well as our excellent 24/7 monitoring and response for your DHCPatriot™. We pledge to help you implement the DHCPatriot™ in a seamless fashion. And to make sure ownership of the DHCPatriot™ is an easy and pleasant experience.

This manual will guide you through the installation, setup, and ongoing usage of the DHCPatriot™. We will begin by discussing the requirements for using the DHCPatriot™ in your network. We will then move on to the physical installation of the devices. This will be followed by configuration instructions. Finally, the proper usage of the Web Administration Interface will be discussed. Several appendices are included to assist in the training of customer service and technical support personnel as well as device troubleshooting and technical applications.

A word on DHCPatriot™ version numbers. Each DHCPatriot™ version (since 3.0.1) is comprised of three numbers separated by periods. The first number in the series indicates the major release. The second number indicates the minor release. The third number indicates the patch level. To clarify, the version number 4.0.0 is the first release in the 4 series. If bugs are found after release in version 4.0.0, then these bugs will be fixed in 4.0.1 which will be the first patch level of the first release in the 4 series. The next edition with minor feature changes or additions would be version 4.1.0 which is the first minor release in the 4 series. This manual applies to release 4.1.x.

Your journey toward freedom for your broadband network begins now.

1 Requirements and Network Integration

This chapter's focus is on what is needed to place the DHCPatriot™ into your network. It is designed to give you an overview of all of the requirements, as well as a description of optional equipment such as the Allot Communications NetEnforcer® or an external RADIUS server.

1.1 Network and Router Requirements

The DHCPatriot™ has only a few network related requirements. They are listed here so that compatibility may be ensured:

1.1.1 DHCP

The customers must use DHCP (see rfc1542 – http://www.faqs.org/rfcs/rfc1542.html) to obtain their dynamic IP Address. The DHCPatriot™ does not support other broadband authentication protocols such as PPPoE.

1.1.2 DHCP Relay Agent Protocol

The gateway routers that the customers are connected to must support the DHCP Relay Agent protocol (see “BOOTP Relay Agent” rfc1542 Section 4 – http://www.faqs.org/rfcs/rfc1542.html) (Cisco® defines this as the 'ip helper address' command). This is important as the DHCPatriot™ cannot exist on the same physical LAN as the customers. It expects to be separated from the customers and interact with a DHCP Relay Agent. Further, the device's DHCP Relay Agent protocol implementation must support DHCP Failover (see http://tools.ietf.org/html/draft-ietf-dhc-failover-07.txt) (Cisco® devices that support 'ip helper address' support DHCP Failover without special modification).

1.1.3 Central Location Requirements

The DHCPatriot™ must NOT be located in a separately uplinked network from the customer network. For example, if you have a remote POP (Point-Of-Presence) that is not directly linked to your network, but which, instead, uses some other backbone provider to link the customers to the Internet, then a single DHCPatriot™ cannot be used centrally in this situation. An additional DHCPatriot™ will be needed for that separate pop. In other words, the customer traffic must not leave your routing control before arriving at the DHCPatriot™. If this is not the case, then the policy based routing mentioned in the next section will not work.

1.1.4 Policy Routing

Some routers in the network will need to support policy based routing. Most Cisco® routers and layer 3 switches support policy based routing. More on this requirement in section 1.5.

1.2 Optional External Equipment

Optional equipment includes the following:

1.2.1 RADIUS server

The DHCPatriot™ may use either the Built-In Authentication, or an optional external RADIUS server for authentication and accounting of customers. But must use one method or the other. More on this in later chapters.
Note: The RADIUS server must at least respond with the Framed-IP-Address attribute set to 255.255.255.254 as discussed in section 4.1.3.

1.2.2 Allot NetEnforcer®

The DHCPatriot™ may be setup to perform certain functions on Allot Communication's NetEnforcer® (http://www.allot.com). A later chapter will discuss the configuration of this option.

1.3 Power and Cabling Requirements

Each DHCPatriot™ device has a single 200w power supply. This power supply is AC (Alternating Current) compatible only. DO NOT plug the devices into DC (Direct Current) power as property damage, serious injury, or death may result! The power supply has an auto-switching capability. It will automatically sense 100-110v or 240v and may be used with those currents. The input rating on the power supply is as follows: 100-240v 60-50Hz 5-3A. This power supply should work in any region that standard computer equipment functions in. If unsure, please consult with a local electrician. First Network Group cannot be held responsible for any damages, injury or loss of life that result from improper power delivery.

The following cables and accessories will be required to complete your installation:

1.3.1 Power Cables

Two power cables (included). NOTE: The DHCPatriot™ ships with power cables suitable for plugging into an American 120V 60Hz outlet. A different cable may be needed in your region. The power supply will accept a standard PC cable from your region.

1.3.2 Serial Console Adapter

Two Serial Console Adapters (included) (see Appendix B for more information) (optional).

1.3.3 Console Cables (optional)

Two console cables (Not Included) for connection of the console ports on the DHCPatriot™ devices to a customer supplied console server (see Appendix B for more information).

1.3.4 Crossover Cable

One gigabit 1-foot crossover Ethernet cable (included).

1.3.5 Ethernet Cables

Two standard 100 megabit (category 5) or gigabit (category 5e or 6) Ethernet cables (Not Included) for connection to customer supplied Ethernet switch. Cables should be chosen that match the expected speed of the link. The DHCPatriot™ devices support 10baseT, 100baseT and 1000baseT in either half or full duplex (full duplex mode is recommended). If the DHCPatriot™ is to be plugged into a gigabit switch (Hubs are not recommended), then a gigabit

Ethernet cable should be used.

1.4 Network Integration

The DHCPatriot™ will replace any existing CPE (Customer Premise Equipment) DHCP server that you may have in your network. It will force authentication of customer equipment utilizing either the Built-In Authentication server or an external RADIUS server. The DHCPatriot™ may optionally interact with a NetEnforcer® utilizing automatic configuration from the Built-In Authentication server or an external RADIUS server via reply attributes. If it is to be used in a cable modem network, the DHCPatriot™ will NOT replace your existing BOOTP and TFTP server used with the cable modems themselves. It WILL replace any CPE related DHCP scopes whether on the BOOTP server, or some other DHCP server in such a network.

1.5 Device Placement

The DHCPatriot™ is designed to be placed in the server farm in the core of your network. It supports centrally serving customers in your network. Placement at the core is not strictly required, however. Figure 1.1 shows placement in a typical network. An example of DHCPatriot™ usage follows. This example will help in the decision regarding DHCPatriot™ placement in your network.

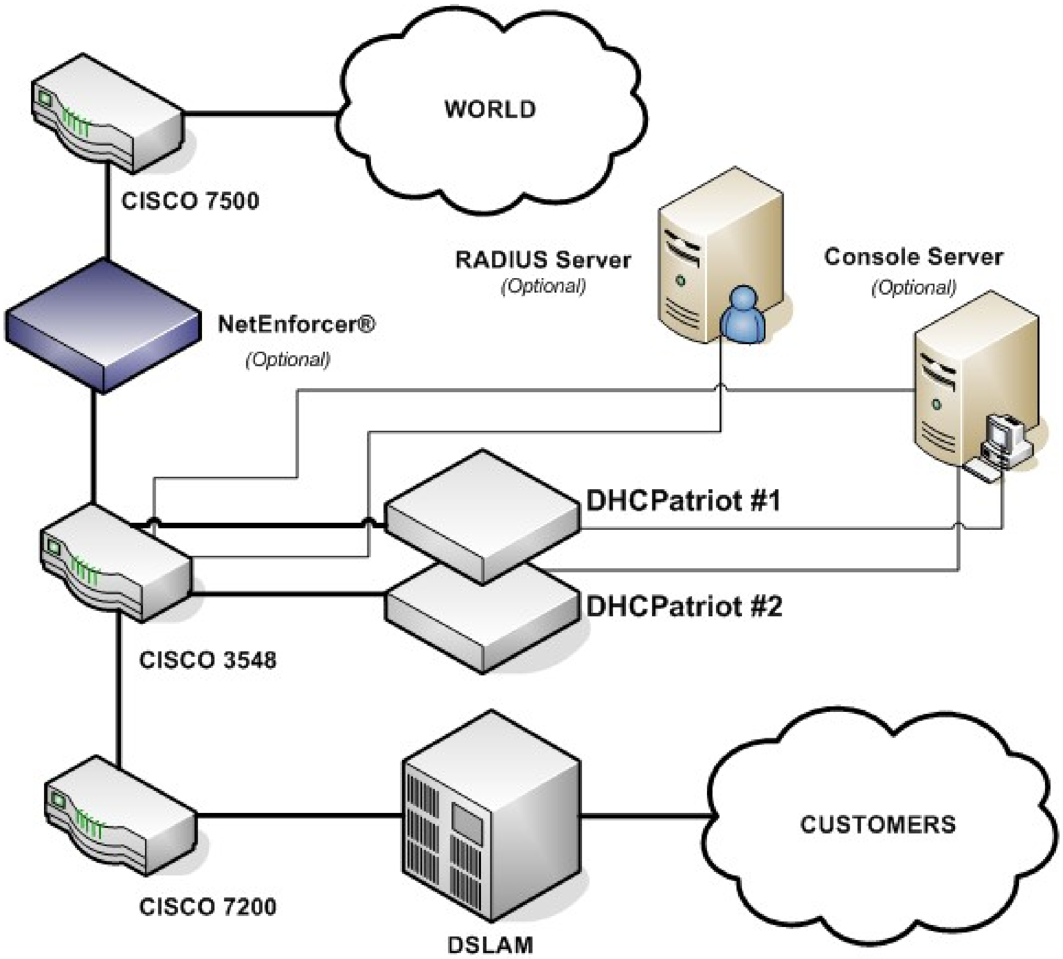


Figure 1.1

In figure 1.1, the optional RADIUS server, console server, and NetEnforcer® are shown. Using the example in figure 1.1, we can construct a proper setup for the DHCPatriot™ system. This will help you understand how the DHCPatriot™ will integrate into your network.

This example network consists of a simple border, server farm and customer network that consists of Ethernet based DSL.. For the purposes of this example, we will assume that the DSLAM is providing only bridging services, not routing. On the Cisco® 7200, the Ethernet from the DSLAM terminates on fastethernet 0/1 and the Ethernet link from the Cisco® 3548 to the Cisco® 7200 terminates on fastethernet 0/0 on the Cisco® 7200. VLAN 3 exists between the Cisco® 3548 and the Cisco® 7200. VLAN 2 exists between the Cisco® 3548 and the server farm which contains the DHCPatriot™ system, the optional RADIUS server and the optional console server. VLAN 1 exists between the Cisco® 3548 and the Cisco® 7500 border router.

In order to better understand how the DHCPatriot™ system functions, it is necessary to describe it from the perspective of new customer device on the network.

Since this is a new device, the MAC Address is unknown to the DHCPatriot™. The DHCPatriot™ will force the device to be authenticated before being allowed on to the network. The customer turns the device on. It is configured for DHCP and therefore requests an IP Address. The Cisco® 7200 router, acting as a DHCP Relay agent, forwards this request to the DHCPatriot™. The DHCPatriot™ responds with an IP Address out of the unauthenticated network.

For the device to receive an authenticated IP Address, the customer must first authenticate the device. The customer opens a web browser on the device in an attempt to begin using the network. The Cisco® 3548 forwards all traffic to the DHCPatriot™ due to the source IP Address originating in the unauthenticated network. The DHCPatriot™ responds by sending the device the authentication page. The customer types his username and password, and the device posts this to the DHCPatriot™. The DHCPatriot™ contacts the optional RADIUS server (or itself in the case of using Built-In Authentication) for authorization. The optional RADIUS server responds with Access-Accept. The DHCPatriot™ adds the device to its database of known devices and responds to it with a *thank you page* stating that the device must be rebooted. The customer reads this page and then reboots the device. The device will not receive an unauthenticated address again, unless it is suspended on the DHCPatriot™.

Upon booting up, the device requests an IP Address from the DHCPatriot™ again. At this time, the Cisco® 7200 again forwards the request to the DHCPatriot™ which responds with an authenticated address. The DHCPatriot™ will authenticate the device with the optional RADIUS server. The optional RADIUS server will again respond with Access-Accept. As a part of that response, the Framed-Filter-Id attribute may optionally be included containing something similar to the following: “NetEnforcer:Gold:GamerPLUS”. The DHCPatriot™, which has been configured to use the NetEnforcer® (see section 3.4 for details), parses this attribute, and adds the device to the NetEnforcer® applying the “Gold” QoS that has been preconfigured on the NetEnforcer®. The DHCPatriot™ will also add the device to the “GamerPLUS” host list that has been preconfigured on the NetEnforcer®. The DHCPatriot™ marks the device as being online in its database, and sends an accounting start to the optional RADIUS server. the device is now able to access the Internet.

Some time passes and the customer shuts the device down. After the lease period expires, the DHCPatriot™ will mark the device as being offline, and send an accounting stop to the optional RADIUS server. It will remove the device's IP Address from the host entry on the NetEnforcer® at this time.

Some configuration changes on external devices to the DHCPatriot™ are required to support the example. On the Cisco® 7200 fastethernet 0/1, the ip helper address command would be added as well as the gateway address of both the authenticated network, as well as the unauthenticated network that the customers will be using (more on these network types in section 3.4):

```
ip address <Customer gateway address (Authenticated)> <netmask>
ip address <Customer gateway address (Unauthenticated)> <netmask> secondary
ip helper-address <DHCPatriot™ primary device IP>
ip helper-address <DHCPatriot™ secondary device IP>
```

On the Cisco® 3548, the policy routing is needed on VLAN 3. This policy routing is used to force unauthenticated customer's outbound traffic to the DHCPatriot™ for forced authentication purposes. The Cisco® 3548 will require two configuration changes to accommodate this setup. First, in the global configuration area:

```
access-list <#> permit ip <Unauthenticated Wire Address> <Reverse Mask> any
access-list <#> deny ip any any
!
route-map <route map name> permit 10
 match ip address <access-list Number>
 set ip next-hop <ip of DHCPatriot™ primary device>
!
```

Second, applied to VLAN 3:

```
ip policy route-map <route map name>
```

Additionally, some configurations are needed on optional devices to support the example. The optional RADIUS server must be configured to allow each DHCPatriot™ device to connect as a RADIUS client. RADIUS must also be configured to respond with the Framed-Filter-Id attribute (attribute number 11) if auto-configuration of users on the NetEnforcer® is to occur. The format of this attribute is as follows:

```
Framed-Filter-Id=”NetEnforcer:[speed package][:[Group1],[Group2],...[Group10],...]”
```

If a speed package and group are not to be used for the customer, then do not send the Framed-Filter-Id attribute in the RAIDUS reply. Any speed package or groups that are sent MUST correspond EXACTLY to configurations on the NetEnforcer® (Yes, they ARE case sensitive).

Speed package corresponds to QoS entries at the virtual channel level (accessible via the Service Catalog Editor) on the NetEnforcer®. Groups correspond to Host lists (accessible via the Host Catalog Editor) on the NetEnforcer®. To enable creation of a Host List, one Host must exist in the Host List. Create a placeholder host first, and add that host to any Host Lists to be created. QoS definitions may be used to allocate bandwidth on a per user basis. Host List definitions may be used for a wide variety of tasks.

Although not used in this example, the optional console server may be used in this example network (See appendix B for details).

2 Physical Installation

This chapter describes the procedures necessary to physically install your DHCPatriot™ system in the Telco rack, connect cables to the devices and properly configure the console server for access to the DHCPatriot™ devices. This manual covers only model 2003-2 and greater DHCPatriot™ systems. Figure 2.1 shows model 2003-2 and greater. If you have the older system, model 2003-1 (see figure 2.2), please use the manual provided with the DHCPatriot™ for physical installation, or contact First Network Group for physical installation instructions.

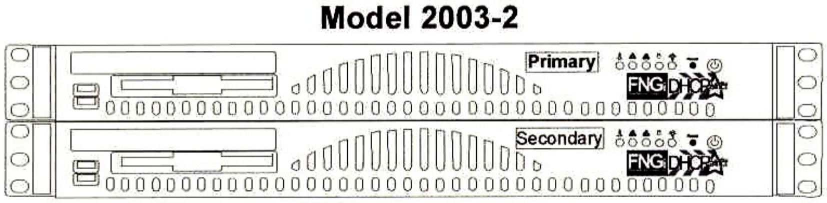


Figure 2.1

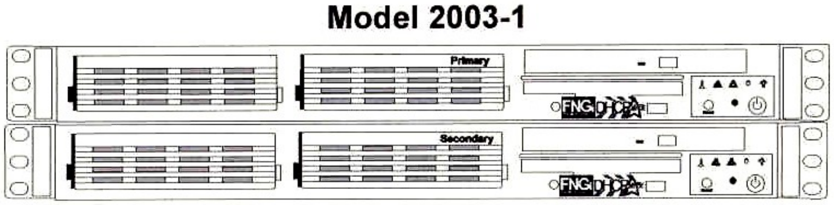


Figure 2.2

2.1 Unpacking the system

You should inspect the box and make note of any damage. If either DHCPatriot™ device shows any damage notify First Network Group immediately. Packed in the boxes are all the parts you should need to mount your server in a Telco or server rack.

PACKING LIST		
Item	**Qty**	**Description**
1	2	DHCPatriot™ units (1 Primary, 1 Secondary)
2	2	DB9 to RJ45 adapter (Serial Console Adapter)
3	2	Power Cable
4	1	Red Crossover Cable
5	1	DHCPatriot™ Boot Disc
6	1	DHCPatriot™ Manual (this document)
7	1	EULA (End User License Agreement)
8	1	Maintenance Contract Quick List
9	1	Maintenance Contract

In addition to the parts listed in the packing list above the customer will need to supply the following items:

- Rack Screws
  Screws and washers to attach the DHCPatriot™ to your Telco or server rack
- Ethernet Cables
  Two standard Ethernet cables of sufficient length to attach the DHCPatriot™ to the Ethernet switch (see section 1.3 for further details).
- Console Cables
  Two cables suitable for the console connection. We will cover the optional console connection in more detail later.

2.2 Mounting in a two or four post rack

The DHCPatriot™ may be mounted in a two post or a four post 19" Telco or server rack. This section describes mounting in a two or four post rack.

The installation steps should be read in their entirety before installation is started. All parts should be unpacked, inspected for damage and checked for completeness before continuing with set up. A suitable location for installation will have a clean, dust free environment that is well ventilated. Do not set up your DHCPatriot™ system in an area where heat, electrical noise, or electromagnetic fields are generated. The area chosen must have close access to a grounded AC power outlet (see section 1.3 for further details).

The location chosen should be climate controlled with a temperature range of 10° to 35° C (50° to 90° F). Relative humidity should be in the range of 8% to 90%. Damage not covered by the maintenance contract may result if the DHCPatriot™ system is operated outside of this temperature or humidity range.

When choosing a location in the rack in which to place the devices, be sure that proper clearance is available in both the front and the back. Front clearance should be no less than 25 inches, and rear clearance should be no less than 30 inches. This ensures proper airflow and cooling around the devices.

Each device is installed by using the customer supplied rack mounting screws. Two screws on each side will secure a DHCPatriot™ device to the rack (see figure 2.3). If it is installed in a four post rack, the back two posts will not be used.

Important! Take great care when installing the devices in the rack. Two people should be involved in the installation. One person should hold the device in the rack while the other one inserts the screws. Be sure each device is secure in the rack. Damage not covered by the Maintenance Contract may occur if a device is dropped, or falls out of the rack.

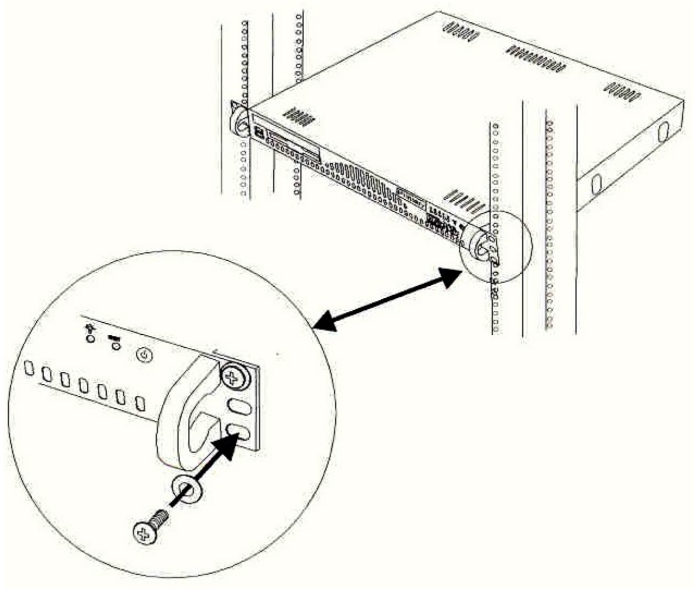


Figure 2.3

2.3 Attaching cables

The power cables supplied with the DHCPatriot™ system may be used in many locations. A standard PC power cable from your region may be required (see section 1.3 for details). Plug a power cable from the standard PC 3 prong outlet on each device. Plug the other end of the power cable into an AC power outlet with the proper specifications (see section 1.3 for details). The red crossover cable (supplied) is used to connect the devices to each other. Connect the cable to the ports on each unit as shown in figure 2.4. The two DB9 to RJ45 serial console adapters (supplied) are connected to the serial port of each device as shown in figure 2.4. Install the adapters even if you do not intend to use the serial console capabilities.

The LAN port is used to connect the DHCPatriot™ to the Ethernet switch. The customer supplied Ethernet cable should be used for this connection (see section 1.3).

A console cable may optionally be connected from the female RJ45 end of each DB9 to RJ45 adapter that are installed in the serial port on the back of each device to the console server (more details about the console connection and configuration can be found in section 2.4 and appendix B).

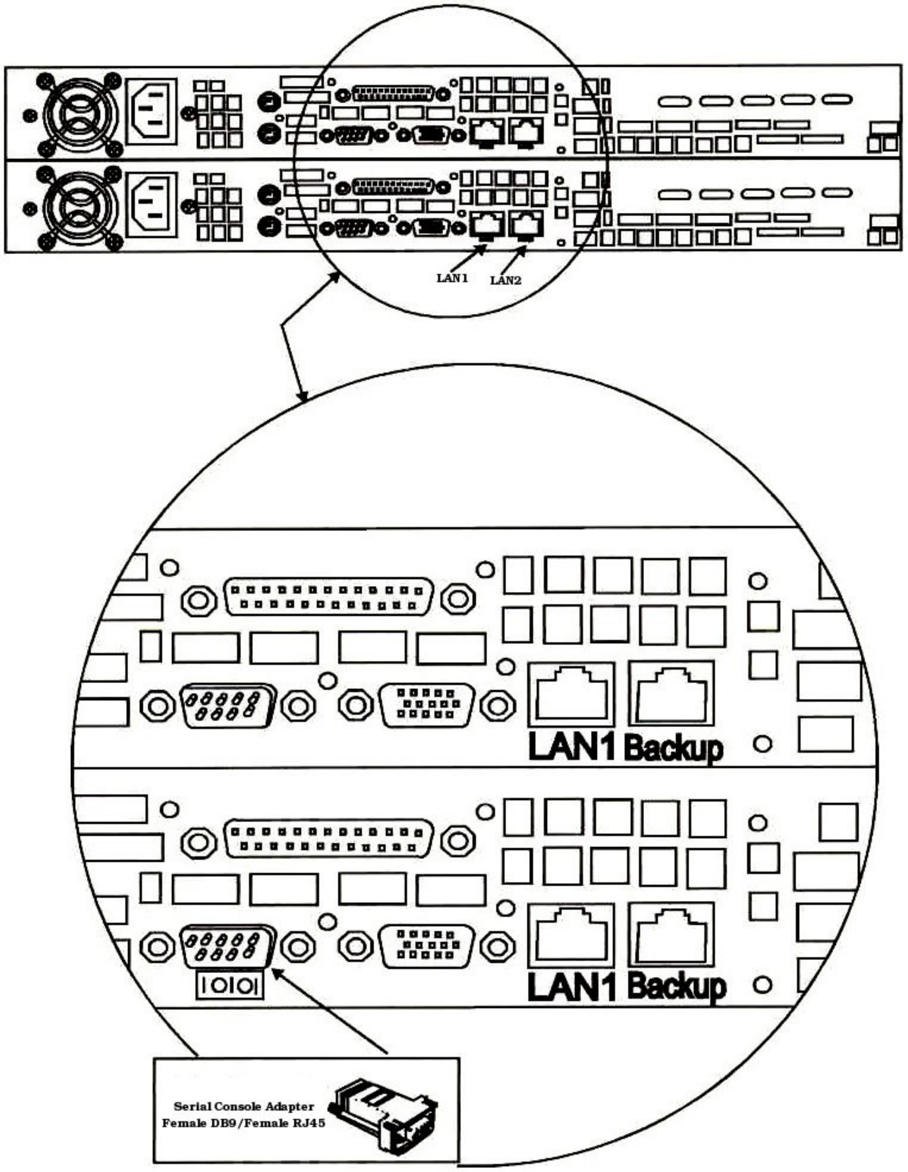


Figure 2.4

2.4 Console Access

The DHCPatriot™ system allows console access to the devices via a standard PC style DB9 male serial port. A female DB9 to female RJ45 serial console adapter is provided. This adapter is well suited to access from most Cisco® compatible console servers (such as Cyclades™ http://www.cyclades.com/ Note: a special Cisco® compatible cable may be required for the Cyclades™ terminal servers). These devices are also compatible with Cisco® console implementation and standard PC

(UNIX and Microsoft® Windows®) style implementations. See appendix B for complete instructions for achieving console access from standard Cisco® devices and ports as well as from standard PC devices. The pin assignment of the Serial Port and RJ45 Port are supplied for use in other situations.

Serial Port Pin out			
Pin#	**Definition**	**Pin#**	**Definition**
1	CD (Carrier Detect)	6	DSR (Data Set Ready)
2	RxD (Receive Data)	7	RTS (Request To Send)
3	TxD (Transmit Data)	8	CTS (Clear To Send)
4	DTR (Data Terminal Ready)	9	RI (Ring Indicator)
5	GND (Ground)		

Serial Console Adapter Female RJ45 Pin out			
Pin#	**Definition**	**Pin#**	**Definition**
1	RTS (Request To Send)	6	RxD (Receive Data)
2	DTR (Data Terminal Ready)	7	DSR (Data Set Ready)
3	TxD (Transmit Data)	8	CTS (Clear To Send)
4	NC (Not Connected)		
5	GND (Ground)		

The next chapter describes how console access may optionally be used to complete the initial configuration of the DHCPatriot™ devices.

Please complete all network design decisions and assign IP Addresses to be used by the DHCPatriot™ devices at this time. The next chapter will begin the configuration of the DHCPatriot™.

3 Configuration

There are two phases to the configuration of your DHCPatriot™ system. The first phase is configuration via the CLI Menu. The first half of this chapter explains how to connect and how to use the menu for this configuration. The second phase will take a bit longer to complete. This phase involves connecting to the Web Administration Interface and using it to configure the DHCPatriot™ system for operation. The latter half of the chapter describes these procedures.

3.1 Connecting to the CLI Menu Interface

There are two basic methods that can be used to connect to the CLI Menu Interface to perform the initial configuration. The first method uses the optional console connection and the console server or router (see section 2.4 and appendix B for information regarding console setup). The second method uses secure shell (SSH) access from a device that supports SSH (Appendix F has details regarding the use of SSH on Microsoft® Windows® and Linux®/UNIX). These methods are described in this section.

Connecting via console requires a console cable connection to each DHCPatriot™ device and a properly setup console port on the console server or router.

Connecting via SSH requires access to the default network that the DHCPatriot™ devices are configured for when shipped. The default network is shown here.

Default Network	
Primary Device IP Address	10.1.1.2
Secondary Device IP Address	10.1.1.3
Gateway IP Address	10.1.1.1
Subnet Mask	255.255.255.0
CIDR Block	10.1.1.0/24
Free IP Address Range	10.1.1.4 – 10.1.1.254

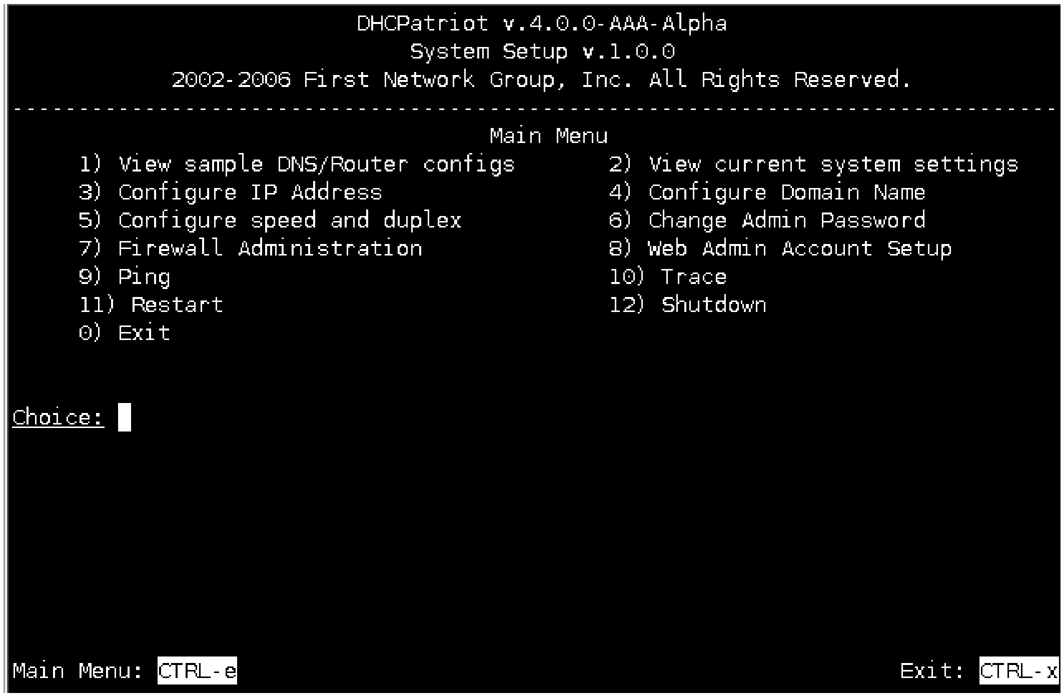
Connecting via SSH further requires the Ethernet connections to the DHCPatriot™ devices described in section 2.3. Access to the default network may be achieved using one of two methods. First, a device that supports SSH could be configured in the default network at one of the free IP Addresses. The second method would require configuring the gateway router interface with the IP Address 10.1.1.1 and then routing the default network to a location of your choice. After completing the necessary routing entries, a device that supports SSH could be used to connect to the DHCPatriot™ devices remotely.

After a method of connecting to the devices is chosen and the proper configurations to support this method have been made, it is possible to connect to the devices. Connecting to the console port on the console server/router (see appendix B) or using SSH (see appendix F) to connect to one of the devices should present you with a screen asking for a username. The username is admin. After typing this username and pressing enter, the screen will prompt you for a password. The default password is cU$0gNn1 (Phonetically spelled here for your convenience: cee->capital you->dollar sign->zero->gee->capital en->en->the number one) NOTE: It is highly recommended that you change the default password upon logging in. More on that in section 3.2. After typing the password correctly and pressing enter, you will be presented with a menu containing several options. Section 3.2 describes the use of these options.

3.2 Configuring via the CLI Menu Interface

This section describes the use of the CLI Menu Interface to configure IP Addresses on the DHCPatriot™ devices, as well as setting the domain name. It also allows you to change the Ethernet media settings as well as a variety of tasks that will allow access to the Web Administration Interface for further configuration.

First, let us describe each option and its function. Figure 3.1 displays the menu interface.



```
                         DHCPatriot v.4.0.0-AAA-Alpha
                             System Setup v.1.0.0
                2002-2006 First Network Group, Inc. All Rights Reserved.
-------------------------------------------------------------------------------
                                    Main Menu
     1) View sample DNS/Router configs       2) View current system settings
     3) Configure IP Address                 4) Configure Domain Name
     5) Configure speed and duplex           6) Change Admin Password
     7) Firewall Administration              8) Web Admin Account Setup
     9) Ping                                 10) Trace
     11) Restart                             12) Shutdown
     0) Exit


Choice: 









Main Menu: CTRL-e                                                  Exit: CTRL-x
```

Figure 3.1 (Your screen appearance may differ slightly depending on the connection method and the software used.)

Each option and its function is listed here for your convenience:
1) displays various sample configurations that may be useful in configuring external devices, such as routers and DNS servers, to function with the DHCPatriot™.
2) displays the current domain name, IP Address, and Ethernet media settings.
3) allows the configuration of the IP Address, the subnet mask and the gateway address.
4) enables configuration of the domain name.
5) allows configuration of the Ethernet Media settings (ie: speed-n-duplex).
6) changes the admin user's password.
7) enables configuration of the built-in white-list style firewall.
8) provides maintenance features for Web Administration Interface users.
9) and 10) allow pinging and trace routing external hosts for use in network troubleshooting.
11) and 12) allow rebooting and halting the device.
0) exits the menu.

Configuring the initial settings on the DHCPatriot™ system must be done on a per device basis (meaning configuration of the IP Address needs to be performed on both the primary and the secondary device, for example), except where noted in the following instructions.

3.2.1 Change admin user password

The very first task to perform is to change the default password for the admin user. This password is widely known (at least among DHCPatriot™ owners) and should not be used after the IP Address is set.

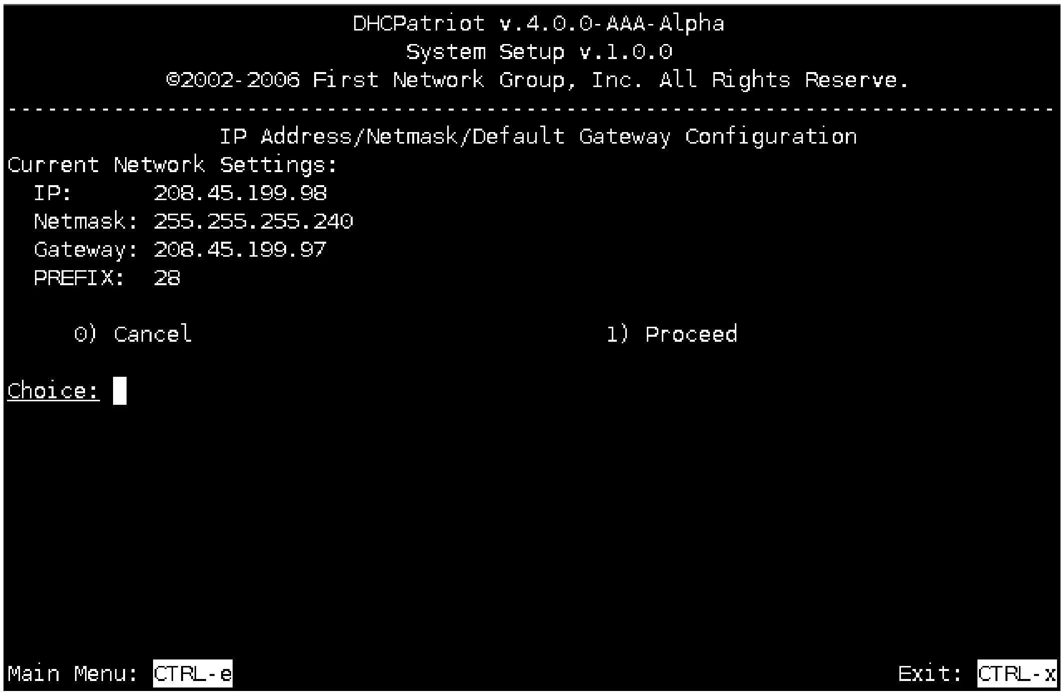
A word on password security. The password chosen should be hard to guess. An example of a bad password choice would be: *fluffy* or even *F1uFfy* as both would be easy for a hacker to guess using a dictionary program (although the second one would be significantly harder). An example of a good password choice would be: !iu56T$R as it is not based on any sort of dictionary word, but rather is quite random. Be sure and either commit the password to memory, or, if absolutely necessary, store it in as secure a place as possible (an unencrypted text file on your computer is NOT a secure location). You should change the password if anyone who knew the password leaves the organization, or at some specified time interval dictated by company policy.

Once a suitable password is chosen, press 6 and then enter to begin the password changing process. Press enter to move to the next screen. You will be prompted for the old password (which will be the default password from section 3.1 if this is your first time changing the password). Type this and press enter. Type the new desired password and press enter. Re-type the new desired password and press enter to confirm. It should report that the password was changed. Press enter. It should report that the password change was successful.

Press enter. You will be returned to the main menu. If anything went wrong, try the procedure again.

3.2.2 IP Address Configuration

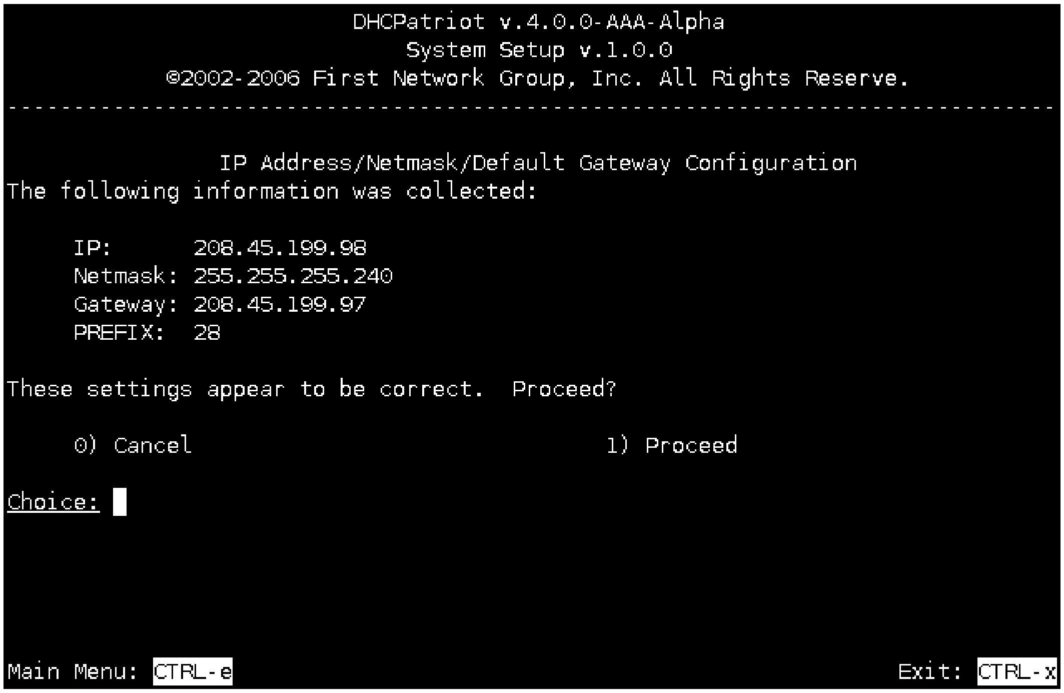
To begin configuration of the IP Address, press 3 and then enter. You will be presented with a screen similar to Figure 3.2



```
                          DHCPatriot v.4.0.0-AAA-Alpha
                              System Setup v.1.0.0
              ©2002-2006 First Network Group, Inc. All Rights Reserve.
------------------------------------------------------------------------------
                IP Address/Netmask/Default Gateway Configuration
Current Network Settings:
  IP:      208.45.199.98
  Netmask: 255.255.255.240
  Gateway: 208.45.199.97
  PREFIX:  28

     0) Cancel                               1) Proceed

Choice: █









Main Menu: CTRL-e                                                 Exit: CTRL-x
```

Figure 3.2 (Your screen appearance may differ slightly depending on the connection method and the software used.)

At this point, press 1 and then enter. That will begin the configuration process. The interface will ask for the IP Address. Type that followed by enter. Then it will ask for the subnet mask. Type that and press enter. Then it will ask for the default gateway. Type that and press enter. It will then show the information that was gathered and ask if you would like to proceed (see figure 3.3). If the information looks correct, press 1 and then enter. If you have mis configured something, press 0 and enter. Then press 3 and enter to return to the IP Address configuration area. and restart the process. You may cancel the process at any time by pressing Ctrl+e to return to the main menu, or by pressing Ctrl+x to exit. No changes will be applied to the Ethernet interface until a reboot of the system is performed. You may change the configuration several times before rebooting.



```
                        DHCPatriot v.4.0.0-AAA-Alpha
                             System Setup v.1.0.0
              ©2002-2006 First Network Group, Inc. All Rights Reserve.
--------------------------------------------------------------------------------

                IP Address/Netmask/Default Gateway Configuration
The following information was collected:

     IP:      208.45.199.98
     Netmask: 255.255.255.240
     Gateway: 208.45.199.97
     PREFIX:  28

These settings appear to be correct.  Proceed?

     0) Cancel                             1) Proceed

Choice: █




Main Menu: CTRL-e                                                  Exit: CTRL-x
```

Figure 3.3 (Your screen appearance may differ slightly depending on the connection method and the software used.)

3.2.3 Domain name configuration

The next task to perform is setting the domain name. At this point, you should be back at the main menu (see figure 3.1). If you are not, please be sure that the IP Address change has been saved properly and then press Ctrl+e to return to the main menu. Press 4 and then enter. The currently configured domain name will be displayed. Press 1 and then enter. It will ask for a new domain name. Each device's host name must begin with either patriot-1 or patriot-2, therefore this is automatically set according to primary or secondary designation. This factory set designation cannot be changed. Only a domain name may be configured here.

A word on domain name choice. If you have only one DHCPatriot™ system, then you may wish to only add your normal domain name (such as example.com) which will create the hosts patriot-1.<domain> and patriot-2.<domain> (patriot-1.example.com and patriot-2.example.com). If more than one DHCPatriot™ system will be employed, then you may wish to use patriot<set #>.<domain> as the domain name (patriot1.example.com patriot2.example.com etc...) which would create devices like patriot-1.patriot<set#>.<domain> and patriot-2.patriot<set #>.<domain> (patriot-1.patriot1.example.com and patriot-2.patriot1.example.com etc...). Another way to denote multiple DHCPatriot™ systems would be to use a location identifier in the domain name (patriot-1.stlouis.example.com and patriot-2.stlouis.example.com and patriot-

1.dallas.example.com and patriot-2.dallas.example.com). The choice is yours, just keep in mind that patriot-1 and patriot-2 will be the host names and may not be changed.

After entering the chosen domain name, press enter. The screen will display your entry and ask for confirmation. Press 1 and then enter to proceed. If you have entered the domain incorrectly, press 0 instead. You will be returned to the main menu. Begin the domain name configuration process from the beginning. The domain name will not be changed until a reboot is performed. You may change it several times before rebooting if necessary. When the changes are complete, you may return to the main menu (0 or Ctrl+e).

The DHCPatriot™ devices will need to be entered into the DNS (Domain Name Service) server. Specific methods for doing this vary depending on the brand of server being used. The following entries must be made:

- Forward lookup for patriot-1.<domain chosen> using the configured IP Address of the primary device.
- Forward lookup for patriot-2.<domain chosen> using the configured IP Address of the secondary device.
- Reverse lookup for the configured IP Address of the primary device returning patriot-1.<domain chosen>.
- Reverse lookup for the configured IP Address of the secondary device returning patriot-2.<domain chosen>.
- Forward lookup for patriot.<domain chosen> that returns both configured IP Addresses.

Menu option 1 contains sample DNS configurations for use with the Bind DNS server implementation (http://www.isc.org).

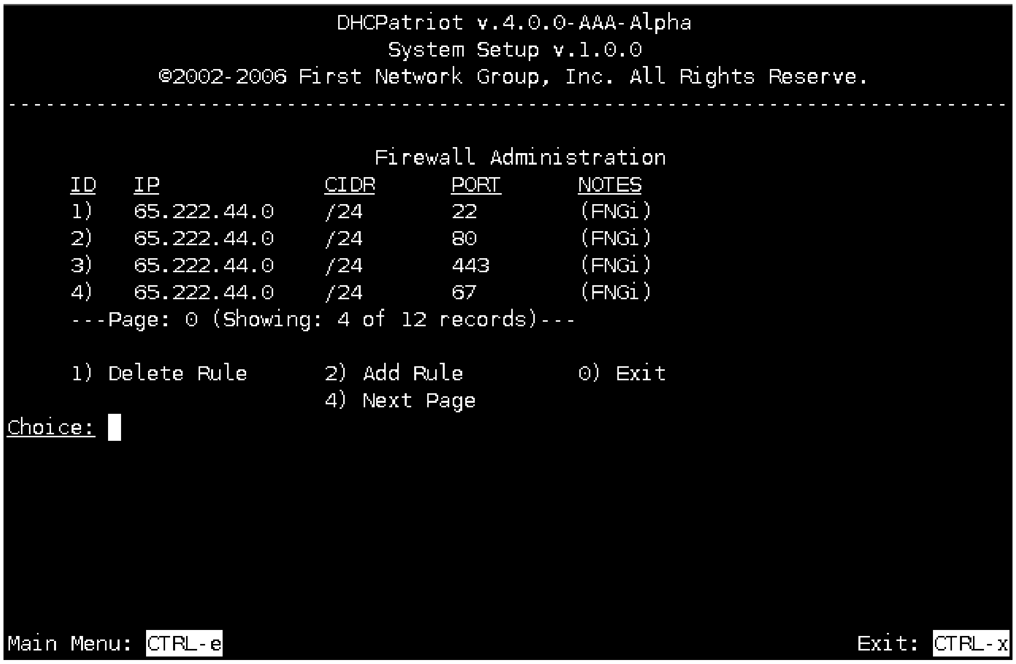
3.2.4 Ethernet Media Settings (Speed and Duplex)

The default configuration is auto negotiation. This will be a suitable setting in the vast majority of situations. In some situations, it is possible that this setting will need to be changed. To change this setting, press 5 and then enter. The current connection settings will be displayed. Press 1 and then enter to change these settings. A list of available options will be displayed. The options have the following format: <speed>/<duplex>. Caution, choosing options that are not supported on your switch (such as 1000baseT/full when your switch only supports 100mbit) will render the DHCPatriot™ unreachable if you are connected via SSH and not the optional console connection (these settings are applied immediately after receiving confirmation). Type the number of the speed and duplex you wish to set and press enter. The chosen setting will be displayed. Press 1 to confirm and 0 to cancel. Return to the main menu.

3.2.5 Configuring the Firewall for the Administration Network

NOTE: Perform these actions on only ONE of the DHCPatriot™ devices as it configures both simultaneously. The DHCPatriot™ employs a white-list-style firewall. You are encouraged to allow access to only the bare minimum of IP Addresses necessary for administration of the DHCPatriot™. At this time you will need to open up access to port 22 (SSH), port 80 (web) and port 443 (secure web) for any IP Address (or subnet) that will be connecting to this device for administration purposes. If the IP Address will only be administering the device via the Web Administration Interface, then you may omit port 22.

To begin the firewall configuration process, press 7 and then enter. You will be presented with a screen similar to figure 3.4.



```
                    DHCPatriot v.4.0.0-AAA-Alpha
                        System Setup v.1.0.0
            ©2002-2006 First Network Group, Inc. All Rights Reserve.
-------------------------------------------------------------------------------

                          Firewall Administration
     ID   IP              CIDR      PORT      NOTES
     1)   65.222.44.0     /24       22        (FNGi)
     2)   65.222.44.0     /24       80        (FNGi)
     3)   65.222.44.0     /24       443       (FNGi)
     4)   65.222.44.0     /24       67        (FNGi)
     ---Page: 0 (Showing: 4 of 12 records)---

     1) Delete Rule      2) Add Rule         0) Exit
                         4) Next Page
Choice: 









Main Menu: CTRL-e                                                 Exit: CTRL-x
```

Figure 3.4 (Your screen appearance may differ slightly depending on the connection method and the software used.)

The first thing you will notice is that there are several rules in with various subnets on various ports that display (FNGi) in the notes column. These are entered by default for remote monitoring purposes. Remote monitoring and response is free for the first year of ownership (subject to limitations in the maintenance contract, refer to that document for details). It is highly recommended that these entries are left untouched.

To navigate this area, press 4 and enter to view the next page. Press 3 and enter to view the previous page.

To add a rule, press 2 and then enter. Type the desired IP Address or subnet wire address that will need access to the DHCPatriot™ for administrative purposes and press enter. You will then be asked for the CIDR block. A CIDR block is another way of representing a subnet mask. A table of common CIDR blocks is included here for your convenience.

CIDR	Subnet Mask	Number of IPs
/32	255.255.255.255	1
/30	255.255.255.252	4
/29	255.255.255.248	8
/28	255.255.255.240	16
/27	255.255.255.224	32
/26	255.255.255.192	64
/25	255.255.255.128	128
/24	255.255.255.0	256

Enter the appropriate CIDR here and press enter. Enter the desired port (only 22 for SSH, 80 for HTTP and 443 for HTTPS should be used) and press enter. Finally, enter a note so that you can remember what the rule is for. Notes may be up to 255 characters in length, but try to keep it as short as possible. You should get a message that the rule was added successfully. You may navigate through the menu to view the rule. Repeat this process until you have added all desired rules.

From time to time it may be necessary to delete a rule if an administration IP Address changes, or a mistake was made when entering a rule. To delete a rule, navigate through the menu to find the rule you wish to delete. Then press 1 and then enter. You will be prompted for a rule to delete. Enter the number of the rule that you wish to delete. Then press enter. It should display deleted rule <the rule number you chose> and then return to the delete prompt. If you do not wish to delete any more rules, press e and then enter to exit the delete prompt.

Changes to the firewall rules are applied immediately, take great care when changing these rules, especially when deleting them. If a rule that is allowing you into the devices is deleted, your access will be cut off!

It is important here that you have added at least the IP Address that you will use to connect to the DHCPatriot™ for the rest of the configuration process. Be sure that you have allowed port 22, port 80 and port 443 for this IP Address. To exit the Firewall Administration area, press 0 and then enter. You will be returned to the main menu.

3.2.6 Initial Configuration Reboot

At this point, we need to reboot the devices and confirm function with the new settings. If you are connected via the optional console connection, this will be rather painless as you will be able to watch it reboot and not loose connection. If you are connected via SSH, then, after rebooting, you will want to ping the new addresses until you see them enter service.

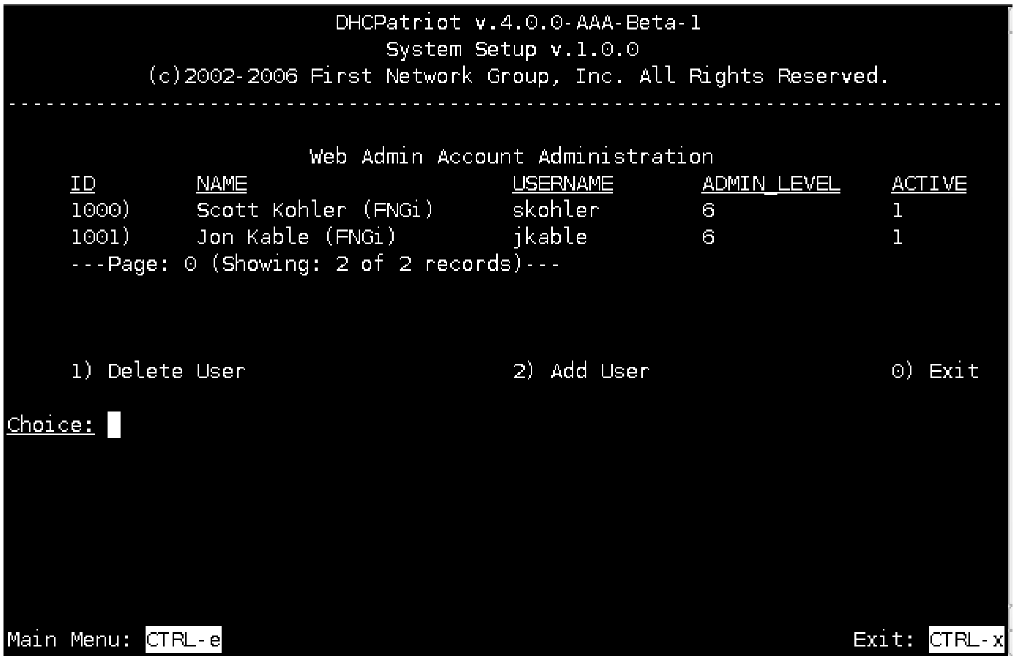
To reboot the device press 11 and then enter. Then press 1 and enter to proceed. When the reboot is complete, reconnect to the device using either the optional console or the SSH method. Use the admin username and the password you created to login. You will be returned to the menu interface.

You may optionally use the ping and trace functionality to confirm that the DHCPatriot™ device is functioning properly. Select an IP Address to ping and trace to that responds to both, and is beyond the default gateway of the DHCPatriot™ system (but is less than 15 hops away as the trace is limited to 15 hops). To ping test, press 9 and then enter. The device will prompt you for the host. Type the aforementioned IP Address. Press enter. Normal ping output will be displayed. It is up to you to interpret this output as the possibilities are to numerous to list here. Press enter to return to the main menu. To test trace, type 10 and then enter. Type the aforementioned IP Address. Press enter. Normal trace output will be displayed. It is up to you to interpret this output as the possibilities are to numerous to list here. Press enter to return to the main menu.

If any problems are encountered during this section, you may need to restart section 3.2 to find what went wrong. If everything appears fine, please read on to complete the initial setup.

3.2.7 Web Administration Interface account setup

NOTE: Perform these actions on only ONE of the DHCPatriot™ devices as it configures both simultaneously. The Web Administration user and password will be used in section 3.3 for connecting to the Web Administration Interface. Press 8 and then enter to begin the configuration process. You should be presented with a screen similar to that shown in figure 3.5.



```
                     DHCPatriot v.4.0.0-AAA-Beta-1
                         System Setup v.1.0.0
            (c)2002-2006 First Network Group, Inc. All Rights Reserved.
-------------------------------------------------------------------------------

                      Web Admin Account Administration
     ID        NAME                     USERNAME      ADMIN_LEVEL    ACTIVE
     1000)     Scott Kohler (FNGi)      skohler       6              1
     1001)     Jon Kable (FNGi)         jkable        6              1
     ---Page: 0 (Showing: 2 of 2 records)---



     1) Delete User                     2) Add User                    0) Exit

Choice: █







Main Menu: CTRL-e                                                Exit: CTRL-x
```

Figure 3.5 (Your screen appearance may differ slightly depending on the connection method and the software used.)

To add a user, type the number 2 and then press enter. You will be prompted for a name. This may be the name of the user you are adding, or it may be a designator for a default administrator account such as: DHCPatriot™ Administrator (it is FNGi's recommendation that a separate username be added for each administrator to avoid possible future problems resulting from personnel change). Enter the name and press enter. The system will then prompt you for a username. A good username choice will be some permutation of the administrators first and last name. Enter the desired username and then press enter. A password prompt will appear. The rules of good password security from section 3.2.1 apply here as well. Type the desired password and press enter. Re-enter the password for verification purposes, and then press enter. You will then be prompted for the user's admin level. The user's admin level controls what functions they have access to. As a general rule, level 0 should be used for customer service personnel. Level 1 should be used for general technical support personnel. Level 5 should be used for ISP (Internet Service Provider) administrators. Level 6 should be used for network administrators. Type the desired admin level and press enter. A message will appear stating that the user was successfully added. Continue adding users as needed. Press 0 and then enter to return to the main menu.

At some point, it may be necessary to delete an administrator due to a mistake when entering the administrator, personnel changes, or some other reason. PLEASE NOTE: It is recommended that you DO NOT delete the users with

(FNGi) appearing after their names. These accounts may be needed by FNGi to assist you with your DHCPatriot™ at some future time. To delete a user, from the main menu press 8 to enter the Web Admin Account Setup function. A screen will appear that will appear similar to figure 3.5. First, find the user that you would like to delete. If the user does not currently appear on the screen, press 4 and then enter to move to the next page. If you need to go back a page, press 3 and then enter. Once you have located the user, press 1 and then enter. Type the ID number of the user that you wish to delete and press enter. You will get a confirmation message that the user was deleted and the list will refresh. You will notice that the user is gone from the list. You may continue and delete other users if you wish. Press e and then enter to exit the delete function. Press 0 and then enter to return to the main menu.

3.3 Connecting to the Web Administration Interface

In this section, we will be making the connection to the Web Administration Interface. This connection is very important for the remainder of this chapter and most of this manual. It is a required connection for the daily use of your DHCPatriot™ system. It is required that the firewall has been modified to allow the appropriate IP Address(es) access to port 80 and 443 (see section 3.2.5 for further information) and that the administrator account(s) has been added (see section 3.2.7) before continuing.

To begin, open your favorite web browser (The DHCPatriot™ Web Administration Interface is known to work on: Firefox 1.0.7 and greater, Konquerer 3.4.3 and greater, Opera 8.54 and greater, Netscape 8.1 and greater, and Internet Explorer 6.0.2900.xpsp_sp2_rtm.040803-2158). In the address bar, type: https://patriot.<domain entered in section 3.2.3> and press enter. If you receive an error message, ensure that the DHCPatriot™ is up and running, that the device you are connecting from is allowed via the firewall (see section 3.2.5) and that the appropriate entries have been made in your DNS server (see section 3.2.3). You may also use https://<IP Address of either the primary or secondary DHCPatriot™ device> to connect. You should receive a screen similar to that shown in figure 3.6.

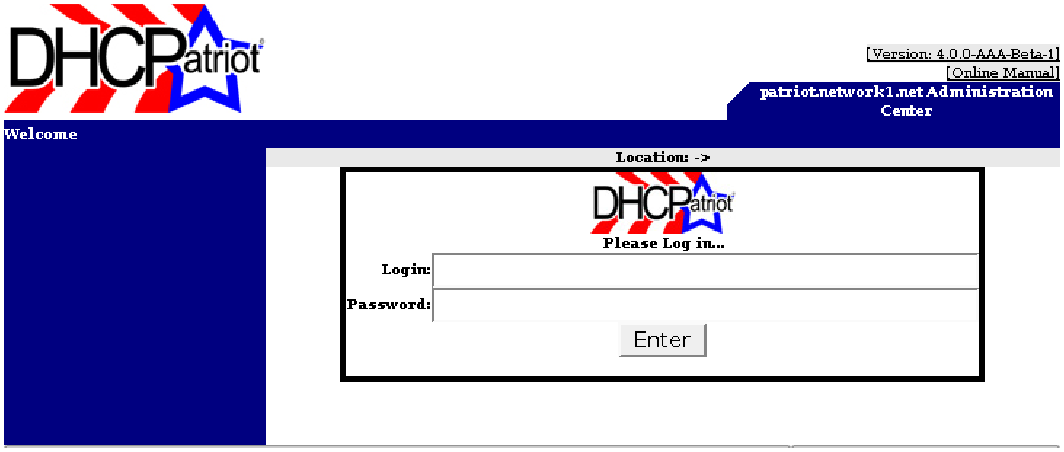
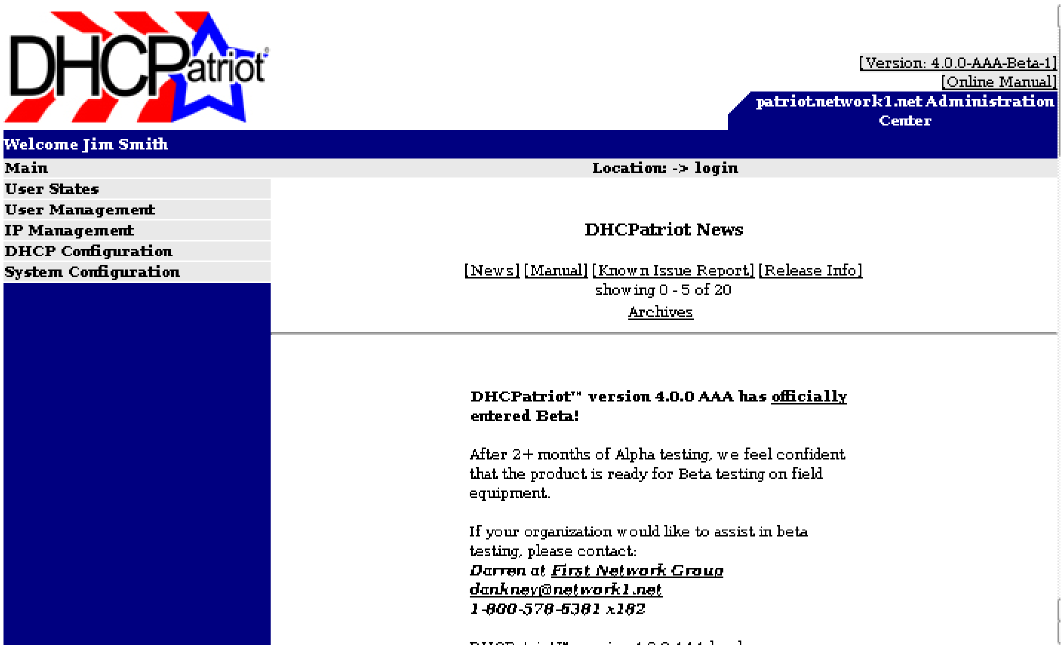


Figure 3.6 (Your screen appearance may differ slightly depending on the software used.)

In the Login field type the username that was created in section 3.2.7. In the Password field, type the password that was created in section 3.2.7. Click on Enter. At this point, you should be logged in. If you instead receive a password error, verify that you entered the Login and Password correctly. If you still are unable to login correctly, revisit section 3.2.7 and make sure the instructions there were performed correctly. Once authentication is successfully performed, a screen similar to figure 3.7 will appear.



DHCPatriot™ version 4.0.0 AAA has officially entered Beta!

After 2+ months of Alpha testing, we feel confident that the product is ready for Beta testing on field equipment.

If your organization would like to assist in beta testing, please contact:
Darren at First Network Group
dankney@network1.net
1-800-578-6381 x182

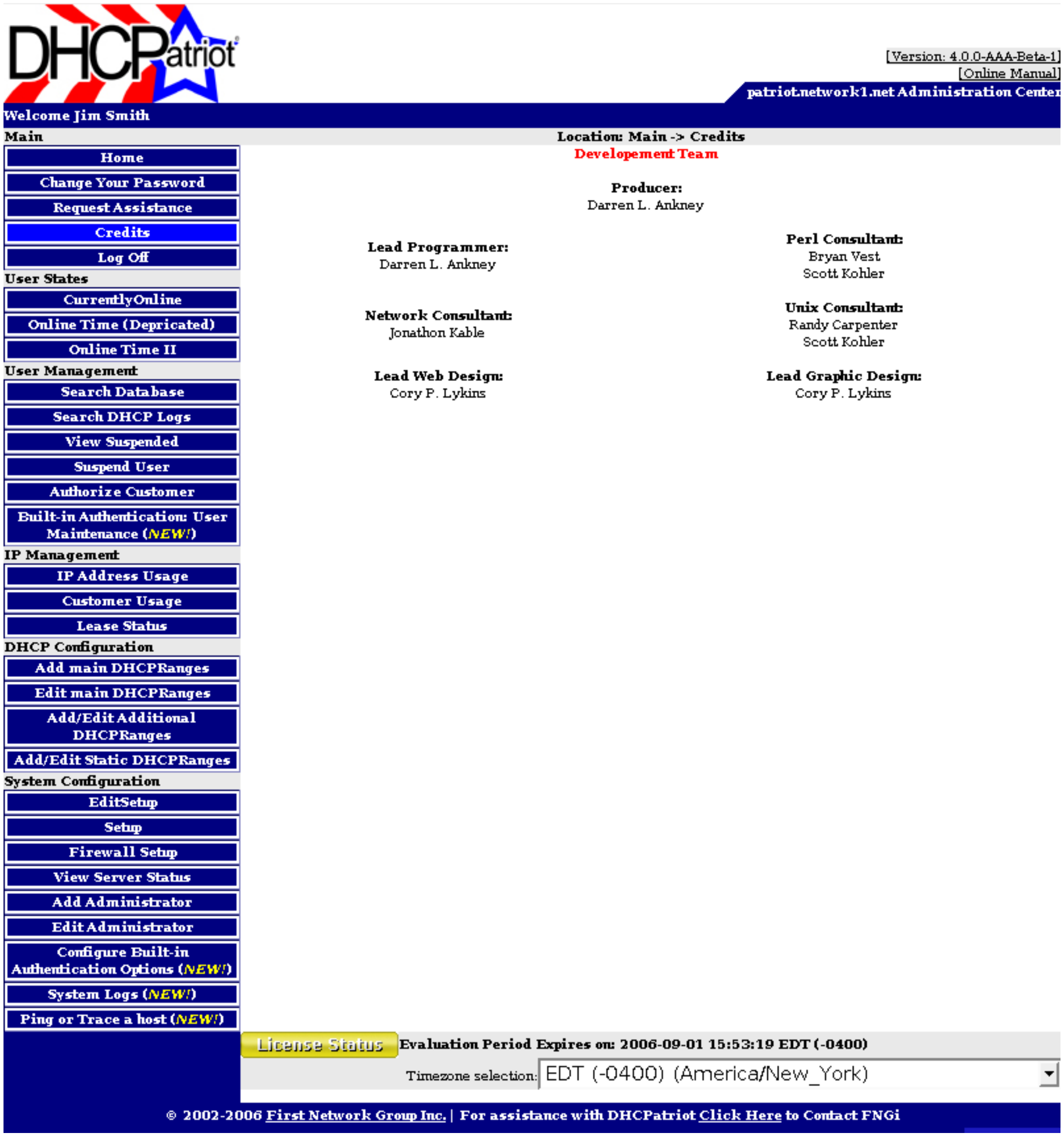
Figure 3.7 (Your screen appearance may differ slightly depending on the software used.)

If you are seeing the screen represented in figure 3.7, you are ready to move on to section 3.4. In that section, we will be configuring the DHCPatriot™ for operation in your network.

3.4 Configuring via the Web Administration Interface

This section describes final configuration of the DHCPatriot™ system. After completing this section, the DHCPatriot™ will be ready for operation.

Before beginning configuration, it may help to familiarize yourself with the menu system used on the DHCPatriot™ Web Administration Interface. Figure 3.8 shows the interface with all of the collapsible menus expanded as it would appear to a level 6 administrator.



Location: Main -> Credits

Developement Team

Producer:
Darren L. Ankney

Lead Programmer:
Darren L. Ankney

Perl Consultant:
Bryan Vest
Scott Kohler

Network Consultant:
Jonathon Kable

Unix Consultant:
Randy Carpenter
Scott Kohler

Lead Web Design:
Cory P. Lykins

Lead Graphic Design:
Cory P. Lykins

Evaluation Period Expires on: 2006-09-01 15:53:19 EDT (-0400)

Timezone selection: EDT (-0400) (America/New_York)

© 2002-2006 First Network Group Inc. | For assistance with DHCPatriot Click Here to Contact FNGi

Figure 3.8 (Your screen appearance may differ slightly depending on the software used.)

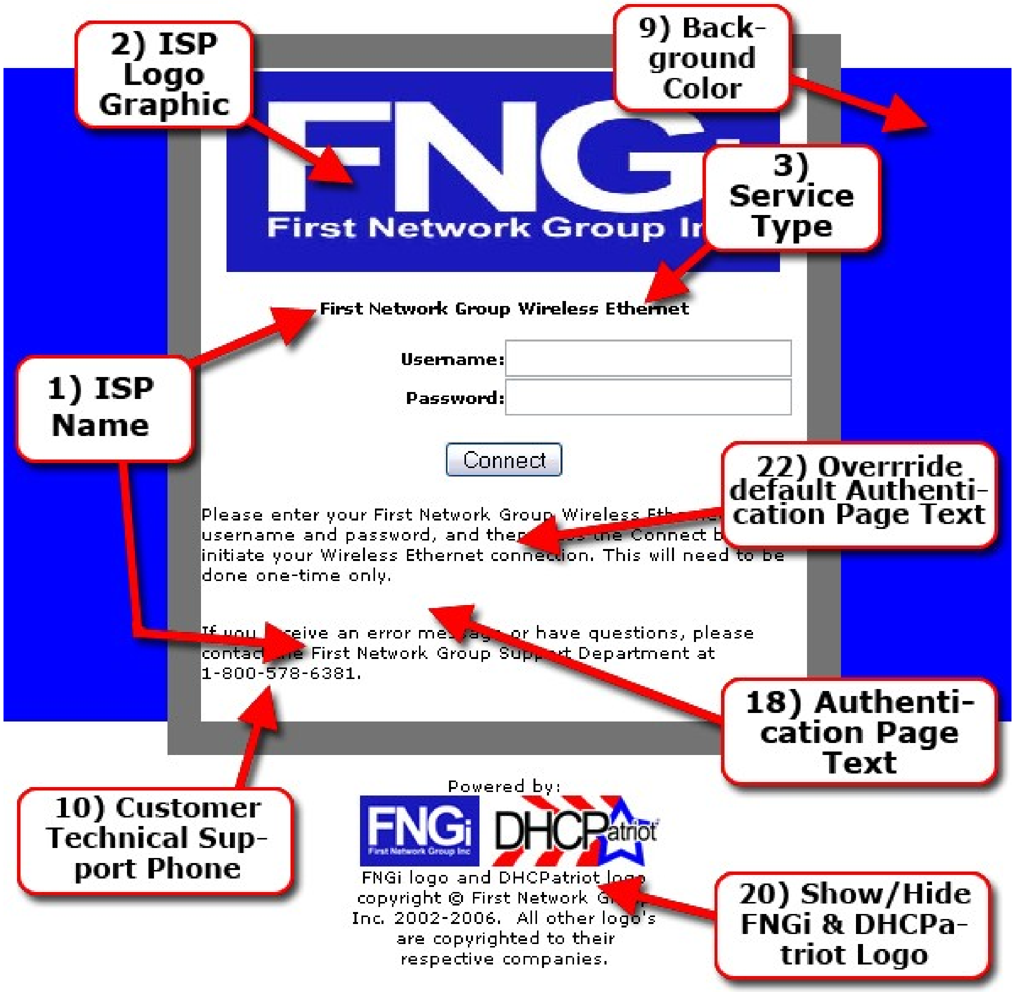
Menu items are as follows:

- Main
  - Home – Return to news.
  - Change Your Password – Change current administrator's password.
  - Request Assistance – Send a message to the DHCPatriot™ support team.
  - Credits – View development team (as seen in figure 3.8).
  - Log Off – End administrative session.
- User States
  - CurrentlyOnline – Display a list of users who are online.

    - Online Time (Deprecated) – Display the user base and their time online.
    - Online Time II – Display a specific user's sessions for the given time period.
  - User Management
    - Search Database – Search for specific sessions using various limiters.
    - Search DHCP Logs – Search for specific DHCP logs using various limiters.
    - View Suspended – Display a list of suspended devices limitable by username.
    - Suspend User – Suspend device(s).
    - Authorize Customer – Manually authenticate a specific device.
    - Built-in Authentication: User Maintenance – Allows the addition and removal of users to be authenticated via the optional Built-in Authentication.
  - IP Management
    - IP Address Usage – Summary of current IP Address utilization on the various configured networks. Usage graphs are accessed via this report.
    - Customer Usage – Estimate of over subscription on the various configured networks.
    - Lease Status – Summary of currently leased IP Addresses on the various configured networks. This report should very closely match the IP Address Usage report.
  - DHCP Configuration
    - Add Main DHCP Ranges – Add a new scope of DHCP addressing (authenticated and unauthenticated).
    - Edit Main DHCP Ranges – Edit an existing scope of DHCP addressing (authenticated and unauthenticated).
    - Add/Edit Additional DHCP Ranges – Add an additional subnet to a scope of DHCP Addressing (or edit an existing).
    - Add/Edit Static DHCP Ranges – Add a static subnet to a scope of DHCP Addressing (or edit an existing).
  - System Configuration
    - Edit Setup – Edit general configuration parameters.
    - Setup – Perform initial general configuration (can only be performed once).
    - Firewall Setup – Administer the built in firewall.
    - View Server Status – View statistics about the running DHCPatriot™ devices.
    - Add Administrator – Add a new administrator to the system.
    - Edit Administrator – Edit an existing administrator.
    - Configure Built-In Authentication Options – If using the optional Built-in Authentication, options (such as NetEnforcer® specific options), may be entered and changed here.
    - System Logs – View and search logs of the DHCPatriot™ system.
    - Ping or Trace a host – Diagnose network problems from the DHCPatriot™ system's perspective.

3.4.1 Initial General Configuration

We will begin the final configuration by performing the initial general configuration. To begin this process, open the System Configuration menu and click on Setup. A screen will appear noting the information that will be required to complete the initial setup. Be sure you have this information available. Then click next. The on-screen help here should be very useful in competing this form. A few fields may require further explanation. Figure 3.9 shows what portion of the customer login screen is controlled by which field in this setup.


2) ISP Logo Graphic
9) Back-ground Color
FNGi
First Network Group In
3) Service Type
1) ISP Name
22) Overrride default Authenti-cation Page Text
18) Authenti-cation Page Text
10) Customer Technical Sup-port Phone
20) Show/Hide FNGi & DHCPa-triot Logo
Connect
Powered by:
FNGi First Network Group Inc
DHCPatriot

First Network Group Wireless Ethernet

Username:

Password:

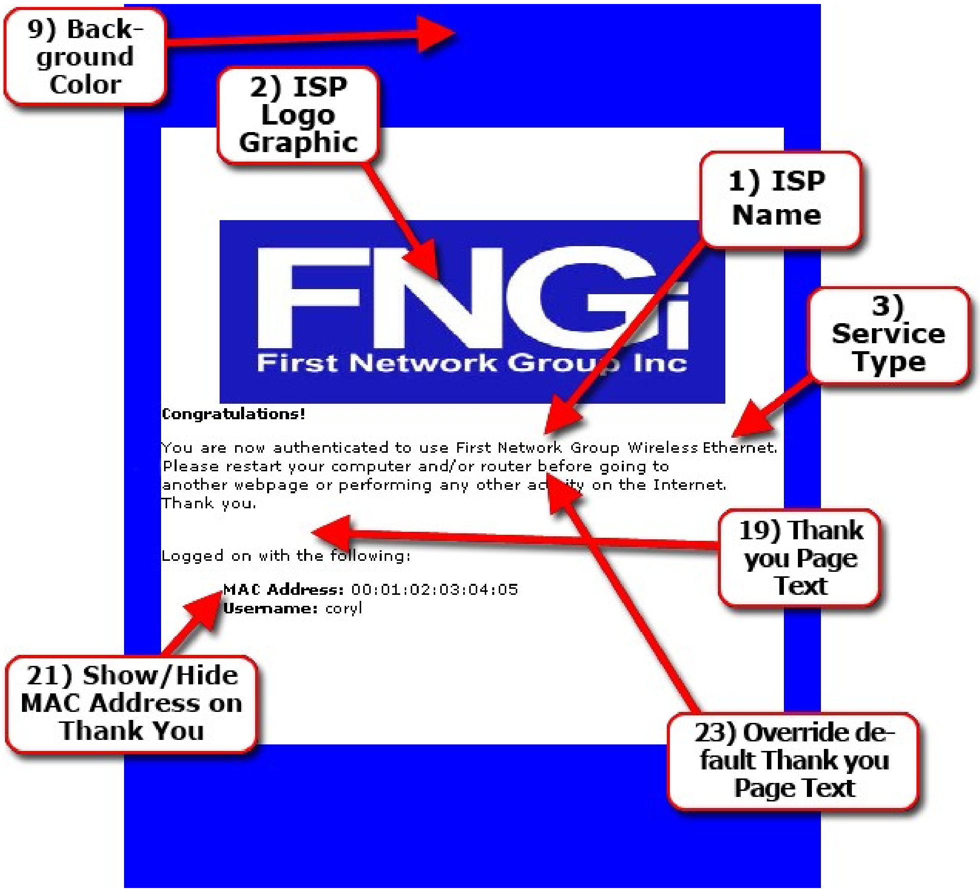
Please enter your First Network Group Wireless Ethernet username and password, and then press the Connect button to initiate your Wireless Ethernet connection. This will need to be done one-time only.

If you receive an error message or have questions, please contact the First Network Group Support Department at 1-800-578-6381.

FNGi logo and DHCPatriot logo copyright © First Network Group, Inc. 2002-2006. All other logo's are copyrighted to their respective companies.

Figure 3.9 (Your screen appearance may differ slightly depending on the software used.)

Figure 3.10 shows which portion of the thank you screen is controlled by what field in this portion of the setup.



Congratulations!

You are now authenticated to use First Network Group Wireless Ethernet.
Please restart your computer and/or router before going to
another webpage or performing any other activity on the Internet.
Thank you.

Logged on with the following:

MAC Address: 00:01:02:03:04:05
Username: coryl

Figure 3.10 (Your screen appearance may differ slightly depending on the software used.)

It may be advisable to wait to customize the login and thank you screens until after the initial configuration is completed. It will be much easier when editing and then previewing changes can be done. More on this in chapter 4.

In the setup, feature 13) DHCPatriot™ Controlled Routing may require further explanation. This feature is meant to provide IP Address Hijacking prevention in the event that your router or other equipment is unable to do so. IP Address Hijacking is when a customer decides that he likes a particular IP Address, and therefore enters the IP Address into his device settings, instead of leaving the device configured for DHCP. If the network does not have some way of controlling this, the customer would be able to use the Internet virtually anonymously from this IP Address. Enabling this setting by itself does not cause the DHCPatriot™ to control routing. Some configuration changes must be made to the policy routing introduced in section 1.5. Specifically, the authenticated addresses outbound traffic must also be policy routed to the DHCPatriot™ along with the unauthenticated outbound traffic. A change in the global configuration would be necessary to change it from this:

```
access-list <#> permit ip <Unauthenticated Wire Address> <Reverse Mask> any
access-list <#> deny ip any any
!
route-map <route map name> permit 10
 match ip address <access-list Number>
 set ip next-hop <ip of DHCPatriot™ primary device>
!
```

To this:

```
access-list <#> permit ip <Unauthenticated Wire Address> <Reverse Mask> any
access-list <#> permit ip <Authenticated Wire Address> <Reverse Mask> any
access-list <#> deny ip any any
!
route-map <route map name> permit 10
 match ip address <access-list Number>
 set ip next-hop <ip of DHCPatriot™ primary device>
!
```

This setting change on the router mentioned in section 1.5 would cause the authenticated network outbound traffic to be sent to the DHCPatriot™. Enabling feature 13 then causes the DHCPatriot™ to drop traffic that originates from an IP Address not allocated via DHCP.

Feature 16) Authenticated Lease Length allows the authenticated lease length to be changed. Some routers have been known to experience problems with VPN connections with short lease times like one of the choices, 10 minutes. The default lease length is 8 hours. A word of warning if you change this setting. The DHCPatriot™ allows an administrator to suspend a user on the DHCPatriot™. Doing this causes their active lease to not be renewed. Once the length of the lease has passed, they will receive an unauthenticated IP Address, and be forced to attempt to register again. If you have set this for a long period of time, for example 8 hours, it will be up to 8 hours before the user is dropped to an unauthenticated lease. DHCP has no provision for revoking leases. Therefore, the client is permitted to use the IP Address until the lease expires. When using a longer lease setting, some other method would need to be employed to stop a customer from using an IP Address immediately if necessary.

Feature 17) Non-Authenticated Lease Length allows the unauthenticated lease length to be changed. It is recommended that this setting be left at the default of 3 minutes. There really isn't a good reason to change it unless there exist some compatibility concern in a special situation.

Once all settings have been entered on this screen, click the next button. This will bring up the 2nd half of the initial general setup. Follow the on-screen instructions to complete this phase of the initial general setup. Click on Finish at the bottom right when all settings are configured as needed.

3.4.2 Configuring DHCP

The next step in getting the DHCPatriot™ setup for use is to create some DHCP scopes that will be used by the customers. The words scope and range are used interchangeably throughout this manual. There are four types of DHCP scopes.

First, there is the main authenticated range or super scope. This is the subnet that will likely contain the primary address on the interface that the customers are directly connected to in most cases.

Along with this main authenticated range, the second type of scope which is the unauthenticated subnet, will also be configured along side the main authenticated range. This is the range of IP Addresses that the customer devices will be using when they are unknown to the DHCPatriot™ or in the suspended state (more on this in chapter 4).

The third type of scope is the additional authenticated range. This range is used when the main authenticated range is no longer large enough to support the customer base on that interface. Add the gateway address that will be used for this range as a secondary on the interface, and on the DHCPatriot™ configure an additional range tied to the main authenticated range.

The final type of scope is the static range, this is added in the same manner as the additional range. More information on these final two types of scopes is available in chapter 4. There may be several interfaces that different groups of customers are connected to throughout the network, so there may be several main authenticated and unauthenticated ranges configured on the DHCPatriot™. This section will describe the configuration of one main authenticated range and its accompanying unauthenticated range.

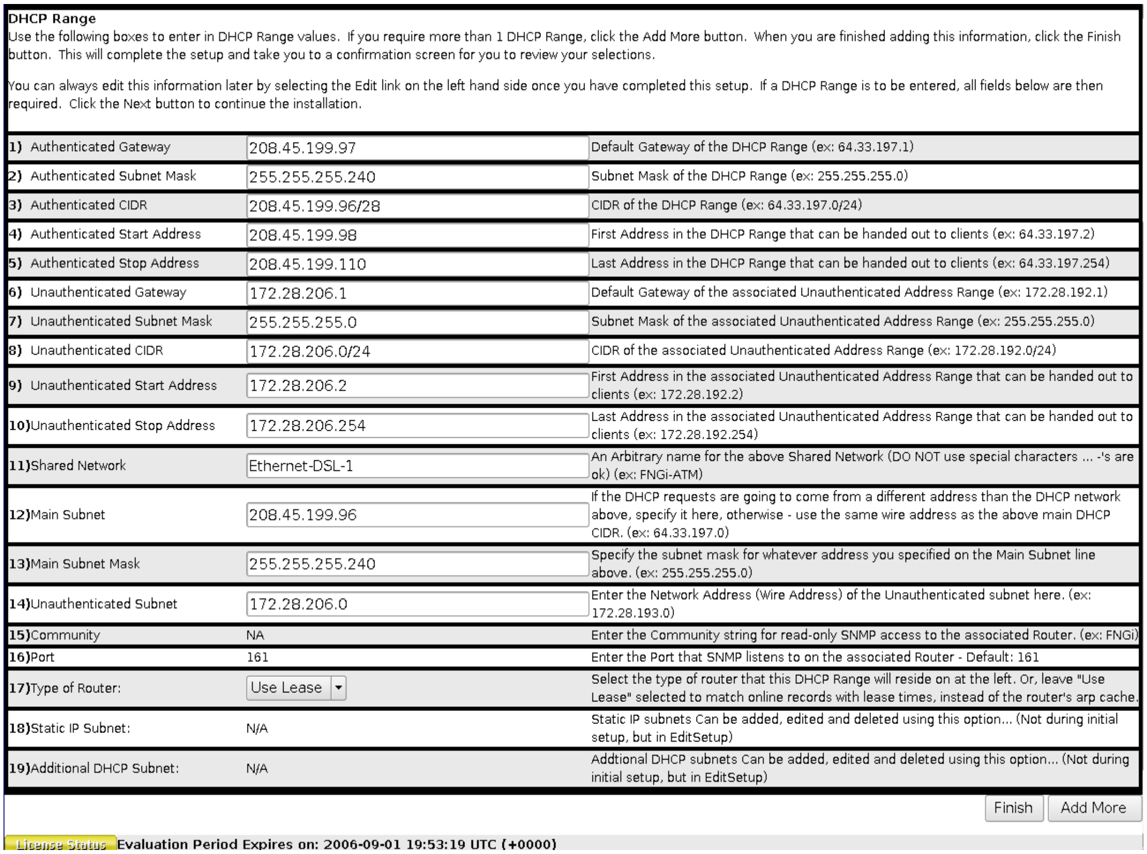
A word on network selection and configuration requirements on the interface to which the customers are directly connected. If you already have an existing DHCP network(s) and the DHCPatriot™ is merely replacing your current DHCP server, then you may re-use these networks. Make sure that you are aware of the source IP of the DHCP Relay Agent. On a Cisco® router, this will be the primary IP Address on the interface that contains the 'ip helper-address' setting. If you are setting up a new DHCP network, please be sure and choose a subnet of sufficient size to serve the expected customer base. If you need to configure additional subnets that are secondary address ranges on this single interface, please see chapter 4 after completing the setup described here.

Consider the following typical Cisco® interface configuration example:

```
interface FastEthernet0/1
description Ethernet DSL 1
ip address 208.45.199.97 255.255.255.240
ip address 172.28.206.1 255.255.255.0 secondary
ip address 208.45.199.113 255.255.255.240 secondary
ip address 208.45.199.129 255.255.255.248 secondary
ip helper-address 65.222.44.132
ip helper-address 65.222.44.133
!
```

The network 208.45.199.96/28 is the main authenticated range or scope. The network 172.28.206.0/24 is the unauthenticated range or scope. The network 208.45.199.112/28 is an additional range or scope, and 208.45.199.128/29 is a static range or scope. Each gateway address from each subnet must be configured on the interface. The example shows the first usable address being used as the gateway. This is merely a convention, some may wish to use the last usable address. This section will demonstrate the setup of the main authenticated and unauthenticated ranges or scopes. For instructions on setting up the additional or static ranges or scopes see chapter 4.

To begin the process, open the DHCP Configuration menu and click Add Main DHCP ranges. Each field is populated in figure 3.11 according to the proper setup from the example network.



DHCP Range

Use the following boxes to enter in DHCP Range values. If you require more than 1 DHCP Range, click the Add More button. When you are finished adding this information, click the Finish button. This will complete the setup and take you to a confirmation screen for you to review your selections.

You can always edit this information later by selecting the Edit link on the left hand side once you have completed this setup. If a DHCP Range is to be entered, all fields below are then required. Click the Next button to continue the installation.

1) Authenticated Gateway	208.45.199.97	Default Gateway of the DHCP Range (ex: 64.33.197.1)
2) Authenticated Subnet Mask	255.255.255.240	Subnet Mask of the DHCP Range (ex: 255.255.255.0)
3) Authenticated CIDR	208.45.199.96/28	CIDR of the DHCP Range (ex: 64.33.197.0/24)
4) Authenticated Start Address	208.45.199.98	First Address in the DHCP Range that can be handed out to clients (ex: 64.33.197.2)
5) Authenticated Stop Address	208.45.199.110	Last Address in the DHCP Range that can be handed out to clients (ex: 64.33.197.254)
6) Unauthenticated Gateway	172.28.206.1	Default Gateway of the associated Unauthenticated Address Range (ex: 172.28.192.1)
7) Unauthenticated Subnet Mask	255.255.255.0	Subnet Mask of the associated Unauthenticated Address Range (ex: 255.255.255.0)
8) Unauthenticated CIDR	172.28.206.0/24	CIDR of the associated Unauthenticated Address Range (ex: 172.28.192.0/24)
9) Unauthenticated Start Address	172.28.206.2	First Address in the associated Unauthenticated Address Range that can be handed out to clients (ex: 172.28.192.2)
10) Unauthenticated Stop Address	172.28.206.254	Last Address in the associated Unauthenticated Address Range that can be handed out to clients (ex: 172.28.192.254)
11) Shared Network	Ethernet-DSL-1	An Arbitrary name for the above Shared Network (DO NOT use special characters ... -'s are ok) (ex: FNGi-ATM)
12) Main Subnet	208.45.199.96	If the DHCP requests are going to come from a different address than the DHCP network above, specify it here, otherwise - use the same wire address as the above main DHCP CIDR. (ex: 64.33.197.0)
13) Main Subnet Mask	255.255.255.240	Specify the subnet mask for whatever address you specified on the Main Subnet line above. (ex: 255.255.255.0)
14) Unauthenticated Subnet	172.28.206.0	Enter the Network Address (Wire Address) of the Unauthenticated subnet here. (ex: 172.28.193.0)
15) Community	NA	Enter the Community string for read-only SNMP access to the associated Router. (ex: FNGi)
16) Port	161	Enter the Port that SNMP listens to on the associated Router - Default: 161
17) Type of Router:	Use Lease ▾	Select the type of router that this DHCP Range will reside on at the left. Or, leave "Use Lease" selected to match online records with lease times, instead of the router's arp cache.
18) Static IP Subnet:	N/A	Static IP subnets Can be added, edited and deleted using this option... (Not during initial setup, but in EditSetup)
19) Additional DHCP Subnet:	N/A	Addtional DHCP subnets Can be added, edited and deleted using this option... (Not during initial setup, but in EditSetup)

Evaluation Period Expires on: 2006-09-01 19:53:19 UTC (+0000)

Figure 3.11 (Your screen appearance may differ slightly depending on the software used.)

Some fields require further explanation. Field 11 (Shared Network) is a text identifier for this main authenticated and all related scopes throughout the DHCPatriot™. An identifier that has some meaning to you for which customers it applies to should be chosen for this field. Fields 12 and 13 (Main Subnet and Main Subnet Mask respectively) can be used to associate a maintenance subnet of some kind that will not be handed out to customers with this scope. If the configuration on our interface from the example instead appeared like this:

```
interface FastEthernet0/1
description Ethernet DSL 1
ip address 208.142.243.1 255.255.255.0
ip address 208.45.199.97 255.255.255.240 secondary
ip address 172.28.206.1 255.255.255.0 secondary
ip address 208.45.199.113 255.255.255.240 secondary
ip address 208.45.199.129 255.255.255.248 secondary
ip helper-address 65.222.44.132
ip helper-address 65.222.44.133
!
```

Fields 12 and 13 would instead be filled out with 208.142.243.0 and

255.255.255.0 respectively. The subnet 208.142.243.0/24 is not a DHCP pool, but it is the subnet that the DHCP Relay Agent traffic will be sourcing. Fill out the fields with values appropriate to your configuration, and press finish. It is normal for the DHCPatriot™ to take some time to process the addition, perhaps even several minutes. Please be patient, an error message will be returned if there is an issue that needs addressed.

This completes the configuration process. Chapter 4 covers the Web Administration Interface in greater detail.

4 Web Administration Interface

This chapter covers the daily use and configuration features of the DHCPatriot™ Web Administration Interface.

4.1 Configuration Options

This section describes the use of the Web Administration Interface in configuring the DHCPatriot™ throughout the life of the product.

4.1.1 Configuring Main Authenticated/Unauthenticated DHCP Ranges (scopes)

The instructions in section 3.4.2 apply here as well. We will continue with the example from section 3.4.2 in sections 4.1.2 and 4.1.3 describing how to add, edit and remove additional and static ranges. The remainder of this section is devoted to editing and removing main DHCP ranges.

Ideally, it is best to add a new main range and cut customers to it and later remove the no longer in use range rather than edit an existing entry (for reasons that will become obvious), but this may not always be possible. Therefore, it is possible to edit main ranges on the DHCPatriot™.

Editing a main DHCP range requires that no user be online using an address out of the range during the editing process. Since it is difficult to get all end users to simultaneously power down their devices, a mechanism is provided in the DHCPatriot™ to achieve this.

Open the DHCP Configuration menu. Click on Edit main DHCP Ranges. A matrix showing each main DHCP Range that is configured on the DHCPatriot™ appears. If the range is currently editable, the authenticated CIDR and unauthenticated CIDR will be click able. If customers are currently using IP Addresses from the range, neither will be click able.

To stop customers from using the range, click disable. This will cause the link to change to an enable link. Over the course of the lease length (see section 4.1.4 for discussion of lease length) customers will drop out of this range. If sufficient additional range space exists, the customers will reacquire a lease from there. If not, then they will not be able to obtain an IP Address until this process is completed. If the reason for editing this range is that more IP Addresses are required, consider adding an additional range as described in section 4.1.2.

Once all of the customers have moved from this range (you can watch the # online column as you refresh the screen by clicking Edit Main DHCP Ranges), the previously mentioned CIDR links will become click able. Click on either one to edit the range. A screen similar to that shown in figure 3.11 will appear. For an explanation of fields and their purposes, see the on-screen instructions and section 3.4.2 for further information. Make whatever changes are necessary and then click on Edit DHCP Range. This may take several minutes to complete. To return to the list of ranges so that the range may be re-enabled, click on Edit Main DHCP Ranges. Click on the enable link for the range that was edited. This will re-enable the range so that customers can use it again. You may also need to make modifications to your router at this time so that users can properly use the range post change.

To delete a range, click Edit Main DHCP Ranges. Locate the range that you wish to delete. Two requirements must first be met. No IP Addresses may be in use from the range to be deleted (the # online column must be 0 – see the instructions previously mentioned in this section for disabling a range). There can be no additional or static ranges attached to this main DHCP range (The # of Additional/Static column must also read 0). If there are additional or static ranges attached to this network, see section 4.1.2 and 4.1.3 respectively for additional instructions.

Once the aforementioned requirements are met, the delete link for the range you wish to delete will become active (you may need to refresh the screen as mentioned previously by clicking Edit Main DHCP Ranges again). To delete the range, click the delete link. This may take several minutes to complete. You may need to make changes to your router at this time to accommodate the changes here.

4.1.2 Configuring Additional DHCP Ranges (scopes)

In section 3.4.2, we introduced the following example configuration on an interface:

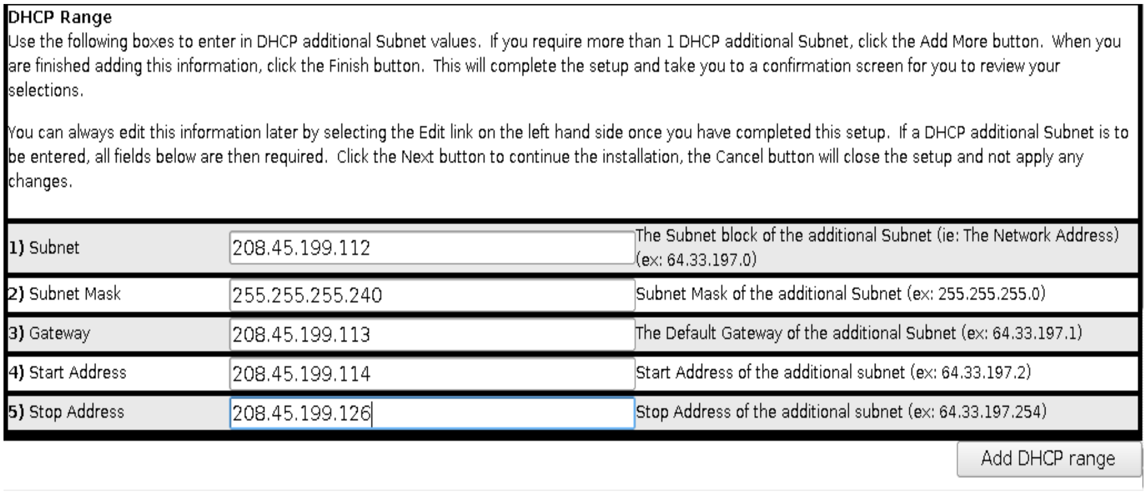
```
interface FastEthernet0/1
description Ethernet DSL 1
ip address 208.45.199.97 255.255.255.240
ip address 172.28.206.1 255.255.255.0 secondary
ip address 208.45.199.113 255.255.255.240 secondary
ip address 208.45.199.129 255.255.255.248 secondary
ip helper-address 65.222.44.132
ip helper-address 65.222.44.133
!
```

To illustrate configuring a main authenticated and unauthenticated range or scope. But what do we do to add the additional and static ranges (208.45.199.112/28 and 208.45.199.128/29 respectively)? This section describes adding, editing and deleting additional ranges. Section 4.1.3 describes adding, editing and deleting static ranges.

We will use the example to show how to add an additional DHCP range. This example shows only one additional DHCP range, but multiple additional DHCP ranges may be added to a single main DHCP range. We will be adding the additional subnet 208.45.199.112/28 as described in the example. This range will be attached to the main DHCP range 208.45.199.96/28 from the example.

To add an additional range, open the DHCP Configuration menu. Then click on Add/Edit Additional DHCP Ranges. A list of all main DHCP ranges configured on the DHCPatriot™ will be displayed here. Locate the one that you wish to attach an additional DHCP range to and click on it (208.45.199.96/28 [Ethernet-DSL-1] from the example in section 3.4.2). A new screen displaying the main DHCP range chosen, as well as any additional DHCP ranges already configured for that main DHCP range will appear.

Click on Add Additional DHCP Range. A screen similar to figure 4.1 will appear.



DHCP Range

Use the following boxes to enter in DHCP additional Subnet values. If you require more than 1 DHCP additional Subnet, click the Add More button. When you are finished adding this information, click the Finish button. This will complete the setup and take you to a confirmation screen for you to review your selections.

You can always edit this information later by selecting the Edit link on the left hand side once you have completed this setup. If a DHCP additional Subnet is to be entered, all fields below are then required. Click the Next button to continue the installation, the Cancel button will close the setup and not apply any changes.

1) Subnet	208.45.199.112	The Subnet block of the additional Subnet (ie: The Network Address) (ex: 64.33.197.0)
2) Subnet Mask	255.255.255.240	Subnet Mask of the additional Subnet (ex: 255.255.255.0)
3) Gateway	208.45.199.113	The Default Gateway of the additional Subnet (ex: 64.33.197.1)
4) Start Address	208.45.199.114	Start Address of the additional subnet (ex: 64.33.197.2)
5) Stop Address	208.45.199.126	Stop Address of the additional subnet (ex: 64.33.197.254)

Figure 4.1 (Your screen appearance may differ slightly depending on the software used.)

Figure 4.1 shows the values that would need to be entered to add the additional DHCP range from our example. Type the values as necessary for your network, and then click Add DHCP Range. This may take several minutes to complete.

Ideally, it is best to add a new additional range and cut customers to it and later remove the no longer in use range rather than edit an existing entry (for reasons that will become obvious), but this may not always be possible. Therefore, it is possible to edit additional ranges on the DHCPatriot™.

Editing an additional DHCP range requires that no user be online using an address out of the range during the editing process. Since it is difficult to get all end users to simultaneously power down their devices, a mechanism is provided in the DHCPatriot™ to achieve this.

Open the DHCP Configuration menu. Click on Add/Edit Additional DHCP Ranges. A matrix showing each main DHCP Range that is configured on the DHCPatriot™ appears. Click on the main DHCP range that contains the additional DHCP range that you wish to edit. A new screen will appear showing which main DHCP range you are configuring along with each additional DHCP range that is attached to this main DHCP range. Find the range you wish to edit. If the range is currently editable, the subnet and subnet mask will be click able. If customers are currently using IP Addresses from the range, neither will be clickable.

To stop customers from using the range, click disable. The link will change to an enable link. Over the course of the lease length (see section 4.1.4 for discussion of lease length) customers will drop out of this range. If sufficient main or additional range space exists, the customers will reacquire a lease from there. If not, then they will not be able to obtain an IP Address until this process is completed. If the reason for editing this range is that more IP Addresses are required, consider adding another additional range as described earlier in this section.

Once all of the customers have moved from this range, the previously mentioned links will become click able. Click on either one to edit the range. A screen similar to that shown in figure 4.1 will appear. For an explanation of fields and their purposes, see the on-screen instructions. Make whatever changes are necessary and then click on Edit DHCP Range. This may take several minutes to complete. To return to the list of ranges so that the range may be re-enabled, click on Add/Edit Additional DHCP Ranges. Click on the enable link for the range that was edited. This will re-enable the range so that customers can use it again. You may also need to make modifications to your router at this time so that users can properly use the range post change.

To delete a range, click Add/Edit Additional DHCP Ranges. Locate the range that you wish to delete. No IP Addresses may be in use from the range to be deleted.

Once the aforementioned requirements are met, the delete link for the range you wish to delete will become active (you may need to refresh the screen as mentioned previously by clicking Add/Edit Additional DHCP Ranges again). To delete the range, click the delete link. This may take several minutes to complete. You may need to make changes to your router at this time to accommodate the changes here.

4.1.3 Configuring Static DHCP Ranges (scopes)

In section 3.4.2, we introduced the following example configuration on an interface:

```
interface FastEthernet0/1
description Ethernet DSL 1
ip address 208.45.199.97 255.255.255.240
ip address 172.28.206.1 255.255.255.0 secondary
ip address 208.45.199.113 255.255.255.240 secondary
ip address 208.45.199.129 255.255.255.248 secondary
ip helper-address 65.222.44.132
ip helper-address 65.222.44.133
!
```

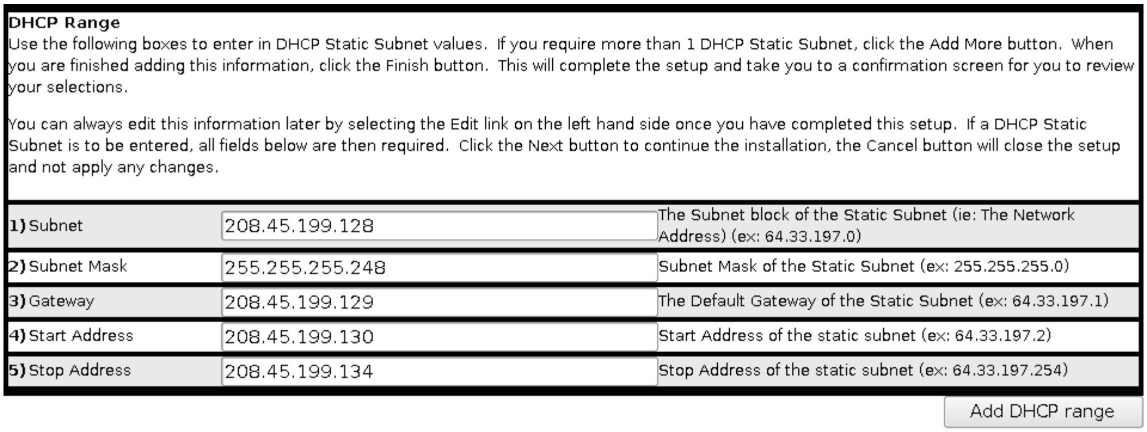
To illustrate configuring a main authenticated and unauthenticated range or scope. In section 4.1.2 we demonstrated how to add an additional DHCP range using this example. But what do we do to add the static range (208.45.199.128/29)? This section describes adding, editing and deleting static ranges.

But first, you might ask how one can have a static IP Address and be using DHCP? The answer involves the optional RADIUS or the Built-in authentication. Section 4.2.2 describes assigning a static IP Address via the Built-in authentication when configuring a user. Using the optional external RADIUS server involves populating reply attribute number 8, Framed-IP-Address, with the static IP Address that you wish for the customer to receive during the authentication process. This static IP Address must be a part of the subnet that we are about to add (208.45.199.128/29 from the example), as this subnet will never be handed out dynamically, but is instead reserved for static IP customers. Normally, the RADIUS server would respond with 255.255.255.254 in the Framed-IP-Address attribute, but when a customer that you wish to receive a specific static IP Address authenticates, this field would be populated with that specific IP Address instead. Methods of accomplishing this on the RADIUS server vary. Please consult your documentation or RADIUS server vendor for assistance.

We will now use the example to show how to add a static DHCP range. This example shows only one static DHCP range, but multiple static DHCP ranges may be added to a single main DHCP range. We will be adding the static subnet 208.45.199.128/29 as described in the example. This range will be attached to the main DHCP range 208.45.199.96/28 from the example.

To add a static range, open the DHCP Configuration menu. Then click on Add/Edit Static DHCP Ranges. A list of all main DHCP ranges configured on the DHCPatriot™ will be displayed here. Locate the one that you wish to attach a static DHCP range to and click on it (208.45.199.96/28 [Ethernet-DSL-1] from the example in section 3.4.2). A new screen displaying the main DHCP range chosen, as well as any static DHCP ranges already configured for that main DHCP range will appear.

Click on Add Static DHCP Range. A screen similar to figure 4.2 will appear.



DHCP Range

Use the following boxes to enter in DHCP Static Subnet values. If you require more than 1 DHCP Static Subnet, click the Add More button. When you are finished adding this information, click the Finish button. This will complete the setup and take you to a confirmation screen for you to review your selections.

You can always edit this information later by selecting the Edit link on the left hand side once you have completed this setup. If a DHCP Static Subnet is to be entered, all fields below are then required. Click the Next button to continue the installation, the Cancel button will close the setup and not apply any changes.

1) Subnet	208.45.199.128	The Subnet block of the Static Subnet (ie: The Network Address) (ex: 64.33.197.0)
2) Subnet Mask	255.255.255.248	Subnet Mask of the Static Subnet (ex: 255.255.255.0)
3) Gateway	208.45.199.129	The Default Gateway of the Static Subnet (ex: 64.33.197.1)
4) Start Address	208.45.199.130	Start Address of the static subnet (ex: 64.33.197.2)
5) Stop Address	208.45.199.134	Stop Address of the static subnet (ex: 64.33.197.254)

Figure 4.2 (Your screen appearance may differ slightly depending on the software used.)

Figure 4.2 shows the values that would need to be entered to add the static DHCP range from our example. Type the values as necessary for your network, and then click Add DHCP Range. This may take several minutes to complete.

To move an existing authenticated customer who is currently at a dynamic address, assign the desired static address in RADIUS or in the Built-in authentication. Then suspend the customer (discussed in section 4.2.6) to force them to authenticate again. The customer will have to wait the length of the lease to receive the authentication screen, or they can perform a release/renew to force it to appear sooner. Once they authenticate, they will receive the static IP Address that was assigned to them.

It is best not to edit a static range after customers are using it, so there is no disable function for this type of subnet. If more capacity is required, add another range for customer use.

You may edit the Static range if no customer is using it, however. Open the DHCP Configuration menu. Click on Add/Edit Static DHCP Ranges. A matrix showing each main DHCP Range that is configured on the DHCPatriot™ appears. Click on the main DHCP range that contains the static DHCP range that you wish to edit. A new screen will appear showing which main DHCP range you are configuring along with each static DHCP range that is attached to this main DHCP range. Find the range you wish to edit. If the range is currently editable, the subnet and subnet mask will be click able. If customers are currently using IP Addresses from the range, neither will be click able. Click on either one to edit the range. A screen similar to that shown in figure 4.2 will appear. For an explanation of fields and their purposes, see the on-screen instructions. Make whatever changes are necessary and then click on Edit DHCP Range. This may take several minutes to complete. You may need to make modifications to your router at this time so that users can properly use the range post change.

To delete a range, click Add/Edit Static DHCP Ranges. Locate the range that you wish to delete. No IP Addresses may be in use from the range to be deleted.

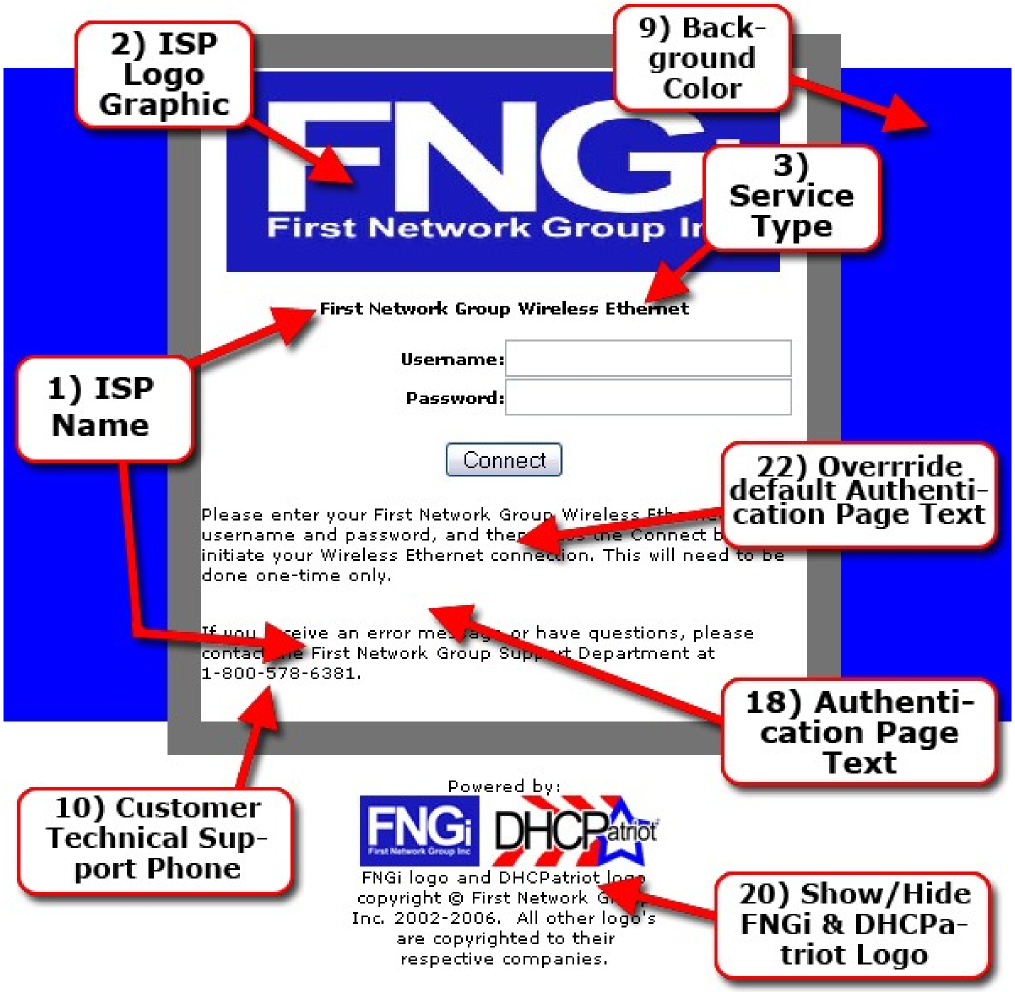
Once the aforementioned requirements are met, the delete link for the range you wish to delete will become active (you may need to refresh the screen as mentioned previously by clicking Add/Edit Static DHCP Ranges again). To delete the range, click the delete link. This may take several minutes to complete. You may need to make changes to your router at this time to accommodate the changes here.

4.1.4 Changing the Basic Setup

Section 3.4.1 explained how to perform the general configuration initially. It is also possible to edit that configuration on an ongoing basis as needs change or new features are to be implemented. This section provides useful information that may be needed to perform that operation.

To begin the edit process, open the System Configuration menu and click on Edit Setup. A screen will appear with two buttons. Click the Edit Basic Information button. The on-screen help here should be very useful in using this form. A few fields may require further explanation.

Much of this setup is devoted to controlling the appearance of the customer login screen. As you make changes you can preview both the login and thank you pages by clicking the links at the bottom of the Basic Setup screen. Be sure and apply changes by clicking the Edit button at the bottom right of the screen before attempting to preview any changes. A screen similar to figure 4.3 will appear as you preview the login screen. Figure 4.3 shows what portion of the customer login screen is controlled by which field in this setup.


2) ISP Logo Graphic
9) Back-ground Color
FNG
First Network Group In
3) Service Type
1) ISP Name
22) Overrride default Authenti-cation Page Text
18) Authenti-cation Page Text
10) Customer Technical Sup-port Phone
20) Show/Hide FNGi & DHCPa-triot Logo
Connect
FNGi First Network Group Inc
DHCPatriot

First Network Group Wireless Ethernet

Username:

Password:

Please enter your First Network Group Wireless Ethernet username and password, and then press the Connect button to initiate your Wireless Ethernet connection. This will need to be done one-time only.

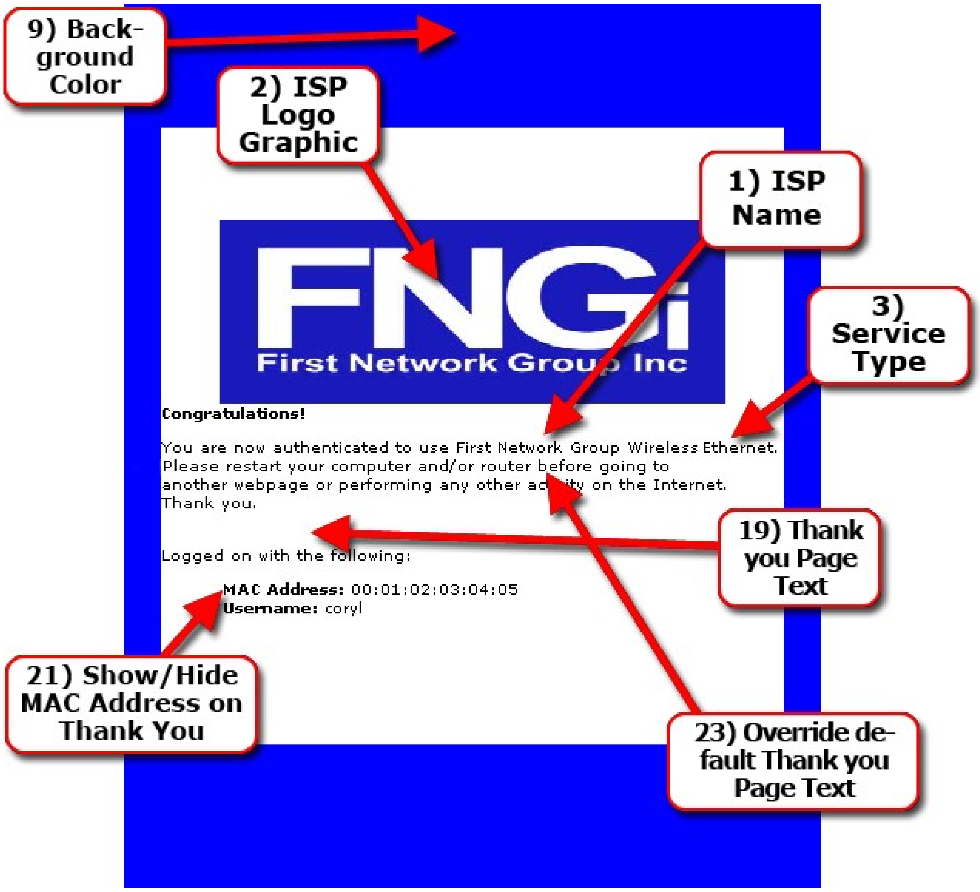
If you receive an error message or have questions, please contact the First Network Group Support Department at 1-800-578-6381.

Powered by:

FNGi logo and DHCPatriot logo copyright © First Network Group, Inc. 2002-2006. All other logo's are copyrighted to their respective companies.

Figure 4.3 (Your screen appearance may differ slightly depending on the software used.)

A screen similar to figure 4.4 shows what will appear if you click the preview thank you page link. Figure 4.4 shows which portion of the thank you screen is controlled by what field in this portion of the setup.



Congratulations!

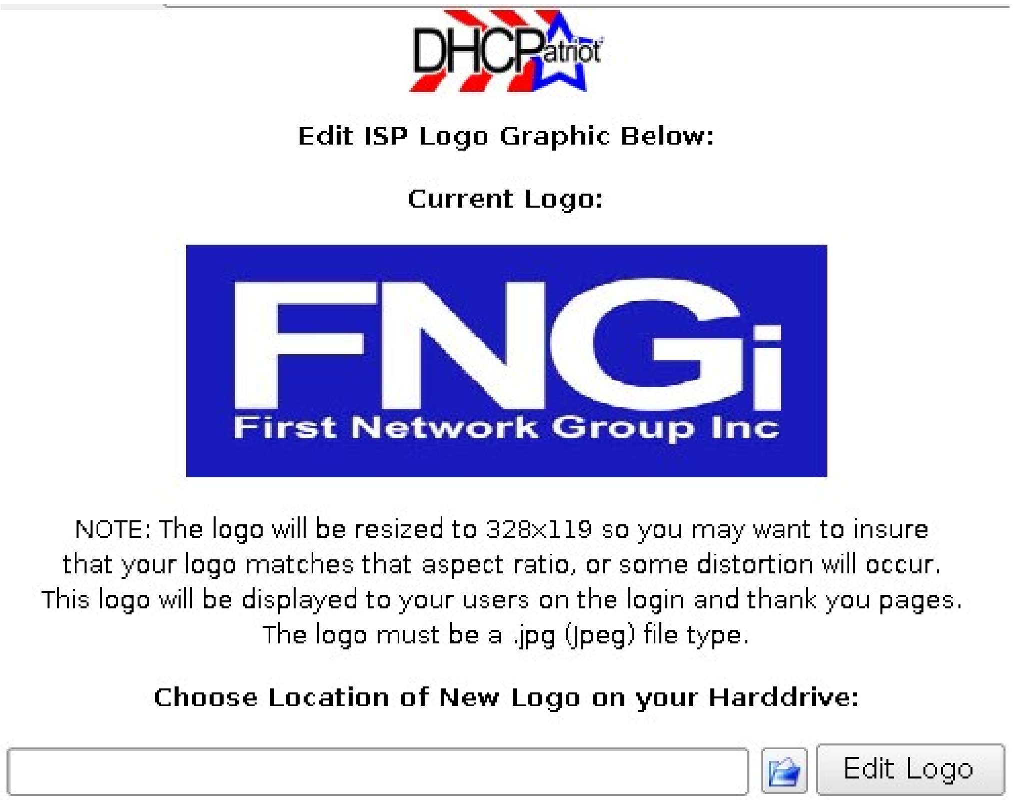
You are now authenticated to use First Network Group Wireless Ethernet. Please restart your computer and/or router before going to another webpage or performing any other activity on the Internet. Thank you.

Logged on with the following:

MAC Address: 00:01:02:03:04:05
Username: coryl

Figure 4.4 (Your screen appearance may differ slightly depending on the software used.)

Feature 2) ISP logo graphic bears further explanation. As you can see from figure 4.3 and 4.4 the logo that is displayed to the customers is customizable using this feature. To edit the logo, click the edit link. A screen will appear similar to that shown in figure 4.5.



Edit ISP Logo Graphic Below:

Current Logo:

NOTE: The logo will be resized to 328x119 so you may want to insure that your logo matches that aspect ratio, or some distortion will occur. This logo will be displayed to your users on the login and thank you pages. The logo must be a .jpg (Jpeg) file type.

Choose Location of New Logo on your Harddrive:

Figure 4.5 (Your screen appearance may differ slightly depending on the software used.)

As noted on the screen, the logo will be resized to 328x119 for display on the login and thank you pages. It is best if your logo is this size already or stretching may occur. The file must be a jpeg (.jpg) file. You may need an editor to work with your existing company logo to meet these requirements. Adobe® Photoshop® (http://www.adobe.com/products/photoshop/) is a good commercial editor. You could also use The Gimp (http://www.gimp.org/) which is a good open source GNU alternative to Adobe® Photoshop®. Once the necessary changes have been made, click the browse (or folder icon – depending upon the web browser you are using) button. Locate the logo file you wish to upload. Confirm the selection. Then click Edit Logo. The logo will be uploaded to the DHCPatriot™. This may take several minutes depending on network congestion. Once this process is complete, you may have to close and reopen this window, or even right click in it and press refresh if your browser stubbornly caches the old logo. Rest assured that if there were no error messages, then the logo was uploaded correctly.

Feature 13) DHCPatriot™ Controlled Routing may require further explanation. This feature is meant to provide IP Address Hijacking prevention in the event that your router or other equipment is unable to do so. IP Address Hijacking is when a customer decides that he likes a particular IP Address, and therefore enters the

IP Address into his device settings, instead of leaving the device configured for DHCP.

If the network does not have some way of controlling this, the customer would be able to use the Internet virtually anonymously from this IP Address. Enabling this setting by itself does not cause the DHCPatriot™ to control routing. Also, some configuration changes must be made to the policy routing introduced in section 1.5.

Specifically, the authenticated addresses outbound traffic must also be policy routed to the DHCPatriot™ along with the unauthenticated outbound traffic. A change in the global configuration would be necessary to change it from this:

```
access-list <#> permit ip <Unauthenticated Wire Address> <Reverse Mask> any
access-list <#> deny ip any any
!
route-map <route map name> permit 10
 match ip address <access-list Number>
 set ip next-hop <ip of DHCPatriot™ primary device>
!
```

To this:

```
access-list <#> permit ip <Unauthenticated Wire Address> <Reverse Mask> any
access-list <#> permit ip <Authenticated Wire Address> <Reverse Mask> any
access-list <#> deny ip any any
!
route-map <route map name> permit 10
 match ip address <access-list Number>
 set ip next-hop <ip of DHCPatriot™ primary device>
!
```

This setting change on the router mentioned in section 1.5 would cause the authenticated network outbound traffic to be sent to the DHCPatriot™. Enabling feature 13 then causes the DHCPatriot™ to drop traffic that originates from an IP Address not allocated via DHCP.

Feature 16) Authenticated Lease Length allows the authenticated lease length to be changed. Some routers have been known to experience problems with VPN connections with short lease times like one of the choices, 10 minutes. The default lease length is 8 hours. A word of warning if you change this setting. The DHCPatriot™ allows an administrator to suspend a user on the DHCPatriot™. Doing this causes their active lease to not be renewed. Once the length of the lease has passed, they will receive an unauthenticated IP Address, and be forced to attempt to register again. If you have set this for a long period of time, for example 8 hours, it will be up to 8 hours before the user is dropped to an unauthenticated lease. DHCP has no provision for revoking leases. Therefore, the client is permitted to use the IP Address until the lease expires. When using a longer lease setting, some other method would need to be employed to stop a customer from using an IP Address immediately if necessary.

Feature 17) Non-Authenticated Lease Length allows the unauthenticated lease length to be changed. It is recommended that this setting be left at the default of 3 minutes. There really isn't a good reason to change it unless there exist some compatibility concern in a special situation.

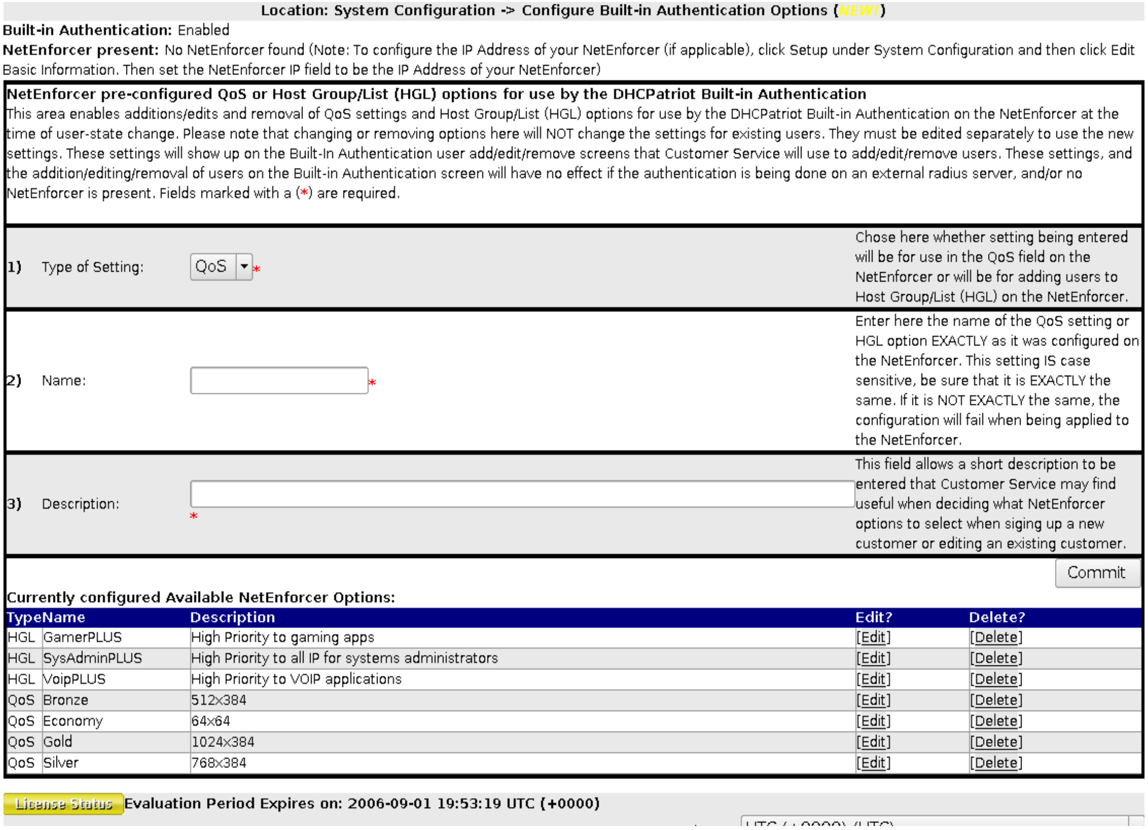
Once all desired setting changes have been performed, click the edit button at the bottom right. Check for any error messages that may occur. You may perform as many changes as need be. Click Edit only as necessary as background operations that occur may negatively affect performance on production systems.

4.1.5 Changing the RADIUS setup

This section applies whether you use an external RADIUS server or the Built-in authentication. The on-screen help should be sufficient here.

4.1.6 Configuring the Optional Built-in Authentication Options

This section exlains the options that may be configured for use in Built-in Authentication. These currently consist of maintaining QoS (Quality of Service) options and HGL (Host Group/List) options that would be used when adding customers to the Built-in Authentication where a NetEnforcer® is present. If you are not using the Built-In Authentication, or you do not have a NetEnforcer®, you may skip this section entirely.
The interface used for configuring the Built-in Authentication options is shown in figure 4.6.



Location: System Configuration -> Configure Built-in Authentication Options (NEW!)

Built-in Authentication: Enabled

NetEnforcer present: No NetEnforcer found (Note: To configure the IP Address of your NetEnforcer (if applicable), click Setup under System Configuration and then click Edit Basic Information. Then set the NetEnforcer IP field to be the IP Address of your NetEnforcer)

NetEnforcer pre-configured QoS or Host Group/List (HGL) options for use by the DHCPatriot Built-in Authentication

This area enables additions/edits and removal of QoS settings and Host Group/List (HGL) options for use by the DHCPatriot Built-in Authentication on the NetEnforcer at the time of user-state change. Please note that changing or removing options here will NOT change the settings for existing users. They must be edited separately to use the new settings. These settings will show up on the Built-In Authentication user add/edit/remove screens that Customer Service will use to add/edit/remove users. These settings, and the addition/editing/removal of users on the Built-in Authentication screen will have no effect if the authentication is being done on an external radius server, and/or no NetEnforcer is present. Fields marked with a (*) are required.

1)	Type of Setting:	QoS *	Chose here whether setting being entered will be for use in the QoS field on the NetEnforcer or will be for adding users to Host Group/List (HGL) on the NetEnforcer.
2)	Name:	*	Enter here the name of the QoS setting or HGL option EXACTLY as it was configured on the NetEnforcer. This setting IS case sensitive, be sure that it is EXACTLY the same. If it is NOT EXACTLY the same, the configuration will fail when being applied to the NetEnforcer.
3)	Description:	*	This field allows a short description to be entered that Customer Service may find useful when deciding what NetEnforcer options to select when siging up a new customer or editing an existing customer.

Currently configured Available NetEnforcer Options:

Type	Name	Description	Edit?	Delete?
HGL	GamerPLUS	High Priority to gaming apps	[Edit]	[Delete]
HGL	SysAdminPLUS	High Priority to all IP for systems administrators	[Edit]	[Delete]
HGL	VoipPLUS	High Priority to VOIP applications	[Edit]	[Delete]
QoS	Bronze	512x384	[Edit]	[Delete]
QoS	Economy	64x64	[Edit]	[Delete]
QoS	Gold	1024x384	[Edit]	[Delete]
QoS	Silver	768x384	[Edit]	[Delete]

Evaluation Period Expires on: 2006-09-01 19:53:19 UTC (+0000)

Figure 4.6 (Your screen appearance may differ slightly depending on the software used.)

HGL entries are used to place users in special host groups or lists on the NetEnforcer® that can be made to do a wide variety of things (see section 1.2.2 for further information). QoS entries are used on the NetEnforcer® to apply bandwidth settings to a Virtual Channel (VC) (see section 1.2.2 for further information).

The only requirement here is that each entry you make here also exist on the NetEnforcer® EXACTLY as the name appears here (yes, they are case sensitive entries). What is entered here will be seen by Customer Service when they are adding users in the Built-in Authentication: User maintenance section. They will have the opportunity to apply one QoS and as many HGL entries as are configured here to each user.

To add an entry, open the System Configuration menu and then click on Configure Built-in Authentication Options. A screen similar to that in figure 4.6 will appear (Currently configured available NetEnforcer® Options are shown for illustrative purposes only and may not appear on your screen). Choose the type of entry to add. Type the name and enter a description that will have some useful meaning for Customer Service and yourself. Click the Commit button. The entry you made will appear under Currently configured available NetEnforcer® Options.

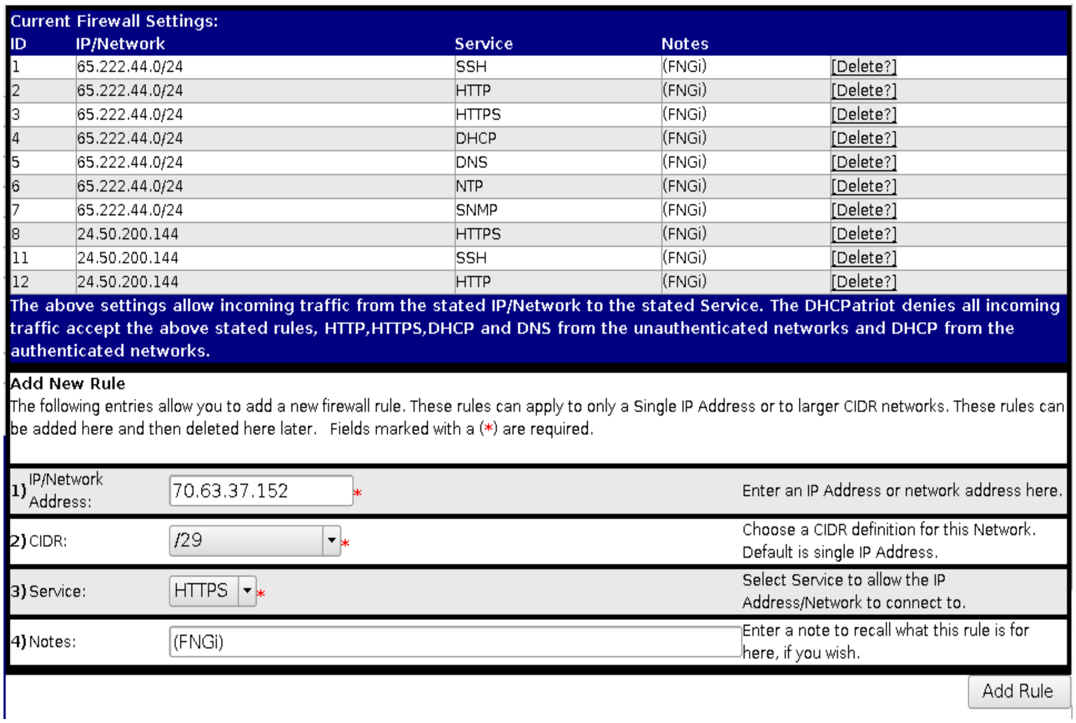
To edit an entry, click the edit link for the entry you wish to edit. Make your changes and click commit. To delete an entry, click its delete link.

Please note: Editing or deleting entries here does NOT affect the current state of customer configuration. Each customer will need to be edited that is affected by changes made here! Changes made here only affect what is available as Customer Service is adding or editing customers.

4.1.7 Configuring the Firewall

The DHCPatriot™ is protected by a white list style firewall. The DHCPatriot™ will only allow inbound connections from hosts it has been specifically told that it should allow. It is automatically told to allow appropriate connections from networks that are configured on it for DHCP. That behavior cannot be modified. The DHCPatriot™ may be told to allow other hosts in, as we saw in section 3.2.5. This section describes how to configure the firewall using the Web Administration Interface.

To administer the firewall, open the System Configuration menu and click on Firewall Setup. A screen similar to figure 4.7 will appear.



Current Firewall Settings:

ID	IP/Network	Service	Notes	
1	65.222.44.0/24	SSH	(FNGi)	[Delete?]
2	65.222.44.0/24	HTTP	(FNGi)	[Delete?]
3	65.222.44.0/24	HTTPS	(FNGi)	[Delete?]
4	65.222.44.0/24	DHCP	(FNGi)	[Delete?]
5	65.222.44.0/24	DNS	(FNGi)	[Delete?]
6	65.222.44.0/24	NTP	(FNGi)	[Delete?]
7	65.222.44.0/24	SNMP	(FNGi)	[Delete?]
8	24.50.200.144	HTTPS	(FNGi)	[Delete?]
11	24.50.200.144	SSH	(FNGi)	[Delete?]
12	24.50.200.144	HTTP	(FNGi)	[Delete?]

The above settings allow incoming traffic from the stated IP/Network to the stated Service. The DHCPatriot denies all incoming traffic accept the above stated rules, HTTP,HTTPS,DHCP and DNS from the unauthenticated networks and DHCP from the authenticated networks.

Add New Rule

The following entries allow you to add a new firewall rule. These rules can apply to only a Single IP Address or to larger CIDR networks. These rules can be added here and then deleted here later. Fields marked with a (*) are required.

1) IP/Network Address:	70.63.37.152 *	Enter an IP Address or network address here.
2) CIDR:	/29 *	Choose a CIDR definition for this Network. Default is single IP Address.
3) Service:	HTTPS *	Select Service to allow the IP Address/Network to connect to.
4) Notes:	(FNGi)	Enter a note to recall what this rule is for here, if you wish.

Figure 4.7 (Your screen appearance may differ slightly depending on the software used.)

You can add rules for single IP Addresses or subnets. Some definition of the services may be in order. SSH is the secure shell protocol that is used to administer the DHCPatriot™ via the menu configuration interface (see sections 3.1 and 3.2). HTTP and HTTPS are web server protocols and will be used for the Web Administration Interface. DHCP, DNS, NTP and SNMP will only be needed for remote health monitoring purposes. With your maintenance contract, First Network Group will monitor the health of the devices remotely using these protocols, as part of your maintenance contract.

Decide what rules need to be added and do so here. You can also delete rules by clicking on the delete link for the desired rule. These changes are applied immediately as rules are added or removed.

4.1.8 Adding/Editing Web Administration Interface Administrators

As discussed in section 3.2.7, it is best that each administrator have his own account. This section describes adding and administering these accounts. Accounts may be added, edited or deleted. To add an administrator, open the System Configuration menu and click on Add Administrator. Follow the on-screen instructions to complete this process. To edit an administrator, click on Edit Administrator. A list of currently configured administrators will appear. Click on the administrator that you wish to edit. A screen similar to the Add Administrator screen will appear. Follow the on-screen instructions to complete this process. To delete an administrator, click on edit administrator. Locate the administrator that you wish to delete in the resulting list. Click the delete link to remove the administrator.

There are some advanced features here that may require further explanation. These features are common to both the add and edit screens. The Encrypted Password feature is one of these. This feature allows an MD5 encrypted password to be pasted here.

MD5 is an encryption mechanism that is one of the most secure. Recent Unix style operating systems such as Linux® use this method to store a user's password. This encryption mechanism is one way and provides randomness by using a random salt. The DHCPatriot™ only supports MD5 encrypted passwords for administrators. You can tell if a password is encrypted using this method by identifying the salt at the beginning of the encrypted password. The password will have an appearance something like this: $1$1e1400b1$y8V/6MU4BCnPuXGwaL7q.0 The salt has been turned red for your convenience.

Passwords of this type may be pasted into the text field in field 4. You will not need to enter a password in field 3. This may be useful for adding existing administrators to the DHCPatriot™ and keeping the same password as is in use on other systems.

Another feature that requires further explanation is the admin level setting. This setting controls what options are available to an administrator at each admin level. In a future version, the admin level required to perform tasks will be configurable. For now, follow these general rules. Admin level 0 should be used for customer service. Admin level 1 should be used for technical support personnel. Admin level 5 should be used for supervisory personnel. Admin level 6 should be used for network administrators. Setting these admin levels for appropriate personnel should allow them to access the tasks necessary to complete their duties. If custom settings are required before the customization interface is available, please contact First Network Group for details.

The CLI user feature allows an administrator to be added that can access the remote CLI like interface API. Checking this box will cause the administrator to be locked out of the Web Administration Interface. Conversely, not having this box checked prevents access to the CLI interface. For details on the CLI interface API, see Appendix G.

Main DHCP Range restriction allows an administrator's interface to be 'cleaned up' so that only those networks that he is concerned with appear for him. This is not a security feature. An example of where this might be used would be in a situation where several ISPs form a consortium to share bandwidth and network infrastructure. A single DHCPatriot™ might be employed to service all customers, but customer service representatives from each ISP might only be concerned with their particular customers. This selection will allow their interface to only show their customers in most reports.

4.2 Daily Use

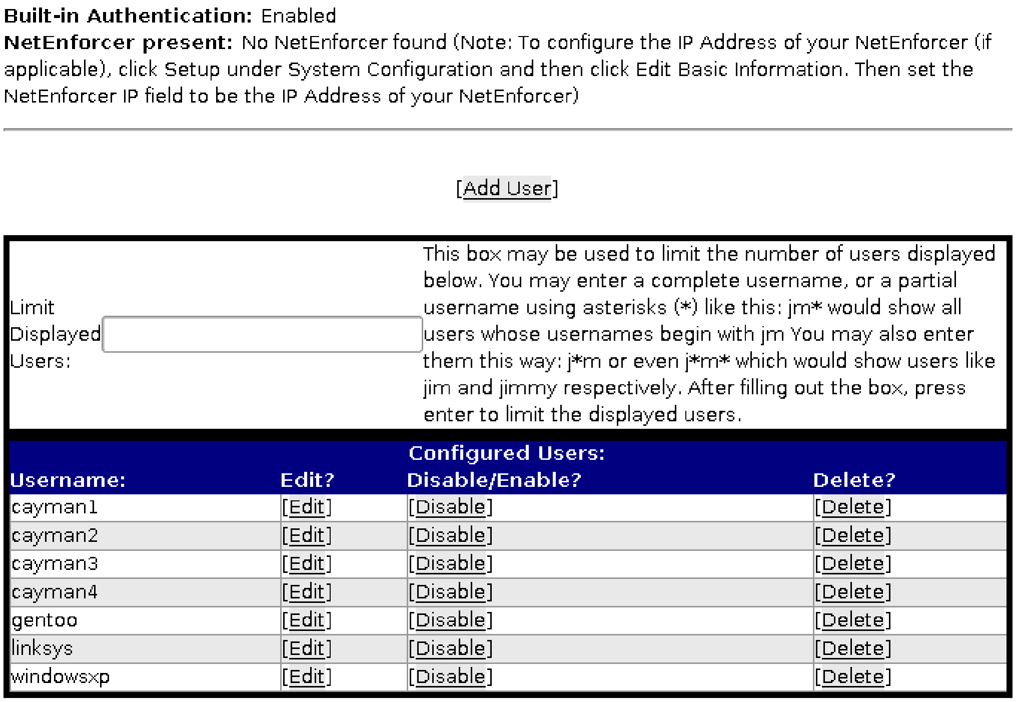
This section describes how to use the DHCPatriot™ for common tasks that may be encountered on a daily basis.

4.2.1 Changing your password

This section describes how an administrator may change his password. A good secure password should contain letters of varying case as well as numbers and even special characters. An example of a good password would be: u*4A#!43 A bad password example would be: *fluffy* The reason for this is that dictionary-based-cracking libraries, the most commonly used cracking algorithms, will contain the latter password, but not the former. To change your password, open the Main menu. Click on Change Your Password. Enter your current password. Then enter and then retype the desired password. Click the Change Password button to complete the process. A success message will appear.

4.2.2 Adding users to the optional Built-in Authentication

This section describes adding, editing, disabling and deleting users for the Built-in Authentication feature of the DHCPatriot™. If you are unsure if you are using this feature, please see your network administrator. Either this feature, or an external RADIUS server is required for the DHCPatriot™. To administer Built-in authentication users, open the User Management menu and click on Built-in Authentication: User Maintenance. A screen similar to figure 4.8 will appear.



Built-in Authentication: Enabled
NetEnforcer present: No NetEnforcer found (Note: To configure the IP Address of your NetEnforcer (if applicable), click Setup under System Configuration and then click Edit Basic Information. Then set the NetEnforcer IP field to be the IP Address of your NetEnforcer)

[Add User]

Limit Displayed Users:	This box may be used to limit the number of users displayed below. You may enter a complete username, or a partial username using asterisks (*) like this: jm* would show all users whose usernames begin with jm You may also enter them this way: j*m or even j*m* which would show users like jim and jimmy respectively. After filling out the box, press enter to limit the displayed users.

		Configured Users:	
Username:	**Edit?**	**Disable/Enable?**	**Delete?**
cayman1	[Edit]	[Disable]	[Delete]
cayman2	[Edit]	[Disable]	[Delete]
cayman3	[Edit]	[Disable]	[Delete]
cayman4	[Edit]	[Disable]	[Delete]
gentoo	[Edit]	[Disable]	[Delete]
linksys	[Edit]	[Disable]	[Delete]
windowsxp	[Edit]	[Disable]	[Delete]

Figure 4.8 (Your screen appearance may differ slightly depending on the software used.)

On this screen you may perform some functions without leaving the screen. The display of users may be limited by typing a partial or complete username into the Limit Displayed Users box. This makes it easier to find the user you need to edit, disable or delete. Once you have located the user to be maintained, you can disable (a temporary way of turning off the users access for reasons such as failure to pay for services). To disable a user click on the Disable link for the chosen user. If a user is leaving the service for good, click on Delete instead to completely remove the user. NOTE: Doing either of these things does not affect any current sessions for the user. To cause the user to be disconnected at the end of their current lease, see the instructions in section 4.2.6.

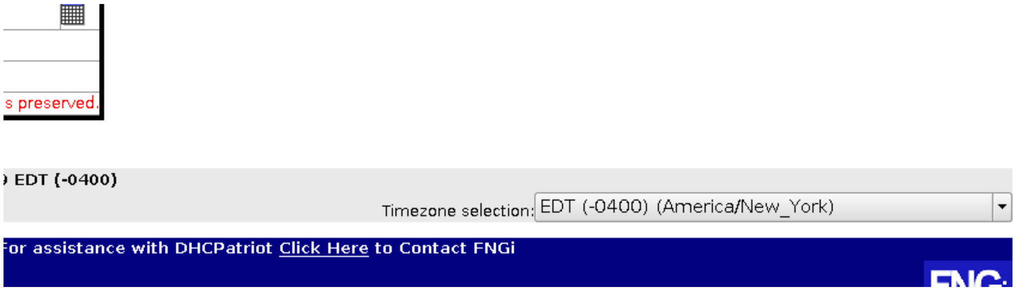
To add or edit an existing user, click the add link as shown in figure 4.8 or click the Edit link for that user. For the most part, the on-screen help should be sufficient to complete this process. If the network administrator has assigned a static IP Address, enter this IP Address into field number 3, Static IP Address. There may be nothing but the Commit button below Static IP Address, or there may be extra fields here. This depends on what was entered in the Built-in Authentication Options setup (see section 4.1.6). These options, if there, will allow bandwidth allocation for the customer as well as possible special rules. There should be a description of each, and the network administrator should have explained what to select for whom given specific parameters (such as selecting a specific bandwidth allocation for a specific price that the customer will be paying). Upon clicking commit, a summary screen showing the changes or additions will appear. Click the continue link to return to the screen shown in figure 4.8.

4.2.3 Manual Customer Authorization

This section describes the usage of the Authorize Customer feature. It may be necessary from time to time to manually authorize customer devices. Sometimes this is necessary because the device has no web browser (such as a PlayStation® 2 or Microsoft® XBox®), or because the device's web browser refuses to display the login screen. This feature may also be useful for preauthorizing customers before moving them to the DHCPatriot™ from some other IP Address allocation method. Required information for using this screen are the user's MAC Address or current unauthenticated IP Address, the user's username and the user's password. To authorize a customer, open the User Management menu and click Authorize Customer. Fill in the appropriate information and click Register User. A message confirming success or failure will appear. See appendix A for possible error messages and their resolution.

4.2.4 Timezone Selection

The DHCPatriot™ allows the timezone used to display results of reports to be changed on the fly. This section describes that procedure. Figure 4.9 shows the position and appearance of the timezone selection box.



s preserved.

EDT (-0400)

Timezone selection: EDT (-0400) (America/New_York)

or assistance with DHCPatriot Click Here to Contact FNGi

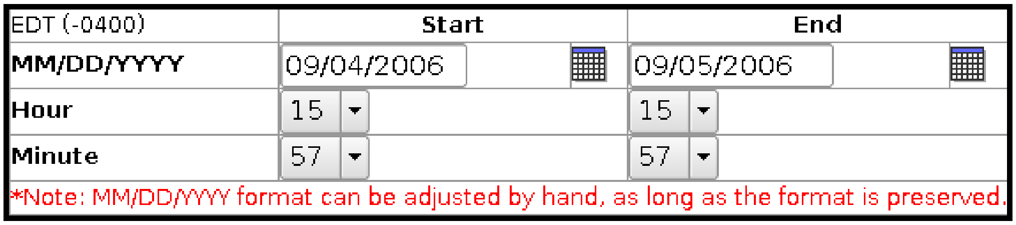
Figure 4.9 (Your screen appearance may differ slightly depending on the software used.)

The timezone selection box is located in the bottom right hand corner of the Web Administration Interface. The selections consist of 3 parts. The actual location based timezone, the offset (+/-) from universal time (GMT/UTC), and the abbreviated timezone. To set the timezone on your Web Administration Interface (note that this is a per user setting, and will not affect other administrator's Web Administration Interface settings), open the select box and locate the timezone you wish to select. You may do this as often as you like. The interface will hold your last selection. It does this via cookies, so if the cookie is not available, then the selection will need to be remade. Changing this selection while viewing a report will cause the report to be recalculated based on the new timezone selection. This can be very useful during abuse complaint resolution.

4.2.5 Report Limitation by Date

Many reports available on the DHCPatriot™ include the ability to change the date and time range of the results that are displayed. This section describes the use of this feature.

Each time that this feature is used, a screen similar to Figure 4.16a will appear.

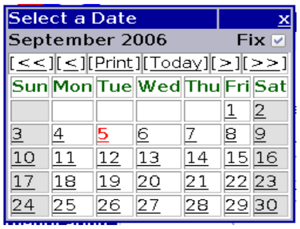


EDT (-0400)	Start	End
MM/DD/YYYY	09/04/2006	09/05/2006
Hour	15	15
Minute	57	57

*Note: MM/DD/YYYY format can be adjusted by hand, as long as the format is preserved.

Figure 4.16a (Your screen appearance may differ slightly depending on the software used.)

Here a start date and time and a stop date and time may be specified. Only records that start, stop, or span the specified time period will be shown. By default, the current day span is selected. To change, either hand edit the date, or click the calender icon next to it. A mini calender will appear allowing you to select the date that you would like. Figure 4.16b shows this mini calender.



Select a Date ×

September 2006 Fix ☑

[<<][<][Print][Today][>][>>]

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

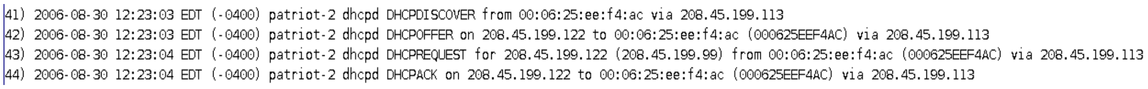
Figure 4.16b (Your screen appearance may differ slightly depending on the software used.)

The calender will appear with the current month shown and the current day red in color. the << and >> will navigate to previous years, or following years respectively. The < and > will navigate to the previous month and following month respectively. Clicking Today will return to the current month with the current day red in color. Clicking print will allow the calender to be printed. Unchecking Fix will allow the calender to be repositioned by dragging on the title bar. Find the date you wish to select and click on it. Click the x on the title bar to cancel. That will automatically fill out the date for you next to the calender icon that was clicked. To change the time, adjust the hour and minute as desired.

4.2.6 Understanding the DHCP logs

This section describes the DHCP logs. To view DHCP logs, open the User Management menu and click on Search DHCP Logs. You can limit the results of your search by MAC Address, IP Address and time period. Fill out the necessary search parameters and then click Search.

Figure 4.10 shows a typical DHCP conversation during IP Address discovery by a DHCP client.



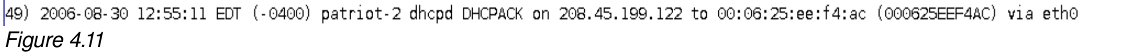
```
41) 2006-08-30 12:23:03 EDT (-0400) patriot-2 dhcpd DHCPDISCOVER from 00:06:25:ee:f4:ac via 208.45.199.113
42) 2006-08-30 12:23:03 EDT (-0400) patriot-2 dhcpd DHCPOFFER on 208.45.199.122 to 00:06:25:ee:f4:ac (000625EEF4AC) via 208.45.199.113
43) 2006-08-30 12:23:04 EDT (-0400) patriot-2 dhcpd DHCPREQUEST for 208.45.199.122 (208.45.199.99) from 00:06:25:ee:f4:ac (000625EEF4AC) via 208.45.199.113
44) 2006-08-30 12:23:04 EDT (-0400) patriot-2 dhcpd DHCPACK on 208.45.199.122 to 00:06:25:ee:f4:ac (000625EEF4AC) via 208.45.199.113
```

Figure 4.10

Each log message has similar components. At the far left is the number of the log message as generated in the search results. Moving to the right, the date and time are next which includes the timezone and offset from UTC that is currently selected via the timezone selection box (see section 4.2.4 for details). Next, the DHCPatriot™ device that generated the log message is displayed (patriot-1 or patriot-2 for primary and secondary respectively). The daemon that generated the message is displayed next (in this case it will always say dhcpd). Next is the actual message. These obviously vary quite a bit. For this discussion the four messages in figure 4.10 will be used.

Line 41 begins the conversation with a DHCPDISCOVER sent from the client machine. The MAC address is shown along with the IP Address of the DHCP relay agent. Line 42 shows the response in the form of a DHCPOFFER from the DHCPatriot™ of 208.45.199.122 to the client device. The Mac address and host name (in parentheses) of the device are shown along with the IP Address of the DHCP relay agent indicating that the DHCPatriot™ is responding via the relay agent. After the client receives the offer, he must place this IP Address on his interface and send another message. Line 43 shows this message, a DHCPREQUEST. This message shows the client officially requesting the offered IP Address via the DHCP relay agent. Line 44 shows the DHCPatriot™ response of DHCPACK indicating that the client is allowed to use that address for the length of the lease (in this case, one hour is configured on the DHCPatriot™ – see section 4.1.4 for information on changing the lease length). This message is sent via the DHCP relay agent to the client. At this point, the client will not converse with the DHCPatriot™ again until half the lease length has passed (in this case 30 minutes).

Figure 4.11 displays a renewal of lease conversation relative to the initial lease granting from figure 4.10.

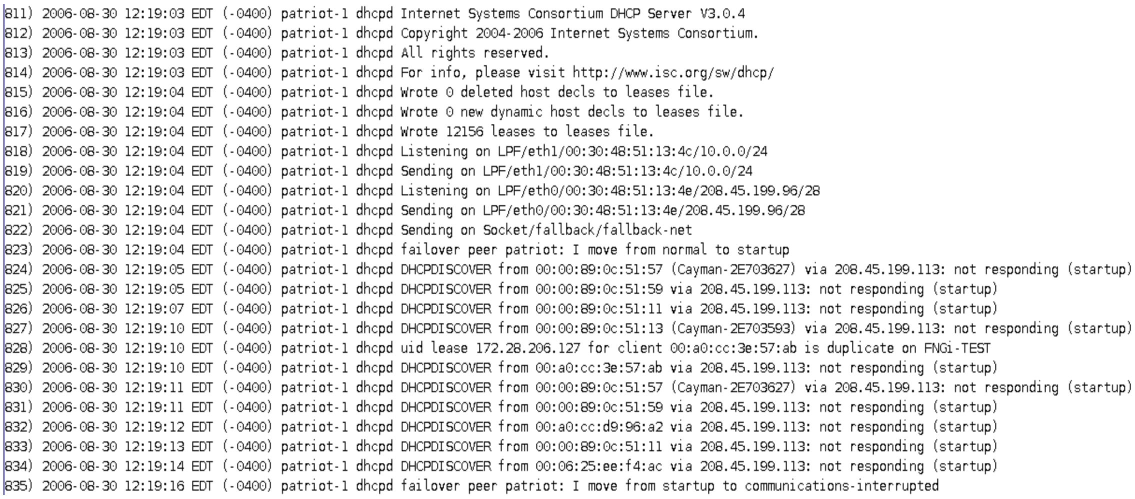


```
48) 2006-08-30 12:55:11 EDT (-0400) patriot-2 dhcpd DHCPREQUEST for 208.45.199.122 from 00:06:25:ee:f4:ac (000625EEF4AC) via eth0
49) 2006-08-30 12:55:11 EDT (-0400) patriot-2 dhcpd DHCPACK on 208.45.199.122 to 00:06:25:ee:f4:ac (000625EEF4AC) via eth0
```

Figure 4.11

Line 48 is generated when the client sends a DHCPREQUEST for the address that he was previously leased by the DHCPatriot™. This should occur at intervals equal to half the lease under normal circumstances. So, if there is a one hour lease initially granted, these renewals should occur every 30 minutes. Line 49 is generated when the DHCPatriot™ responds with DHCPACK meaning that the client can continue using the IP Address for another lease length period (in this case, one hour).

Figure 4.12 displays messages that might be seen when the DHCP server restarts, as is required under certain circumstances.

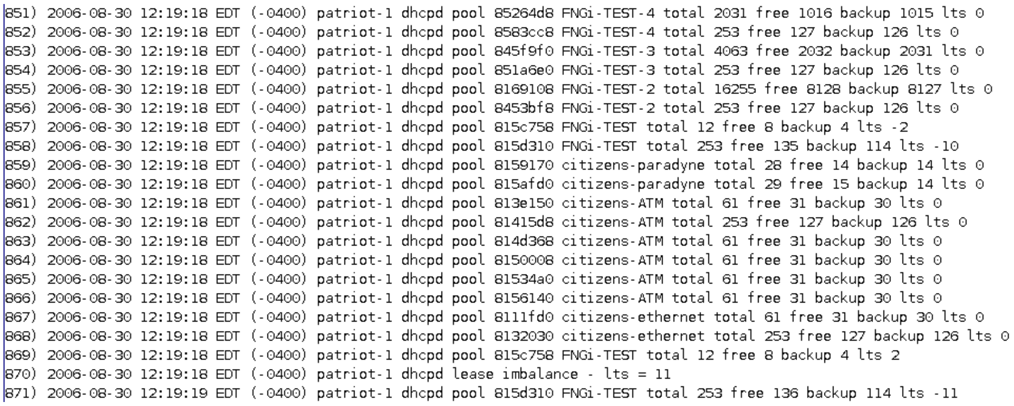


```
811) 2006-08-30 12:19:03 EDT (-0400) patriot-1 dhcpd Internet Systems Consortium DHCP Server V3.0.4
812) 2006-08-30 12:19:03 EDT (-0400) patriot-1 dhcpd Copyright 2004-2006 Internet Systems Consortium.
813) 2006-08-30 12:19:03 EDT (-0400) patriot-1 dhcpd All rights reserved.
814) 2006-08-30 12:19:03 EDT (-0400) patriot-1 dhcpd For info, please visit http://www.isc.org/sw/dhcp/
815) 2006-08-30 12:19:04 EDT (-0400) patriot-1 dhcpd Wrote 0 deleted host decls to leases file.
816) 2006-08-30 12:19:04 EDT (-0400) patriot-1 dhcpd Wrote 0 new dynamic host decls to leases file.
817) 2006-08-30 12:19:04 EDT (-0400) patriot-1 dhcpd Wrote 12156 leases to leases file.
818) 2006-08-30 12:19:04 EDT (-0400) patriot-1 dhcpd Listening on LPF/eth1/00:30:48:51:13:4c/10.0.0/24
819) 2006-08-30 12:19:04 EDT (-0400) patriot-1 dhcpd Sending on LPF/eth1/00:30:48:51:13:4c/10.0.0/24
820) 2006-08-30 12:19:04 EDT (-0400) patriot-1 dhcpd Listening on LPF/eth0/00:30:48:51:13:4e/208.45.199.96/28
821) 2006-08-30 12:19:04 EDT (-0400) patriot-1 dhcpd Sending on LPF/eth0/00:30:48:51:13:4e/208.45.199.96/28
822) 2006-08-30 12:19:04 EDT (-0400) patriot-1 dhcpd Sending on Socket/fallback/fallback-net
823) 2006-08-30 12:19:04 EDT (-0400) patriot-1 dhcpd failover peer patriot: I move from normal to startup
824) 2006-08-30 12:19:05 EDT (-0400) patriot-1 dhcpd DHCPDISCOVER from 00:00:89:0c:51:57 (Cayman-2E703627) via 208.45.199.113: not responding (startup)
825) 2006-08-30 12:19:05 EDT (-0400) patriot-1 dhcpd DHCPDISCOVER from 00:00:89:0c:51:59 via 208.45.199.113: not responding (startup)
826) 2006-08-30 12:19:07 EDT (-0400) patriot-1 dhcpd DHCPDISCOVER from 00:00:89:0c:51:11 via 208.45.199.113: not responding (startup)
827) 2006-08-30 12:19:10 EDT (-0400) patriot-1 dhcpd DHCPDISCOVER from 00:00:89:0c:51:13 (Cayman-2E703593) via 208.45.199.113: not responding (startup)
828) 2006-08-30 12:19:10 EDT (-0400) patriot-1 dhcpd uid lease 172.28.206.127 for client 00:a0:cc:3e:57:ab is duplicate on FNGi-TEST
829) 2006-08-30 12:19:10 EDT (-0400) patriot-1 dhcpd DHCPDISCOVER from 00:a0:cc:3e:57:ab via 208.45.199.113: not responding (startup)
830) 2006-08-30 12:19:11 EDT (-0400) patriot-1 dhcpd DHCPDISCOVER from 00:00:89:0c:51:57 (Cayman-2E703627) via 208.45.199.113: not responding (startup)
831) 2006-08-30 12:19:11 EDT (-0400) patriot-1 dhcpd DHCPDISCOVER from 00:00:89:0c:51:59 via 208.45.199.113: not responding (startup)
832) 2006-08-30 12:19:12 EDT (-0400) patriot-1 dhcpd DHCPDISCOVER from 00:a0:cc:d9:96:a2 via 208.45.199.113: not responding (startup)
833) 2006-08-30 12:19:13 EDT (-0400) patriot-1 dhcpd DHCPDISCOVER from 00:00:89:0c:51:11 via 208.45.199.113: not responding (startup)
834) 2006-08-30 12:19:14 EDT (-0400) patriot-1 dhcpd DHCPDISCOVER from 00:06:25:ee:f4:ac via 208.45.199.113: not responding (startup)
835) 2006-08-30 12:19:16 EDT (-0400) patriot-1 dhcpd failover peer patriot: I move from startup to communications-interrupted
```

Figure 4.12

These messages are normal and can be safely ignored.

Figure 4.13 displays messages that might be seen as the two DHCPatriot™ devices balance their pools.

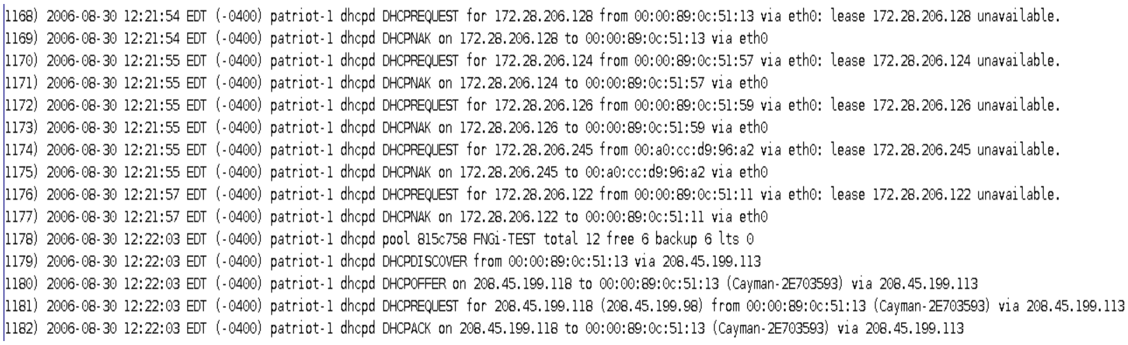


```
851) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 85264d8 FNGi-TEST-4 total 2031 free 1016 backup 1015 lts 0
852) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 8583cc8 FNGi-TEST-4 total 253 free 127 backup 126 lts 0
853) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 845f9f0 FNGi-TEST-3 total 4063 free 2032 backup 2031 lts 0
854) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 851a6e0 FNGi-TEST-3 total 253 free 127 backup 126 lts 0
855) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 8169108 FNGi-TEST-2 total 16255 free 8128 backup 8127 lts 0
856) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 8453bf8 FNGi-TEST-2 total 253 free 127 backup 126 lts 0
857) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 815c758 FNGi-TEST total 12 free 8 backup 4 lts -2
858) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 815d310 FNGi-TEST total 253 free 135 backup 114 lts -10
859) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 8159170 citizens-paradyne total 28 free 14 backup 14 lts 0
860) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 815afd0 citizens-paradyne total 29 free 15 backup 14 lts 0
861) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 813e150 citizens-ATM total 61 free 31 backup 30 lts 0
862) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 81415d8 citizens-ATM total 253 free 127 backup 126 lts 0
863) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 814d368 citizens-ATM total 61 free 31 backup 30 lts 0
864) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 8150008 citizens-ATM total 61 free 31 backup 30 lts 0
865) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 81534a0 citizens-ATM total 61 free 31 backup 30 lts 0
866) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 8156140 citizens-ATM total 61 free 31 backup 30 lts 0
867) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 8111fd0 citizens-ethernet total 61 free 31 backup 30 lts 0
868) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 8132030 citizens-ethernet total 253 free 127 backup 126 lts 0
869) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd pool 815c758 FNGi-TEST total 12 free 8 backup 4 lts 2
870) 2006-08-30 12:19:18 EDT (-0400) patriot-1 dhcpd lease imbalance - lts = 11
871) 2006-08-30 12:19:19 EDT (-0400) patriot-1 dhcpd pool 815d310 FNGi-TEST total 253 free 136 backup 114 lts -11
```

Figure 4.13

These messages are also normal and may be safely ignored.

When a user authenticates you may see messages similar to those shown in figure 4.14.



```
1168) 2006-08-30 12:21:54 EDT (-0400) patriot-1 dhcpd DHCPREQUEST for 172.28.206.128 from 00:00:89:0c:51:13 via eth0: lease 172.28.206.128 unavailable.
1169) 2006-08-30 12:21:54 EDT (-0400) patriot-1 dhcpd DHCPNAK on 172.28.206.128 to 00:00:89:0c:51:13 via eth0
1170) 2006-08-30 12:21:55 EDT (-0400) patriot-1 dhcpd DHCPREQUEST for 172.28.206.124 from 00:00:89:0c:51:57 via eth0: lease 172.28.206.124 unavailable.
1171) 2006-08-30 12:21:55 EDT (-0400) patriot-1 dhcpd DHCPNAK on 172.28.206.124 to 00:00:89:0c:51:57 via eth0
1172) 2006-08-30 12:21:55 EDT (-0400) patriot-1 dhcpd DHCPREQUEST for 172.28.206.126 from 00:00:89:0c:51:59 via eth0: lease 172.28.206.126 unavailable.
1173) 2006-08-30 12:21:55 EDT (-0400) patriot-1 dhcpd DHCPNAK on 172.28.206.126 to 00:00:89:0c:51:59 via eth0
1174) 2006-08-30 12:21:55 EDT (-0400) patriot-1 dhcpd DHCPREQUEST for 172.28.206.245 from 00:a0:cc:d9:96:a2 via eth0: lease 172.28.206.245 unavailable.
1175) 2006-08-30 12:21:55 EDT (-0400) patriot-1 dhcpd DHCPNAK on 172.28.206.245 to 00:a0:cc:d9:96:a2 via eth0
1176) 2006-08-30 12:21:57 EDT (-0400) patriot-1 dhcpd DHCPREQUEST for 172.28.206.122 from 00:00:89:0c:51:11 via eth0: lease 172.28.206.122 unavailable.
1177) 2006-08-30 12:21:57 EDT (-0400) patriot-1 dhcpd DHCPNAK on 172.28.206.122 to 00:00:89:0c:51:11 via eth0
1178) 2006-08-30 12:22:03 EDT (-0400) patriot-1 dhcpd pool 815c758 FNGi-TEST total 12 free 6 backup 6 lts 0
1179) 2006-08-30 12:22:03 EDT (-0400) patriot-1 dhcpd DHCPDISCOVER from 00:00:89:0c:51:13 via 208.45.199.113
1180) 2006-08-30 12:22:03 EDT (-0400) patriot-1 dhcpd DHCPOFFER on 208.45.199.118 to 00:00:89:0c:51:13 (Cayman-2E703593) via 208.45.199.113
1181) 2006-08-30 12:22:03 EDT (-0400) patriot-1 dhcpd DHCPREQUEST for 208.45.199.118 (208.45.199.98) from 00:00:89:0c:51:13 (Cayman-2E703593) via 208.45.199.113
1182) 2006-08-30 12:22:03 EDT (-0400) patriot-1 dhcpd DHCPACK on 208.45.199.118 to 00:00:89:0c:51:13 (Cayman-2E703593) via 208.45.199.113
```

Figure 4.14

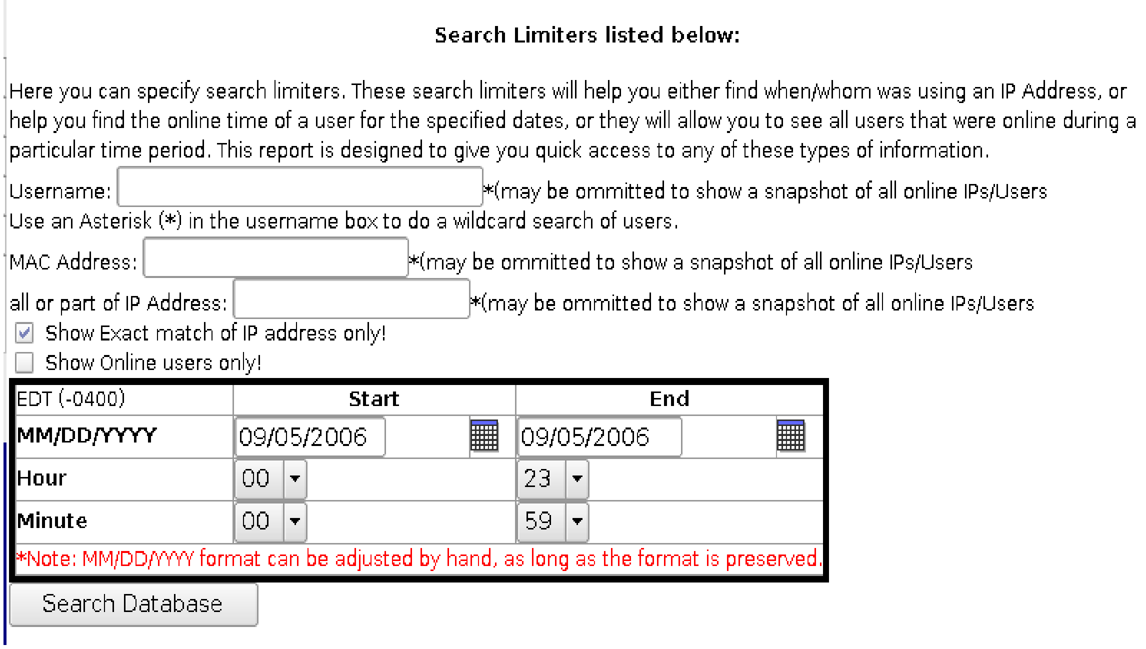
These messages merely mean that the client is being denied renewing his unauthenticated address via DHCPNAK messages until the lease expires. At that point, the client does a DHCPDISCOVER looking for a new IP Address and gets an authenticated address.

Occasionally, you may see other messages not mentioned here. Refer to Appendix A, Appendix E, or contact First Network Group if need be for further information.

4.2.7 Finding a user

The primary purpose of the DHCPatriot™ is to allow administrators to locate information regarding the use of IP Addresses by specific users at specific points in time. This easily accessible information allows administrators to respond to abuse complaints, network problems caused by abusive customers or subpoena requests in a timely fashion. This helps the ISP comply with local laws, such as CALEA (http://www.askcalea.net/), and provides a smoother running network. This section describes the method used for accessing this information.

The primary method of accessing this information is to use the Search Database function. To access this function, open the User Management menu and click on Search Database. A screen similar to figure 4.15 will appear.



Search Limiters listed below:

Here you can specify search limiters. These search limiters will help you either find when/whom was using an IP Address, or help you find the online time of a user for the specified dates, or they will allow you to see all users that were online during a particular time period. This report is designed to give you quick access to any of these types of information.

Username: ____ *(may be ommitted to show a snapshot of all online IPs/Users
Use an Asterisk (*) in the username box to do a wildcard search of users.

MAC Address: ____ *(may be ommitted to show a snapshot of all online IPs/Users

all or part of IP Address: ____ *(may be ommitted to show a snapshot of all online IPs/Users

☑ Show Exact match of IP address only!
☐ Show Online users only!

EDT (-0400)	Start	End
MM/DD/YYYY	09/05/2006	09/05/2006
Hour	00	23
Minute	00	59

*Note: MM/DD/YYYY format can be adjusted by hand, as long as the format is preserved.

Figure 4.15 (Your screen appearance may differ slightly depending on the software used.)

As shown in figure 4.15, there are several limiters that may be used in your search. You may use any combination of these limiters (with the exception of date/time – that limiter cannot be removed). The function of each of the limiters will be described, combinations of limiters are left to your imagination.

The first limiter, Username, will limit results to a specific username. Asterisks (*) may also be used as a wild card character. If a username is typed like this: *jim* Then only sessions with the username of *jim* will be shown. However, if the username is typed like this: *jim** then *jim* and also *jimbo* will be matched. Further, you can use multiple asterisks like so: *j*m** which will match *jim*, *jym*, *jimbo* and *jymbo*.

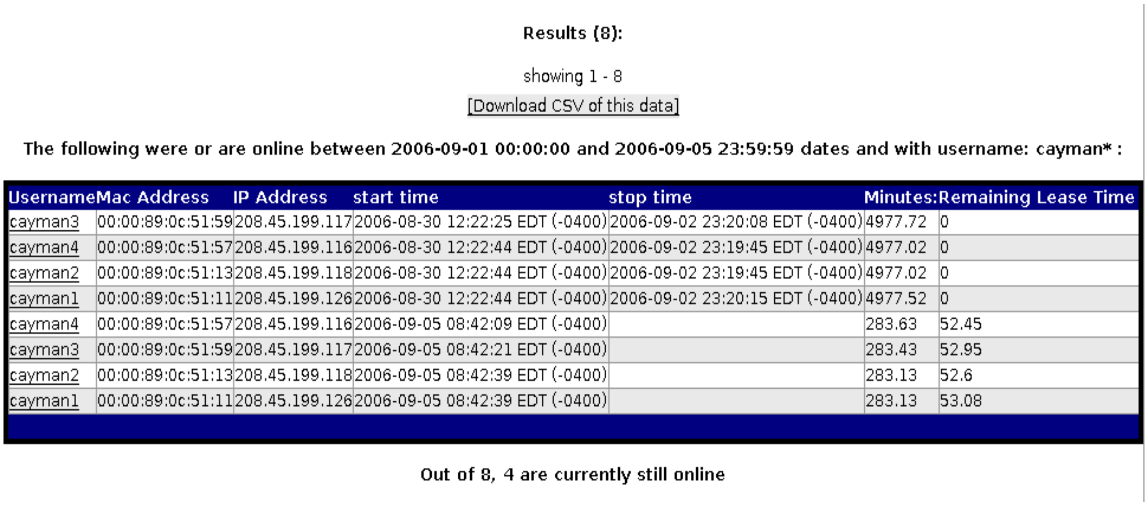
The second limiter is Media Access Control (MAC) Address (http://en.wikipedia.org/wiki/MAC_address). A devices MAC Address may be used here to limit the search results. The MAC Address consists of 12 hexadecimal notation (0-9 a-f) characters in the format xx:xx:xx:xx:xx:xx For example: 00:0e:e9:cf:d8:2a Case is important here, make sure you type the MAC Address in lowercase.

The next limiter is IP Address. All or part of an IP Address may be used. Uncheck Show exact match of IP Address only! to search for a partial IP Address. For instance, 208.45.199.116 will match 208.45.199.116 while 208.45.199.11, coupled with unchecking the aforementioned box, will match 208.45.199.11* where * is any number 0-9.

If you only wish to see currently open sessions returned, place a check in Show online users only! and only sessions that are currently open will be returned.

The final limiter is the date and time limiter. See section 4.2.5 for information regarding the date limiter.

Using these limiters allows quick access to only the needed data when searching for activity for any purpose. Set the limiters as needed, and click Search Database. A screen similar to figure 4.16 will appear.



Results (8):

showing 1 - 8

[Download CSV of this data]

The following were or are online between 2006-09-01 00:00:00 and 2006-09-05 23:59:59 dates and with username: cayman* :

Username	Mac Address	IP Address	start time	stop time	Minutes:	Remaining Lease Time
cayman3	00:00:89:0c:51:59	208.45.199.117	2006-08-30 12:22:25 EDT (-0400)	2006-09-02 23:20:08 EDT (-0400)	4977.72	0
cayman4	00:00:89:0c:51:57	208.45.199.116	2006-08-30 12:22:44 EDT (-0400)	2006-09-02 23:19:45 EDT (-0400)	4977.02	0
cayman2	00:00:89:0c:51:13	208.45.199.118	2006-08-30 12:22:44 EDT (-0400)	2006-09-02 23:19:45 EDT (-0400)	4977.02	0
cayman1	00:00:89:0c:51:11	208.45.199.126	2006-08-30 12:22:44 EDT (-0400)	2006-09-02 23:20:15 EDT (-0400)	4977.52	0
cayman4	00:00:89:0c:51:57	208.45.199.116	2006-09-05 08:42:09 EDT (-0400)		283.63	52.45
cayman3	00:00:89:0c:51:59	208.45.199.117	2006-09-05 08:42:21 EDT (-0400)		283.43	52.95
cayman2	00:00:89:0c:51:13	208.45.199.118	2006-09-05 08:42:39 EDT (-0400)		283.13	52.6
cayman1	00:00:89:0c:51:11	208.45.199.126	2006-09-05 08:42:39 EDT (-0400)		283.13	53.08

Out of 8, 4 are currently still online

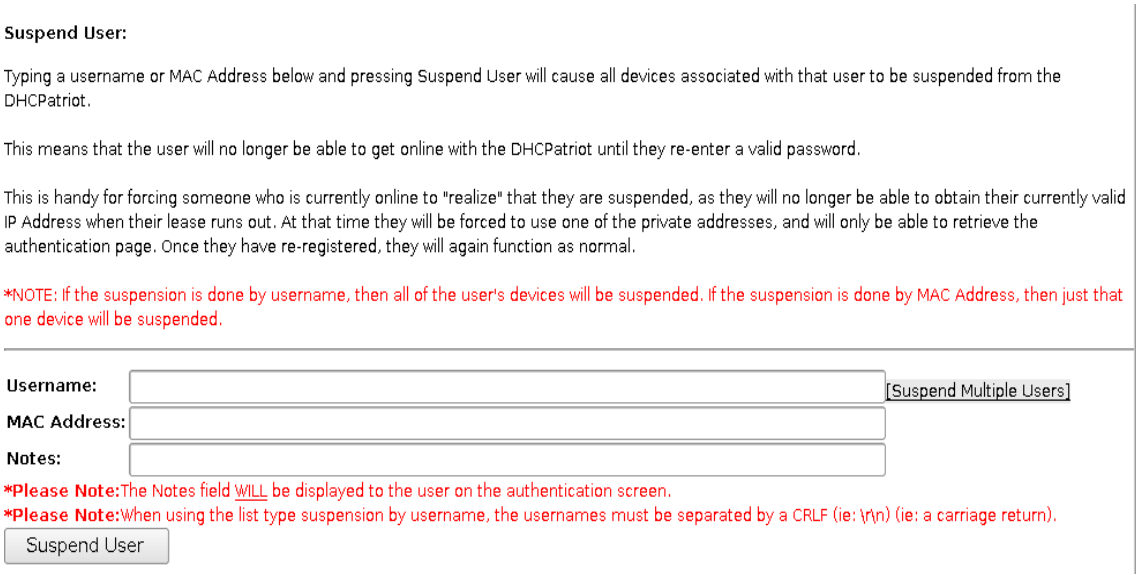
Figure 4.16 (Your screen appearance may differ slightly depending on the software used.)

The fields displayed should be self explanatory. Next and Back links will appear for moving forward and backward through pages if more than 50 results are returned. Clicking download CSV of this data will output a comma separated value (CSV) file of the returned data (all data, not just the current page, if more than 50 results are returned) that may be opened with popular spreadsheet programs such as *Microsoft® Excel®* and *OpenOffice.org Calc*.

4.2.8 Suspending a user

A user may be suspended by MAC Address to suspend only one of his devices, or by username to suspend all his devices. One user may be suspended at a time, or multiple users may be suspended at once. A note may be left for the user, or no note may be specified. Depending on whether the user is also suspended on the Built-in Authentication or external RADIUS server or not the user may receive a temporary suspension or a permanent suspension. This section describes this functionality.

To begin the user suspension process, first the type of suspension must be decided upon. If this user is to be permanently suspended so that he cannot get back online without intervention from customer service, first suspend his account in the RADIUS server or click the disable link in the Built-in Authentication (see section 4.2.2). If this is to be a temporary suspension, you may proceed directly to the Suspend User function. To access this function, open the User Management menu and click on Suspend User. A screen similar to figure 4.17 will appear.



Suspend User:

Typing a username or MAC Address below and pressing Suspend User will cause all devices associated with that user to be suspended from the DHCPatriot.

This means that the user will no longer be able to get online with the DHCPatriot until they re-enter a valid password.

This is handy for forcing someone who is currently online to "realize" that they are suspended, as they will no longer be able to obtain their currently valid IP Address when their lease runs out. At that time they will be forced to use one of the private addresses, and will only be able to retrieve the authentication page. Once they have re-registered, they will again function as normal.

*NOTE: If the suspension is done by username, then all of the user's devices will be suspended. If the suspension is done by MAC Address, then just that one device will be suspended.

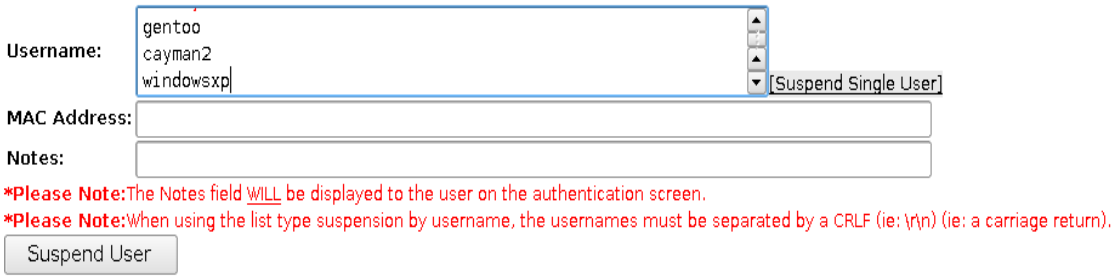
Username: [Suspend Multiple Users]
MAC Address:
Notes:

***Please Note:**The Notes field WILL be displayed to the user on the authentication screen.
***Please Note:**When using the list type suspension by username, the usernames must be separated by a CRLF (ie: \r\n) (ie: a carriage return).

Figure 4.17 (Your screen appearance may differ slightly depending on the software used.)

To suspend a single user or MAC Address type that username or MAC Address (one or the other, not both, please) into the appropriate box. You may optionally add a note. It is important that you remember that what is typed in the notes box will appear on the customer's authentication screen!

To suspend multiple users, click the Suspend Multiple Users button at the end of the Username box. Type the multiple users separated by a carriage return as shown in figure 4.18.



Username: gentoo
cayman2
windowsxp [Suspend Single User]

MAC Address:

Notes:

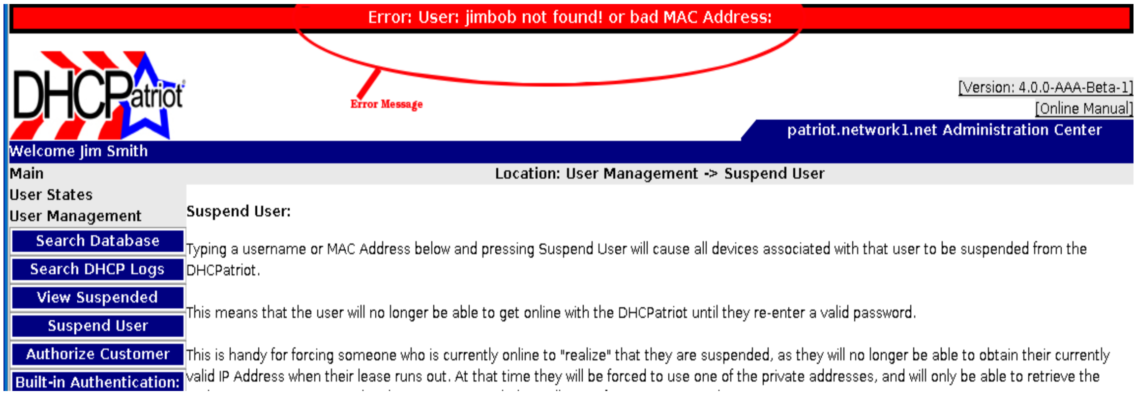
*Please Note:The Notes field WILL be displayed to the user on the authentication screen.

*Please Note:When using the list type suspension by username, the usernames must be separated by a CRLF (ie: \r\n) (ie: a carriage return).

Figure 4.18 (Your screen appearance may differ slightly depending on the software used.)

You may still add a note when suspending multiple users, and the note will be added to each user's device. To exit suspend multiple user mode, click Suspend Single User at the end of the Username box.

Once the desired user(s) or MAC Address has been typed, and the note, if desired, has been entered, click on Suspend User. If a username or MAC Address is encountered which cannot be found on the system an error message will appear and the suspend user screen will return as shown in figure 4.19.



Error: User: jimbob not found! or bad MAC Address:

Location: User Management -> Suspend User

Suspend User:

Typing a username or MAC Address below and pressing Suspend User will cause all devices associated with that user to be suspended from the DHCPatriot.

This means that the user will no longer be able to get online with the DHCPatriot until they re-enter a valid password.

This is handy for forcing someone who is currently online to "realize" that they are suspended, as they will no longer be able to obtain their currently valid IP Address when their lease runs out. At that time they will be forced to use one of the private addresses, and will only be able to retrieve the

Figure 4.19 (Your screen appearance may differ slightly depending on the software used.)

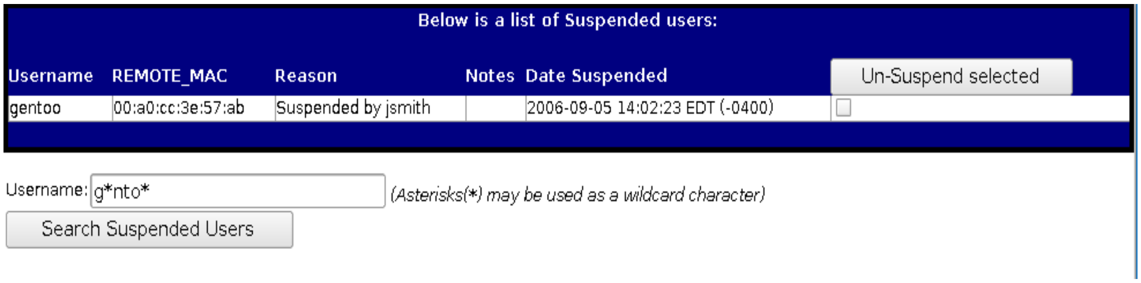
If everything is fine, the View Suspended screen will be returned (see section 4.2.8).

Please note that nothing will happen for the user until the current lease runs out (if they are currently using a lease on some device), they perform a release, or reboot any connected devices. You can find out if they are currently using a lease, and how much time is left in the lease by searching for the username or MAC Address (see section 4.2.6).

4.2.9 Viewing and Unsuspending users

Finding out if a user's device is suspended can greatly help in the troubleshooting process. Also, being able to unsuspend a device once found may make the whole process more seamless for both the customer and technical support or customer service. This section describes the viewing and unsuspending of users.

To access the View Suspended function, open the User Management menu and click on View Suspended. You may type a username to limit your results. You may use Asterisks (*) as a wild card. For instance, typing jim will only match jim. However, if you type j*m then jim and jym will be matched. Click on Search Suspended Users. A screen will be returned similar to figure 4.20.



Below is a list of Suspended users:

Username	REMOTE_MAC	Reason	Notes	Date Suspended	Un-Suspend selected
gentoo	00:a0:cc:3e:57:ab	Suspended by jsmith		2006-09-05 14:02:23 EDT (-0400)	□

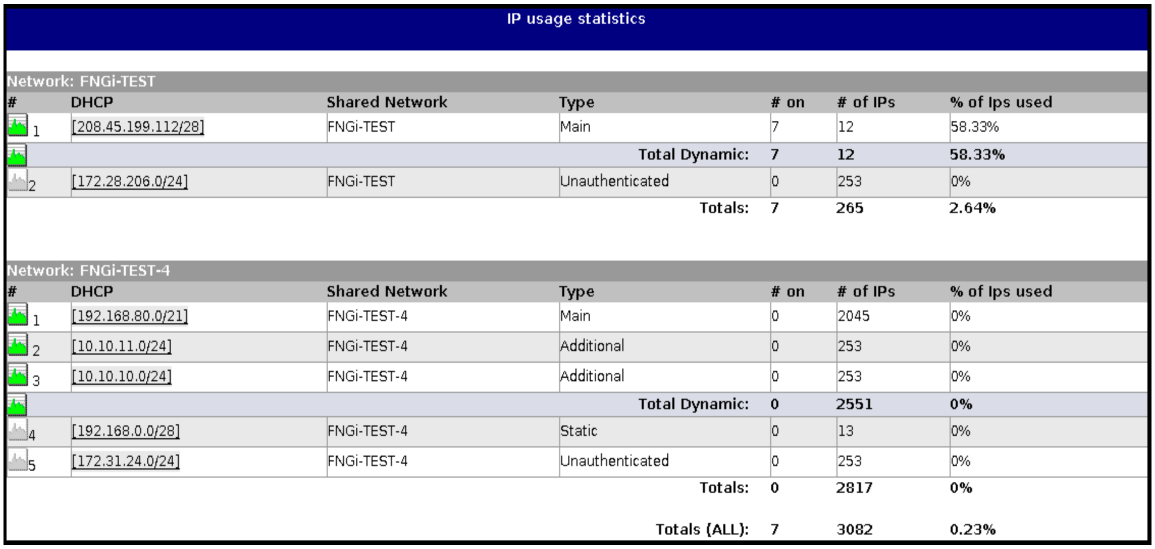
Username: g*nto* *(Asterisks(*) may be used as a wildcard character)*

Figure 4.20 (Your screen appearance may differ slightly depending on the software used.)

To unsuspend a specific device(s), place a check mark in the last column in the row(s) for the device(s) that you wish to unsuspend. Once all devices have been selected that you wish to unsuspend, click the Un-Suspend selected button at the top of that column. There may be a wait of several seconds, then the View Suspended screen will return. If the user is still suspended in the Built-in Authentication (see section 4.2.2), or external RADIUS server, then unsuspending them here will not do any good. Their device will end up back in this list when they attempt to use their connection.

4.2.10 Understanding IP Address usage statistics

The second most important purpose of the DHCPatriot™ is to provide administrators with a good idea as to their IP Address usage on their networks. The primary report used in this capacity is IP Address Usage. To access this report, open the IP Management menu and click on IP Address Usage. A screen similar to figure 4.21 will appear.



IP usage statistics

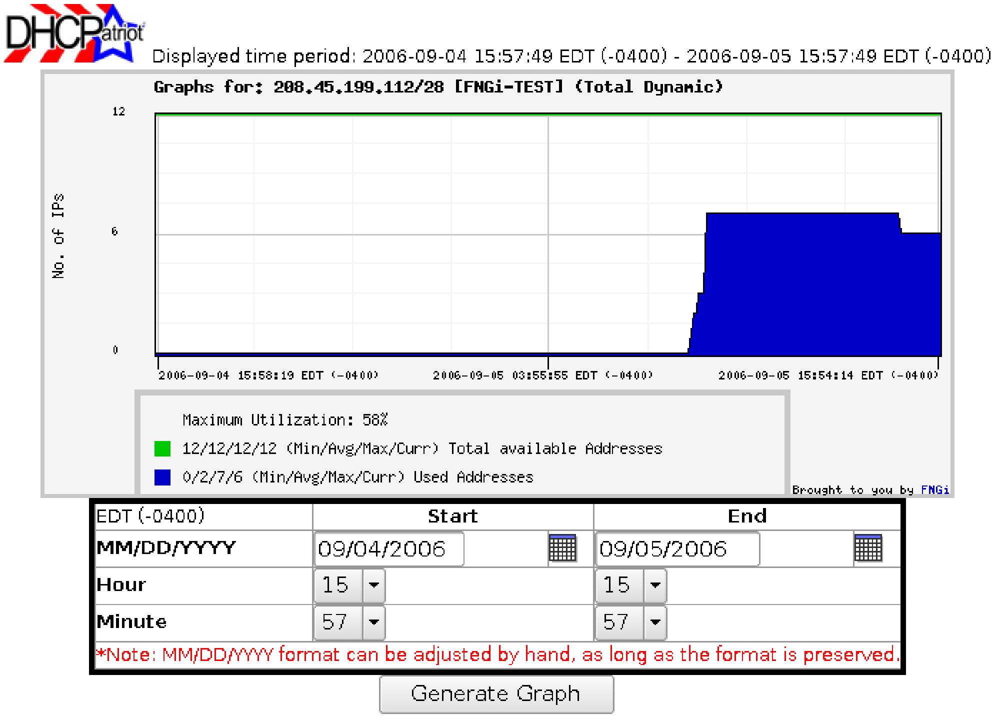
#	DHCP	Shared Network	Type	# on	# of IPs	% of Ips used
Network: FNGi-TEST						
📈 1	[208.45.199.112/28]	FNGi-TEST	Main	7	12	58.33%
📈			Total Dynamic:	7	12	58.33%
📈 2	[172.28.206.0/24]	FNGi-TEST	Unauthenticated	0	253	0%
			Totals:	7	265	2.64%
Network: FNGi-TEST-4						
📈 1	[192.168.80.0/21]	FNGi-TEST-4	Main	0	2045	0%
📈 2	[10.10.11.0/24]	FNGi-TEST-4	Additional	0	253	0%
📈 3	[10.10.10.0/24]	FNGi-TEST-4	Additional	0	253	0%
📈			Total Dynamic:	0	2551	0%
📈 4	[192.168.0.0/28]	FNGi-TEST-4	Static	0	13	0%
📈 5	[172.31.24.0/24]	FNGi-TEST-4	Unauthenticated	0	253	0%
			Totals:	0	2817	0%
			Totals (ALL):	7	3082	0.23%

Figure 4.21 (Your screen appearance may differ slightly depending on the software used.)

Each main DHCP range that is configured on the DHCPatriot™ (see section 4.1.1) will have a separate section on this screen labeled Network: <the name of the shared-network>. The dynamic ranges of types Main and Additional are displayed separately from the static and unauthenticated ranges. The total dynamic line lets you decide when a new range needs to be added.

To see a list of users currently connected on a specific network, click the CIDR block shown in the DHCP column. A screen will appear giving you known information, such as IP Address, MAC Address, and username (if known), about the users connected to that network. A CSV download option is provided here for your convenience.

This report shows a snapshot of current usage only. To view usage trends, graphs are provided. Each dynamic range has a graph icon, as well as the total dynamic. Click on a graph icon at the left side of the screen next to the desired network. A screen similar to figure 4.22 will appear.



Displayed time period: 2006-09-04 15:57:49 EDT (-0400) - 2006-09-05 15:57:49 EDT (-0400)

Graphs for: 208.45.199.112/28 [FNGi-TEST] (Total Dynamic)

No. of IPs
12
6
0
2006-09-04 15:58:19 EDT (-0400)
2006-09-05 03:55:55 EDT (-0400)
2006-09-05 15:54:14 EDT (-0400)
Brought to you by FNGi

Maximum Utilization: 58%

🟩 12/12/12/12 (Min/Avg/Max/Curr) Total available Addresses

🟦 0/2/7/6 (Min/Avg/Max/Curr) Used Addresses

EDT (-0400)	Start	End
MM/DD/YYYY	09/04/2006	09/05/2006
Hour	15	15
Minute	57	57

*Note: MM/DD/YYYY format can be adjusted by hand, as long as the format is preserved.

Figure 4.22 (Your screen appearance may differ slightly depending on the software used.)

By default, the past 24 hours of usage are displayed. It is possible to adjust the time period displayed here using the provided time limiter function. See section 4.2.5 for further details. Once the desired time period is chosen, click Generate Graph to show the results.

NOT FOR END USER DISTRIBUTION

This guide is to serve as an overview on issues that may be encountered by End Users (EU) who connect via the DHCPatriot™ and to assist support personnel in troubleshooting these issues.

We hope this guide serves as a launching point for assisting EU's, however if you need further information, you can always contact First Network Group Inc. or if you are one of our Technical Support Customer's our Technical Support Center will be happy to help your EU's with whatever they need.

A-1 Setup Overview:

The EU's computer should be setup to dynamically pull an IP address and DNS. All computers with a network card are setup like this out-of-the-box. Existing users being converted over to the DHCPatriot™ may need to have their settings adjusted to this mode from what they were using before.

The EU's computer will also need a functioning web browser to establish authentication with the DHCPatriot™. EU's that do not have a functioning web browser or have a system, such as an Online Gaming Console (OGM) (ex: Microsoft® Xbox®) that does not include a web browser, can be provisioned at the office via the DHCPatriot™'s interface.

The EU can also use a router to connect multiple computers to their connection as before, as long as the router is setup to dynamically pull an IP address (default out-of-the-box configuration).

A-2 Web Browser Requirements:

The only requirement is that the EU's web browser supports form submissions as specified by the W3C (www.w3c.org). All current web browsers are known to support these standards.

There are no known issues with any specific Web Browser that would not allow a user to connect via the DHCPatriot™.

A-3 EU Information Requirements:

The only information the EU will be required to know is their account's valid username and password.

A-4 Supported Operating Systems:

There are no known issues with any specific Operating Systems that would not allow a user to connect via the DHCPatriot™.

A-5 Firewalls:

If the user is running a firewall program, it may be setup to block certain types of DHCP traffic which will not allow the machine to function correctly with the DHCPatriot™. If you believe the firewall is causing these issues, please disable the firewall and try again. If the firewall is blocking DHCP traffic, it will need to be reconfigured as per its documentation.

All firewall setups (hardware and software) must be setup to allow ICMP traffic for proper functioning as ARPA is updated on Internet routers via ICMP.

A-6 Known Issues:

The issues presented here are coupled with possible resolutions that may be employed by Technical Support in assisting customers with the usage of the DHCPatriot™.

NOT FOR END USER DISTRIBUTION

Issue 1:

User receives message "Username or Password is incorrect …" after attempting to login to the DHCPatriot™ Login Page.

Cause:

The user has received this message because their account is either disabled or they have entered incorrect information for the username or password.

Resolution:

Please double-check information entered and retype or copy and paste the information.

If this does not correct the issue, please verify that the account is enabled and you have the correct information.

Issue 2:

User receives message "You must supply a Username and Password …" after attempting to login to the DHCPatriot™ Login Page.

Cause:

The user has not entered a username and/or password into the appropriate fields on the Login Page.

Resolution:

Please have the user revisit the Login Page and enter in the valid username and password for the account.

Issue 3:

User makes a successful login, but is constantly presented with the login page when attempting to go to another website(s).

However the user is able to send and receive e-mail and the machine is reporting a valid public IP address given from the DHCPatriot™.

Cause:

This happens because the web browser is not refreshing the page from its source, but displaying it from the cache on the computer.

Resolution:

Please clear the browser's cache, and then close and re-open the web browser.

If problem still persists, please reboot the computer.

If the problem persists after a reboot, please adjust your browser's cache settings to allow for web page content to be checked for a newer version "every time a page is visited".

Issue 4:

User makes a successful login, but is constantly presented with the login page when attempting to go to another website.

The user is also unable to receive e-mail and is not receiving a valid public IP address given from the DHCPatriot™. The IP shown on the user's computer is still a private address given from the DHCPatriot™.

Cause:

This is due to the Operating system settings being set to static information or the Operating System not correctly updating to the new dynamic IP received via DHCP.

Resolution:

Please reboot the computer and try again.

If the problem still persists, please uninstall and reinstall the TCP/IP Protocol associated with the Network Card and reinstall as prescribed by the Operating System.

Issue 5:

User is unable to load the login page and is receiving a valid private address given from the DHCPatriot™.

Cause:

This is due to the user's home page being set to an address that is not resolvable by DNS (Example: The user's homepage is set to a file on their computer or local network by private address).

Resolution:

Type a valid public URL in the Web Browser, such as www.google.com – this will then force the login page to load instead of Google.

-OR-

Reset the user's homepage settings, within their web browser, to a valid public URL such as www.google.com

Issue 6:

User is unable to pull a valid public or valid private IP Address from the DHCPatriot™. The are receiving an address such as 169.x.x.x

Cause:

This is due to the user's operating system, or network card not functioning correctly or a service related outage.

Resolution:

If the broadband service appears to be functioning correctly, the user needs to contact their Internet Technical Support or possibly their Hardware Manufacturer for help with this.

Issue 7:

The user is behind a HUB or Switch with multiple computers and only one computer is able to login, all other computers are unable to authenticate on the login page.

Cause:

This is due to the amount of Simultaneous uses setup in their RADIUS account information or on the DHCPatriot™ being set to a number less than the number of computers the user has.

Resolution:

In this setup, the user will require one Simultaneous Use in RADIUS (or on the DHCPatriot™) for each computer they would like to have on the internet.

Please update their Simultaneous Uses within RADIUS (or the DHCPatriot™). The customer can also use a Router instead that will do Network Address Translation (NAT).
Please Note: Simultaneous use is a global setting on the DHCPatriot™.

Issue 8:

The user is behind a Router which supports Network Address Translation (NAT) and is not presented with the Login Page.

Cause:

This is due to the user's router not being correctly configured to dynamically pull a WAN IP Address and/or DNS or could be the result of one of the issues listed above.

Resolution:

The user will need to setup their router to dynamically assign WAN IP Address and/or DNS according to their router's documentation. If this is setup correctly, please select the most appropriate issue listed above.

Issue 9:

The user receives the message "Server Problems …" when attempting to login to the DHCPatriot™.

Cause:

This is a result of a malfunction on the server.

Resolution:

Please contact the DHCPatriot™ Administrator immediately.

Issue 10:

The user receives the message "Server Problem: We are unable to verify your account at this time, try again in 30 seconds …" when attempting to login to the DHCPatriot™.

Cause:

The user's private IP lease has either not been recorded yet or the user is already authenticated.

Resolution:

The user should try to authenticate again in 1 minute.

The user may already be authenticated; please check the DHCPatriot™ logs and refer to an issue listed above.

Issue 11:

The user receives the message "Warning: Your MAC Address is 00:00:00:00:00:00, please call support …" when attempting to login to the DHCPatriot™.

Cause:

This happens if the user attempts to use an invalid MAC Address composed of all zeros.

Resolution:

The user will need to reset his MAC Address to the one specified with the hardware that is being used to connect.

Issue 12:

The user receives the message "Server Problem: Unable to Authenticate you at this time. Try again in 'x' minutes …" when attempting to login to the DHCPatriot™.

Cause:

The user’s last login session with this device has not yet expired.

Resolution:

Once the lease for the previous connection has expired, they will again be able to authenticate. Please wait the appropriate time for this to clear.

NOT FOR END USER DISTRIBUTION

A-7 DHCP Log Based Troubleshooting:

It is possible to diagnosis some problems that the customers have by viewing the DHCP logs for their device. Understanding the DHCP logs is discussed in section 4.2.5 of the manual. Check there for information pertaining to viewing the logs, and how to interpret what is found. Some error conditions can be identified by what appears in the logs.

- ***Customer's device has no logs at all.***

The customer's device may not be connected properly, may have a software or hardware issue, or the customer's broadband connection may be down.

Ensure that all connections and software are in order. Reboot the device. Try a different device, if available. If the customer's device seems to be in working order, contact the systems administrators for further instructions.

- ***DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK repeat over and over or more frequently than they should based on lease length.***
- ***DHCPDISCOVER, DHCPOFFER repeat over and over.***
- ***DHCPREQUEST, DHCPACK repeat more often than they should, and at the end of lease length since the initial DHCPDISCOVER, the device performs another DHCPDISCOVER.***

The Customer may have serious issues with this device, or the broadband connection may be broken in some way. The customer may have a firewall blocking traffic. The customer's device may need a software or firmware update.

Disable any firewall found. Have the customer perform DHCP with the device (reboot the connected device) and see if any normal logs appear. If they do not, a site visit may be required to determine the problem. If the problem persists, and the customer is using a router, make sure they are running the latest firmware. If it is a computer, make sure they have all software patches.

If the problem still persists, contact the systems administrators for further instructions.

- ***Peer holds all free leases or no free leases message in response to DHCPDISCOVER***

The subnet the customer is part of may be out of IP Addresses.

Contact the systems administrators immediately.

Serial console to DHCPatriot™ Devices

Two Serial Console Adapters (Female DB9 to Female RJ45 converters) will be supplied with your DHCPatriot™ purchase. Plug these into the serial ports on the DHCPatriot™ devices.

B-1 Console from AUX on a Cisco® router:

Plug one end of a Cisco® 'flat black' cable into the desired AUX port on the Cisco® router.

Plug the other end of a Cisco® 'flat black' cable into the Female RJ45 on the console shell attached to the desired DHCPatriot™ device.

Configure the AUX port thusly for console access:

```
line aux <line number>
description DHCPatriot™-<#> console
password <your password>
login
transport input telnet
terminal-type vt100
```

B-2 Console from an OCTAL cable connected to an ASYNC port

Connect the desired octal cable to the Female RJ45 on the console shell attached to the desired DHCPatriot™ device.

Configure the ASYNC port thusly for console access:

```
line async <line number>
description DHCPatriot™-<#> console
password <your password>
login
transport input telnet
terminal-type vt100
```

B-3 Console from a serial (DB9) port on a standard PC

A 'Null Modem' shell must be created. If you have a standard Female DB9 to Female RJ45 blank shell (converter), The pin out is this way:

black -> 2;
yellow -> 3;
brown -> 4;
green -> 5;
orange -> 6;
white -> 7;
blue -> 8;
red -> unused;

Attach this 'Null Modem' shell to your favorite serial port on your standard PC (laptops work great in this mobile type situation)

Microsoft® Windows® based instructions:

Using Hyperterminal (or equivalent), connect to the serial port (usually COM1 or COM2) with these settings:

Hardware Flow control: on

Data bits: 8
Parity: None
Stop bits: 1

UNIX based instructions:

Use 'cu' to connect to the serial port (usually ttyS0 or ttyS1) with this command:

```
cu -l ttyS0 -s 9600
```

cu is usually a part of a uucp package (http://en.wikipedia.org/wiki/UUCP) on Linux® distributions such as Red Hat Linux®.

Customer Service Quick Guide

This one page FAQ provides a quick reference for Customer Service Personnel.

Q: How do I suspend a user?

A: Open the User Management menu and click on Suspend User. Either enter a MAC Address and an optional note, or enter a username or list of usernames and an optional note. Then click Suspend User. ***(see section 4.2.7 of the manual)***

Q: How do I unsuspend a user?

A: Open the User Management menu and click on View Suspended. Locate the user you wish to unsuspend by searching for them. Place a check mark next to the user you wish to unsuspend and click the Un-Suspend selected button. ***(see section 4.2.8 of the manual)***

Q: How do I add a user? (Built-in Authentication)

A: Open the User Management menu and click on Built-in Authentication: User Maintenance. Click Add User. Fill out the form. Click on Commit. ***(see section 4.2.2 of the manual)***

Q: How do I edit a user? (Built-in Authentication)

A: Open the User Management menu and click on Built-in Authentication: User Maintenance. Limit the Displayed Users to find the user you wish to edit. Click Edit for the user. Make your changes here and click on Commit. ***(see section 4.2.2 of the manual)***

Q: How do I change a user's password? (Built-in Authentication)

A: Open the User Management menu and click on Built-in Authentication: User Maintenance. Limit the Displayed Users to find the user you wish to edit. Click Edit for the user. Blank out the Password box and either type a new password or leave it blank to auto-generate a new password. Click on Commit. ***(see section 4.2.2 of the manual)***

Q: How do I disable a user's account? (Built-in Authentication)

A: Open the User Management menu and click on Built-in Authentication: User Maintenance. Limit the Displayed Users to find the user you wish to edit. Click Disable next to the user you wish to disable. ***(see section 4.2.2 of the manual)***

Q: How do I enable a user's account? (Built-in Authentication)

A: Open the User Management menu and click on Built-in Authentication: User Maintenance. Limit the Displayed Users to find the user you wish to edit. Click Enable next to the user you wish to enable. ***(see section 4.2.2 of the manual)***

Q: How do I delete a user? (Built-in Authentication)

A: Open the User Management menu and click on Built-in Authentication: User Maintenance. Limit the Displayed Users to find the user you wish to delete. Click Delete next to the user you wish to delete. ***(see section 4.2.2 of the manual)***

Technical Support Quick Guide

This one page FAQ provides a quick reference for Technical Support Personnel.

Q: How do I determine if a user is receiving an IP Address?

A: Obtain the user's MAC Address. Then open the User Management menu and click on Search DHCP Logs. Enter the user's MAC Address and click search. If you see a DHCPREQUEST and DHCPACK for a specific IP Address in here within the current time minus the length of the lease, they are receiving an IP Address. ***(see section 4.2.5 of the manual)***

Q: How do I manually authorize a customer?

A: Obtain the user's MAC Address, username and password. Open the User Management menu and click on Authorize Customer. Fill in the MAC Address, username and password boxes. Click on Register User. ***(see section 4.2.3 of the manual)***

Q: How do I find a customer's current IP Address and MAC Address?

A: Obtain the user's username. Click on Search Database. Type their username in the appropriate box. Click on Search Database. Their IP Address(es) and MAC Address(es) from any current sessions or, by default, sessions from the last 24 hours are shown. You may need to adjust the time period searched for to find what you are looking for. ***(see section 4.2.6 of the manual)***

Q: How do I view DHCP logs?

A: Open the User Management menu and click on Search DHCP Logs. You may limit the search, or simply click Search Database to view all logs. ***(see section 4.2.5 of the manual)***

Q: How do I know if DHCP logs are normal?

A: If logs are normal, they will contain DHCPREQUEST and DHCPAK messages at every half lease length interval. For example, if a 4 hour lease length is configured on the DHCPatriot™, then those messages should appear every two hours for a currently connected device. You may also see a DHCPDISCOVER, DHCPOFFER, DHCPREQUEST and DHCPAK series of messages. These appear at the beginning of the lease and should not appear while the lease is being maintained. ***(see section 4.2.5 of the manual)***

Q: How do I see if a user is suspended on the DHCPatriot™?

A: Obtain the user's username and MAC Address. Open the User Management menu and click on View Suspended. Type the username in the appropriate box. Click on Search Suspended Users. If the username and MAC Address obtained previously are in the list, the user is suspended. ***(see section 4.2.8 of the manual)***

Q: How do I check a user's status? (Built-in Authentication)

A: Open the User Management menu and click on Built-in Authentication: User Maintenance. Limit the Displayed Users to find the user you wish to check. If an Enable link appears, then the user is disabled. ***(see section 4.2.2 of the manual)***

The purpose of this appendix is to provide answers to possible problems that may be encountered when using the DHCPatriot™.

Q: The device(s) will not power on, what should I do?

A: First, confirm that this is indeed the problem. On the front of each DHCPatriot™ device, there are several lights. The light on the far right, next to the reset button, should be lit. If it is not, then the device may not be powered on. Press the red button to the right of the reset button. This should light the aforementioned power light. If the light still does not illuminate, there may be a problem with the power cable, delivery method, or the device itself. ***(see section 1.3 of the manual)***

Q: The device(s) refuse to respond to pings and are inaccessible. There does appear to be power to the device(s). What do I do?

A: Be sure that the Ethernet cable is connected correctly. On the back of the devices, where the cable plugs in, a link light will appear when the cable is connected correctly. Connect to the device via serial console and ensure that the IP Address and speed or duplex have been set correctly. ***(see sections 1.3, 2.1.2, 2.3, and 3.2.2 of the manual)***

Q: How do I contact First Network Group for further assistance?

A: First Network Group can be reached in the following ways:

Email:	DHCPatriot@network1.net
Phone:	(800)578-6381 x7 (*outside of U.S. (419)739-9240 x7*)
Web:	http://www.network1.net
Mail:	First Network Group, inc 4-6 Perry St. P.O. Box 1662 Wapakoneta, OH. 45895

This document describes the use of Secure Shell (SSH) on various operating systems (Microsoft® Windows®, Mac OSX, Linux®). SSH is needed to connect to the DHCPatriot™ menu configuration interface remotely. Section 3.1 details using the menu configuration interface.

Microsoft® Windows®
Microsoft® Windows® does not come with a built-in SSH client. There are various free and commercial products available. One such product is called PuTTY. We will demonstrate the use of this one. Follow these steps to use PuTTY: 1) Download PuTTY (http://www.putty.nl/download.html). You only need putty.exe This is a self contained program that does not require installation. 2) Double click on the putty.exe program where you saved it. 3) A screen will appear. Enter the IP Address or name of the DHCPatriot™ device you wish to connect to in the hostname box. Select SSH as the connection type. 4) Click on Open. 5) A screen will appear giving details of the security certificate. Click on Yes to allow PuTTY to permanently accept the certificate. 6) A username prompt will appear. Type the username (admin) and press enter. 7) A password prompt will appear. Type your password and press enter. 8) At this point, the menu configuration interface will appear.
Mac OSX
Mac OSX includes a command line SSH client that is similar to other Unix variant's implementation. To access the DHCPatriot™ using this client follows these steps: 1) Open the hard disk. 2) Open the Applications folder. 3) Open the Utilities folder. 4) Double click on Terminal. 5) Type: ssh admin@<host> where host is either the IP Address of or the hostname of the DHCPatriot™ you wish to connect to. 6) A message will appear verifying that you wish to accept the security certificate. Answer yes. 7) A password prompt will appear. Type your password and press enter. 8) At this point, the menu configuration interface will appear.
Linux®
Most Linux® distributions will include an openssh client. These instructions apply to that client. Follow these steps to connect to the DHCPatriot™ from Linux®: 1) Open a terminal window (methods for this vary depending on the distribution and software installed). 2) Type: ssh admin@<host> where host is either the IP Address of or the hostname of the DHCPatriot™ you wish to connect to. 3) A message will appear verifying that you wish to accept the security certificate. Answer yes. 4) A password prompt will appear. Type your password and press enter. 5) At this point, the menu configuration interface will appear.

This document describes the web based API features that are available on the DHCPatriot™ and how they may be used. These features are useful for integrating into automated scripts to perform some task. They consist of sending a specific GET via secure web (HTTPS) on port 443. Each of these features requires that an administrator be setup with appropriate admin level and CLI user access (see section 4.1.8).

Suspend User

This allows a user to be suspended on the DHCPatriot™. It will suspend all devices belonging to the specified username. The default admin level required for this feature is 5. The GET string to send is as follows:
https://patriot.[domain]/cli/remotesuspend.php?username=[username]&password=[password]&action=suspend&user=[username to suspend]

Unsuspend user

This allows a user to be unsuspended on the DHCPatriot™. It will unsuspend all devices belonging to the specified username. The default admin level required for this feature is 5. The GET string to send is as follows:
https://patriot.[domain]/cli/remotesuspend.php?username=[username]&password=[password]&action=unsuspend&user=[username to unsuspend]

Remote Search

This allows a remote search of the session data present on the DHCPatriot with several available search parameters. The result is returned in an XML format similar to that shown here:

```
<result>
        <record>
                <username>jim</username>
                <mac>00:00:89:0c:51:13</mac>
                <ip>192.168.12.74</ip>
                <start_time>1167259985</start_time>
                <stop_time>1168675010</stop_time>
                <sessionID>97365674.4843597</sessionID>
                <DHCPLeaseStart/>
                <DHCPLeaseEnd/>
        </record>
        <record>
                <username>jane</username>
                <mac>00:a0:cc:d9:96:a2</mac>
                <ip>192.168.12.83</ip>
                <start_time>1167171398</start_time>
                <stop_time/>
                <sessionID>283270913.23436</sessionID>
                <DHCPLeaseStart>1173372194</DHCPLeaseStart>
                <DHCPLeaseEnd>1173400994</DHCPLeaseEnd>
        </record>
</result>
```

As many or as few records will be returned as are retrieved using the available search parameters. Search parameters may contain more than one search condition separated by commas (excluding the on line search parameter which consists of 0=off line 1=on line and no value=all). Here are the available search parameters:

- user – use this parameter to limit results to one or more user names.
- mac – use this parameter to limit results to one or more MAC addresses.
- ip – use this parameter to limit results to one or more IP addresses.
- online – use this parameter to limit results to either off line, on line or all sessions.

The default admin level required for this feature is 6. The GET string to send is as follows:

https://patriot.[domain]/cli/remotelist.php?username=[username]&password=[password]&action=search&user=&mac=&ip=&online=

Some examples:

- *https://patriot.[domain]/cli/remotelist.php?username=[username]&password=[password]&action=search&user=* ***jim*** *&mac=&ip=&online=* would return all sessions for the user: jim.
- *https://patriot.[domain]/cli/remotelist.php?username=[username]&password=[password]&action=search&user=* ***jim,jane*** *&mac=&ip=&online=* would return all sessions for either the user: jim or jane.
- *https://patriot.[domain]/cli/remotelist.php?username=[username]&password=[password]&action=search&user=* ***jim,jane*** *&mac=* ***00:00:89:0c:51:13*** *&ip=&online=* would return all sessions for user: jim or jane but only if their MAC address is: 00:00:89:0c:51:13
- *https://patriot.[domain]/cli/remotelist.php?username=[username]&password=[password]&action=search&user=* ***jim,jane*** *&mac=* ***00:00:89:0c:51:13*** *&ip=&online=* ***1*** would return all sessions for user: jim or jane but only if their MAC address is: 00:00:89:0c:51:13 and they are currently online.

You can of course use any combination of these search parameters. The search parameters must always exist in the GET string, but may have blank values.

The DHCPatriot, in addition to the standard Linux SNMP access, the DHCPatriot also contains some custom OID values that will allow access to monitoring of certain parts of the device and also statistical returns regarding network utilization for use with MRTG or similar SNMP based graphing software. The DHCPatriot must be told to allow connections on port 161 for SNMP from the IP address or addresses that will need SNMP access. You may do this either via the CLI based menu configuration or the Web based configuration (see sections 3.2.5 and 4.1.7 respectively for further information).

The DHCPatriot can return several status messages via SNMP regarding certain services. To effectively use these SNMP messages for monitoring of the devices, both devices must be monitored. These messages will always be of the format: <EPOCH>:<status> where EPOCH is the time stamp of the last check and status is up (1), or down (999). If the time stamp is more than 3 minutes old, the result should be considered unreliable, and the service down. The DHCPatriot can return the following status information for services as shown below:

Disk space
OID: 1.3.6.1.4.1.2021.51.1 This OID will return down (999) when Disk space used on the file system reaches 98%.
Database Status
OID: 1.3.6.1.4.1.2021.51.2 This OID will return down (999) when the database server is not running on the device.
Database Sync Status
OID: 1.3.6.1.4.1.2021.51.3 This OID will return down (999) when the database servers are not in sync across the two devices.
DHCPatriot software health
OID: 1.3.6.1.4.1.2021.51.9 This OID will return down (999) if an error condition exists with some facet of the DHCPatriot software.

The DHCPatriot can also return several computed values useful for on going graphing of trends of certain aspects of the system. Here as well, to create an accurate picture both devices should be graphed. The responses messages to each OID will be an integer. What OID to use and what the response means is detailed below:

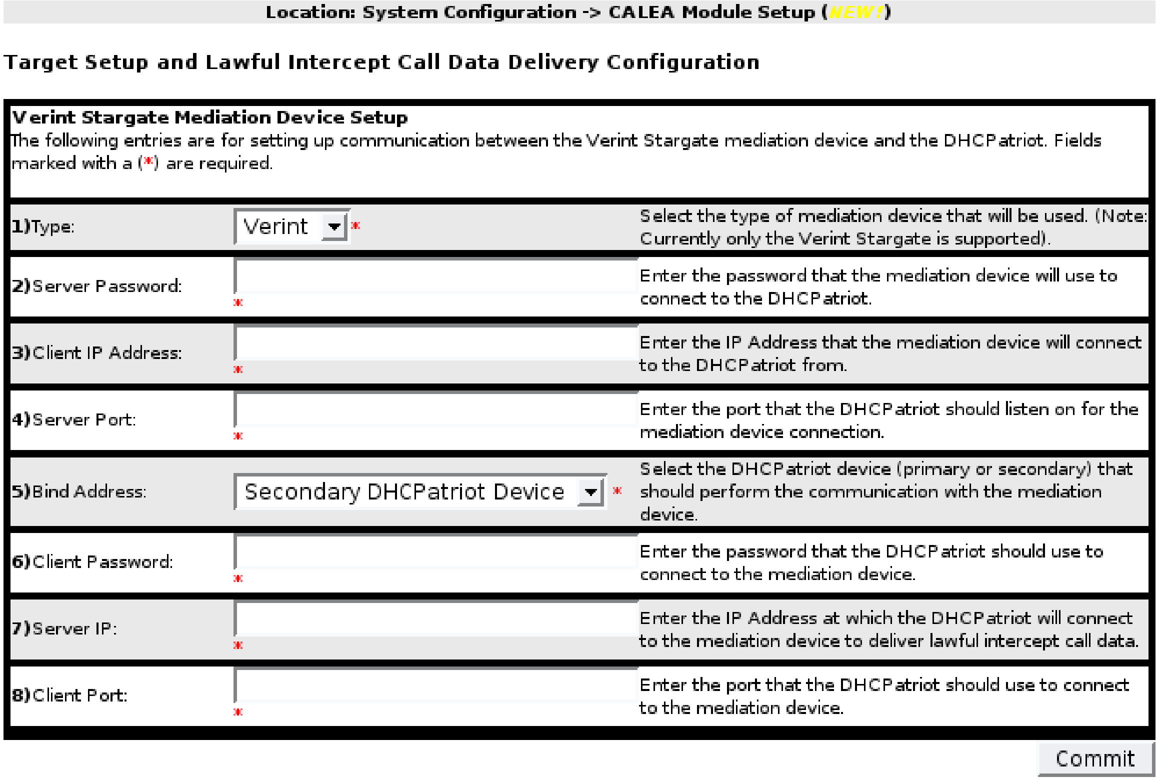
Percentage of CPU used
OID: 1.3.6.1.4.1.2021.50.1.101.1 This OID will return an integer equal to the average CPU percentage used on the device over a recent 5 minute interval.
Percentage of CPU used for IO
OID: 1.3.6.1.4.1.2021.50.10.101.1

This OID will return the average percentage of CPU that was involved in IO operations on the device over a recent 5 minute interval.
Load Average
OID: 1.3.6.1.4.1.2021.50.2.101.1 This OID will return the most recent value of the 15 minute load average for the device. The load average has been multiplied by 100 to make it an integer. Divide by 100 to arrive at the original value.
Total Memory
OID: 1.3.6.1.4.1.2021.50.20 and 1.3.6.1.4.1.2021.50.22 These OIDs will return the total amount of memory installed in the device in Mega Bytes.
Total Memory in use
OID: 1.3.6.1.4.1.2021.50.21 This OID will return the total amount of memory used on the device for any purpose in Mega Bytes.
Memory in use by programs
OID: 1.3.6.1.4.1.2021.50.23 This OID will return the total amount of memory, in Mega Bytes, used on the device by programs. The amount of memory in use for disk buffers and cache is omitted from this return.
Total Swap file size
OID: 1.3.6.1.4.1.2021.50.24 This OID will return the total size of the swap file in Mega Bytes on the device.
Swap file used
OID: 1.3.6.1.4.1.2021.50.25 This OID will return the amount of the swap file used, in Mega Bytes, on the device.
Database Threads
OID: 1.3.6.1.4.1.2021.50.45 This OID will return the total number of database threads that are currently running on the device.
Database Queries per Second
OID: 1.3.6.1.4.1.2021.50.46 This OID will return the average number of database queries per second over the most recent 5 minute interval. This number is rounded to the nearest whole number.
DHCP Queries per Second
OID: 1.3.6.1.4.1.2021.50.70 This OID will return the average number of DHCP queries per second over the most recent 5 minute interval. This number is rounded to the nearest whole number.
Total Disk Space

OID: 1.3.6.1.4.1.2021.50.50.3 This OID will return the total amount of disk space on the device's file system in Mega Bytes.
Disk Space Used
OID: 1.3.6.1.4.1.2021.50.50.4 This OID will return the amount of disk space used on the device's file system in Mega Bytes.
IP Address Utilization
OID: 1.3.6.1.4.1.2021.50.60.3.0.<Gateway address of Main DHCP range> Example: 1.3.6.1.4.1.2021.50.60.3.0.208.45.199.113 This OID will return a measurement of the total number of IP addresses in use on a particular dynamic network in the most recent 5 minute interval. This is the same measurement used to compute the Total Dynamic graphs in IP Address Usage (see section 4.2.10).

If the CALEA module has been purchased, the DHCPatriot can communicate directly with a Verint Systems Inc. mediation device. The DHCPatriot can return session data for a lawful intercept target directly to the Verint Systems Inc. mediation device.

Configuration of this module is accessed via the System Configuration menu. Click on CALEA Module Setup to proceed. A screen similar to figure I-1 will be displayed.



Location: System Configuration -> CALEA Module Setup (NEW!)

Target Setup and Lawful Intercept Call Data Delivery Configuration

Verint Stargate Mediation Device Setup

The following entries are for setting up communication between the Verint Stargate mediation device and the DHCPatriot. Fields marked with a (*) are required.

1)Type:	Verint *	Select the type of mediation device that will be used. (Note: Currently only the Verint Stargate is supported).
2)Server Password:	*	Enter the password that the mediation device will use to connect to the DHCPatriot.
3)Client IP Address:	*	Enter the IP Address that the mediation device will connect to the DHCPatriot from.
4)Server Port:	*	Enter the port that the DHCPatriot should listen on for the mediation device connection.
5)Bind Address:	Secondary DHCPatriot Device *	Select the DHCPatriot device (primary or secondary) that should perform the communication with the mediation device.
6)Client Password:	*	Enter the password that the DHCPatriot should use to connect to the mediation device.
7)Server IP:	*	Enter the IP Address at which the DHCPatriot will connect to the mediation device to deliver lawful intercept call data.
8)Client Port:	*	Enter the port that the DHCPatriot should use to connect to the mediation device.

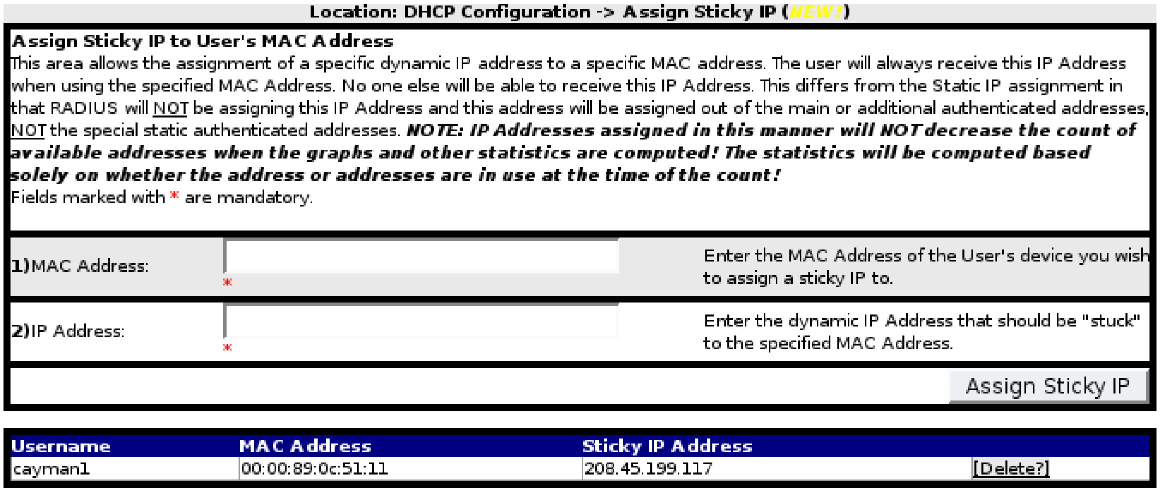
Figure I-1: CALEA module configuration

Follow the on screen instructions for completing the configuration of the mediation device call data delivery. Make sure that the DHCPatriot can communicate with the device configured here. Follow Verint Systems Inc.'s recommendations for IPSEC as necessary. Make sure that the values configured on the DHCPatriot for the Verint Systems Inc. mediation device match what was configured on the actual mediation device.

The DHCPatriot has two methods of assigning the same IP address to the same MAC address on an ongoing basis. The first of these involves a special static subnet, and having a specific IP Address returned from either the built-in authentication or RADIUS (see section 4.1.3 for details). The second method is called Sticky IP and is discussed in this appendix.

A Sticky IP is an IP address assigned to a specific MAC address out of a dynamic IP address pool, such as is configured in the Main or Additional DHCP range (see sections 4.1.1 and 4.1.2 respectively). Please note that assigning a Sticky IP will NOT reduce the count of dynamic IP addresses as reported in IP Address Usage (see section 4.2.10) or via SNMP (see Appendix H). The purpose of the Sticky IP is so that ISPs can offer a non changing IP address (ie: a static IP address) while still maintaining authentication via DHCP using the DHCPatriot and without the need of special RADIUS or built-in authentication configuration or the need of a special static subnet as is the case with the Static IP address (see section 4.1.3 for details). If enough IP addresses exist in the network to allow for one or more special static IP address subnets, that method is preferred. Please note that beyond checking that the MAC address and IP address are of the valid format, and are not already assigned as a Sticky IP, no other checking is performed when adding a Sticky IP assignment, so please be careful.

To access the Sticky IP configuration, open the DHCP Configuration menu and click on Assign Sticky IP. A screen similar to that shown in figure J-1 will appear.


Location: DHCP Configuration -> Assign Sticky IP (NEW!)

Assign Sticky IP to User's MAC Address

This area allows the assignment of a specific dynamic IP address to a specific MAC address. The user will always receive this IP Address when using the specified MAC Address. No one else will be able to receive this IP Address. This differs from the Static IP assignment in that RADIUS will NOT be assigning this IP Address and this address will be assigned out of the main or additional authenticated addresses, NOT the special static authenticated addresses. ***NOTE: IP Addresses assigned in this manner will NOT decrease the count of available addresses when the graphs and other statistics are computed! The statistics will be computed based solely on whether the address or addresses are in use at the time of the count!***

Fields marked with * are mandatory.

1)MAC Address:	*	Enter the MAC Address of the User's device you wish to assign a sticky IP to.
2)IP Address:	*	Enter the dynamic IP Address that should be "stuck" to the specified MAC Address.

Username	MAC Address	Sticky IP Address	
cayman1	00:00:89:0c:51:11	208.45.199.117	[Delete?]

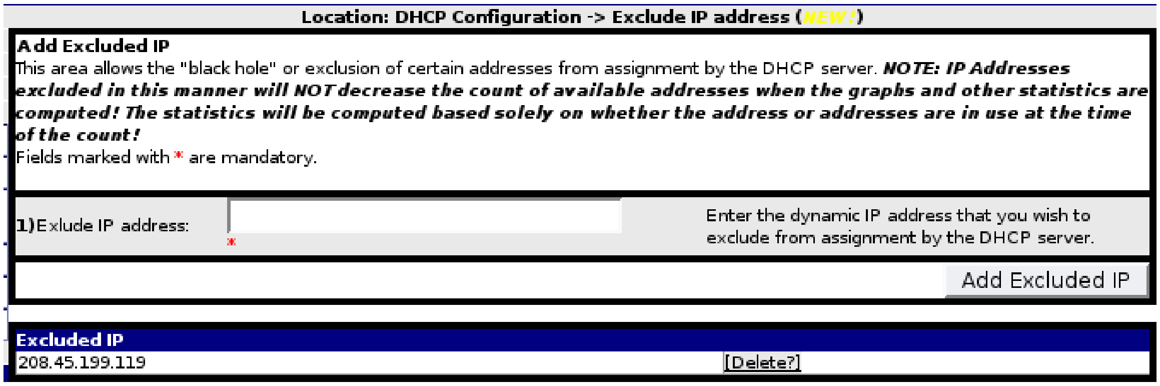
Figure J-1: Sticky IP configuration

Follow the on screen instructions to assign or delete an assignment of a Sticky IP. Please note that the device will not be able to retrieve the Sticky IP if some other device is currently using it. The IP can be retrieved immediately if not in use by another device. Simply have the user release and renew or reboot to attempt to retrieve the Sticky IP.

In some situations, it may become necessary to exclude certain IP addresses due to abuse or other challenges. This appendix describes the method for doing so on the DHCPatriot.

Once an IP address is excluded, it will not be handed out to any device. Please note that no sanity checking, other than determining that the IP address is of the correct format, will be done. Further, note adding an excluded IP address will NOT reduce the count of dynamic IP addresses as reported in IP Address Usage (see section 4.2.10) or via SNMP (see Appendix H). Please be careful when adding an IP address for exclusion.

To access the Exclude IP configuration area, open the DHCP Configuration menu and click on Exclude IP Address. A screen similar to that shown in figure K-1 will appear.



Location: DHCP Configuration -> Exclude IP address (*NEW!*)

Add Excluded IP

This area allows the "black hole" or exclusion of certain addresses from assignment by the DHCP server. ***NOTE: IP Addresses excluded in this manner will NOT decrease the count of available addresses when the graphs and other statistics are computed! The statistics will be computed based solely on whether the address or addresses are in use at the time of the count!***

Fields marked with * are mandatory.

1)Exlude IP address: *

Enter the dynamic IP address that you wish to exclude from assignment by the DHCP server.

Excluded IP	
208.45.199.119	[Delete?]

Figure K-1: Exclude IP configuration

Follow the on screen instructions to add or delete an excluded IP address. Any excluded IP addresses in the list will not be handed out to any device. However, if a device already received the address, the lease will have to expire, or the device will need to be rebooted (or have a release and renew performed) in order to retrieve a different IP address.