Operations Manual

Version 5

Table of Contents

Chapter 1: Requirements 9

Network and Router Requirements 9
Optional External Equipment 9
Power and Cabling Requirements 9

Chapter 2: Network Integration and Example 11

Device Placement 11
Authenticated DHCP Installation Example 11
Example External Device Configuration for Authenticated DHCP 12

Chapter 3: Installation 14

Installing the Hardware 14
Unpacking the system 14
Mounting in a two or four post rack 15
Attaching Cables 16

Chapter 4: Initial Configuration 17

Menu Interface 17
Serial Console Access 17
Console from AUX on a Cisco® 17
Console from an OCTAL cable connected to an ASYNC port 18
Console from a serial (DB9) port on a standard PC 18
Secure Shell (SSH) Access 19
Configuring the Menu Interface 20
Changing the ‘admin’ user password 20
IP Address Configuration 20
IPv6 Address Configuration (Optional) 21
Domain Name Configuration 21
Ethernet Media Settings (Speed and Duplex) 22
Configuring the Firewall for the Administration Network 22
Initial Configuration Reboot 23
Web Administration Interface Account Setup 24
Web Administration Interface 25

 This document © 2011 First Network Group Inc. All Rights Reserved

Connecting to the Web Administration Interface 25
Configuring the General Settings in General Setup 26
Chapter 5: General Tasks 28
Administrative User Maintenance 28
Built-in Firewall Configuration 29
IPv6 Built-in Firewall Configuration 29
System Logs 30
Changing Your Password 30
Chapter 6: Authenticated DHCP 32
Configuring Authenticated DHCP 32
Authentication Servers 32
Internal (Built-in Authentication) 33
External 33
Captive Portal 33
Adding 34
Editing 35
Removal 35
Shared Network Configuration 35
Shared Network 35
Adding 36
Editing 36
Removal 36
Unauthenticated Subnet 37
Adding 37
Editing 37
Disable 37
Removal 38
Authenticated Subnet 38
Adding 38
Editing 38
Disable 38
Removal 39
Static Subnet 39

 This document © 2011 First Network Group Inc. All Rights Reserved

Adding 39
Editing 39
Removal 39
Maintenance Subnet 40
Adding 40
Editing 40
Removal 40
Special Reports 40
View Authenticated Users 41
Users Using Multiple IPs 41
Chapter 7: Standard DHCP 42
Shared Network Configuration 42
Shared Network 42
Adding 43
Editing 43
Removal 43
Dynamic Subnet 43
Adding 44
Editing 44
Disable 44
Removal 44
Static Subnet 44
Adding 45
Editing 45
Removal 45
Maintenance Subnet 45
Adding 46
Editing 46
Removal 46
Additional Configuration Tasks 46
Known Client 46
Adding 47
Editing 47

 This document © 2011 First Network Group Inc. All Rights Reserved

Removal 47
Static IP Assignment 47
Adding 47
Editing 48
Removal 48
TFTP File Maintenance 48
Adding 49
Mass Change of TFTP File Assignments 49
Editing 49
Removal 49
Chapter 8: Common Authenticated and Standard DHCP Actions and Reports 50
Sticky IP Address 50
Adding 50
Editing 50
Removal 51
Exclude IP Address 51
Adding 51
Removal 51
Deny Mac Address 52
View Address Usage 52
Search Sessions 53
Possible hijacked IP Addresses 54
Chapter 9: DHCPv6 Configuration and Maintenance 55
IPv6 Primer 55
DHCPv6 Primer 56
Configuration and Maintenance of DHCPv6 on the DHCPatriot 58
Chapter 10: Monitoring and Graphing the System 62
Allowing Subnets to Monitor the DHCPatriot 62
Monitoring Critical Services and Their Importance 63
Graphing System Performance 66
Graphing Address Utilization 68

 This document © 2011 First Network Group Inc. All Rights Reserved

Miscellaneous SNMP Information 71
Server Status on the Web Administration Interface 71
Chapter 11: Remote Access API 73
Setting up the User for API Access 73
User Access 73
Authenticate Device 74
Suspend Device 74
Enable Device 75
Search Authenticated Devices 75
Sticky IP Add 76
Sticky IP Delete 76
Sticky IP List 77
Built-in Authentication 77
List Customers 78
Add Customer 78
Edit Customer 79
Suspend Customer 79
Enable Customer 79
Delete Customer 80
Change Password 80
Remote Search 81
Get Network Config 82
Standard DHCP 83
List Known Client 83
Add Known Client 84
Edit Known Client 84
Delete Known Client 85
List Static IP Assignments 85
Add Static IP Assignment 86
Edit Static IP Assignment 86
Delete Static IP Assignment 87
Chapter 12: Supporting DHCPatriot End-Users 88
How to Troubleshoot 88

 This document © 2011 First Network Group Inc. All Rights Reserved

Authenticated DHCP 88
Authorize Customer 88
Standard DHCP 89
Search DHCP Logs 89
General Troubleshooting Techniques 90
Authentication Problems 92

Chapter 13: User Based Tasks for Customer Service 94

Suspend User 94
Built-in Authentication: User Maintenance 95
Adding a User 95
Editing a User 96
Suspending One or More Users / Enabling suspended users 96
Deleting a User 97
Built-in Authentication: User Import 97
Device Import 98

 This document © 2011 First Network Group Inc. All Rights Reserved

Chapter 1: Requirements

Network and Router Requirements

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

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 system 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) (Cisco® devices that support 'ip helper-address' support DHCP Failover without special modification).

The DHCPatriot system 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 system cannot be used centrally in this situation. An additional system will be needed for that separate pop. In other words, the customer traffic must not leave your routing control before arriving at the DHCPatriot system. If this is not the case, then the policy based routing will not work for the optional authentication.

Some routers in the network will need to support policy based routing. Most Cisco® routers and layer 3 switches support policy based routing in order for the optional authentication to function.

Optional External Equipment

The DHCPatriot system may use either the Built-in Authentication, or an optional external RADIUS server for authentication and accounting of customers. It must use one method or the other. Note: The RADIUS server must at least respond with the Framed-IP-Address attribute set to 255.255.255.254.

Power and Cabling Requirements

PLEASE NOTE: This section applies to only AC powered DHCPatriot systems. DC powered systems use 48 volt DC.

Each DHCPatriot device has a single power supply. This power supply is AC (Alternating Current) compatible only. DO NOT plug the devices into DC (Direct

 This document © 2011 First Network Group Inc. All Rights Reserved

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 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. Note that there is now a DC (Direct Current) version available.

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

Two power cables (included). Note: The DHCPatriot system ships with power cables suitable for plugging into an American 120v 60 Hz outlet. A different cable may be needed in your region. The power supply will accept a standard PC cable from your region. Please note that if the DC version is purchased it will not come with power cabling.

Two serial console adapters (included) (optional). Two console cables (not included) for connection of the console ports on the DHCPatriot devices to a customers supplied console server.

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

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 devices are to be plugged into a gigabit switch (hubs are not recommended), then a gigabit Ethernet cable should be used.

 This document © 2011 First Network Group Inc. All Rights Reserved

Chapter 2: Network Integration and Example

The DHCPatriot system can replace any existing DHCP server that you may have in your network. It can force authentication of customer equipment using either the Built-in Authentication server or an external RADIUS server. The system may optionally interact with an external RADIUS server.

Device Placement

The DHCPatriot system 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 2.1 shows placement in a typical network. An example of usage follows. This example will help in the decision regarding placement in your network.

Authenticated DHCP Installation Example

In figure 2.1, the optional RADIUS server and console server are shown. Using the example in figure 2.1, we can construct a proper setup for the DHCPatriot system. This will help you understand how the DHCPatriot will integrate into your network.

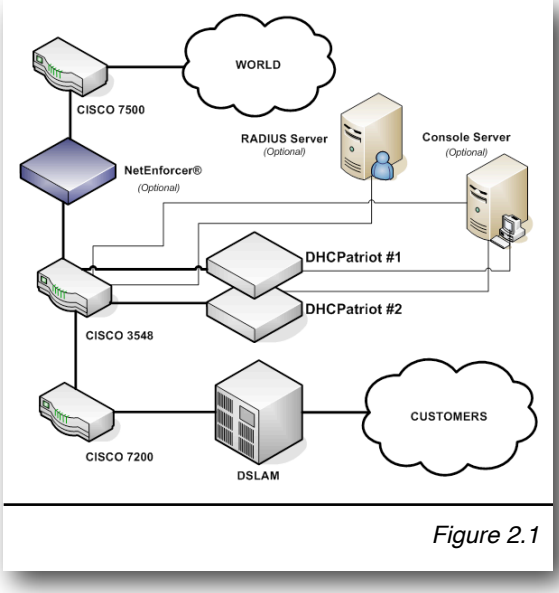


Figure 2.1

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.

To better understand how the system functions, it is necessary to describe it from the perspective of a new customer device on the network.

Since this is a new device, the MAC Address is unknown to the DHCPatriot system. The system will force the device to be authenticated before being allowed on to the network (optional). 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

 This document © 2011 First Network Group Inc. All Rights Reserved

agent, forwards this request to the system. The DHCPatriot system 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 system due to the source IP address originating in the unauthenticated network. The system responds by sending the device the authentication page. The customer types his username and password, and the device posts this to the DHCPatriot system. The system 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 system 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 system.

Upon booting up, the device requests an IP Address from the DHCPatriot system again. At this time, the Cisco® 7200 again forwards the request to the system which responds with an authenticated address. The system will authenticate the device with the optional RADIUS server. The optional RADIUS server will again respond with Access-Accept. The DHCPatriot system 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 system will mark the device as being offline, and send an accounting stop to the optional RADIUS server.

Example External Device Configuration for Authenticated DHCP

Some configuration changes on external devices to the DHCPatriot system 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:

```
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 system for forced authentication purposes. The Cisco® 3548 will require two configuration changes to accommodate this setup. First, in the global configuration area:

 This document © 2011 First Network Group Inc. All Rights Reserved

```
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 #>
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.

Although not described in this example, the optional console server may be used in this example network allowing connection to the DHCPatriot for some administrative tasks.

Please note that as of 5.3.0 it is possible to configure a third IP address that “floats” between the two devices via VRRP, a floating IP address if you will. This is configured in the web administration interface under General Setup which will be covered later in the manual. It is now recommended that this floating IP address be configured and used in place of the ip of DHCPatriot primary device in the above example.

 This document © 2011 First Network Group Inc. All Rights Reserved

Chapter 3: Installation

Installing the Hardware

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 3.1 shows model 2003-2 and greater. If you have the older system, model 2003-1 (see figure 3.2), please use the original manual provided with the DHCPatriot system for physical installation, or contact First Network Group for physical installation instructions.

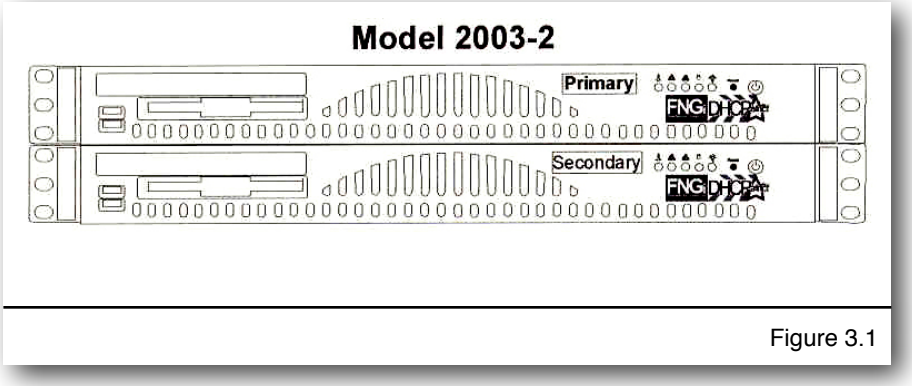


Figure 3.1

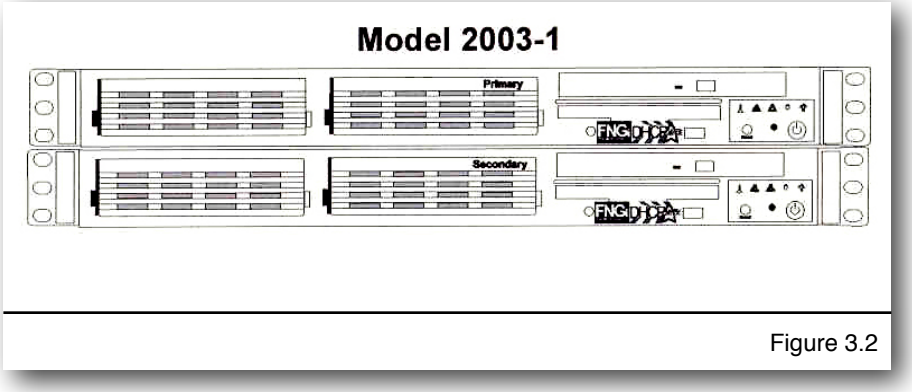


Figure 3.2

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.

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 devices to your 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 Manual (this document)
6	1	EULA (End User License Agreement)
7	1	Maintenance Contract Quick List
8	1	Maintenance Contract
9	1	IP/Hostname Notice (regarding Maintenance Contract activation)
10	1	Return Policy Statement

 This document © 2011 First Network Group Inc. All Rights Reserved

- Ethernet Cables - Two standard Ethernet cables of sufficient length to attach the DHCPatriot devices to the Ethernet switch.
- Console Cables (optional) - Two cables suitable for the console connection. We will cover the optional console connection in more detail later.

Mounting in a two or four post rack

The DHCPatriot system 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.

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.

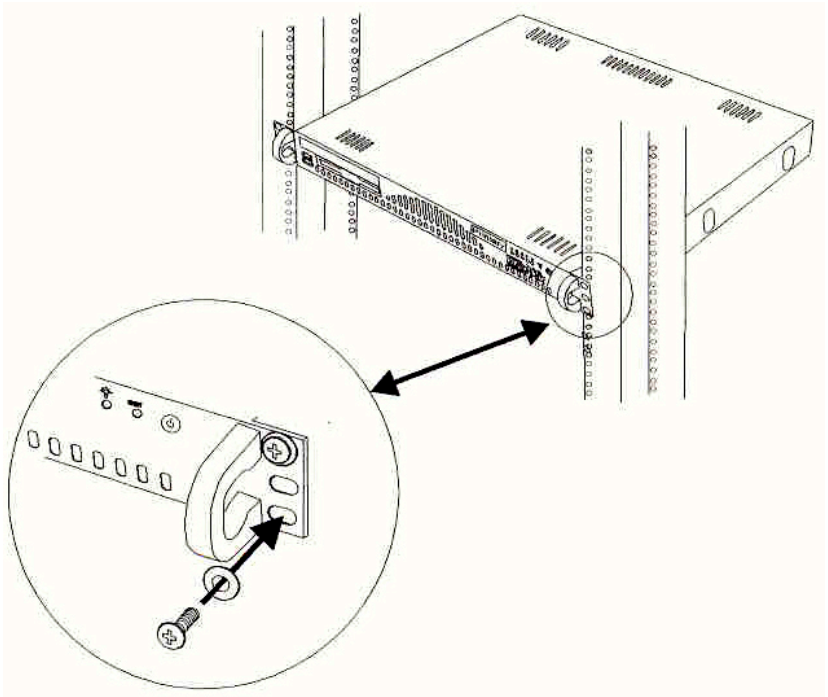


Figure 3.3

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 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.

 This document © 2011 First Network Group Inc. All Rights Reserved

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 3.3). 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.

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. 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. 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 3.4. The two DB9 to RJ45 serial console adapters (supplied) are connected to the serial port of each device as shown in figure 3.4. Install the adapters even if you do not intend to use the serial console capabilities.

The LAN port is used to connect the DHCPatriot system to the Ethernet switch. The customer supplied Ethernet cable should be used for this connection.

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.

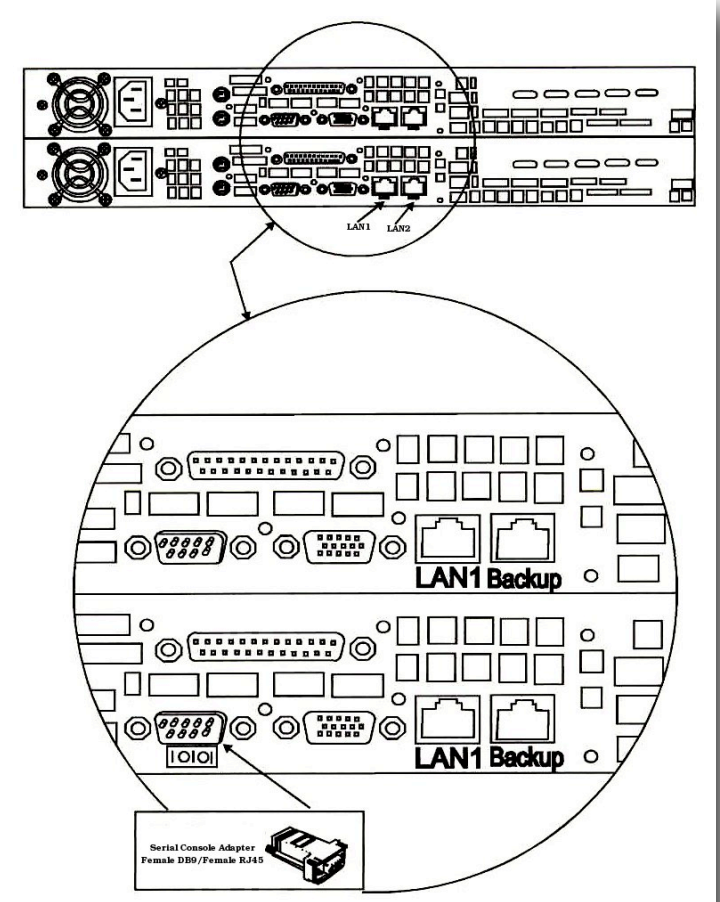


Figure 3.4

Note that as of hardware model 2013-1, the ports are now reversed. The Backup port is now closest to the VGA port and the LAN1 port is now furthest from the VGA port.

 This document © 2011 First Network Group Inc. All Rights Reserved

Chapter 4: Initial Configuration

The DHCPatriot system has two stages of initial configuration. First the menu interface must be accessed via serial console or SSH (Secure Shell). During this configuration such things as IP Address, domain name and web administration interface users are configured. After this, then the General settings must be set on the Web administration interface. The DHCPatriot system is then ready to use and can be configured for DHCP etc...

Menu Interface

The menu interface is the first stage of configuration. This is accessed via SSH or serial console. The username '`admin`' with the password '`cU$0gNn1`' is used to login to the interface.

Serial 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. These devices are also compatible with Cisco® console implementation and standard PC (UNIX based OSs, Microsoft® Windows® and Apple® Mac® systems) implementations. 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)	9	NC (Not Connected)
5	GND (Ground)		

Console from AUX on a Cisco®

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 thus for console access:

 This document © 2011 First Network Group Inc. All Rights Reserved

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

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 thus for console access:

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

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 shown in the chart to the right.

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

Serial Port Adapter Female RJ45 Pin Out			
PIn #	Color	Pin #	Color
1	Unused	6	Orange
2	Black	7	White
3	Yellow	8	Blue
4	Brown	9	Unused
5	Green	Unused	Red

UNIX based instructions:

- Use 'cu' to connect to the serial port (usually ttyS0 or ttyS1) with this command:
  - cu -l ttyS0 -s 9600

 This document © 2011 First Network Group Inc. All Rights Reserved

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

Secure Shell (SSH) Access

The tables below describe the use of Secure Shell (SSH) on various operating systems (Microsoft® Windows®, Mac OSX, and Linux®). SSH is needed to connect to the DHCPatriot menu interface remotely.

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 call 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 as 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 very similar, or even the same as, other UNIX variant's implementation. Please note that the method described here applies to Mac OSX 10.4.x (Tiger) or greater. To access a DHCPatriot device using this client, follow these steps: 1) Press Command + Space bar to open spotlight. 2) Type the word Terminal in the resulting bar and press enter. 3) On the resulting terminal screen, type: ssh admin@<host> where host is either the IP address or the hostname of the DHCPatriot device you wish to connect to. 4) A message will appear verifying that you wish to accept the security certificate. Answer yes. 5) A password prompt will appear. Type your password and press enter. 6) At this point, the menu configuration interface will appear.
Linux®

 This document © 2011 First Network Group Inc. All Rights Reserved

Most Linux® distributions will include an openssh client. These instructions apply to that client. Follow these steps to connect to a DHCPatriot device 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 or the hostname of the DHCPatriot device 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.

Configuring the Menu Interface

After connecting and logging on using the administrator username, a menu will be presented like the one in figure 4.1. A series of steps are necessary to complete this portion of the configuration before moving on to the Web Administration Interface configuration stage.

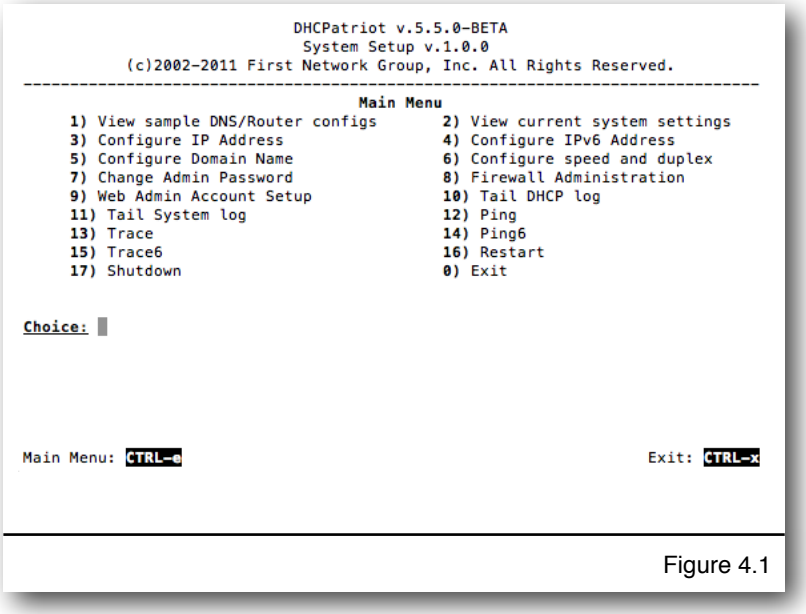


Figure 4.1

Changing the '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 system owners) and should not be used after the IP address is set.

Once a suitable password is chosen, press 7 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. Type this and press enter. Type the new desired password and press enter. Retype 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.

IP Address Configuration

NOTE: Do not reboot until both the IP Address and domain name have been configured. If the domain name is left at the default example.com, then the IP address will be returned to default upon reboot.

To begin configuration of the IP address, press 3 and then enter. At this point, press 1 and then enter. That will begin the configuration process. The interface will ask for the

 This document © 2011 First Network Group Inc. All Rights Reserved

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. If the information looks correct, press 1 and then enter. If you have misconfigured something, press 0 and enter. Then press 3 and enter to return to the IP address configuration area to 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.

IPv6 Address Configuration (Optional)

From the main CLI menu screen, press 4 to enter the IPv6 address assignment area. The current IPv6 network settings are shown here. Press 1 to proceed and configure the address. You will first be asked for the IP address, this should be entered as address/prefix length (ex: 2001:db8:0:0:1/64). Press enter to continue. Then the gateway will be requested. This must be an address in the same subnet as the IP address entered previously. Press enter to continue. A summary will then be shown asking if you would like to proceed. Press 1 and then enter to proceed. Return to the main menu (CTRL+e).

Domain Name Configuration

NOTE: It is important that both the primary and secondary DHCPatriot devices be set to the same domain name.

The next task to perform is setting the domain name. At this point, you should be back at the main menu (see figure 4.1). If you are not, please be sure that the IP address has been saved properly and then press Ctrl+e to return to the main menu. Press 5 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 the primary or secondary designation. This factory set designation cannot be changed. Only a domain name may be configured here.

After entering the chosen domain name, press enter. The screen will display your entry and ask for confirmation. Press 1 and then enter to continue. 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:

 This document © 2011 First Network Group Inc. All Rights Reserved

- 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 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).

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 6 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 device 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.

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 system employs a white-list-style firewall. You are encouraged to allow access to only the minimum of IP addresses necessary for administration of the DHCPatriot system. 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 the system 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 8 and then enter. The first thing you will notice is that there are several rules 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.

 This document © 2011 First Network Group Inc. All Rights Reserved

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 system 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 IP Addresses
/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 system 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.

Initial Configuration Reboot

 This document © 2011 First Network Group Inc. All Rights Reserved

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 16 and then enter. Then press 1 and enter to continue. 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.

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 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 12 (14 for IPv6) 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 13 (15 for IPv6) 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.

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 for connecting to the Web Administration Interface later to continue configuring the DHCPatriot. Press 9 and then enter to begin the configuration process.

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. Enter the desired username and then press enter. A password prompt will appear. 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.

 This document © 2011 First Network Group Inc. All Rights Reserved

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 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 system at some future time. To delete a user, from the main menu press 8 to enter the Web Admin Account Setup function.

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 to 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.

Web Administration Interface

The second half of the initial configuration is performed from the Web Administration Interface. This is actually the easiest part as configuration is minimal. Once this is complete, subnets may be added and the DHCPatriot is ready to use.

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 and that the administrator account(s) has been added

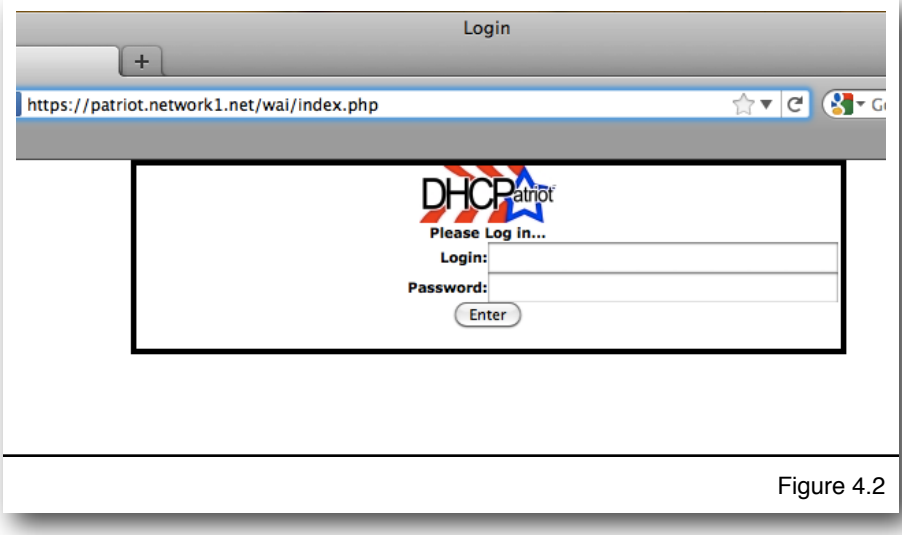


Figure 4.2

 This document © 2011 First Network Group Inc. All Rights Reserved

before continuing.

To begin, open your favorite web browser. In the address bar, type: https://patriot.<domain> and press enter. If you receive an error message, ensure that the DHCPatriot system is up and running, that the device you are connecting from is allowed via the firewall and that the appropriate entries have been made in your DNS server. 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 4.2.

In the login field type the username that was created in the Menu Configuration interface. In the password field, type the password that was created in the Menu Configuration interface.
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 are still unable to login, revisit the Menu Configuration Interface in Initial configuration section and make sure the instructions there were performed correctly. Once authentication is successfully performed, a screen similar to figure 4.3 will appear.

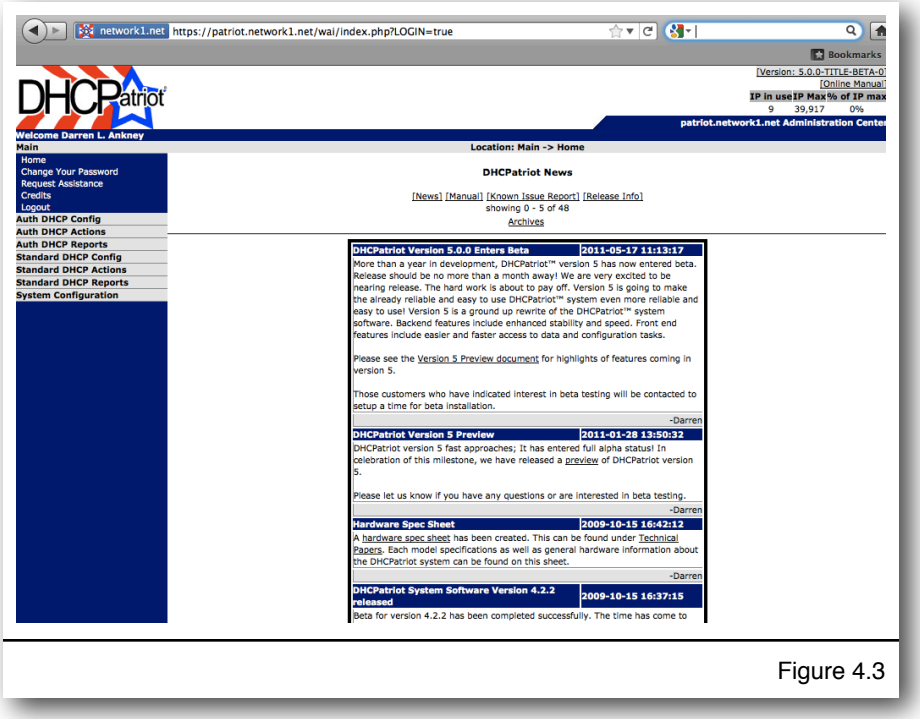


Figure 4.3

Configuring the General Settings in General Setup

There is a very short General Settings section that must be visited before any further configurations can occur. To access these settings, expand the System Configuration Menu and click on General Setup. You should get a screen that looks like figure 4.4.

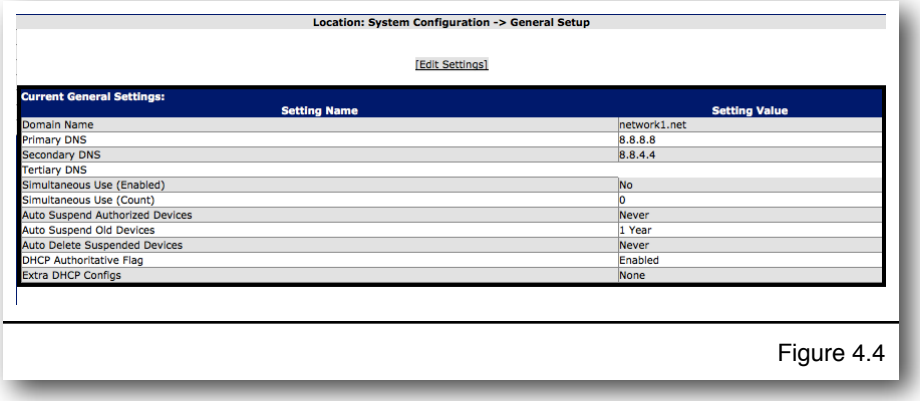


Figure 4.4

There are several settings here. To see a description of

 This document © 2011 First Network Group Inc. All Rights Reserved

each setting and what it does as well as to change the setting, click on Edit Settings. At that point you should have a screen similar to figure 4.5. Some of these settings will have defaults entered. These can be safely left alone if you do not know what to do. Of particular importance are the Domain Name, the Primary DNS and Secondary DNS.

Another minor note are the three settings which allow older / unused devices to be suspended and cleaned from the system. It is also possible to force a periodic login for devices to make sure they are still associated with the same user.

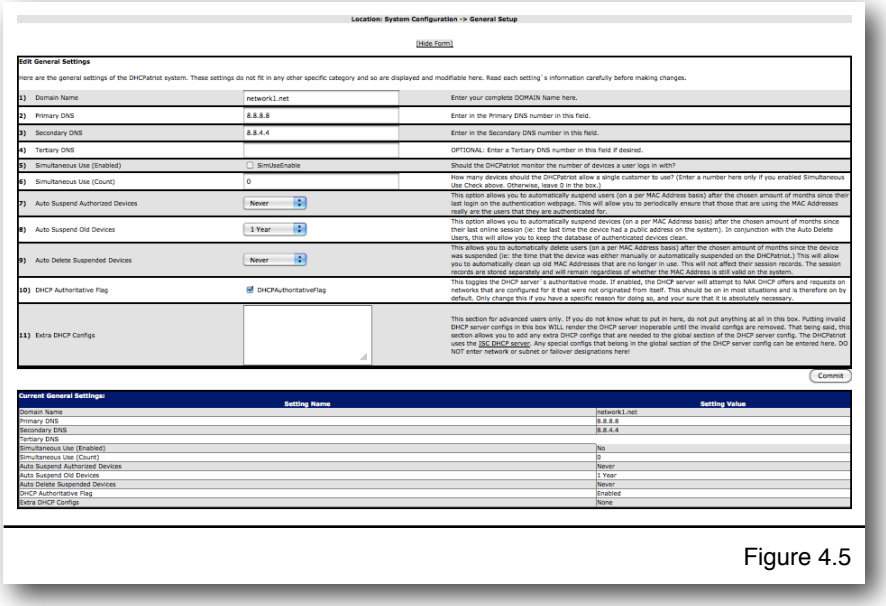


Figure 4.5

These settings are ‘Auto Suspend Authorized Devices’, ‘Auto Suspend Old Devices’, and ‘Auto Delete Suspended Devices’. Use ‘Auto Suspend Authorized Devices’ to force an authentication recheck of the device in the specified time period. This allows you to periodically make sure that the device still belongs to the same user. Use ‘Auto Suspend Old Devices’, and ‘Auto Delete Suspended Devices’ to keep old devices churning out of the system. Devices are considered old and suspended when the time period you specified passes with no DHCP activity from the device. Devices will be deleted after being suspended for the time period you specify.

Please note that as of 5.3.0 Floating IP (VRRP) is available here as well. That allows the configuration of a third floating IP address on the DHCPatriot system that can be used for high availability of the web server (for administration and customer login).

Complete these settings and then click on Commit. The DHCPatriot system is then setup for initial operation and other tasks can be performed such as adding networks for either authenticated or standard (or both) type DHCP networks. If you are unsure what to do next, have a look around the interface and the manual. If you need further assistance, please feel free to contact First Network Group.

 This document © 2011 First Network Group Inc. All Rights Reserved

Chapter 5: General Tasks

Administrative User Maintenance

The DHCPatriot system supports multiple administrative type users each with different passwords and permission levels. These permission levels range from 0-6. 0 should be used for customer service personnel as it allows access to a minimal set of functions. Level 1 should be used for technical support personnel as it allows access to a wider variety of functions that would be useful in troubleshooting user problems. Admin level 5 is meant for higher level administrative personnel such as various managers of Technical Support or Customer Service. Level 6 is meant for IT administrators who will be responsible for actually setting up networks, subnets and general settings on the DHCPatriot system.

Other important settings are API user which, if checked, means the user has access only to the remote access API. If it is not checked, then the user has access to only the Web Administration Interface. The two Admin User Restriction (Auth and Standard) settings are used for restricting user access to certain networks. This is not a security feature, but rather an interface cleanup feature that hides irrelevant information from users. Any networks that are checked will show for the user and other networks will be hidden, but data could be found in other places such as Search DHCP Logs.

The configuration screen for Administrative users is accessed by opening the System Configuration menu and clicking on Administrators. You will be shown a form and a list of users as shown in figure 5.1. To Add a user, simply complete the form and click Commit. To edit a user, click on Edit and the form will auto-fill with their information. Make the appropriate changes and click on Commit. To delete a user, click on Delete and answer OK to the question of if you are sure.

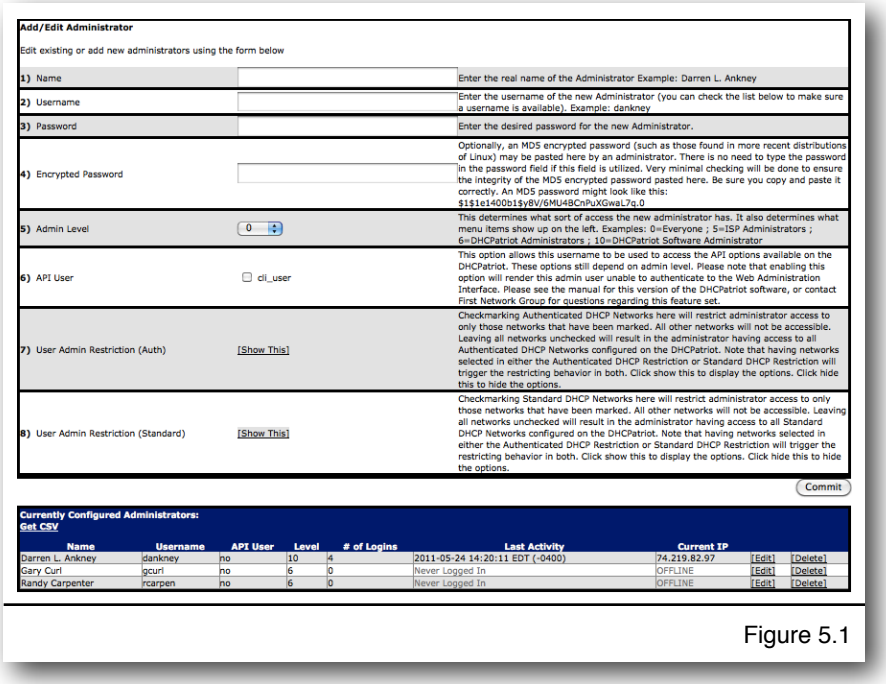


Figure 5.1

 This document © 2011 First Network Group Inc. All Rights Reserved

Built-in Firewall Configuration

The DHCPatriot system includes a white list firewall. Basically, all incoming traffic is blocked unless specifically allowed. The good news is that anything customer related is automatically allowed such as communication with the DHCP server or access to the login page among other services. Additionally, monitoring subnets that are configured are also automatically allowed appropriate access so that monitoring can be performed.

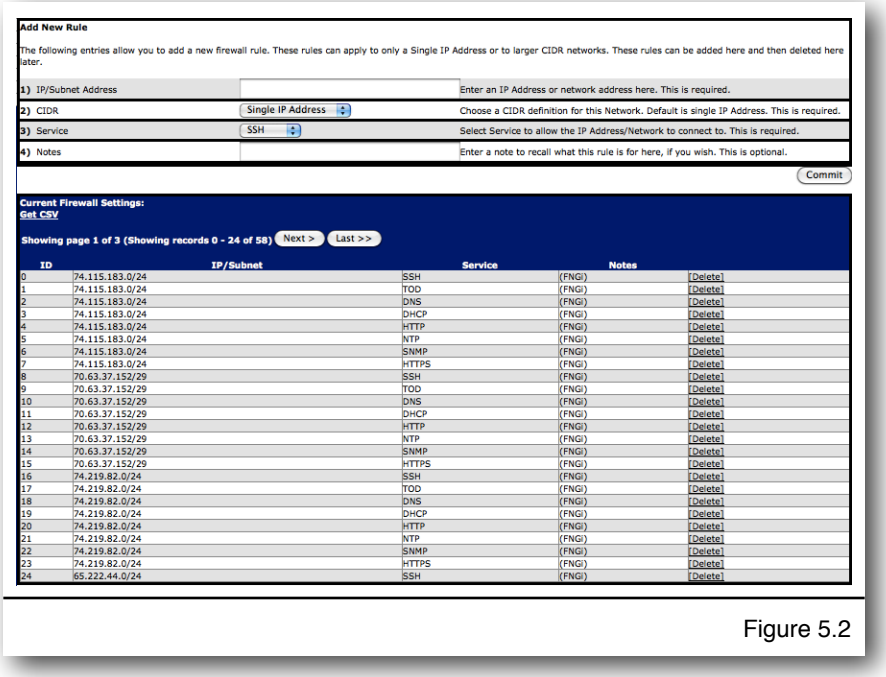


Figure 5.2

Configuration is fairly easy. Click on System Configuration and then Firewall. A screen will appear that is similar to figure 5.2. The modification and addition of rules is limited to certain services in this area. To have full control for any port, use the Menu Configuration Interface covered earlier in the manual.

To add a rule simply use the form at the top. Make the appropriate selections and click Commit. To delete a rule click on Delete and then OK when it asks if you are sure. It is recommended that you not delete any rules that are marked (FNGi) as these are used by First Network Group to gain access to the devices to assist you in troubleshooting or to repair problems, in the case that you have a maintenance contract.

IPv6 Built-in Firewall Configuration

IPv6, being a completely separate network stack, does require a completely separate set of firewall rules. To this end, we have added a new configuration area for allowing access to the DHCPatriot via IPv6 addressing. The IPv6 firewall, like the IPv4 firewall, is a white list firewall. All traffic not explicitly allowed is denied. The DHCPatriot system does automatically allow access to necessary services, such as DHCP, by clients in the configured networks on the system. All you have to worry about is allowing access to administrative services from administrative devices or subnets. This is easily done with the Firewallv6 area on the Web Administration Interface.

 This document © 2011 First Network Group Inc. All Rights Reserved

To configure the IPv6 firewall, open the Firewallv6 configuration by going to System Configuration -> Firewallv6. To add a rule, enter an IP address (or subnet in the form of 2001:db8:0:0::1/64), choose a service and add a note if desired. Click on Commit.

A list of the current firewall rules are shown at the bottom. Clicking Delete on any of these rules will remove them from the DHCPatriot system. Either adding or deleting will affect both devices in the system, not just the device you are administering.

System Logs

System logs are important for troubleshooting of DHCPatriot problems. All kinds of system logs are included here. These can be searched by generic text, daemon, host, administrator, and date/time parameters. Results can be further drilled down by using the limit displayed entries box. To open system logs, open the System Configuration menu and then click on System Logs. A screen similar to figure 5.3 will appear.

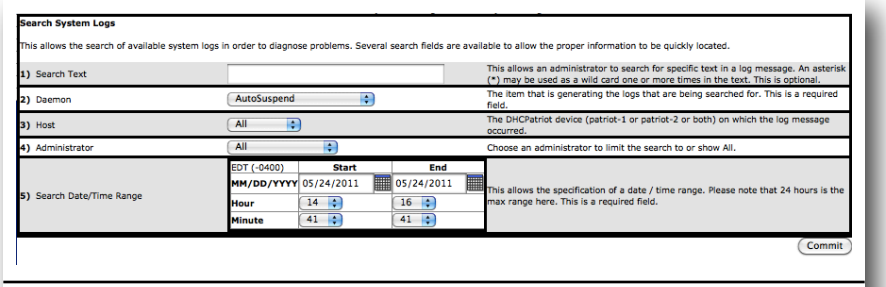


Figure 5.3

Select the appropriate entries and enter any text that is needed. Click on Commit and results will be shown below the form similar to figure 5.4. These results can be further limited by using the Limit Displayed entries box. The results are displayed in reverse chronological order. Twenty-five results are shown per page. There are page navigation buttons at the top of the results list (if there are multiple pages).

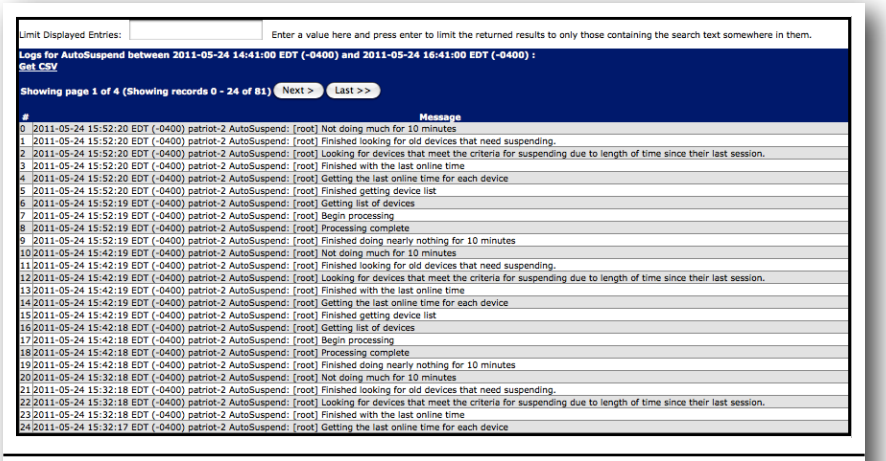


Figure 5.4

Changing Your 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

 This document © 2011 First Network Group Inc. All Rights Reserved

password example would be: fluffy The reason for this is that the 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 retype the desired password. Click the Commit button to complete the process. A success message will appear.

 This document © 2011 First Network Group Inc. All Rights Reserved

Chapter 6: Authenticated DHCP

Configuring Authenticated DHCP

Configuration of the DHCPatriot system for use with authenticated DHCP is slightly more involved than configuration for standard DHCP. The following sections outline each element that must be configured in order to use authenticated DHCP. Generally speaking: an Authentication server or servers must be specified; at least the default Captive Portal definition must be configured; a Shared Network must be setup; at least one Unauthenticated and one Authenticated subnet must be added. Instructions for each of these things follow as well as other less mandatory things related to authentication including report viewing. Not all topics are covered here as some are covered elsewhere in the manual in more appropriate sections.

Authentication Servers

There are two types of Authentication Servers, the internal (local) or built-in server, and an external RADIUS server.
These two types of servers are generally mutually exclusive, however, there is nothing preventing you from configuring both in some type of failover manner, or using one for authentication and the other for accounting records. To enter the Authentication server configuration area, expand the Auth DHCP Config menu and click on Authentication. You should get a screen that looks like figure 6.1.

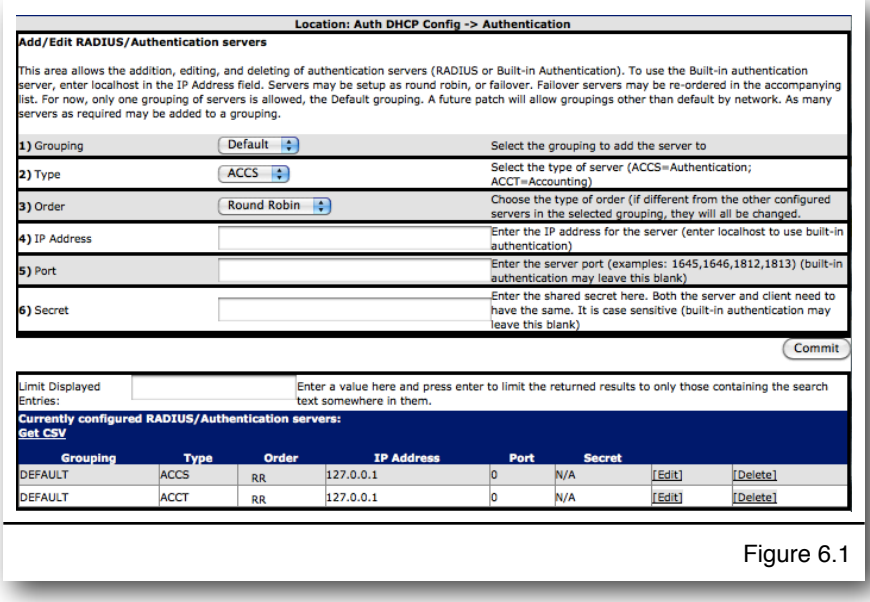


Figure 6.1

Please note that as of 5.3.0, two features have been addded. A new packet, interim-update (ALIVE) accounting packets can be sent from the DHCPatriot system to the RADIUS server. Turning this setting on in System Configuration -> General Setup will cause the DHCPatriot system to send an ALIVE packet each time the lease is renewed. This could be problematic on systems with many broken devices sending lots of renews rapidly. Secondly, forwarding of RADIUS accounting packets to one or more arbitrary destinations has been added. A new type of server (AFOR) has been added to the authentication setup. The DHCPatriot does not wait for an accounting response with these types of destinations. This feature can be used for sending accounting data to Sandvine or Procera traffic shapers or various CALEA devices, for example.

 This document © 2011 First Network Group Inc. All Rights Reserved

Internal (Built-in Authentication)

The DHCPatriot system makes provision for those who wish to use Authenticated DHCP but do not wish to use, or do not have an external RADIUS server. As many users as are needed may be entered directly on the DHCPatriot system (discussed later in the CSR section). Static IP Addresses can also be entered here so that a user will get the specified address.

To setup the DHCPatriot system to use Built-in Authentication, enter localhost in the IP Address box. There are two types of servers that are required for correct operation of the DHCPatriot system. Access and accounting. You may use the Built-in Authentication for either or both as needed. For example, you could setup localhost for the accounting and an external RADIUS server for the authentication if you do not wish to store the accounting records on your RADIUS server. When finished configuring click on Commit. Don't forget that users must be configured on the system before anyone will be able to authenticate. That process is covered later in the manual.

External

If the Built-in Authentication is not to be used, then an external RADIUS server must be used. You could also use a combination of an external RADIUS server as well as the Built-in Authentication as described in the Internal (Built-in Authentication) section. The DHCPatriot can also support multiple RADIUS servers in either a round robin or a failover configuration. You can setup multiples of each type of authentication server (access and accounting). You can specify whether they are round robin or failover. The DHCPatriot will randomly choose a server of each type in round robin mode, and will try until it finds a working server in the failover mode.

It is also possible to configure a RADIUS server for a specific shared network. The shared network must already be configured. In the grouping drop down, choose the shared network that you would like the RADIUS server to apply to. Please note that there must first be a default grouping before you can configure a specific RADIUS server. The RADIUS server will apply only to users using that specific shared network.

To configure each RADIUS server, choose the type of device that it is, then choose round robin or failover. Please note that you cannot mix and match round robin and failover in the same server type. Enter the IP Address, port and shared secret. Click commit. Repeat this process for all RADIUS servers to be added. Please note that if you only have one RADIUS server, you do not need to worry about the order.

Captive Portal

To properly authenticate users on the DHCPatriot system, it is required that at least the default captive portal configuration be made. This is necessary so that the authentication webpage can be shown to the user. To configure the Captive Portal,

 This document © 2011 First Network Group Inc. All Rights Reserved

open the 'Auth DHCP Config' menu and click on Captive Portal. A screen similar to figure 6.2 will be shown.

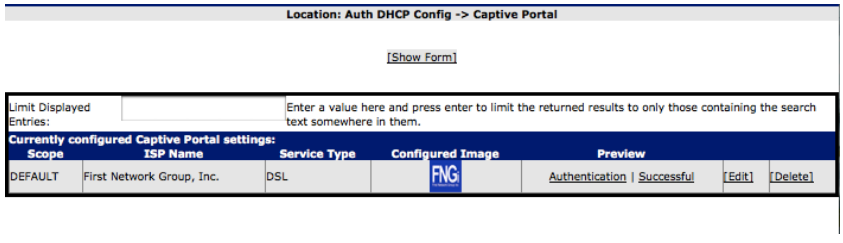


Figure 6.2

Please note that there is a special feature here as well. A default Captive Portal can be setup. Further, additional Captive Portal screens can be setup that are specific to other networks. If a network specific Captive Portal screen is configured, it will inherit all of the properties that were configured in the default Captive Portal. Only those items that are entered on the network specific Captive Portal screen will be changed when someone from that network retrieves it.

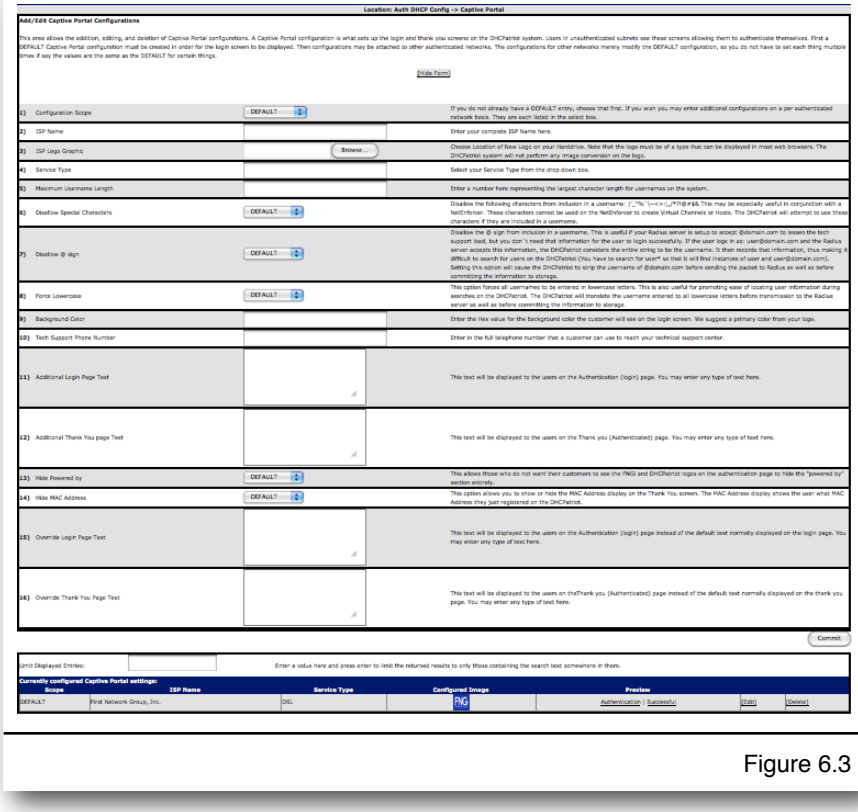


Figure 6.3

Any of the listings of Captive Portal definitions can be previewed to see what they look like to the customer. There are two parts to the screen, Authentication and Successful. Clicking either of these links in the desired Captive Portal definition will show a popup screen as shown in figure 6.4 and 6.5 respectively. Please note that these will not change until Commit has been clicked when editing.

A new feature was added in 5.3.0 that protects the DHCPatriot from automated clients overrunning the database/web server. This feature, called captive portal protection, may be enabled under System Configuration -> General Setup. This feature enables a simple math question that must be answered before the login page is displayed. As of 5.4.0, in the same area a new option has appeared that allows the captive portal protection page to be supplied by the administrator. It will need to contain a certain link or form to submit (as noted in the on-screen help) in order to function. This can be used if the math problem is not well received or a custom page is required.

Adding

 This document © 2011 First Network Group Inc. All Rights Reserved

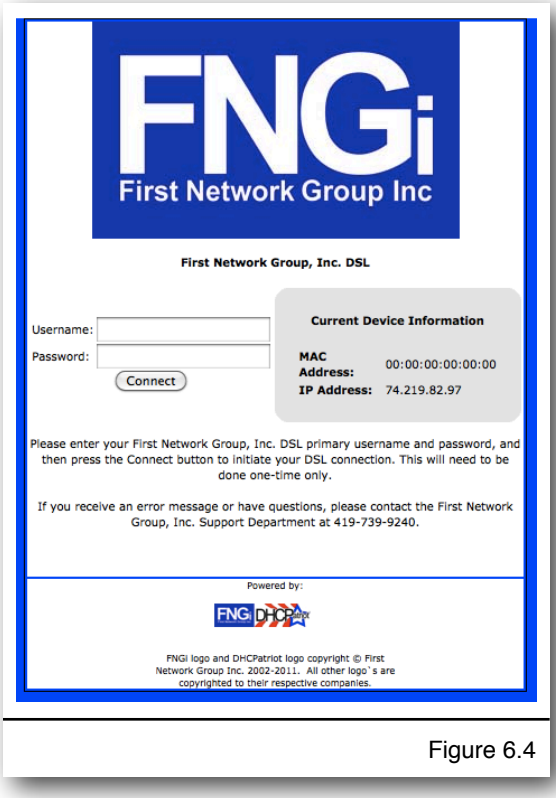


Figure 6.4

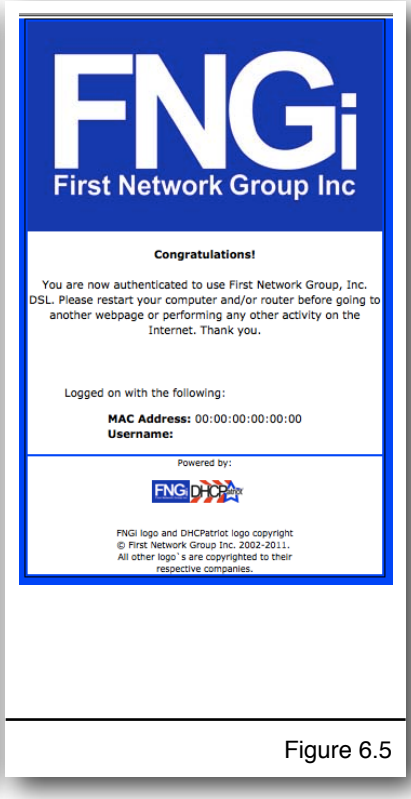


Figure 6.5

To add a new Captive Portal definition, click on the Show Form link. You should get a screen similar to figure 6.3. Elements on this form control how the Captive Portal appears to the customer. The onscreen descriptions of these elements should be sufficient to describe what effect each element has on the login and successful screens (figures 6.4 and 6.5).

Editing

To edit an existing Captive Portal definition, simply find the entry in the list of entries. Click on the edit link. The form will appear with entries from the chosen Captive Portal definition. Make whatever necessary changes, then click on Commit.

Removal

To remove a Captive Portal definition, find the desired entry in the list. Click on Delete. A popup will appear confirming that you really wish to remove the definition. Click on OK. The definition will be removed at that point.

Shared Network Configuration

The DHCPatriot system can support one or more authenticated DHCP networks. Each network can support one or more subnets in each subnet type. All that is required to have a functioning authenticated DHCP network is one Authenticated and one Unauthenticated DHCP subnet. The source network that the client device is based in is determined by the source address of the relay agent. Please note that a relay agent is a requirement to use the DHCPatriot. It does not support broadcast DHCP on the local LAN (local to the DHCPatriot), but rather requires that the traffic be relayed through a router or some other relay agent. Cisco devices become relay agents when the `ip helper address` directive is used.

Shared Network

 This document © 2011 First Network Group Inc. All Rights Reserved

To start each Authenticated Network, a Shared Network must be configured. The Shared Network provides an identifier, some basic settings and a framework for the subnets of the Authenticated Network.

Think of it as a container that will contain the subnets that will be configured. This keeps the networks and subnets well organized so that you can easily see what is happening with a particular network in the reports. It also provides the DHCPatriot with information regarding which subnets belong together so that it knows what IP addresses from which subnets to hand out to a particular client.

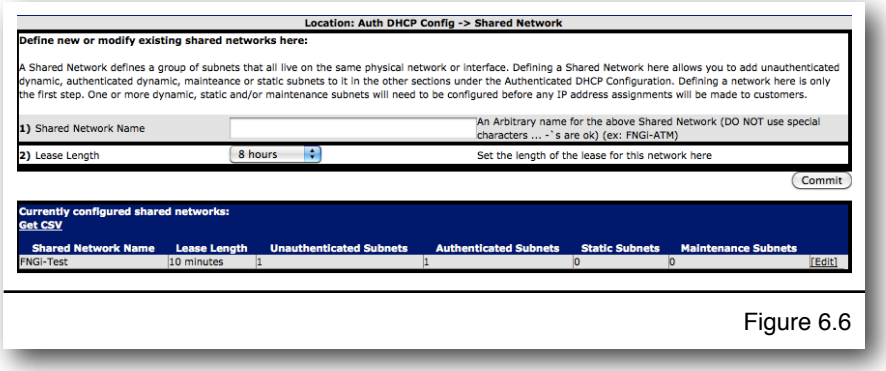


Figure 6.6

One or more Shared Network may be configured. To access the Shared Network Configuration, expand the Auth DHCP Config menu. Then click on Shared Network. Figure 6.6 shows what the Shared Network configuration screen looks like.

Adding

To add a Shared Network, simply choose a name of some type to identify the network. Please note that this name will appear throughout the interface as an identifier for the network. It is best to choose a descriptive name. The name can only contain dashes, underscores, and alpha-numeric characters. Choose the desired lease length. The default 8 hours is a good choice, but there are both higher and lower lengths available. DNS servers and NTP servers may also be set here. If these servers are set, they will override the default settings from General Settings for this particular Shared Network. Click Commit and the network should appear in the list at the bottom.

Editing

Editing a Shared Network consists of finding the network to be edited in the list, and clicking on Edit. The form will be populated with the appropriate values. Simply make any desired changes and click on Commit. The changes should be reflected in the list at that point.

Removal

To remove a Shared Network, click on Delete. A confirmation dialog will appear. Click on OK and the Shared Network will be removed. The delete link will not appear if there are subnets configured that are attached to the Shared Network container. The subnets need to be removed before the Shared Network can be removed.

 This document © 2011 First Network Group Inc. All Rights Reserved

Unauthenticated Subnet

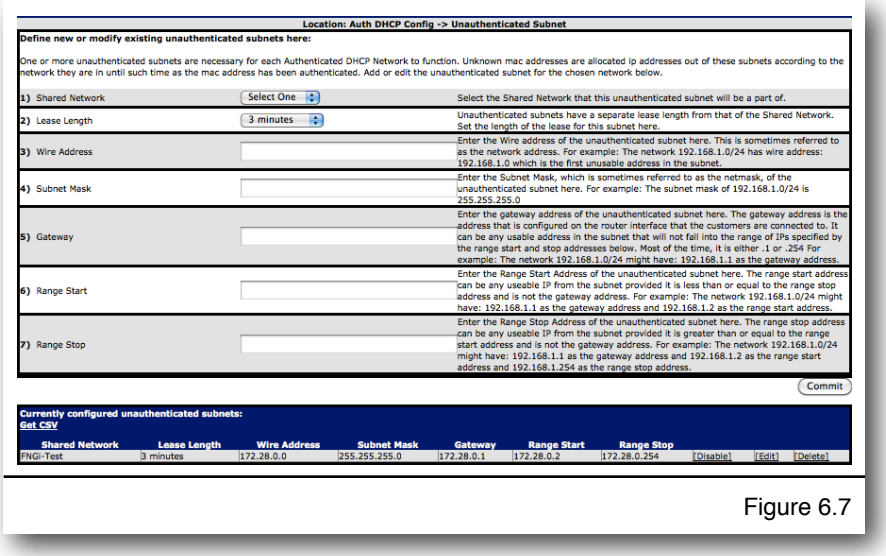


Figure 6.7

At least one Unauthenticated Subnet is required before a Shared Network is complete. This is the subnet that non-registered or suspended users will receive an IP Address from prior to registration. This subnet also requires policy routing to force the user to the login page.

One or more Unauthenticated Subnets may be configured. To access the Unauthenticated Subnet configuration, expand the Auth DHCP Config menu. Then click on Unauthenticated Subnet. Figure 6.7 shows what the Unauthenticated Subnet configuration screen looks like.

Adding

Choose the Shared Network that the Unauthenticated Subnet should be a part of. Choose an appropriate lease length. The default of three minutes is appropriate as after authentication, it will only take three minutes until the client gets an authenticated IP address, regardless of actions on the part of the end-user. Other lease lengths are available, however. Fill out the rest of the form according to the subnet values. On screen help is available if needed. Click on Commit, and a new subnet will appear in the list at the bottom of the screen.

Editing

This is much the same as adding. Click on the Edit link of the desired Unauthenticated Subnet and the form will be auto completed with the values from that choice. Make whatever changes are needed. Click on Commit to save the changes. The changes should be reflected in the list at that point.

Disable

An unauthenticated subnet can also be disabled. Possible reasons for doing this are to numerous to list here. A disabled subnet will no longer be available for leasing of IP Addresses. It will still show up in the reports along with any users who currently have an IP Address out of the subnet but the users will no longer be able to renew this IP Address so they will move to a different available subnet, if any.

 This document © 2011 First Network Group Inc. All Rights Reserved

Removal

To remove a subnet, click on the Delete link. A confirmation dialogue will appear. Click OK and the subnet should be removed.

Authenticated Subnet

At least one authenticated subnet is required before a shared network is complete. These subnets are what customers will receive IP Addresses from after authenticating themselves initially. To access Authenticated Subnet configuration, expand the Auth DHCP Config menu. Click on Authenticated Subnet in the resulting list. A screen similar to figure 6.8 should appear.

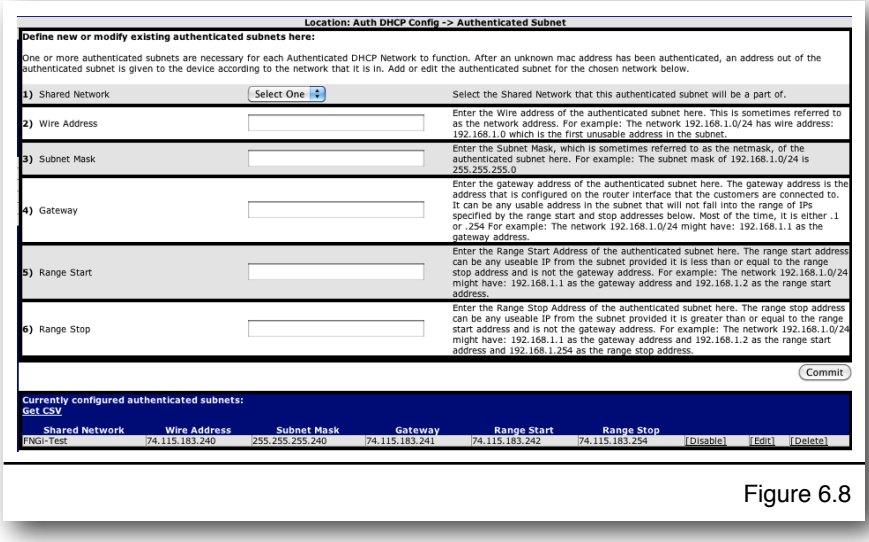


Figure 6.8

Adding

To add an authenticated subnet, choose the shared network that the subnet will be part of. Complete the rest of the form shown in figure 6.8. On screen help is available if needed, but it should be pretty straight forward. Click on Commit.

Editing

This is much the same as adding. Click on the Edit link of the desired Authenticated Subnet and the form will be auto completed with the values from that choice. Make whatever changes are needed. Click on Commit to save the changes. The changes should be reflected in the list at that point.

Disable

An authenticated subnet can also be disabled. Possible reasons for doing this are to numerous to list here. A disabled subnet will no longer be available for leasing of IP Addresses. It will still show up in the reports along with any users who currently have an IP Address out of the subnet but the users will no longer be able to renew this IP Address so they will move to a different available subnet, if any.

 This document © 2011 First Network Group Inc. All Rights Reserved

Removal

To remove a subnet, click on the Delete link. A confirmation dialogue will appear. Click OK and the subnet should be removed.

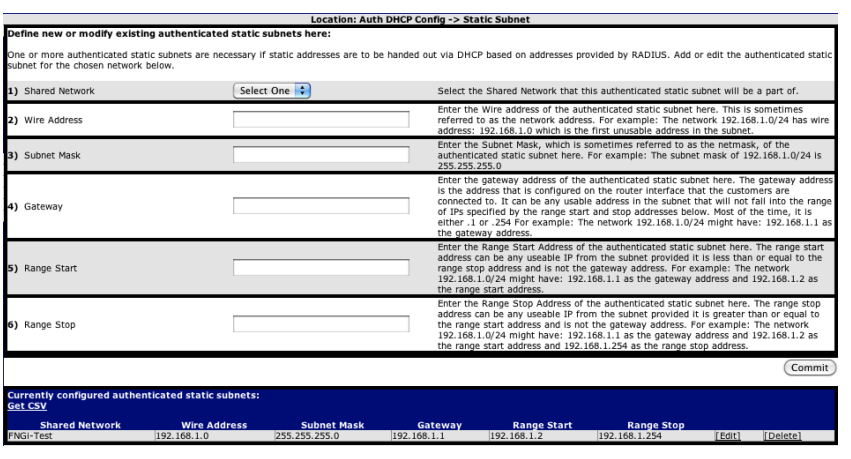


Figure 6.9

Static Subnet

A static subnet is an optional subnet that would be used for devices that are to be at a specific IP address, and are to be associated with this address by username. The address is associated with the DHCPatriot system by RADIUS or the Built-in Authentication. Specifically, the Framed-Address attribute (8) should contain the static address to be handed to the customer. The Built-in Authentication handles this for you when a static address is configured. An external RADIUS server will likely require some modification to support this. The address must be part of a static subnet that was configured in this area. To access the static subnet configuration, expand the Auth DHCP Config menu, then click on Static Subnet. A screen similar to that shown in figure 6.9 should appear.

Adding

Choose the Shared Network that the Static Subnet should be a part of. Fill out the rest of the form according to the subnet values. On screen help is available if needed. Click on Commit, and a new subnet will appear in the list at the bottom of the screen.

Editing

This is much the same as adding. Click on the Edit link of the desired Static Subnet and the form will be auto completed with the values from that choice. Make whatever changes are needed. Click on Commit to save the changes. The changes should be reflected in the list at that point.

Removal

To remove a subnet, click on the Delete link. A confirmation dialogue will appear. Click OK and the subnet should be removed.

 This document © 2011 First Network Group Inc. All Rights Reserved

Maintenance Subnet

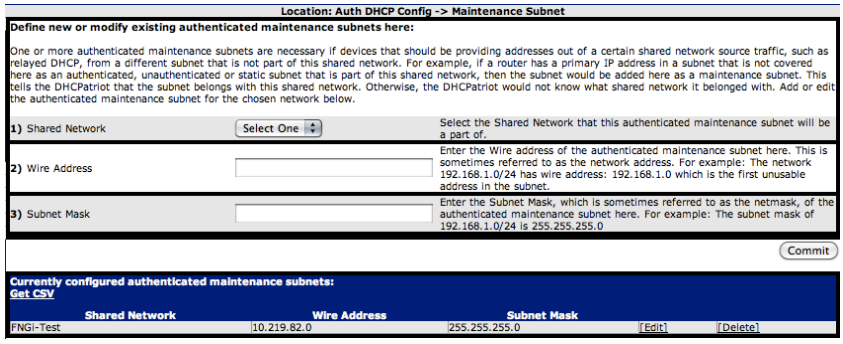


Figure 6.10

A maintenance subnet is used to define a subnet that a DHCP relay agent may talk from but that is not part of any DHCP pool in the given network.

For example, a Cisco router may be set up as a DHCP relay agent by having ip helper-address configured on an ethernet interface facing customers. If the primary IP address on that ethernet interface is NOT part of a DHCP pool for use by those customers, the relayed traffic will not be known to the DHCPatriot system as it is part of no subnets that it has configured. Hence, we add the subnet that the aforementioned IP address is part of as a maintenance subnet on the DHCPatriot system attached to the network in question. That way the DHCPatriot system knows that when it gets relayed DHCP from any IP in that maintenance subnet that it goes with the attached network.

To access the configuration screen for maintenance subnet as shown in figure 6.10, simply expand the Auth DHCP Config menu, and click on Maintenance Subnet. A screen similar to the one in figure 6.10 should appear. On this screen, you can add, edit or delete maintenance subnets.

Adding

To add a maintenance subnet to a network, first choose the Shared Network that the subnet will be attached to. Then type the wire address of the subnet. Enter the subnet mask. Then click on Commit. On screen help is available if you are unsure how to complete the form.

Editing

To edit a maintenance subnet, simply click Edit on the desired subnet in the list at the bottom. The form will be populated with the current values. Make changes as necessary and then click on Commit.

Removal

To delete a maintenance subnet, click on the Delete link of the subnet you wish to delete in the list at the bottom. A confirmation dialog will appear. Click OK to delete the subnet, or click Cancel to not delete and return to the list and form.

Special Reports

 This document © 2011 First Network Group Inc. All Rights Reserved

There are multiple reports pertaining to Authenticated DHCP. Not all will be covered here as some are shared with Standard DHCP. Those will be covered in a later unified section. The reports covered below are exclusive to Authenticated DHCP.

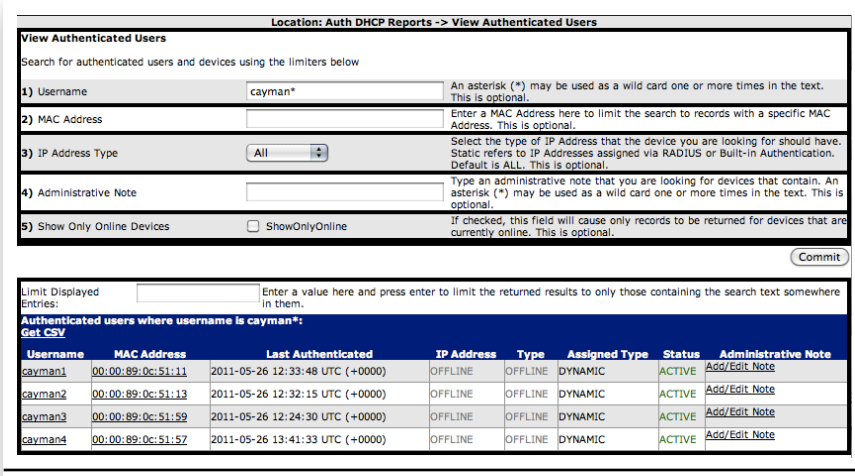


Figure 6.11

View Authenticated Users

The View Authenticated Users report allows you to search for users that have been authenticated under authenticated DHCP on the DHCPatriot system. Users may be searched by username, mac address, IP address type (ALL, Static, and Dynamic), Administrative note, and can be limited to only currently online users. These limiters may be combined in any way you wish. Usernames can have a * as a wildcard so that multiple similar results can be shown (as seen in figure 6.11). The output gives important information such as the username, MAC address, and the last authenticated date and time (the last time the user typed their username and password at the authentication window). It also shows the current IP address and type if the user is currently online. It also notes whether the user or device is assigned a static IP address. Status tells whether their account is active, and administrative note is available and can be edited here for notes about the device.

Users Using Multiple IPs

Users using multiple IPs is very similar to View Authenticated Users. The report is not searchable other than the usual limit displayed entries box. It appears very similar to the list at the bottom of figure 6.11. It lacks a form as shown in figure 6.11. It specifically shows a list of user devices where the username is using multiple IPs. The same columns appear and have the same function. It has one additional column, IP #, which counts up the number of IPs in use by each username. Some ISPs need this report so that they can find violators of simultaneous use restrictions.

 This document © 2011 First Network Group Inc. All Rights Reserved

Chapter 7: Standard DHCP

Standard DHCP, as defined by FNGi, means a more traditional form of DHCP without authentication. It also supports things like delivering boot files via TFTP and static assignments by option 82. Dynamic subnets can be restricted to only known clients. It is meant for use with cable modems, ONT devices, set top boxes and the like. It can be used for end-customer devices as well if that is desired over Authenticated DHCP. Standard DHCP is also configured with high availability just like Authenticated DHCP. All services are redundant under this configuration (TFTP, DHCP etc...). Please note that the DHCPatriot does contain a built-in TFTP server. An external TFTP server may also be used, if desired.

Shared Network Configuration

At least one Shared Network, and one subnet of dynamic or static types is required to have a functioning Standard DHCP network. Instructions for configuration of each type follow. Please note that a relay agent is a requirement to use the DHCPatriot. It does not support broadcast DHCP on the local LAN (local to the DHCPatriot), but rather requires that the traffic be relayed through a router or some other relay agent. Cisco devices become relay agents when the `ip helper address` directive is used.

Shared Network

To start each Standard Network, a Shared Network must be configured. The Shared Network provides an identifier, some basic settings and a framework for the subnets of the Standard Network.

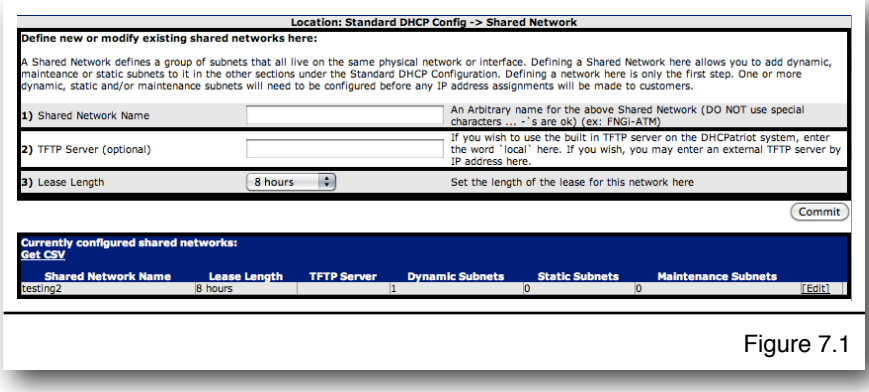


Figure 7.1

Think of it as a container that will contain the subnets that will be configured. This keeps the networks and subnets well organized so that you can easily see what is happening with a particular network in the reports. It also provides the DHCPatriot with information regarding which subnets belong together so that it knows what IP addresses from which subnets to hand out to a particular client.

One or more Shared Network may be configured. To access the Shared Network Configuration, expand the Auth DHCP Config menu. Then click on Shared Network. Figure 7.1 shows what the Shared Network configuration screen looks like.

 This document © 2011 First Network Group Inc. All Rights Reserved

Adding

To add a Shared Network, simply choose a name of some type to identify the network. Please note that this name will appear throughout the interface as an identifier for the network. It is best to choose a descriptive name. The name can only contain dashes, underscores, and alpha-numeric characters. Choose the desired lease length. The default 8 hours is a good choice, but there are both higher and lower lengths available. It is also possible to add DNS and NTP servers to the Shared Network. If these are added, they will override the default settings from General Settings. Click Commit and the network should appear in the list at the bottom.

Editing

Editing a Shared Network consists of finding the network to be edited in the list, and clicking on Edit. The form will be populated with the appropriate values. Simply make any desired changes and click on Commit. The changes should be reflected in the list at that point.

Removal

To remove a Shared Network, click on Delete. A confirmation dialog will appear. Click on OK and the Shared Network will be removed. The delete link will not appear if there are subnets configured that are attached to the Shared Network container. The subnets need to be removed before the Shared Network can be removed.

Dynamic Subnet

At least one Dynamic or Static Subnet is required before a Shared Network is complete. This is the subnet that non-registered or suspended users will receive an IP Address from prior to registration.

If allow only known clients is selected for the dynamic subnet, then known clients must be added with the Known Client editor which is covered later in the manual. If the clients are not added then they will not be able to use the subnet.

One or more Dynamic Subnets

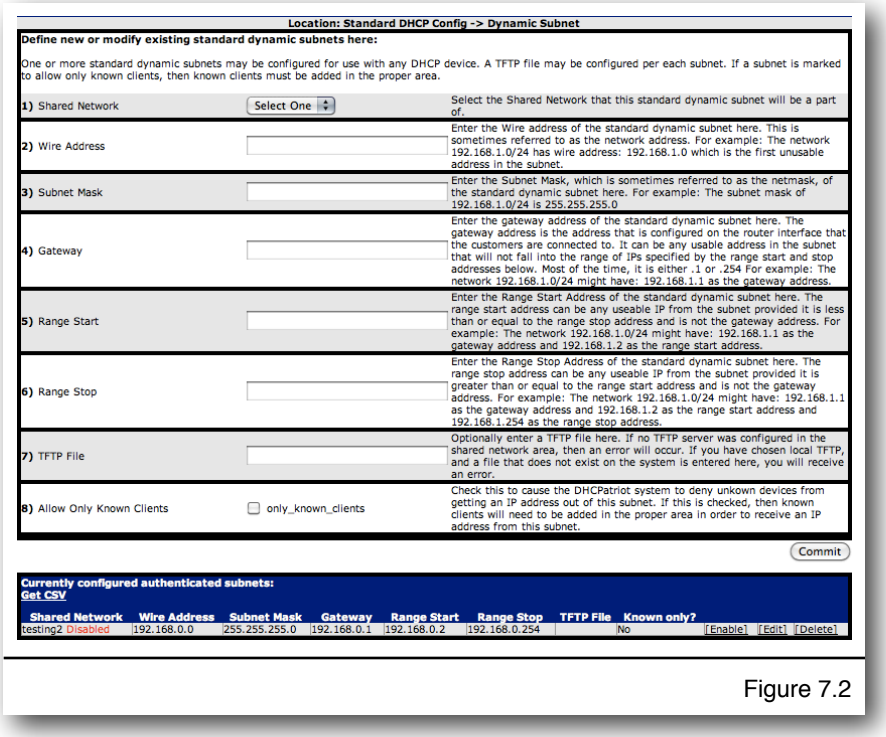


Figure 7.2

 This document © 2011 First Network Group Inc. All Rights Reserved

may be configured. To access the Dynamic Subnet configuration, expand the Standard DHCP Config menu. Then click on Dynamic Subnet. Figure 7.2 shows what the Dynamic Subnet configuration screen looks like.

Adding

Choose the Shared Network that the Dynamic Subnet should be a part of. Fill out the rest of the form according to the subnet values. On screen help is available if needed. Click on Commit, and a new subnet will appear in the list at the bottom of the screen.

Editing

This is much the same as adding. Click on the Edit link of the desired Dynamic Subnet and the form will be auto completed with the values from that choice. Make whatever changes are needed. Click on Commit to save the changes. The changes should be reflected in the list at that point.

Disable

A dynamic subnet can also be disabled. Possible reasons for doing this are to numerous to list here. A disabled subnet will no longer be available for leasing of IP Addresses. It will still show up in the reports along with any users who currently have an IP Address out of the subnet but the users will no longer be able to renew this IP Address so they will move to a different available subnet, if any.

Removal

To remove a subnet, click on the Delete link. A confirmation dialogue will appear. Click OK and the subnet should be removed.

Static Subnet

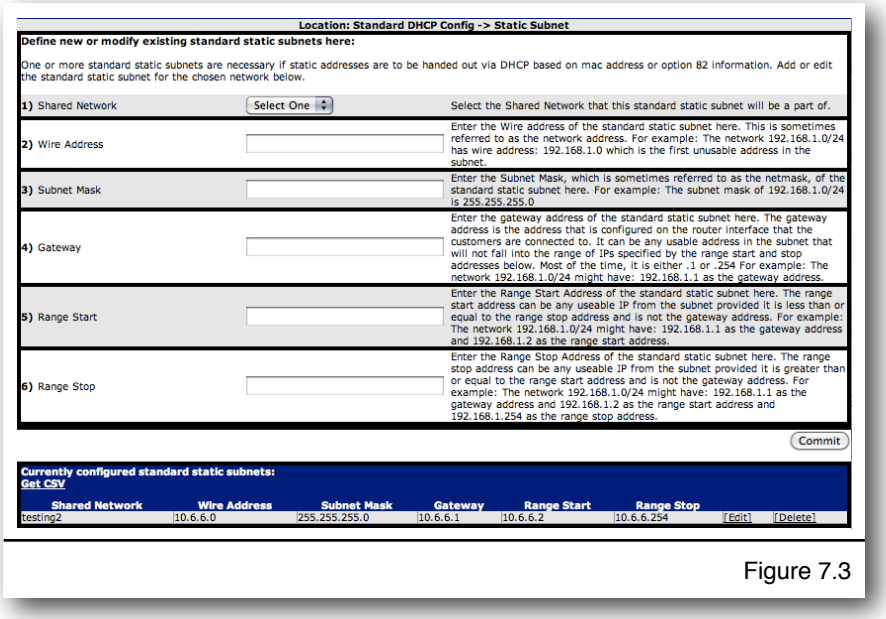


Figure 7.3

A static subnet is an optional subnet that would be used for devices that are to be at a specific IP address, and are to be associated with this address by some means such as MAC address or option 82 information. Devices can be assigned to a static address under Static IP Assignment covered later in the manual. To access the static subnet configuration, expand the Standard DHCP Config menu, then click on Static Subnet. A screen similar to that shown in figure 7.3 should appear.

 This document © 2011 First Network Group Inc. All Rights Reserved

Adding

Choose the Shared Network that the Static Subnet should be a part of. Fill out the rest of the form according to the subnet values. On screen help is available if needed. Click on Commit, and a new subnet will appear in the list at the bottom of the screen.

Editing

This is much the same as adding. Click on the Edit link of the desired Static Subnet and the form will be auto completed with the values from that choice. Make whatever changes are needed. Click on Commit to save the changes. The changes should be reflected in the list at that point.

Removal

To remove a subnet, click on the Delete link. A confirmation dialogue will appear. Click OK and the subnet should be removed.

Maintenance Subnet

A maintenance subnet is used to define a subnet that a DHCP relay agent may talk from but that is not part of any DHCP pool in the given network.

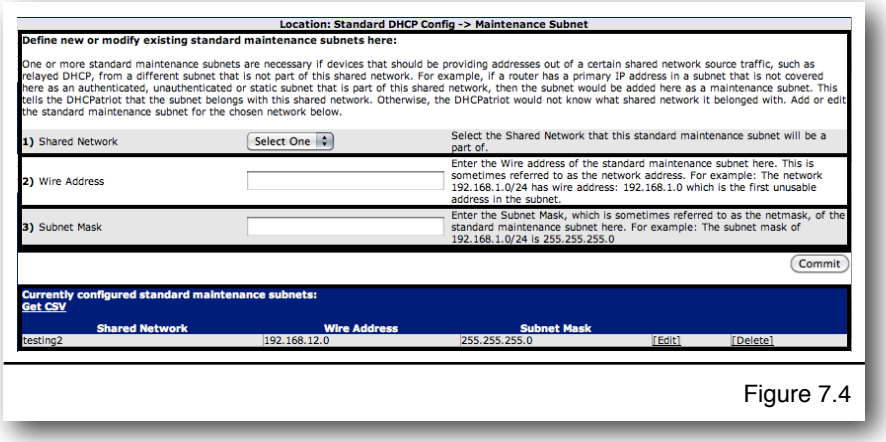


Figure 7.4

For example, a Cisco router may be set up as a DHCP relay agent by having ip helper-address configured on an ethernet interface facing client devices. If the primary IP address on that ethernet interface is NOT part of a DHCP pool for use by those client devices, the relayed traffic will not be known to the DHCPatriot system as it is part of no subnets that it has configured. Hence, we add the subnet that the aforementioned IP address is part of as a maintenance subnet on the DHCPatriot system attached to the network in question. That way the DHCPatriot system knows that when it gets relayed DHCP from any IP in that maintenance subnet that it goes with the attached network.

To access the configuration screen for maintenance subnet as shown in figure 7.4, simply expand the Standard DHCP Config menu, and click on Maintenance Subnet. A screen similar to the one in figure 7.4 should appear. On this screen, you can add, edit or delete maintenance subnets.

 This document © 2011 First Network Group Inc. All Rights Reserved

Adding

To add a maintenance subnet to a network, first choose the Shared Network that the subnet will be attached to. Then type the wire address of the subnet. Enter the subnet mask. Then click on Commit. On screen help is available if you are unsure how to complete the form.

Editing

To edit a maintenance subnet, simply click Edit on the desired subnet in the list at the bottom. The form will be populated with the current values. Make changes as necessary and then click on Commit.

Removal

To delete a maintenance subnet, click on the Delete link of the subnet you wish to delete in the list at the bottom. A confirmation dialog will appear. Click OK to delete the subnet, or click Cancel to not delete and return to the list and form.

Additional Configuration Tasks

The Standard DHCP Actions menu contains several tasks that will be covered here. They are covered here because it is assumed that systems administrators will be performing these tasks as opposed to tech support or customer service. We thave grouped tasks common to those disciplines later in the manual.

There is also a Standard DHCP Reports menu section with some reports in it. These reports are common to both Authenticated and Standard DHCP and therefore are covered in the same section later in the manual.

Known Client

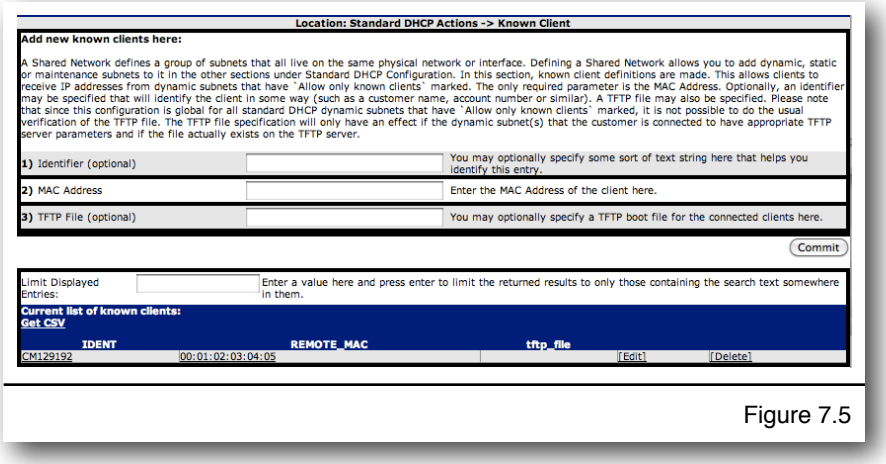


Figure 7.5

If one or more of your dynamic subnets have been configured to allow only known clients, then said known clients must be configured here before they will be able to obtain an IP address. Clients that are not configured here will not be able to obtain an IP address unless another dynamic subnet exists that does not have allow only known clients checked. A mixture of known clients and static IP assignments could also exist. Some may find this

 This document © 2011 First Network Group Inc. All Rights Reserved

useful, particularly cable modem operators, so that a client cable modem could be suspended in case of non-pay.

Adding

To add a new known client, simply enter an identifier (if desired) the MAC address, and a TFTP file (if necessary). Click on Commit.

Editing

To edit a known client entry, simply click on Edit. The form will be populated with the information from the existing entry. Make the necessary changes then click on Commit.

Removal

To remove a known client entry, click on the Delete link. A confirmation dialog will appear. Answer OK and the entry will be deleted.

Static IP Assignment

If Standard Static networks have been configured, user devices will need to be assigned to some IP address. Static IP Assignment is the place to do that. IP Addresses can be assigned based on MAC Address or Option 82 information. Option 82 circuit-id or remote-id can be used to match the client. In addition a TFTP file may optionally be specified.

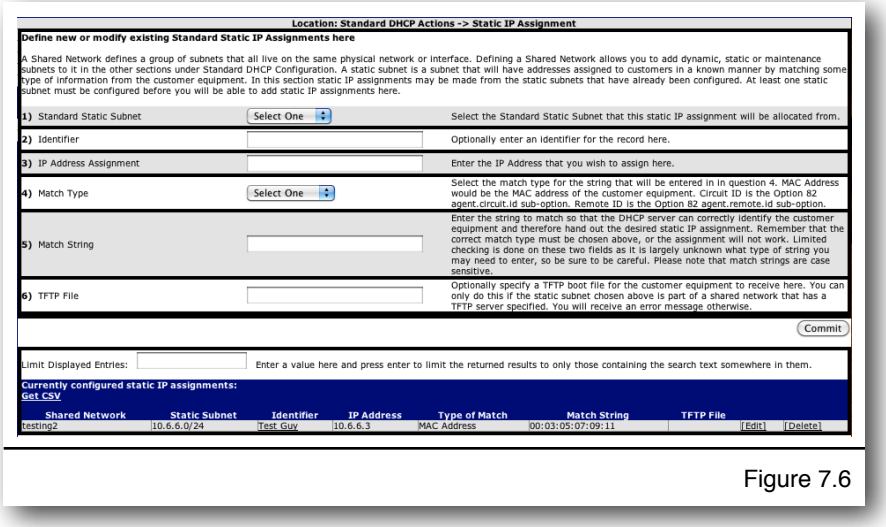


Figure 7.6

To access Static IP Assignment, expand the Standard DHCP Actions menu. Click on Static IP Assignment. A screen similar to figure 7.6 should appear.

Adding

To add an assignment of a static IP address to a client, complete the form and click on Commit. Start by selecting a static subnet to assign from. Optionally type an identifier. Type the IP address that should be assigned. Select the type of match (MAC address, Circuit ID or Remote ID - note that Circuit ID and Remote ID require the option 82 information to be present in the DHCP packets). The match string is either the MAC address or the option 82 information to be matched. Optionally specify a TFTP file, but

 This document © 2011 First Network Group Inc. All Rights Reserved

only if you have set a TFTP server when configuring the shared network container. Then click on Commit. A new entry should appear in the list at the bottom.

Please note that as of 5.3.0 it is possible to perform a mass add of static assignments in this same area. There is a link in the description to click to show the scripted mass add form. Follow the on-screen instructions to perform a mass add of static entries.

Editing

To edit an assignment, find the assignment that you wish to load in the list at the bottom, and click on the Edit link. The form should be populated with the data from the selected entry. Make changes to the entry as necessary, then click on Commit. Your changes should be reflected in the list below.

Removal

To remove an entry, find it in the list at the bottom, then click the Delete link. Confirm that you wish to delete the entry. The entry should disappear from the list.

TFTP File Maintenance

The DHCPatriot has a built-in TFTP server that may be used in conjunction with client's that need a boot file or configuration file of some kind. If a TFTP server was specified in the Shared Network configuration, and was further specified as 'local' meaning that the DHCPatriot itself is to be used, then some files must be uploaded to the DHCPatriot system for them to be handed to clients.

Although the DHCPatriot will allow you to upload files of any type of name including special characters and spaces, such as 'T%!@# boot file.cfg', it is best to stick with alpha numeric characters and no spaces. You can safely use dashes and underscores. This just avoids problems with the client / server TFTP conversation.

The list at the bottom gives you file size, date last modified, and an MD5 sum that may be used to verify the integrity of the file. Simply record this information somewhere when you upload the file, and you can check the list at any time to make sure that the file has not changed.

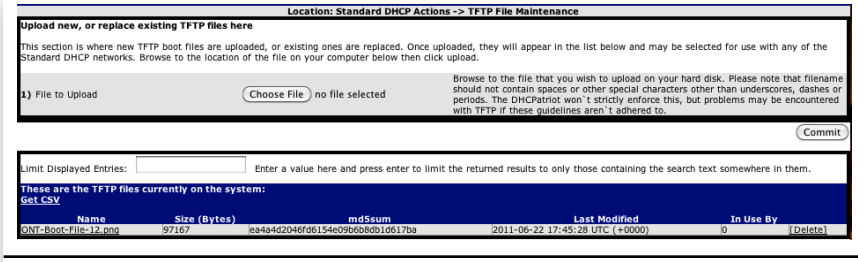


Figure 7.7

To access TFTP File Maintenance, expand the Standard DHCP Actions menu, and click on TFTP File Maintenance. A screen similar to figure 7.7 should appear.

 This document © 2011 First Network Group Inc. All Rights Reserved

Adding

To add a new file, locate the file on your PC, and make sure it is named appropriately. Click on Browse or Choose file and locate the file on your PC. Click on Commit and your file should be uploaded. It may take some time depending on the size of the file. It is a good idea to copy down the file size, date last modified and MD5 sum from the list after the file appears there, this can be used to verify file integrity later.

Mass Change of TFTP File Assignments

It is also possible to mass change TFTP file assignments. This form appears between the interface for adding a TFTP file and the list of currently present TFTP files. Simply put in the current file name. Then the name you would like it changed to and press commit. It will allow you to confirm by showing you what is going to be changed and asking if you are sure. This feature lets you change an assignment to a different file without visiting every single instance that is assigned to the file in both Known Client and Static IP Assignment.

Editing

To edit a file, make your changes to the file on your PC. Make sure the name is the same of the file you wish to edit. Then click on Browse or Choose file and locate the file on your PC. Click on Commit. Your modified file will replace the current file. The list at the bottom should display a different MD5 sum and date modified at the least. It may also have a different file size.

Removal

To remove a file, make sure it is not in use by any client designations or subnets. Click on the Delete link. Confirm that you wish to delete the file. The file should disappear from the list at the bottom.

 This document © 2011 First Network Group Inc. All Rights Reserved

Chapter 8: Common Authenticated and Standard DHCP Actions and Reports

Several reports and actions are common to both Authenticated and Standard DHCP. These are detailed here.

Sticky IP Address

A Sticky IP Address is an address that can be pinned to a client by either username or MAC Address (Except in Standard DHCP where only the MAC Address can be used). This is useful for either quickly pinning someone to a specific address, in the case where not enough subnets are available to dedicate a subnet for specific static address usage, or in the case where only a very small amount of users will be pinned to a specific address.

To access the Sticky IP Address settings, expand either the Auth DHCP Config or Standard DHCP Config menus and click on Sticky IP Address. A screen similar to figure 8.1 should appear. Please note that the username field will not be available if accessed from Standard DHCP.

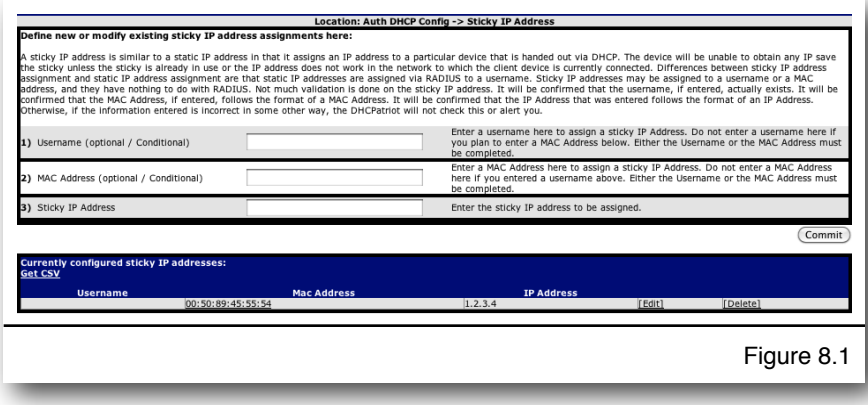


Figure 8.1

Please note that as of 5.3.0, static IP addresses assigned via RADIUS now show up in this list. They can be deleted only. If they are still assigned to the user in RADIUS (or the built-in authentication) they will likely reappear in the future.

Adding

To add a sticky IP address entry, fill out either the username or mac address fields and enter the IP Address. An optional note can be entered. Click on Commit. The new entry should appear in the list.

Editing

Find the entry in the list at the bottom that you wish to edit. Click on the Edit link. The form should be populated with the values from the entry. Make whatever changes are necessary. Click on Commit. The changes should be reflected in the list at the bottom.

 This document © 2011 First Network Group Inc. All Rights Reserved

Removal

To remove an entry, find the appropriate entry in the list at the bottom and click on the Delete link. Confirm that you wish to delete the entry. The entry should no longer appear at the bottom.

Exclude IP Address

Excluding an IP address allows you to disallow one or more addresses from various pools on your DHCP server. For example, it may be that you need to place some equipment in the client network that doesn't support DHCP. Using Exclude IP Address, you can exclude the IP address that you decide to assign to this equipment. This gives you the freedom to assign any address you like without having to modify any DHCP pools. The excluded IP address will not be handed to clients by the DHCP server at all.

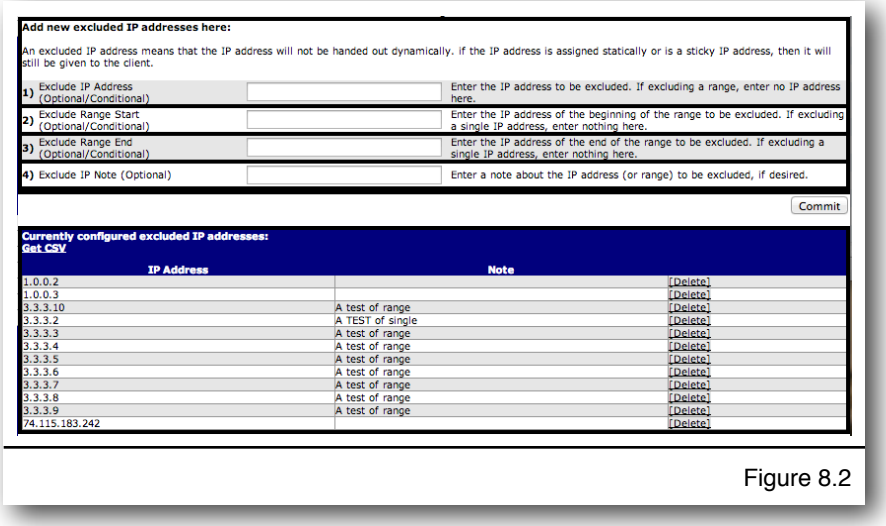


Figure 8.2

To access Exclude IP Address, expand either the Auth DHCP Config or the Standard DHCP Config menu. Click on Exclude IP Address. A screen similar to figure 8.2 should appear.

Adding

To add an IP Address to the list, simply type the IP address into the field and click on Commit. NOTE: An optional note can be entered. The address should appear at the bottom. As of 5.4.0, a range of IP addresses may be excluded instead of a single IP.

Removal

To remove an excluded IP address, find the appropriate entry in the list at the bottom. Click on the Delete link. Confirm that you are sure that you would like to remove it. At that point, the IP address should no longer appear in the list.

 This document © 2011 First Network Group Inc. All Rights Reserved

Deny Mac Address

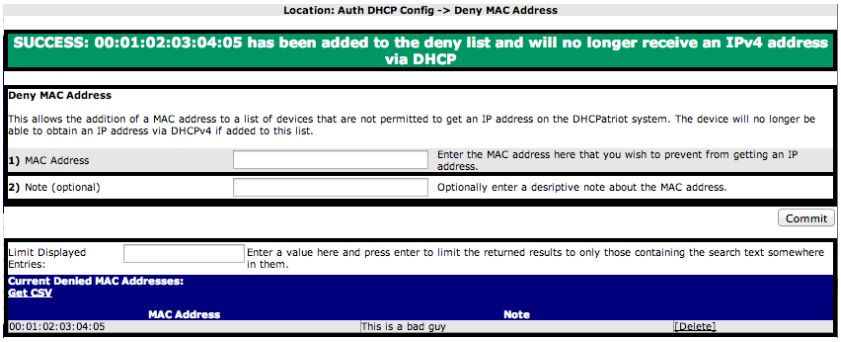


Figure 8.3

This function, located under the Auth DHCP Config or Standard DHCP Config menus, allows and administrator to stop a certain device, by MAC address, from getting an IPv4 address via DHCP. Situations where this might be useful are many and varied. It is up to the administrator to determine when this function should be used.

Adding a MAC address to this list will cause the DHCP server to no longer respond to DHCPv4 requests from the device. Access this function by expanding either the Auth DHCP Config or Standard DHCP Config menus and clicking on Deny MAC Address. A screen similar to figure 8.3 should appear. Use this screen to add devices to, remove devices from, and view devices in the list of denied MAC addresses. A note can be included so that it can be remembered why the device was denied access. On screen help is available for the various functions should you need it.

View Address Usage

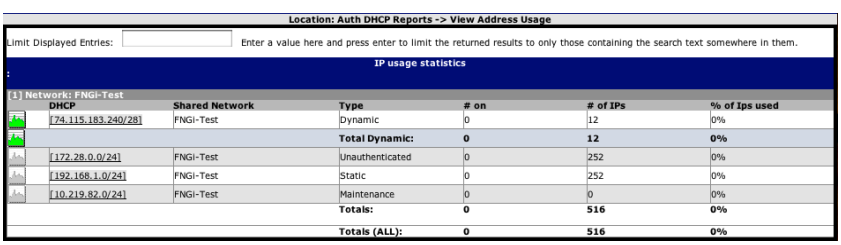


Figure 8.4

The DHCPatriot system makes it easy to confirm the current and past status of the networks and subnets configured on the system. The View Address Usage report located in both the authenticated and standard DHCP sections reports current address usage values. It also has a graph feature that allows the administrator to check address usage for up to the past year.

View address usage is available in both Authenticated DHCP Reports and Standard DHCP Reports. To view the report, expand one of those menus (depending on which type of address usage you wish to view) and click on View Address Usage. A screen similar to figure 8.4 will appear. On this screen, each configured subnet can be viewed laid out by network. The number of IP Addresses currently in use, the max available and the percentage of maximum can be

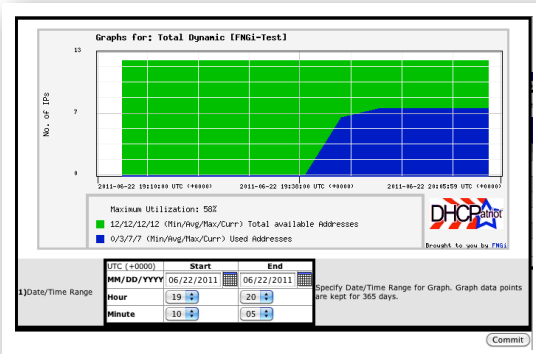
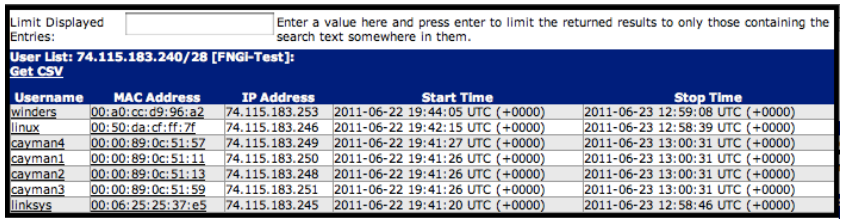


Figure 8.5

 This document © 2011 First Network Group Inc. All Rights Reserved

seen here. Each subnet has individual numbers. In addition, a total dynamic line is shown for each network. This is particularly useful when multiple dynamic subnets make up a network.

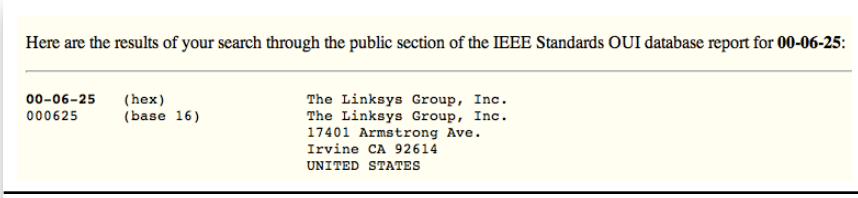

Limit Displayed Entries: Enter a value here and press enter to limit the returned results to only those containing the search text somewhere in them.

User List: 74.115.183.240/28 [FNGI-Test]:
Get CSV

Username	MAC Address	IP Address	Start Time	Stop Time
winders	00:a0:cc:d9:96:a2	74.115.183.253	2011-06-22 19:44:05 UTC (+0000)	2011-06-23 12:59:08 UTC (+0000)
linux	00:50:da:cf:ff:7f	74.115.183.246	2011-06-22 19:42:15 UTC (+0000)	2011-06-23 12:58:39 UTC (+0000)
cayman4	00:00:89:0c:51:57	74.115.183.249	2011-06-22 19:41:27 UTC (+0000)	2011-06-23 13:00:31 UTC (+0000)
cayman1	00:00:89:0c:51:11	74.115.183.250	2011-06-22 19:41:26 UTC (+0000)	2011-06-23 13:00:31 UTC (+0000)
cayman2	00:00:89:0c:51:13	74.115.183.248	2011-06-22 19:41:26 UTC (+0000)	2011-06-23 13:00:31 UTC (+0000)
cayman3	00:00:89:0c:51:59	74.115.183.251	2011-06-22 19:41:26 UTC (+0000)	2011-06-23 13:00:31 UTC (+0000)
linksys	00:06:25:25:37:e5	74.115.183.245	2011-06-22 19:41:20 UTC (+0000)	2011-06-23 12:58:46 UTC (+0000)

Figure 8.6

Each line also contains an icon on the far left that allows showing graphs of address usage in the past. These graphs have five minute average resolutions. Only those icons that are green contain graph data. Non-dynamic, and non-authenticated subnets are not tracked. To view a graph, click on the appropriate graph link. A screen similar to figure 8.5 will appear. Here, the total number of addresses available is represented by the green shading. The blue shading shows the address usage. Additionally, statistics regarding maximum percentage and other stats are shown for each at the bottom. The default time period is the last 24 hours, however this time period may be changed using the date form shown in figure 8.5.

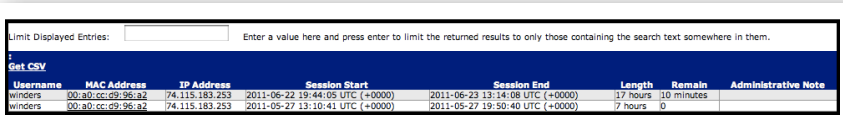

Here are the results of your search through the public section of the IEEE Standards OUI database report for **00-06-25**:

00-06-25 (hex) The Linksys Group, Inc.
000625 (base 16) The Linksys Group, Inc.
17401 Armstrong Ave.
Irvine CA 92614
UNITED STATES

Figure 8.7

Back on the View Address Usage screen, you'll notice that each subnet is clickable. Clicking a subnet will bring up a screen similar to figure 8.6. This screen shows a list of devices that currently are using an IP address. The lease start and end are shown here as well as the IP address, MAC address and username (if available). Clicking on the MAC address will show who manufactured the device according to the IEEE database as shown in figure 8.7. Clicking a username will show a list of the past sessions for that user as shown in figure 8.8.

Search Sessions


Limit Displayed Entries: Enter a value here and press enter to limit the returned results to only those containing the search text somewhere in them.

Get CSV

Username	MAC Address	IP Address	Session Start	Session End	Length	Remain	Administrative Note
winders	00:a0:cc:d9:96:a2	74.115.183.253	2011-06-22 19:44:05 UTC (+0000)	2011-06-23 13:14:08 UTC (+0000)	17 hours	10 minutes	
winders	00:a0:cc:d9:96:a2	74.115.183.253	2011-05-27 13:10:41 UTC (+0000)	2011-05-27 19:50:40 UTC (+0000)	7 hours	0	

Figure 8.8

A key feature of the DHCPatriot system is the ability to search sessions both present and past. There is no time limit to the storage of old sessions with virtually all systems containing sessions dating back to the original date of deployment.

These sessions are searchable by date and time, username, MAC address, IP address, and limiting by only online sessions. The resulting output contains information such as

 This document © 2011 First Network Group Inc. All Rights Reserved

username (if available), MAC address, IP address, session start; end; length; and remaining time.

Please note that as of 5.3.0 option 82 information can be searched as well. Searching by option 82 information may significantly increase the duration to receive results. This is especially true of high traffic systems.

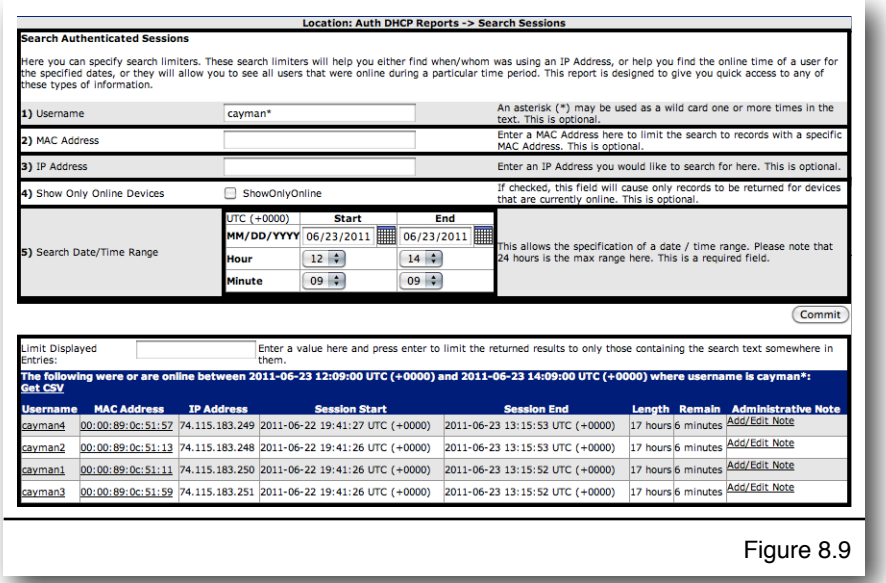


Figure 8.9

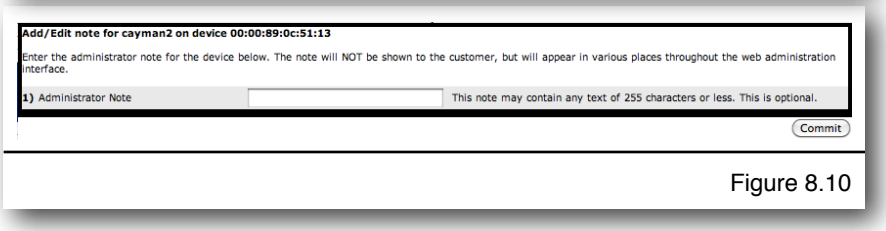


Figure 8.10

To access this report, expand either the Standard DHCP Reports menu or the Authenticated DHCP Reports menu and click on Search Session. Fill out the form as needed, or leave blank and click on commit. Clicking on the username will bring up a list of past sessions for that user as shown in figure 8.8. Clicking on the MAC address will show you the manufacturer of the equipment as shown in figure 8.7.

Administrative notes about the device can also be added/edited and viewed here. To add or edit an administrative note, click on the Add/Edit Note link (or if a note is already set, click on the note). A form will appear as shown in figure 8.10.

New as of version 5.2.0, a number 82 which is a link will appear with each session. Clicking this link will bring a popup screen which will show you option 82 information for the session, if available.

Possible hijacked IP Addresses

This report shows a list of IP addresses that have been “declined” by a client one or more times. They remain in the list until deleted. This can be an indicator that someone has manually configured a device at that IP address.

What is a declined IP address you ask? When some clients are given an IP address by a DHCP server, it will first do an arp request to find out if any device is using the IP address. If it is found that another device is already using the address, the client will send what is known as a DHCPDECLINE telling the DHCP server that it does not want to use that IP address. Then it will request another. This is the basis of this list.

 This document © 2011 First Network Group Inc. All Rights Reserved

Chapter 9: DHCPv6 Configuration and Maintenance

IPv6 Primer

IP version 4 (IPv4) addressing began in 1981 and since then has seen many subdivisions to expands its addressing capacity, however we are reaching the limit of this natural capacity. The IP addresses that we have come to know are about to run out. IPv4 has around 4 billion addresses. With the rapid expansion of the internet starting in the 1990s, the Internet Engineering Task Force (IETF) started to research and design a suitable replacement for what was then simply known as the "Internet Protocol" (IP). They (quite accurately) predicted that we would run out of IPv4 addresses sometime between 2010 and 2017. To combat the address exhaustion and bottle-necking that would occur, IP version 6 (IPv6), was created. It's basic form was completed, tested and available for production staring in 1999. IPv6 has 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses. Let us compare the number of IPv4 vs. IPv6 addresses:

IPv4: 4,294,967,296 or 2^{32}
IPv6: 340,282,366,920,938,463,463,374,607,431,768,211,456 or 2^{128}

IPv4 was a 32 bit addressing scheme. IPv6 is a 128 bit addressing scheme. This creates an exponential increase in the number of IP addresses available. A real world comparison would be if the IPv4 addressing capacity was the size of a golf ball, then IPv6 addressing capacity would be the size of the entire planet.

It helps to understand that there is a fundamental philosophy change in IPv6. We no longer think in terms of a single address. We think in terms of subnets. And by subnet, we mean a single physical network to which hosts that can communicate directly with each other are connected. With both IPv4 and IPv6, a subnet is defined by a network prefix, which is the number of bits that define the network. In IPv4, common prefixes were /24,/25,/29, etc., and you normally had to specify a netmask to configure a device (255.255.255.0, 255.255.255.128, 255.255.255.248 for the previous prefix examples) We no longer need to specify netmasks for IPv6 networks (well, technically they still exist behind the scenes, but we won't need to express them that way). For instance, it is currently recommended that any single subnet anywhere should have a 64 bit prefix length. This would be written like this, for example: 2001:db8:0:0::/64 A host in such a subnet might be expressed like this, for example: 2001:db8:0:0::1/64. You would likely see this kind of notation directly on the interface when viewing interface information. A single 64 bit prefix length contains many more than the IP addresses of the entire IPv4 space (2^{64} vs. 2^{32}). We usually express these as powers of two as the numbers are so huge. If we were to write the numbers:

IPv4: 4,294,967,296 or 2^{32}
IPv6 (/64): 18,446,744,073,709,551,616 or 2^{64}

DHCPatriot Version 5 Operations Manual This document © 2011 First Network Group Inc. All Rights Reserved

You might be tempted to think that we are going to run out of IPv6 addresses in a hurry if we setup each subnet as a /64. Currently, however, there are about 7 billion people on the earth. That is somewhat less than 2^{33} . There are 2^{64} /64 subnets in the IPv6 space. This means that we could give every man woman and child on the earth 2^{31} /64 subnets. So, each person on the earth could have approximately 2 billion subnets all to themselves before we ran out of IPv6 addresses. Current population projections have the world population growth leveling off around 9 billion. That is slightly more than 2^{33}. As you will learn later in the document, conventional wisdom states that we do use DHCP to award each household/business a /48 for use on the local network. There are 2^{48} (or 281,474,976,710,656) /48 subnets in the entire IPv6 space. That is still well beyond the expected 9 billion people on the planet and far beyond the number of households and businesses.

Here is a simple chart showing IPv6 size:

	Prefix	RPL	# of this prefix length in IPv6 space	# of addresses in this prefix length
/128	128	0	340,282,366,920,938,463,463,374,607,431,768,211,456	1
/96 (IPv4 space)	96	32	79,228,162,514,264,337,593,543,950,336	4,294,967,296
/64 (Subnet)	64	64	18,446,744,073,709,551,616	18,446,744,073,709,551,616
/48	48	80	281,474,976,710,656	1,208,925,819,614,629,174,706,176
/32	32	96	4,294,967,296	79,228,162,514,264,337,593,543,950,336
/16	16	112	65,536	5,192,296,858,534,827,628,530,496,329,220,096
/8	8	120	256	1,329,227,995,784,915,872,903,807,060,280,344,576
/4	4	124	16	21,267,647,932,558,653,966,460,912,964,485,513,216
/0	0	128	1	340,282,366,920,938,463,463,374,607,431,768,211,456
World Pop (2012) (est)			7,000,000,000	
World Pop (2050) (est)			9,000,000,000	
World ISP Count (est)			15,000	

Figure 9.1

DHCPv6 Primer

Most current clients that support IPv6 will have at least two modes of operation that can be set: manual and automatic. When set to automatic, clients will receive network information from the local router using a special procedure called Router Announcements (RA). This information includes the network prefix to use, the default gateway, and which method should be used to obtain or set an IP address on the client's connected interface.

At this point, the client has already established communication with the link local network. The link local network is a special network that each host becomes a part of just by having IPv6 enabled. Addresses are created based on the MAC address on the connected interface of machinery connected to the network. Systems on the network can communicate with each other via these addresses. The gateway for the client will

 This document © 2011 First Network Group Inc. All Rights Reserved

normally be set to the router's link local address, although at this time, it varies by router manufacturer.

The router, if configured as such, will tell the client to get its address via DHCPv6. The client will then ask the DHCP server for an address via a special local multi-cast address (To simplify we will assume a local DHCP server). The DHCP server will give the client an address to use for a specified time range.

The client, if it needs to provide addresses to equipment connected to it on another interface (such as is the case with a customer home router), may also ask for a prefix delegation. Prefix delegation refers to assigning a network to be used by a router on the local subnet for connected devices on another subnet. This is necessary as Network Address Translation (NAT) is no longer available, or needed, in IPv6 and all equipment that needs Internet access must have a globally routable (in IPv4 language a "public") address. Please note that most customer equipment (and much of the carrier equipment) is not ready to deploy IPv6 at this time. As IPv6 fully matures over the coming years more devices will employ these capabilities.

DHCPv6 is currently the only method in IPv6 for providing such a delegated network.

The current prevailing wisdom among network operators, regarding the size of the prefix that should be assigned to each, is to assign a /48 prefix length per end-user. This may sound like a lot. Indeed it is larger than the entire IPv4 address space which is 2^{32} IP addresses. A /48 is 2^{80} IP addresses. However, it is designed to provide for future expansion in the end-user's network. Current standards also state that any subnet on any network will be a /64.

And while all major computer operating systems have built-in support for IP addressing, consumer equipment has been slow to adopt firmware that supports most, if any, of the IPv6 constructs. Newly emerging consumer routers from manufacturers such as D-Link are able to receive the prefix delegation and select a /64 for use internally. It is expected that future consumer routers will have the capability, not only of maintaining several discreet /64 subnets, but also of aggregating subnets to other equipment in the household or business for various purposes. Each of these discreet internal subnets will also require a /64 and a beginning subnet, received via Prefix Delegation, of sufficient size so that the aggregation may occur.

In most cases an ISP will receive at least a /32 (a very small ISP - less than 4096 customers and less than 4 POPs). In a /32 there are 2^{16} /48 subnets. An ISP can split the /32 into 2^4 /36 subnets for use in their core network as well as in outlying pops. Each subnet would be of size /64. Each POP with customers would also need a /40, for example, for distribution of /48 subnets to customers. At most small ISPs this should be an entirely reasonable allocation policy. This model also scales as medium and large ISPs will receive appropriately larger allocations.

 This document © 2011 First Network Group Inc. All Rights Reserved

Configuration and Maintenance of DHCPv6 on the DHCPatriot

To help you begin getting your feet wet with IPv6 and DHCPv6 we have began supporting these constructs in this new version (v5.1.0) so you can begin testing the deployment within your networks. We at First Network Group wanted to, as quickly as possible, provide support for DHCPv6 so that our DHCPatriot customers could begin testing IPv6 deployment on their networks. To that end, in version 5.1.0, we have added support for DHCPv6.

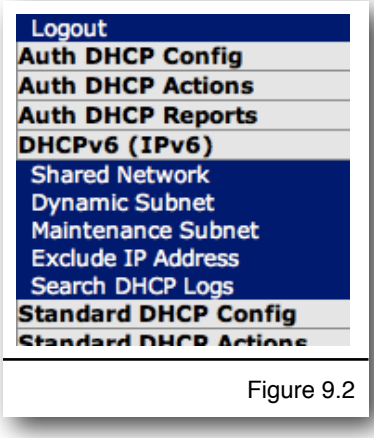


Figure 9.2

The DHCPatriot system now supports DHCPv6 including Prefix Delegation. A new configuration menu called DHCPv6 (IPv6), see figure 9.2, has been added with several areas for configuring networks and subnets related to DHCPv6.

Currently DHCPv6 standards and the ISC DHCP server have some limitations which prevent the tracking of sessions and authentication. Customers taking advantage of the DHCPv6 features in the DHCPatriot system should do so with testing in mind, and understand that they may not want to do so on production networks. We are actively working and engaged in the community as the RFC's for these constructs are finalized and made ready for implementation.

When setting up a brand new DHCPv6 network on the DHCPatriot system, the first thing to do is to enter the Shared Network area (figure 9.3) under the DHCPv6 menu. A Shared Network is a container that will hold all of the subnets that exist together on a particular customer facing network. The name and lease length are set here.

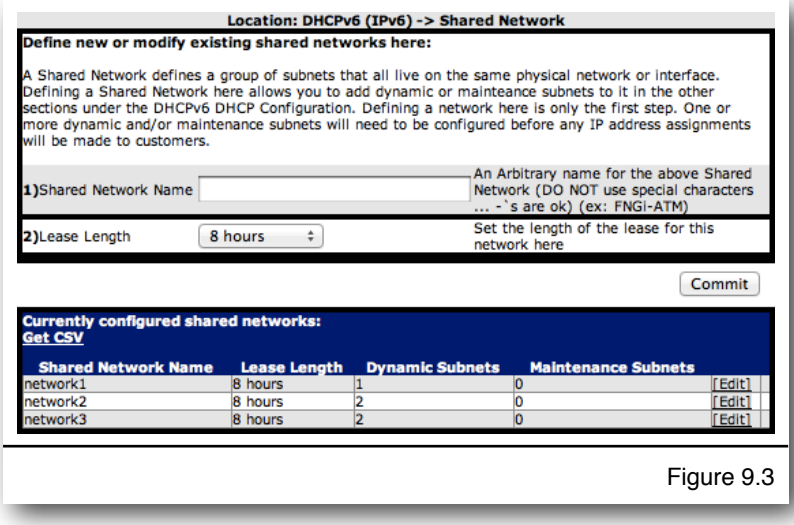


Figure 9.3

 This document © 2011 First Network Group Inc. All Rights Reserved

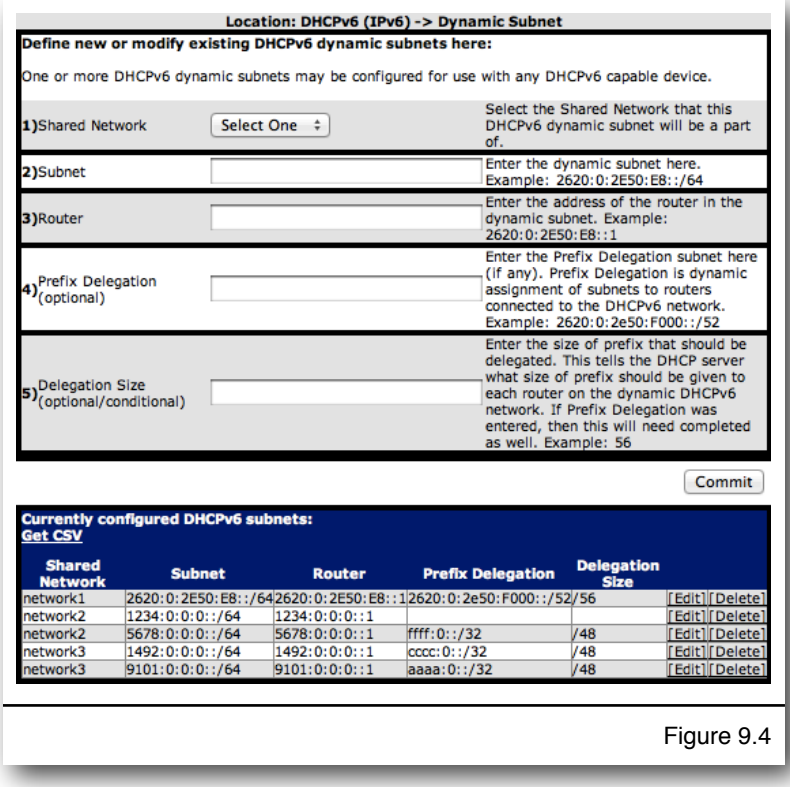


Figure 9.4

A DHCPv6 network would not be much without a subnet of addresses that is to be handed out to customers dynamically. After creating a Shared Network, the next step is to add a dynamic subnet via the Dynamic Subnet sub menu (figure 9.4). All that is required here is to choose the Shared Network that the subnet should belong to and a subnet declaration and the router address in that subnet. Optionally, a prefix delegation may be specified here. The DHCPatriot system will take care of the rest allocating ranges etc. It is recommended that the subnet have a 64 bit prefix length and that the delegated prefix (Delegation Size on the form) be of 48 bit length, although any values will work. Press commit and you are done.

Sometimes the relay agent that is forwarding the DHCP packets to the DHCPatriot may not be in the same subnet as the dynamic subnet that was specified previously. If this is the case, what we call a maintenance subnet may be specified. The Maintenance Subnet area (figure 9.5) under the DHCPv6 menu is provided for this purpose. Simply choose the Shared Network that the Maintenance Subnet should belong to. Type the maintenance subnet and press commit.

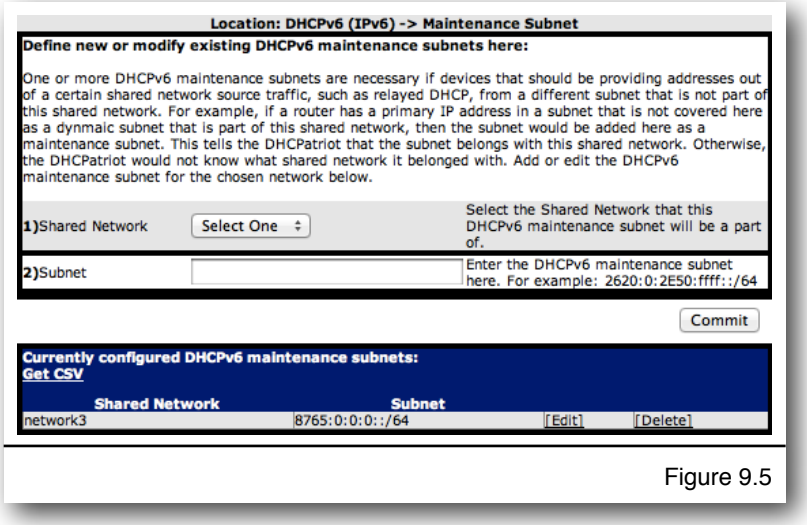


Figure 9.5

 This document © 2011 First Network Group Inc. All Rights Reserved

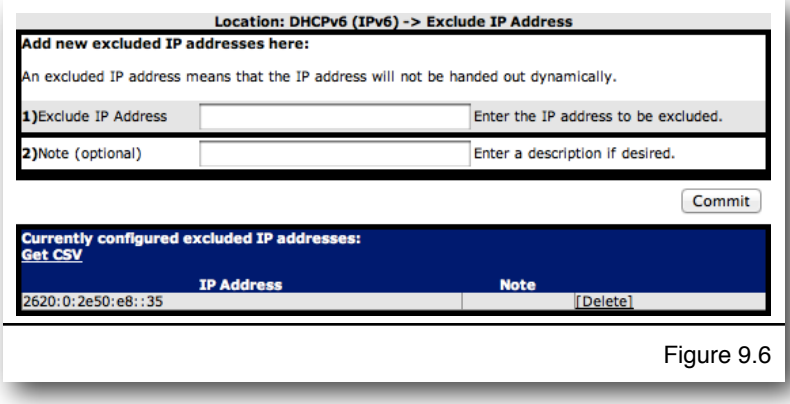


Figure 9.6

From time to time, it may be necessary to stop a certain IP address from being allocated to a client. This could be necessary due to an address conflict, placement of an administrative device in the subnet that is normally all dynamically assigned via DHCPv6, or simply because you need a client to vacate a certain IP address for other purposes. The DHCPatriot supports excluding an IP address from being assigned dynamically. Enter the Exclude IP Address area (figure 9.6) under the DHCPv6 menu. Type the address that you wish to exclude. Add a note if desired and press commit. This address will then be excluded from dynamic assignment.

DHCPv6 has a completely different logging structure at the present time. The logs are not nearly as verbose as they were in DHCPv4.

```
Mar  8 21:06:47 patriot-2 dhcpd: Relay-forward message from 2001:db8:0:f::b port 547,
link address 2001:db8:0:e8::1, peer address fe80::250:daff:fecf:ff7f
Mar  8 21:06:47 patriot-2 dhcpd: Picking pool address
2001:db8:0:e8:ffff:ffff:ffff:fffe
Mar  8 21:06:47 patriot-2 dhcpd: Sending Relay-reply to 2001:db8:0:f::b port 547
```

Exchanges, such as this one above, can be useful for noting that there was a DHCPv6 exchange involving a certain relay agent but may not always be useful for diagnosing a particular client's problems. As DHCPv6 is finalized we are pursing options to address these issues.

 This document © 2011 First Network Group Inc. All Rights Reserved

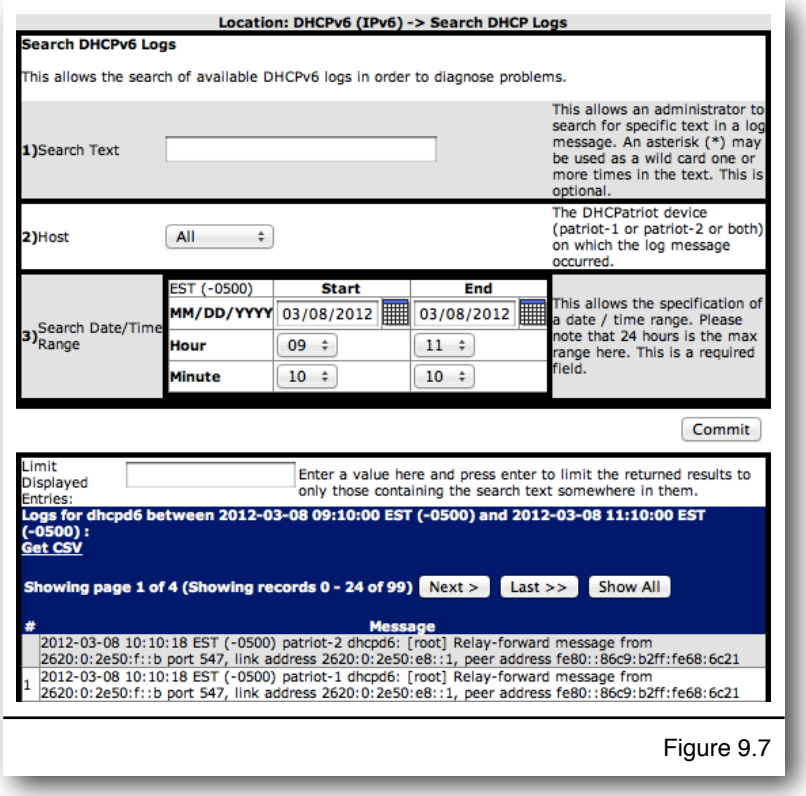


Figure 9.7

The DHCPatriot system provides access to these logs now. To access these logs, enter the Search DHCP Logs area (figure 9.7) under the DHCPv6 menu. Time period, host and text to search are all available parameters to perform the search. Results are displayed at the bottom in reverse chronological order.

 This document © 2011 First Network Group Inc. All Rights Reserved

Chapter 10: Monitoring and Graphing the System

The DHCPatriot has a number of performance monitoring tools that are available both on the system itself and also remotely via SNMP. Also, it is possible to remotely access address utilization data via SNMP for use in some graphing system such as Cacti.

It is possible to remotely monitor a variety of services on the DHCPatriot system. Some are monitored via SNMP, others are monitored by connecting to the actual service to confirm that it is running.

Allowing Subnets to Monitor the DHCPatriot

It is simple to allow subnets to monitor the DHCPatriot system devices. A function is included that allows setting up monitoring on a per-subnet basis. This function is shown in figure 10.1.

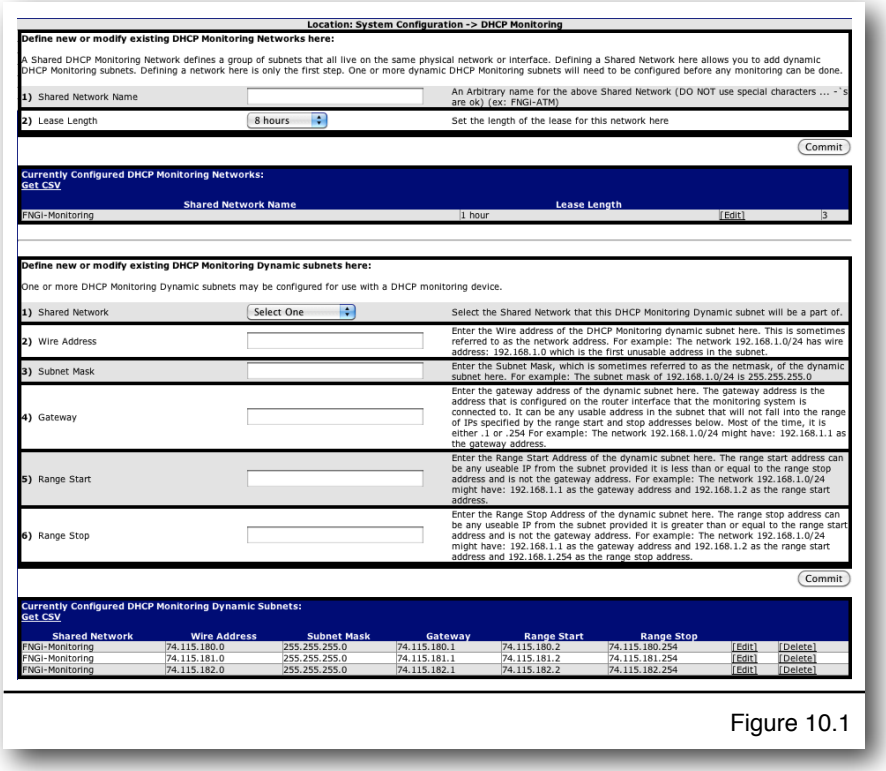


Figure 10.1

Adding a subnet(s), as shown in figure 10.1, allows those addresses to monitor all facets of the DHCPatriot system, as described later in the manual. The firewall will automatically be opened allowing access to services that may need monitoring, and DHCP ranges will be created so that monitoring can be done of DHCP by actually performing DHCP operations. This ensures that the service really is answering requests as opposed to just running as can be told via SNMP.

The configuration of the subnets is setup in much the same way it is elsewhere in the DHCPatriot system when adding DHCP ranges. A container network must be created using the form at the top. The list immediately below that form can be used to edit and delete network entries. The bottom form is used for adding subnets to the configured networks. The list at the bottom of the page is used edit and delete subnet entries.

You will notice some default entries in here noted as FNGi-Monitoring. These entries should not be changed or deleted or First Network Group personnel may not be able to help you with any DHCPatriot problem that would require access to the system.

 This document © 2011 First Network Group Inc. All Rights Reserved

Monitoring Critical Services and Their Importance

Along with the standard Linux SNMP (http://en.wikipedia.org/wiki/SNMP) access, the DHCPatriot system also contains some custom OID values that will allow access to monitoring of certain parts of the device and statistical returns regarding network utilization for use with MRTG (http://en.wikipedia.org/wiki/MRTG) or similar SNMP based graphing software. If the subnet(s) has already been setup in DHCP Monitoring, then devices in that subnet should be able to connect to port 131 on the DHCPatriot system. The system supports SNMP version 1 only. The community string to allow access is lnx-snmp.

The DHCPatriot system 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 system can return the following status information about services as listed in the table below.

Disk Space
OID: 1.3.6.1.4.1.2021.51.1.4.1.2.9.68.73.83.75.83.80.65.67.69.1 This OID will return down (999) when disk space used on the file system reaches 98% It is important to monitor this as when the disk is full, the DHCPatriot system will cease to function correctly.
Database Status
OID: 1.3.6.1.4.1.2021.51.2.4.1.2.5.77.89.83.81.76.1 This OID will return down (999) when the database server is not running on the device. The database is the storage engine of the DHCPatriot system. With this engine down (on both servers), the DHCPatriot system will not be able to perform many functions.
Database Sync Status
OID: 1.3.6.1.4.1.2021.51.3.4.1.2.16.77.89.83.81.76.82.69.80.76.73.67.65.84.73.79.78.1 This OID will return down (999) when the database servers are not in sync across the two devices. If the database is out of sync, the system may obtain wrong answers as pertains to critical pieces of data that allow it to make decisions regarding what addresses to hand out as well as many other things. It is important that this service stay up as long as both devices are running.

 This document © 2011 First Network Group Inc. All Rights Reserved

DHCPatriot System Software Health

OID: 1.3.6.1.4.1.2021.51.9.4.1.2.6.72.69.65.76.84.72.1
This OID will return down (999) if an error condition exists with some facet of the DHCPatriot system software. This is a mashup of many services that could possibly be broken on the DHCPatriot system but cannot be monitored in some other way. When this service goes down, there is some problem with one or more software programs on the DHCPatriot system. You can get a list of these individual software programs by doing something like this:

```
Shell #> snmpwalk -v1 -On -c lnx-snmp patriot-1.network1.net .1.3.6.1.4.1.2021.51.10
.1.3.6.1.4.1.2021.51.10.1 = STRING: "patriot-1,AutoSuspend,1309195964"
.1.3.6.1.4.1.2021.51.10.1.1 = STRING: "patriot-1,AutoSuspend,1309195964"
.1.3.6.1.4.1.2021.51.10.1.2 = STRING: "patriot-1,DHCPatriotLogRead,1309195992"
.1.3.6.1.4.1.2021.51.10.1.3 = STRING: "patriot-1,dhcpdLogRead,1309195957"
.1.3.6.1.4.1.2021.51.10.1.4 = STRING: "patriot-1,DHCPDwrapper,1309195943"
.1.3.6.1.4.1.2021.51.10.1.5 = STRING: "patriot-1,fcron,1309195984"
.1.3.6.1.4.1.2021.51.10.1.6 = STRING: "patriot-1,GraphDataGen,1309195734"
.1.3.6.1.4.1.2021.51.10.1.7 = STRING: "patriot-1,HealthMonitor,1309195984"
.1.3.6.1.4.1.2021.51.10.1.8 = STRING: "patriot-1,klogd,1309195984"
.1.3.6.1.4.1.2021.51.10.1.9 = STRING: "patriot-1,LeaseUpdater,1309195956"
.1.3.6.1.4.1.2021.51.10.1.10 = STRING: "patriot-1,NetEnforcerPreProcess,1309195979"
.1.3.6.1.4.1.2021.51.10.1.11 = STRING: "patriot-1,RADIUS,1309195954"
.1.3.6.1.4.1.2021.51.10.1.12 = STRING: "patriot-1,radiusd,1309195984"
.1.3.6.1.4.1.2021.51.10.1.13 = STRING: "patriot-1,RadiusDispatch,1309195954"
.1.3.6.1.4.1.2021.51.10.1.14 = STRING: "patriot-1,syslogd,1309195984"
.1.3.6.1.4.1.2021.51.10.1.15 = STRING: "patriot-1,tftpd,1309195984"
.1.3.6.1.4.1.2021.51.10.1.16 = STRING: "patriot-1,todTCP,1309195984"
.1.3.6.1.4.1.2021.51.10.1.17 = STRING: "patriot-1,todUDP,1309195984"
.1.3.6.1.4.1.2021.51.10.1.18 = STRING: "patriot-1,traffic_shaper_commands,
1309195956"
.1.3.6.1.4.1.2021.51.10.1.19 = STRING: "patriot-2,AutoSuspend,1309195996"
.1.3.6.1.4.1.2021.51.10.1.20 = STRING: "patriot-2,DHCPatriotLogRead,1309195938"
.1.3.6.1.4.1.2021.51.10.1.21 = STRING: "patriot-2,dhcpdLogRead,1309195921"
.1.3.6.1.4.1.2021.51.10.1.22 = STRING: "patriot-2,DHCPDwrapper,1309195924"
.1.3.6.1.4.1.2021.51.10.1.23 = STRING: "patriot-2,fcron,1309195993"
.1.3.6.1.4.1.2021.51.10.1.24 = STRING: "patriot-2,GraphDataGen,1309195854"
.1.3.6.1.4.1.2021.51.10.1.25 = STRING: "patriot-2,HealthMonitor,1309195993"
.1.3.6.1.4.1.2021.51.10.1.26 = STRING: "patriot-2,klogd,1309195993"
.1.3.6.1.4.1.2021.51.10.1.27 = STRING: "patriot-2,LeaseUpdater,1309195920"
.1.3.6.1.4.1.2021.51.10.1.28 = STRING: "patriot-2,NetEnforcerPreProcess,1309195968"
.1.3.6.1.4.1.2021.51.10.1.29 = STRING: "patriot-2,RADIUS,1309195982"
.1.3.6.1.4.1.2021.51.10.1.30 = STRING: "patriot-2,radiusd,1309195963"
.1.3.6.1.4.1.2021.51.10.1.31 = STRING: "patriot-2,RadiusDispatch,1309195987"
.1.3.6.1.4.1.2021.51.10.1.32 = STRING: "patriot-2,syslogd,1309195993"
.1.3.6.1.4.1.2021.51.10.1.33 = STRING: "patriot-2,tftpd,1309195993"
.1.3.6.1.4.1.2021.51.10.1.34 = STRING: "patriot-2,todTCP,1309195963"
.1.3.6.1.4.1.2021.51.10.1.35 = STRING: "patriot-2,todUDP,1309195963"
.1.3.6.1.4.1.2021.51.10.1.36 = STRING: "patriot-2,traffic_shaper_commands,
1309195945"
```

 This document © 2011 First Network Group Inc. All Rights Reserved

DHCP
After adding the monitoring subnet(s), DHCP packets can be sent directly to the DHCP service. These packets should be of type DHCPREQUEST for some address out of the DHCP monitor subnet and will then be answered with DHCPACK. Additionally, DHCP can be monitored with SNMP. OID: 1.3.6.1.4.1.2021.52.6.4.1.2.4.68.72.67.80.1 It is, however, better to monitor with real DHCP packets.
DNS
The DHCPatriot system also runs an internal DNS server. The response to any lookup will always be its own IP address. This sever is used only for the Authenticated DHCP. The best way to monitor this service is to connect to it and receive an answer for a lookup. It can, however, be monitored via SNMP. OID: 1.3.6.1.4.1.2021.52.1.4.1.2.3.68.78.83.1
HTTP
The DHCPatriot system has a built-in web server that customers use as the captive portal authentication mechanism. It only matters if this service is running to customers that are utilizing Authenticated DHCP. The best way to monitor this service is by connecting to port 80 to see if some sort of data is returned. The monitoring is available via SNMP, however. OID: 1.3.6.1.4.1.2021.52.2.4.1.2.4.72.84.84.80.1
HTTPS
The secure web server is used for the Web Administration Interface. It is important that this service be running for management of the devices. The best way to check is to create a secure connection to port 443 and see if some sort of data is returned. The status is also available via SNMP. OID: 1.3.6.1.4.1.2021.52.3.4.1.2.5.72.84.84.80.83.1
NTP
The DHCPatriot system has a built-in NTP server. The status of this can be monitored using the OID below. This is not the best method of monitoring NTP, however. It is best to actually connect to the NTP service with an NTP client and attempt to get the time. The OID below only states whether the process is running. OID: 1.3.6.1.4.1.2021.52.4.4.1.2.3.78.84.80.1

 This document © 2011 First Network Group Inc. All Rights Reserved

SSH
The system contains an SSH server for remote access to the menu interface, as well as for use by FNGi personnel to affect repairs. This service is best monitored by making a remote connection to the server periodically with an SSH client to check if it is responding. The service can also be monitored via SNMP with the OID below. OID: 1.3.6.1.4.1.2021.52.5.4.1.2.3.83.83.72.1

Graphing System Performance

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

 This document © 2011 First Network Group Inc. All Rights Reserved

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 five 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 five 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.

 This document © 2011 First Network Group Inc. All Rights Reserved

Graphing Address Utilization

The DHCPatriot also allows the graphing of address utilization on some graphing system such as Cacti. The OIDs necessary are detailed in the table below.

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 subnet in the most recent five minute interval. This is the same measurement used to compute the dynamic graphs in IP Address Usage (see section 4.2.10). Additionally, there are more advanced options for retrieving data about subnets and totals of dynamic networks. These options allow the listing of data sources as well as data retrieval. **Per Subnet data** • 1.3.6.1.4.1.2021.50.80.1 will list all available dynamic subnets for which used and available data may be retrieved • 1.3.6.1.4.1.2021.50.90.1.(gateway address result from 1.3.6.1.4.1.2021.50.80.1) will retrieve used IP address number from the chosen subnet • 1.3.6.1.4.1.2021.50.100.1.(gateway address result from 1.3.6.1.4.1.2021.50.80.1) will retrieve total available IP address number from the chosen subnet For example: This command will list all available subnets for per subnet graphs: *snmpwalk -On -v 1 -c lnx-snmp patriot-1.network1.net 1.3.6.1.4.1.2021.50.80.1* Output would look something like this: *1.3.6.1.4.1.2021.50.80.1.1 = STRING: "**10.31.128.1**"* *1.3.6.1.4.1.2021.50.80.1.2 = STRING: "10.69.254.1"* *1.3.6.1.4.1.2021.50.80.1.3 = STRING: "172.16.254.1"* *1.3.6.1.4.1.2021.50.80.1.4 = STRING: "208.45.199.113"* *1.3.6.1.4.1.2021.50.80.1.5 = STRING: "10.31.128.1"* *1.3.6.1.4.1.2021.50.80.1.6 = STRING: "10.69.254.1"* *1.3.6.1.4.1.2021.50.80.1.7 = STRING: "172.16.254.1"* *1.3.6.1.4.1.2021.50.80.1.8 = STRING: "208.45.199.113"* *1.3.6.1.4.1.2021.50.80.1.8 = STRING: "208.45.199.113"* *Error: OID not increasing: 1.3.6.1.4.1.2021.50.80.1.8* *>= 1.3.6.1.4.1.2021.50.80.1.8*

 This document © 2011 First Network Group Inc. All Rights Reserved

Ignore the error message, it is normal signifying the end of the data list. The string values that are returned, which are each gateway address of each dynamic subnet on the system, are the identifiers used to reference usage and total available data for each subnet. For example:
This command will retrieve the used IP addresses on the subnet 10.31.128.0/24:

*snmpget -On -v 1 -c lnx-snmp patriot-1.network1.net 1.3.6.1.4.1.2021.50.90.1.**10.31.128.1***

Output would look something like this:

*.1.3.6.1.4.1.2021.50.90.1.**10.31.128.1** = INTEGER: 0*

And this command will retrieve the total available IP address on the subnet 10.31.128.0/24:

*snmpget -On -v 1 -c lnx-snmp patriot-1.network1.net 1.3.6.1.4.1.2021.50.100.1.**10.31.128.1***

Output would look something like this:

*.1.3.6.1.4.1.2021.50.100.1.**10.31.128.1** = INTEGER: 253*

Total Dynamic data per network

- 1.3.6.1.4.1.2021.50.110.(1/2 for type of network auth/standard) will list all available dynamic networks for which used and available data may be retrieved. The returned string will consist of the network name, as well as an id number in brackets. For example: .1.3.6.1.4.1.2021.50.110.2.15 = STRING: "FNGiTEST[15]". The ID number in brackets is the id used to retrieve the data.
- 1.3.6.1.4.1.2021.50.120.(1/2 for type of network auth/standard).(id from the brackets) will retrieve total used IP address number for dynamic from the chosen network
- 1.3.6.1.4.1.2021.50.130.(1/2 for type of network auth/standard).(id from the brackets) will retrieve total available IP address number for dynamic from the chosen network

 This document © 2011 First Network Group Inc. All Rights Reserved

For example:

This command will list all available standard DHCP networks that total dynamic data may be available for:

snmpwalk -On -v1 -c lnx-snmp patriot-1.network1.net .
1.3.6.1.4.1.2021.50.110.2

Output would look something like this:

*.1.3.6.1.4.1.2021.50.110.2.15 = STRING: "FNGiTEST[**15**]"*
.1.3.6.1.4.1.2021.50.110.2.16 = STRING: "CPI[16]"
.1.3.6.1.4.1.2021.50.110.2.17 = STRING: "Calix-C7-KamasCO[17]"

The number in brackets at the end of the string is the ID that of the network that can be used to get available IPs as well as total used IPs for each dynamic network. For example, using FNGiTEST ID of 15:

This command will get the used dynamic IP addresses for FNGiTEST[**15**]:

snmpget -On -v1 -c lnx-snmp patriot-1.network1.net .
*1.3.6.1.4.1.2021.50.120.2.**15***

Output would look something like this:

*.1.3.6.1.4.1.2021.50.120.2.**15** = INTEGER: 6*

This command will get the total available dynamic IP addresses for FNGiTEST[**15**]:

snmpget -On -v1 -c lnx-snmp patriot-1.network1.net .
*1.3.6.1.4.1.2021.50.130.2.**15***

Output would look something like this:

*.1.3.6.1.4.1.2021.50.130.2.**15** = INTEGER: 13*

 This document © 2011 First Network Group Inc. All Rights Reserved

Miscellaneous SNMP Information

The DHCPatriot system can also send some other miscellaneous types of information back. These are detailed in the table below.

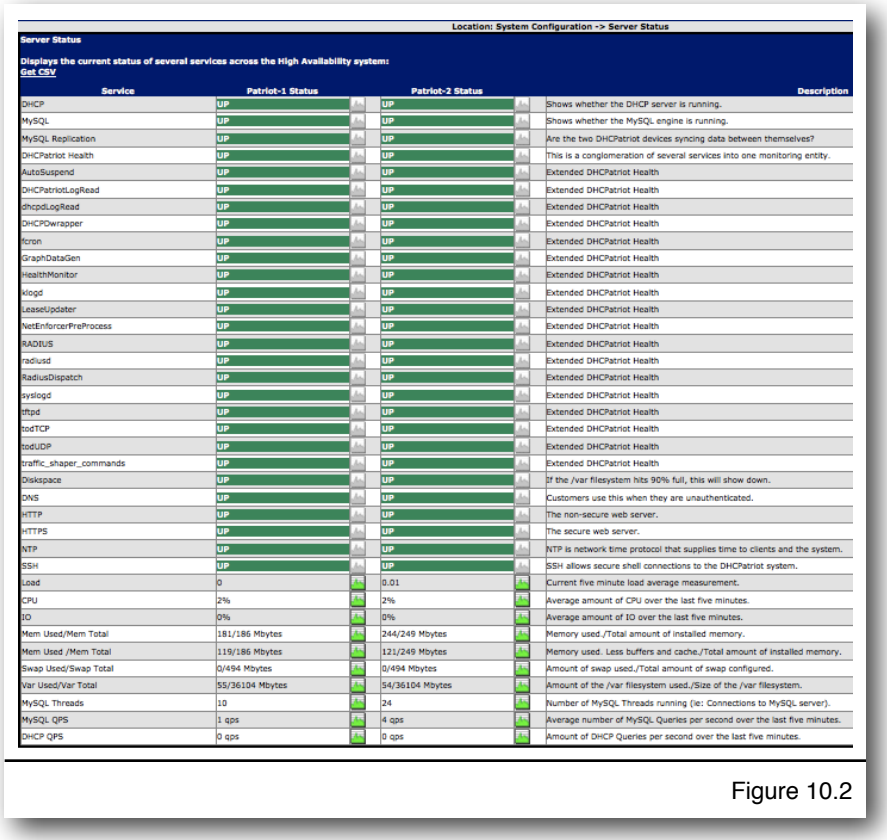
License Status
OID: 1.3.6.1.4.1.2021.51.12.101.1 Returns Output: LIMITED:[EPOCH TIME] if the license has an expiry date where EPOCH TIME is the expire date and time of the license (expressed as UNIX EPOCH). Returns Output: FULL:0 if the license is a non-expiry full license.
Current Time
OID: 1.3.6.1.4.1.2021.51.13.101.1 Returns the DHCPatriot system device's current time (expressed as UNIX EPOCH).

Server Status on the Web Administration Interface

The DHCPatriot system also has an extensive health monitoring function that shows the current status of the system as well as some graphs. This function shows all services that may be monitored and their current status on each device. The service name, its status on each device, and a description of the service are shown.

In addition to the these services, current activity on the system is shown as well. Current CPU utilization, I/O, and load values are shown. Memory usage statistics as well as database and DHCP activity are all shown here. Figure 10.2 shows an example of this function.

Each of the activity measures also has an icon next to it



Location: System Configuration -> Server Status

Server Status

Displays the current status of several services across the High Availability system:

Get CSV

Service	Patriot-1 Status	Patriot-2 Status	Description
DHCP	UP	UP	Shows whether the DHCP server is running.
MySQL	UP	UP	Shows whether the MySQL engine is running.
MySQL Replication	UP	UP	Are the two DHCPatriot devices syncing data between themselves?
DHCPatriot Health	UP	UP	This is a conglomeration of several services into one monitoring entity.
AutoSuspend	UP	UP	Extended DHCPatriot Health
DHCPatriotLogRead	UP	UP	Extended DHCPatriot Health
dhcpdLogRead	UP	UP	Extended DHCPatriot Health
DHCPDwrapper	UP	UP	Extended DHCPatriot Health
fcron	UP	UP	Extended DHCPatriot Health
GraphDataGen	UP	UP	Extended DHCPatriot Health
HealthMonitor	UP	UP	Extended DHCPatriot Health
klogd	UP	UP	Extended DHCPatriot Health
LeaseUpdater	UP	UP	Extended DHCPatriot Health
NetEnforcerPreProcess	UP	UP	Extended DHCPatriot Health
RADIUS	UP	UP	Extended DHCPatriot Health
radiusd	UP	UP	Extended DHCPatriot Health
RadiusDispatch	UP	UP	Extended DHCPatriot Health
syslogd	UP	UP	Extended DHCPatriot Health
tftpd	UP	UP	Extended DHCPatriot Health
todTCP	UP	UP	Extended DHCPatriot Health
todUDP	UP	UP	Extended DHCPatriot Health
traffic_shaper_commands	UP	UP	Extended DHCPatriot Health
Diskspace	UP	UP	If the /var filesystem hits 90% full, this will show down.
DNS	UP	UP	Customers use this when they are unauthenticated.
HTTP	UP	UP	The non-secure web server.
HTTPS	UP	UP	The secure web server.
NTP	UP	UP	NTP is network time protocol that supplies time to clients and the system.
SSH	UP	UP	SSH allows secure shell connections to the DHCPatriot system.
Load	0	0.01	Current five minute load average measurement.
CPU	2%	2%	Average amount of CPU over the last five minutes.
IO	0%	0%	Average amount of IO over the last five minutes.
Mem Used/Mem Total	181/186 Mbytes	244/249 Mbytes	Memory used./Total amount of installed memory.
Mem Used /Mem Total	119/186 Mbytes	121/249 Mbytes	Memory used. Less buffers and cache./Total amount of installed memory.
Swap Used/Swap Total	0/494 Mbytes	0/494 Mbytes	Amount of swap used./Total amount of swap configured.
Var Used/Var Total	55/36104 Mbytes	54/36104 Mbytes	Amount of the /var filesystem used./Size of the /var filesystem.
MySQL Threads	10	24	Number of MySQL Threads running (ie: Connections to MySQL server).
MySQL QPS	1 qps	4 qps	Average number of MySQL Queries per second over the last five minutes.
DHCP QPS	0 qps	0 qps	Amount of DHCP Queries per second over the last five minutes.

Figure 10.2

 This document © 2011 First Network Group Inc. All Rights Reserved

representing a graph. These icons, when clicked, show a graph of past activity of the particular statistic. This data is collected and kept for one year. Past activity can be viewed by changing the form at the bottom and clicking on Commit. The default is to show the last twenty-four hours of data. Figure 10.3 shows an example using CPU usage.

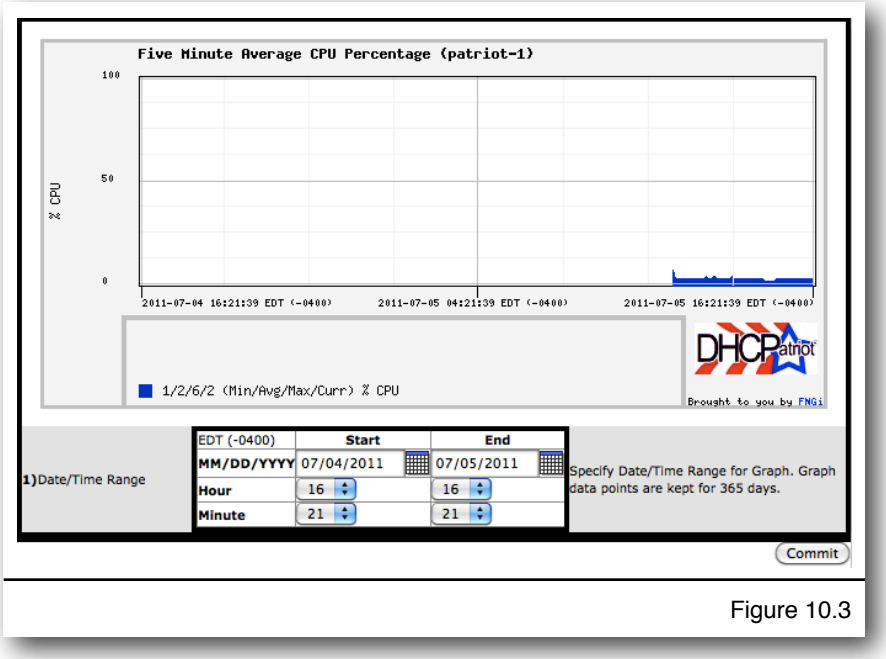


Figure 10.3

That is not to say that the server status should be thought of as a replacement for remote monitoring with a monitoring system. It can be mistaken as it is all done via SNMP, which is limited to noting that the process is running. It cannot be determined from this method whether the service in question is actually performing what it is supposed to, but merely that it is running.

 This document © 2011 First Network Group Inc. All Rights Reserved

Chapter 11: Remote Access API

This chapter describes the web based API features that are available on the DHCPatriot system 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.

Setting up the User for API Access

A special user must be configured to access the API. This user will not be able to access the Web Administrations Interface. Similarly, existing Web Administration Interface users will not be able to access the API.

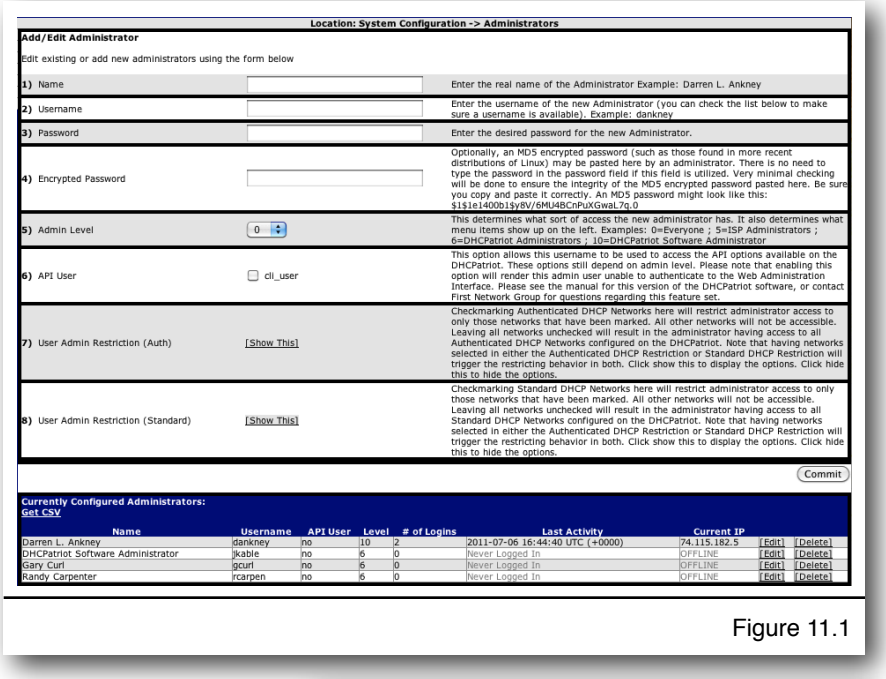


Figure 11.1

To setup this user, connect to the Web Administration Interface. Click on System Configuration. Click on Administrators. You should get a screen similar to figure 11.1.

Figure 11.2

Fill out the name, username and password, or use encrypted password if you have a pre-encrypted password to be used. The encrypted password must be an MD5 encrypted password, if used. Admin level should be set to level six. Of particular importance is item number six, API User as shown in figure 11.2. This field must be checked for an API user. Checking this field makes the Web Administration Interface unavailable to the user. The user admin restriction fields are not needed as the restrictions are not applied to the API User whom is admin level six.

User Access

This set of functions is useful only to the Authenticated DHCP. They consist of authenticating, suspending and enabling user devices. Standard DHCP contains no such designation and so these do not apply.

 This document © 2011 First Network Group Inc. All Rights Reserved

Authenticate Device

This API function allows a user device to be authenticated remotely similarly to what can be done with manually authorizing customers. The default admin level required for this feature is five. As of version 5.4.0, you can authenticate the device using its current IP address as the identifier. The MAC address would be omitted in that case.

The GET string to send is as follows:
https://patriot.[domain]/cli/?function=AuthorizeCustomer&username=[API username]&password=[API Password]&user=[username for device]&pass=[password for device]&MAC=[MAC address of device]&ip=[current device IP]&note=[optional url encoded note]

Here is an example of what a properly formatted URL might look like for the authorize device API:
https://patriot.network1.net/cli/?function=AuthorizeCustomer&username=apiuser&password=apipass&user=linux&pass=Geqp9t4k&MAC=00:a0:cc:d9:9 6:a2&note=Jim+Smith's+Xbox360

Success will present the text RETURN=1. Failure will present RETURN=0 with some text given below as a reason for the failure.

Suspend Device

This allows a user to be suspended on the DHCPatriot system. It will suspend all devices belonging to the specified username. The default admin level required for this feature is five. This feature behaves the same as the Suspend User function on the web administration interface with the exception that mass suspending is not possible, each user must be sent one at a time.

The GET string to send is as follows: https://patriot.[domain]/cli/?function=SuspendEnable&username=[username]&password=[password]&action=suspend&user=[username to suspend]&note=[optional url encoded note]

As of version 4.2.1, the suspension note can now be included just as if you were suspending from the suspend user page. The customer WILL see the contents of this note on the login screen. Please be sure to URL encode the note string as spaces and other special characters will not be passed properly in a URL without proper encoding.

Here is an example of what a properly formatted URL might look like:
https://patriot.[domain]/cli/?function=SuspendEnable&username=apiuser&password=apipass&action=suspend&user=linux&note=Please+contact+our+billing+office.

 This document © 2011 First Network Group Inc. All Rights Reserved

Please note that as of 5.3.0 you can pass &mac=[optional mac address] instead of &user=[username to suspend] An example would look like: https://patriot.[domain]/cli/?function=SuspendEnable&username=apiuser&password=apipass&action=suspend&mac=00:01:02:03:04:05&note=Please+contact+our+billing+office.
This allows a device to be suspended by mac address instead of username (which suspends ALL of their mac addresses).

Success will present the text RETURN=1. Failure will present RETURN=0 with some text given below as a reason for the failure.

Enable Device

This allows a suspended user's devices to be enabled on the DHCPatriot system. It will enable all devices belonging to the specified username. The default admin level required for this feature is five. This would be the same as using the enable user link in the Suspend User function on the Web Administration Interface. As of 5.3.0, you can pass a MAC address instead of a username to enable a single device. As of version 5.4.0, you can include the optional parameter AuthTest=true to force the DHCPatriot to attempt to authenticate the user before enabling them as is done when using the Suspend User web interface.

The GET string to send is as follows: https://patriot.[domain]/cli/?function=SuspendEnable&username=[username]&password=[password]&action=unsuspend&user=[username to enable]&mac=[MAC address to be enabled]&AuthTest=true

Here is an example of what a properly formatted URL might look like for enable user: https://patriot.network1.net/cli/?function=SuspendEnable&username=apiuser&password=apipass&action=unsuspend&user=linux

Success will present the text RETURN=1. Failure will present RETURN=0 with some text given below as a reason for the failure.

Search Authenticated Devices

This provides an API method to access the list of authenticated devices and search it based on several parameters such as MAC address, admin note, username, address type, and current online status. The return data is provided in XML format.

The GET string to send is as follows: https://patriot.[domain]/cli/?function=SearchAuthDevices&username=[apiusername]&password=[apipassword]&mac=[MAC]&AdminNote=[URLencodedNote]&user=[username]&ShowOnlyOnline=[TRUE]&AddressType=[STATIC/DYNAMIC]

 This document © 2011 First Network Group Inc. All Rights Reserved

Here is an example of what a properly formatted URL might look like to search for authenticated devices: https://patriot.network1.net/cli/?function=SearchAuthDevices&username=apiuser&password=apipass&mac=&AdminNote=&user=bobjim&ShowOnlyOnline=&AddressType=

The result will look something like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
        <record>
                <Username>bobjim</Username>
                <MACAddress>0c:0c:0c:0d:0d:01</MACAddress>
                <LastAuthenticated>1408035713</LastAuthenticated>
                <IPAddress>OFFLINE</IPAddress>
                <Type>OFFLINE</Type>
                <AssignedType>1.2.3.4</AssignedType>
                <Status>ACTIVE</Status>
                <AdministrativeNote/>
        </record>
</result>
```

Sticky IP Add

This allows a sticky IP address to be added via the API. The Sticky IP may be assigned by MAC address or username and may contain a note. The admin level required for the api user is 6. Please be sure and URL encode any fields that will contain special characters so that the URL works properly.

The GET string to send is as follows: https://patriot.[domain]/cli/?username=[apiusername]&password=[apipassword]&function=StickyIPs&action=ADD&Stickymac=[MAC]&Stickyusername=[username]&Stickyip=[stickyip]&Stickynote=[note]

Here is an example of what a properly formatted URL might look like to add a sticky IP: https://patriot.network1.net/cli/?username=apiuser&password=apipass&function=StickyIPs&action=ADD&Stickymac=&Stickyusername=bobjim&Stickyip=3.3.3.6&Stickynote=

Success will present the text RETURN=1. Failure will present RETURN=0 with some text given below as a reason for the failure.

Sticky IP Delete

This allows an assigned Sticky IP address to be removed via the API. The function supports deleting Sticky IP addresses that were assigned by MAC address, assigned Sticky IP address, or by username.

 This document © 2011 First Network Group Inc. All Rights Reserved

The GET string to send is as follows: https://patriot.[domain]/cli/?username=[apiusername]&password=[apipassword]&function=StickyIPs&action=DELETE&Stickymac=[MAC]&Stickyusername=[username]&Stickyip=[StickyIPaddress]

Here is an example of what a properly formatted URL might look like to remove a sticky IP:
https://patriot.network1.net/cli/?username=apiuser&password=apipass&function=StickyIPs&action=DELETE&Stickymac=&Stickyusername=bobjim&Stickyip=
Success will present the text RETURN=1. Failure will present RETURN=0 with some text given below as a reason for the failure.

Sticky IP List

This allows a list of all Sticky IP assignments to be returned via the API. This function will return a list of all of the assignments in XML format.

The GET string to send is as follows: https://patriot.[domain]/cli/?username=[apiusername]&password=[apipassword]&function=StickyIPs&action=LIST

Here is an example of what a properly formatted URL might look like to list the Sticky IP address assignments on the device:
https://patriot.network1.net/cli/?username=apiuser&password=apipass&function=StickyIPs&action=LIST

The result will look something like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<result>
        <record>
                <username></username>
                <mac>00:02:04:ff:ee:dd</mac>
                <stickyip>1.2.0.55</stickyip>
                <note></note>
        </record>
</result>
```

Built-in Authentication

This API allows users to be configured in the Built-in Authentication (NOT an external RADIUS server). These functions are obviously only relevant to the Authenticated DHCP.

 This document © 2011 First Network Group Inc. All Rights Reserved

List Customers

This API call will retrieve a list of customers from Auth DHCP Actions -> Built-In Authentication: User Maintenance in the web administration interface. A list will be returned in XML format similar to the following:

```
<result>
        <record>
                <identifier>John Doe</identifier>
                <UserName>jdoe</UserName>
                <StaticIP/>
                <SimUse/>
                <Status>Active</Status>
        </record>
</result>
```

The GET string to send is as follows: https://patriot.network1.net/cli/BuiltInAuthAPI.php?function=BASearchCustomers&username=[user]&password=[pass]&identifier=[sometext]&user=[someuser]&staticip=[someip]&simuse=[someinteger]&status=[Suspended/Active] All of the parameters are optional with the exception of username and password. Each parameter can be used to limit the search to only results containing the values from those parameters.

Here is an example of a properly formatted URL that would provide some specific results: https://patriot.network1.net/cli/BuiltInAuthAPI.php?username=apiuser&password=apipass&function=BASearchCustomers&identifier=18806&user=148892&staticip=1.3.5.7&simuse=3&status=

Add Customer

This allows adding a customer to the Built-in Authentication. This would be the same as adding a customer in the Built-in Authentication: User Maintenance under Auth DHCP Actions in the Web Administration Interface.

The GET string to send is as follows: https://patriot.[domain]/cli/?function=BAAddCustomer&username=[user]&password=[pass]&identifier=[sometext]&user=[someuser]&pass=[somepass]&staticip=[someip]&simuse=[someinteger] simuse and identifier are optional.

Here is an example of what a properly formatted URL might look like for adding a customer: https://patriot.network1.net/cli/?function=BAAddCustomer&username=apiuser&password=apipass&identifier=Jim%20Smith&user=jsmith&pass=12345678&staticip=1.2.3.4&simuse=2

Success will present the text RETURN=1. Failure will present RETURN=0 with some text given below as a reason for the failure.

 This document © 2011 First Network Group Inc. All Rights Reserved

Edit Customer

This allows editing a customer in the Built-in Authentication. This would be the same as editing a customer in the Built-in Authentication: User Maintenance under Auth DHCP Actions in the Web Administration Interface.

The GET string to send is as follows: https://patriot.[domain]/cli/?function=BAEditCustomer&username=[user]&password=[pass]&identifier=[sometext]&user=[someuser]&pass=[somepass]&newuser=[someuser]&staticip=[someip]&simuse=[someinteger]

Here is an example of what a properly formatted URL might look like for editing a customer: https://patriot.network1.net/cli/?function=BAEditCustomer&username=apiuser&password=apipass&identifier=John%20Smithson&user=jsmith&pass=12345678&newuser=jsmithson&staticip=1.2.3.4&simuse=3

Success will present the text RETURN=1. Failure will present RETURN=0 with some text given below as a reason for the failure.

Suspend Customer

This allows suspending a customer in the Built-in Authentication. This would be the same as suspending a customer in the Built-in Authentication: User Maintenance under Auth DHCP Actions in the Web Administration Interface.

The GET string to send is as follows: https://patriot.[domain]/cli/?function=BASuspendCustomer&username=[user]&password=[pass]&user=[someuser]

Here is an example of what a properly formatted URL might look like for suspending a customer: https://patriot.network1.net/cli/?function=BASuspendCustomer&username=apiuser&password=apipass&user=jsmithson

Success will present the text RETURN=1. Failure will present RETURN=0 with some text given below as a reason for the failure.

Enable Customer

This allows enabling a suspended customer in the Built-in Authentication. This would be the same as enabling a customer in the Built-in Authentication: User Maintenance under Auth DHCP Actions in the Web Administration Interface.

 This document © 2011 First Network Group Inc. All Rights Reserved

The GET string to send is as follows: https://patriot.[domain]/cli/?function=BAEnableCustomer&username=[user]&password=[pass]&user=[someuser]

Here is an example of what a properly formatted URL might look like for enabling a suspended customer: https://patriot.network1.net/cli/?function=BAEnableCustomer&username=apiuser&password=apipass&user=jsmithson

Success will present the text RETURN=1. Failure will present RETURN=0 with some text given below as a reason for the failure.

Delete Customer

This allows deleting a suspended customer in the Built-in Authentication. This would be the same as deleting a suspended customer in the Built-in Authentication: User Maintenance under Auth DHCP Actions in the Web Administration Interface.

The GET string to send is as follows: https://patriot.[domain]/cli/?function=BADeleteCustomer&username=[user]&password=[pass]&user=[someuser]

Here is an example of what a properly formatted URL might look like for deleting a suspended customer: https://patriot.network1.net/cli/?function=BADeleteCustomer&username=apiuser&password=apipass&user=jsmithson

Success will present the text RETURN=1. Failure will present RETURN=0 with some text given below as a reason for the failure.

Change Password

This allows the password for a specific user in the Built-in Authentication to be changed. This would be the same as modifying the password in Built-in Authentication: User Maintenance under Auth DHCP Actions in the Web Administration Interface.

The GET string to send is as follows: https://patriot.[domain]/cli/?function=BAChangePass&username=[user]&password=[pass]&action=changepass&user=[someuser]&newpass=[somepass]

Here is an example of what a properly formatted URL might look like for changing the password of a specific user: https://patriot.network1.net/cli/?function=BAChangePass&username=apiuser&password=apipass&action=changepass&user=linux&newpass=123abc

Success will present the text RETURN=1. Failure will present RETURN=0 with some text given below as a reason for the failure.

 This document © 2011 First Network Group Inc. All Rights Reserved

Remote Search

This allows a remote search of the session data present on the DHCPatriot system with several available search parameters. Sessions presented could either be in the Authenticated DHCP or the Standard DHCP or both depending on search parameters. The result is returned in XML format similar to that shown here:

```
<result>
	<record>
		<username/>
		<mac>00:30:48:42:62:58</mac>
		<ip>74.115.180.91</ip>
		<start_time>1309878834</start_time>
		<stop_time/>
		<sessionID>ea1068fc5a4adf6f6b2ee3191536dc74</sessionID>
		<DHCPLeaseStart>1309878834</DHCPLeaseStart>
		<DHCPLeaseEnd>1310055414</DHCPLeaseEnd>
	</record>
	<record>
		<username/>
		<mac>00:30:48:80:31:22</mac>
		<ip>74.115.180.92</ip>
		<start_time>1309879128</start_time>
		<stop_time/>
		<sessionID>bba9e106f8eaac0c6fb1a4f5c31d9b92</sessionID>
		<DHCPLeaseStart>1309879128</DHCPLeaseStart>
		<DHCPLeaseEnd>1310055412</DHCPLeaseEnd>
	</record>
	<record>
		<username>linux</username>
		<mac>00:50:da:cf:ff:7f</mac>
		<ip>74.115.183.253</ip>
		<start_time>1310050251</start_time>
		<stop_time/>
		<sessionID>e0a956f323ba223f4fe5546096a13f9e</sessionID>
		<DHCPLeaseStart>1310050251</DHCPLeaseStart>
		<DHCPLeaseEnd>1310079814</DHCPLeaseEnd>
	</record>
</result>
```

The default admin level required for this feature is 6. The GET string to send is as follows: https://patriot.[domain]/cli/?function=SearchSessions&username=[username]&password=[password]&action=search&user=&mac=&ip=&online=&start=&stop=

 This document © 2011 First Network Group Inc. All Rights Reserved

An example of a properly formatted URL that would return all session records (not recommended) is as follows:
https://patriot.network1.net/cli/?function=SearchSessions&username=apiuser&password=apipass&action=search&user=&mac=&ip=&online=&start=&stop=

You can mix and match the search parameters which are username (user), MAC address (mac), IP Address (ip), online (online), start and stop. Most of these are self explanatory. Start and Stop are EPOCH times of which, if specified, a session must overlap in some way before it will be returned.

Example searches:

https://patriot.network1.net/cli/?function=SearchSessions&username=apiuser&password=apipass&action=search&user=jim&mac=&ip=&online=&start=&stop= would return all sessions for the user: jim.

https://patriot.network1.net/cli/?function=SearchSessions&username=apiuser&password=apipass&action=search&user=jim,jane&mac=&ip=&online=&start=&stop= would return all sessions for either the user jim or jane.

https://patriot.network1.net/cli/?function=SearchSessions&username=apiuser&password=apipass&action=search&user=jim&mac=00:00:89:0c:51:13&ip=&online=&start=&stop= would return all sessions for user: jim, but only if his MAC address is: 00:00:89:0c:51:13

https://patriot.network1.net/cli/?function=SearchSessions&username=apiuser&password=apipass&action=search&user=jim&mac=00:00:89:0c: 51:13&ip=&online=1&start=&stop= would return all sessions for user: jim, but only if his MAC address is: 00:00:89:0c:51:13 and they are currently online.

https://patriot.network1.net/cli/?function=SearchSessions&username=apiuser&password=apipass&action=search&user=jim&mac=00:00:89:0c:51:13&ip=&online=1&start=1222796365&stop=1225388388 would return all sessions for user: jim, but only if his MAC address is: 00:00:89:0c:51:13 and he is currently online and only if some part of the session overlapped the start-stop time period given.

Get Network Config

This API call will return an XML formatted result set containing the entire DHCPatriot Shared Network and subnet of Authenticated DHCP, Standard DHCP and DHCPv6. This is useful as some of the IDs that are returned may be needed by other API

 This document © 2011 First Network Group Inc. All Rights Reserved

functions to identify the record you want to work with. A result will look something like the sample below:

```
<result>
        <SharedNetwork>
                <NetworkName>SomeNetwork</NetworkName>
                <NetworkType>Authenticated</NetworkType>
                <NetworkID>6</NetworkID>
                <Subnet>
                        <SubnetType>Unauthenticated</SubnetType>
                        <SubnetID>3</SubnetID>
                        <wire>3.3.3.0</wire>
                        <mask>255.255.255.0</mask>
                        <gateway>3.3.3.1</gateway>
                        <start>3.3.3.2</start>
                        <stop>3.3.3.254</stop>
                </Subnet>
                <Subnet>
                        <SubnetType>Authenticated</SubnetType>
                        <SubnetID>9</SubnetID>
                        <wire>4.4.4.0</wire>
                        <mask>255.255.255.0</mask>
                        <gateway>4.4.4.1</gateway>
                        <start>4.4.4.2</start>
                        <stop>4.4.4.254</stop>
                </Subnet>
        </SharedNetwork>
</result>
```

The GET string for this API call is: https://patriot.network1.net/cli/?function=GetNetworkConfig&username=[user]&password=[pass]

A correctly formatted URL would look like this: https://patriot.network1.net/cli/?function=GetNetworkConfig&username=apiuser&password=apipass

Standard DHCP

These API calls provide access to certain Standard DHCP configuration items.

List Known Client

This API call returns an XML list of the Standard DHCP Actions -> Known client assignments in the Web Administration Interface. A sample of the result is shown below:

 This document © 2011 First Network Group Inc. All Rights Reserved

```
<result>
        <record>
                <IDENT>John Doe</IDENT>
                <REMOTE_MAC>00:03:05:fc:fe:fa</REMOTE_MAC>
                <tftp_file/>
                <ID>1</ID>
        </record>
</result>
```

The GET URL to use is as follows: https://patriot.network1.net/cli/?function=KnownClient&username=[user]&password=[pass]&ACTION=LIST

A properly formatted URL would look like this: https://patriot.network1.net/cli/?function=KnownClient&username=apiuser&password=apipass&ACTION=LIST

Add Known Client

This allows a known client to be added via the API. Known client can be found in the Web Administration Interface under Standard DHCP Actions.

The GET URL to use is as follows: https://patriot.network1.net/cli/?function=KnownClient&username=apiuser&password=apipass&ACTION=ADD&mac=[some mac]&IDENT=[some text]&TFTPfile=[some file] IDENT and TFTPfile are optional. mac is required.

A properly formatted URL should look something like this: https://patriot.network1.net/cli/?function=KnownClient&username=apiuser&password=apipass&ACTION=ADD&mac=01:03:05:11:10:09&IDENT=Jose%20Aldo&TFTPfile=some.file

Edit Known Client

This API call allows the complete edit of an entry under Standard DHCP Actions -> Known Client in the Web Administration Interface. First, the List Known Client API call must be used to get the ID of the entry that you wish to edit as it must be supplied during the edit.

The GET URL to use is as follows: https://patriot.network1.net/cli/?function=KnownClient&username=apiuser&password=apipass&ACTION=EDIT&mac=[some mac]&IDENT=[some text]&TFTPfile=[some mac]&id=[id] mac and id are required fields. Please note that this works more like a replacement as you will need to fill out all of the fields with the values you want in the entry. If the field is left blank, then it will become blank in the entry.

 This document © 2011 First Network Group Inc. All Rights Reserved

A properly formatted URL should look something like this: https://patriot.network1.net/cli/?function=KnownClient&username=apiuser&password=apipass&ACTION=EDIT&mac=01:03:05:11:10:45&IDENT=John%20Doe&TFTPfile=some.other.file&id=1

Delete Known Client

This API call allows the deletion of an entry from Standard DHCP Actions -> Known Client in the Web Administration Interface. First, the List Known Client API call must be used to get the ID of the entry that you wish to delete as it must be supplied during the delete operation.

The GET URL is as follows: https://patriot.network1.net/cli/?function=KnownClient&username=apiuser&password=apipass&ACTION=DELETE&id=[id] id is a required field.

A properly formatted URL should looks something like this: https://patriot.network1.net/cli/?function=KnownClient&username=apiuser&password=apipass&ACTION=DELETE&id=1

List Static IP Assignments

This API call returns an XML list of the Standard DHCP Actions -> Static IP Assignment in the Web Administration Interface. A sample of the result is shown below:

```
<result>
        <record>
                <SharedNetwork>test</SharedNetwork>
                <StaticSubnet>1.1.1.0/24</StaticSubnet>
                <Identifier>John Doe</Identifier>
                <IPAddress>1.1.1.10</IPAddress>
                <TypeofMatch>Circuit ID</TypeofMatch>
                <MatchString>1/4/ethernet42/vlan4</MatchString>
                <TFTPFile/>
                <id>34288</id>
        </record>
</result>
```

The GET URL is as follows: https://patriot.network1.net/cli/?function=StaticIPassign&username=[user]&password=[pass]&ACTION=LIST

A properly formatted URL would look something like this: https://patriot.network1.net/cli/?function=StaticIPassign&username=apiuser&password=apipass&ACTION=LIST

 This document © 2011 First Network Group Inc. All Rights Reserved

Add Static IP Assignment

This allows a Standard Static Assignment to be added via the API. Standard Static Assignment can be found in the Web Administration Interface under Standard DHCP Actions. Please note that an id of the appropriate subnet must be obtained from the Get Network Config API call to be used during the add.

The GET URL is as follows: https://patriot.network1.net/cli/?function=StaticIPassign&username=apiuser&password=apipass&ACTION=ADD&StaticSubnetID=[some id]&Ident=[some text]&IP=[some ip]&MatchType=[REMOTE_MAC/agent_circuit_id/agent_remote_id]&MatchString=[some match string]&TFTPfile=[some tftp file] StaticSubnetID, IP, MatchType and MatchString are all required fields. Ident and TFTPfile are optional.

A properly formatted URL looks like: https://patriot.network1.net/cli/?function=StaticIPassign&username=apiuser&password=apipass&ACTION=ADD&StaticSubnetID=3&Ident=Jose%20Aldo&IP=10.22.22.3&MatchType=REMOTE_MAC&MatchString=99:98:97:00:01:02&TFTPfile=PlusSign.png

Edit Static IP Assignment

This allows a Standard Static Assignment to be edited via the API. Standard Static Assignment can be found in the Web Administration Interface under Standard DHCP Actions. Please note that an id of the appropriate subnet must be gotten from the Get Network Config API call to be used during the edit. Additionally, the List Static IP Assignments must be used to get the id of the entry that you wish to edit.

The GET URL is as follows: https://patriot.network1.net/cli/?function=StaticIPassign&username=[user]&password=[pass]&ACTION=EDIT&StaticSubnetID=[some subnet id]&Ident=[some text]&IP=[some ip]&MatchType=[REMOTE_MAC/agent_circuit_id/agent_remote_id]&MatchString=[some match string]&TFTPfile=[some tftp file]&id=[some entry id] StaticSubnetID, IP, MatchType, id and MatchString are all required fields. Ident and TFTPfile are optional. Please note that this works more like a replacement as you will need to fill out all of the fields with the values you want in the entry. If the field is left blank, then it will become blank in the entry.

A properly formatted URL looks like: https://patriot.network1.net/cli/?function=StaticIPassign&username=apiuser&password=apipass&ACTION=EDIT&StaticSubnetID=4&Ident=John%20Doe&IP=10.23.23.12&MatchType=agent_circuit_id&MatchString=chassis12:vlan4:port1&TFTPfile=UserManual-v.5.4.pdf&id=34292

 This document © 2011 First Network Group Inc. All Rights Reserved

Delete Static IP Assignment

This API call allows the deletion of an entry from Standard DHCP Actions -> Static IP Assignment in the Web Administration Interface. First, the List Static IP Assignment API call must be used to get the ID of the entry that you wish to delete as it must be supplied during the delete operation.

The GET URL is as follows: https://patriot.network1.net/cli/?function=StaticIPassign&username=[user]&password=[pass]&ACTION=DELETE&id=[id] id is a required field.

A properly formatted URL looks like: https://patriot.network1.net/cli/?function=StaticIPassign&username=apiuser&password=apipass&ACTION=DELETE&id=34292

DHCPatriot Version 5 Operations Manual This document © 2011 First Network Group Inc. All Rights Reserved

Chapter 12: Supporting DHCPatriot End-Users

Supporting end users on the DHCPatriot system is easy compared to other similar systems due to the tools available on the Web Administration Interface. These tools will help support personnel diagnose the problem quickly. Diagnosis is usually the longest part of any support call, and so support personnel will appreciate this.

How to Troubleshoot

The first step is to find out whether the customer is on Authenticated or Standard DHCP. This may be well known if the ISP is only using one or the other, or if customer equipment is only on Authenticated DHCP, for example. After that, find out if the user is able to receive an IP address. If they are getting an IP address and their equipment is setup for DHCP, then the DHCPatriot system is working properly. If they have not gotten an IP address, then the problem lies in one of three places: customer equipment; transport (such as DSLAM or Cable Access Router or connections in between); or with the DHCPatriot. Follow the sections below for further information.

Authenticated DHCP

Authenticated DHCP requires the customer to register (authenticate) their device before they can use a public address. The user may get an unauthenticated address (usually this is a private address of some kind). The user may also get an authenticated address (this is usually a public address).

If the customer is getting a private (unauthenticated) address, they have not yet registered or they are suspended. If they cannot get the login page, have them try browsing directly to the IP address of the primary DHCPatriot device. If they get the login page, have them log in. If they do not, you can manually authenticate them.

After they get the public (authenticated) IP address, they may or may not be able to browse. If they can, then there may be a routing problem with the private addresses. If they cannot browse, and there is no network outage, then the problem likely lies with their device and should be troubleshot normally. If they were able to get the login page by IP but not when visiting http://www.microsoft.com, for example, then there is probably a problem with the policy routing. Network personnel should be contacted.

If the customer device is NOT getting an IP address, then Search DHCP Logs and or General Troubleshooting Techniques later in this chapter should be consulted.

Authorize Customer

From time to time, it may be necessary for technical support personnel to authorize a customer device. The customer may not be able to get to the login page. Some devices do not have a web browser, such as a Playstation 3 or an Xbox 360. If a router of some

 This document © 2011 First Network Group Inc. All Rights Reserved

kind is not deployed at the customer border, these devices may need to be manually authenticated by technical support personnel.

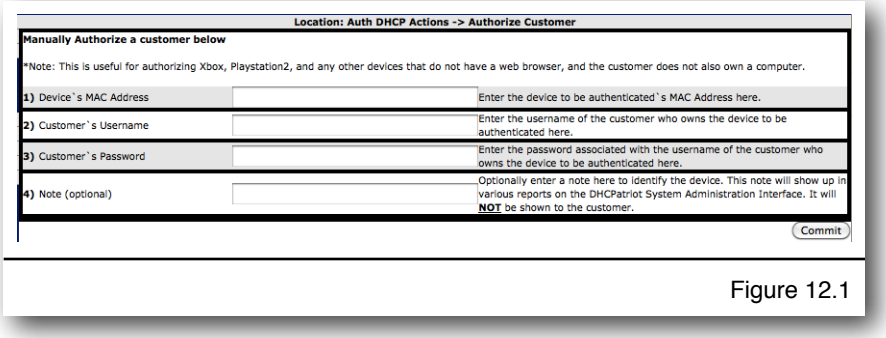


Figure 12.1

To authorize a customer device, expand the Auth DHCP Actions menu and click on Authorize Customer. A screen similar to that shown in figure 12.1 should appear. Enter the user device's MAC address or current IP address, the customer's username and password. Enter a note, if desired. These notes will show up in various places throughout the interface in conjunction with the device. These notes are typically used to note what type of hardware the device is, if necessary. Click on Commit to complete the process. Error messages will be similar to those mentioned in the Authentication Problems section later in this chapter.

Standard DHCP

Standard DHCP does not require authentication. There are, however, a couple situations where the user device may need to be included in the DHCPatriot interface for the user to get an IP address.

If the user device is not getting an IP address, and is setup for DHCP, verify that the client does not need to be a known client, or is in the known client table (Standard DHCP Actions -> Known Client on the Web Administration Interface). Contact your network administrator if you have questions about this.

It could also be that the client needs to have a static assignment. Verify that the client does not need a static assignment or is listed in the static assignment table (Standard DHCP Actions -> Static Assignment on the Web Administration Interface). Contact your network administrator if you have any doubts.

If the device still cannot obtain an IP address, there may be a problem on the device or on the network. Searching the DHCP logs and other things can be used to obtain more information. Take a look at Search DHCP Logs and General Troubleshooting Techniques later in the chapter.

Search DHCP Logs

The DHCP logs are available under both the Auth DHCP Reports and Standard DHCP Reports menus. These reports are essentially the same. They show the same results and have the same method of operation.

To access this report, expand the Auth DHCP Reports menu and then click on Search DHCP Logs. A screen similar to figure 12.2 should appear. You can search by some

 This document © 2011 First Network Group Inc. All Rights Reserved

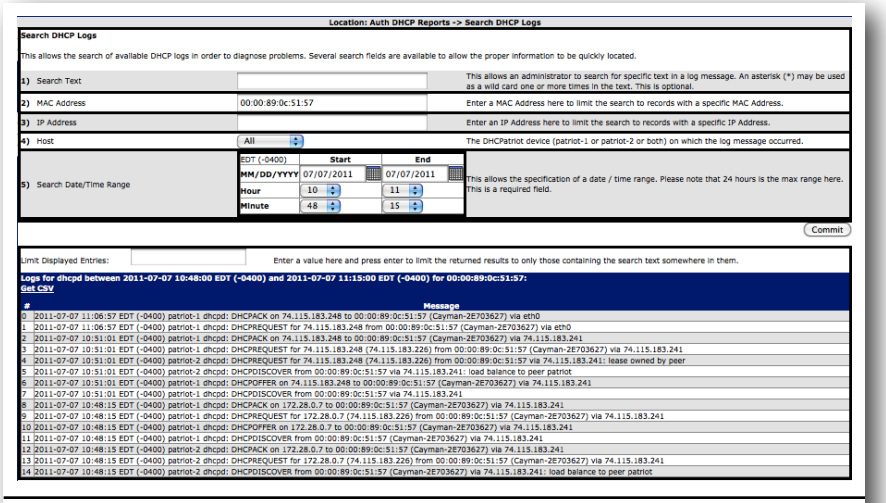


Figure 12.2

arbitrary text, MAC address, IP address, Host, and time period. The maximum time period that can be displayed is 26 hours (any 26 hour time period for the last 30 days). The default search time period is from one hour before now to one hour after now. This makes it easy to just look at current logs.

The results are shown newest first extending back to oldest. If no search parameters are entered (such as MAC address or IP address) you will likely see informational messages that do not pertain to a specific client. You also may see information about other clients that may make it difficult to find the specific results that you are looking for.

General Troubleshooting Techniques

This section will guide you through the techniques used to discover the likely problem that a client may have with DHCP. It should not be considered a guide to repairing problems that a client may have as repair techniques vary widely based on the involved equipment. It should help you isolate the problem, however, so that a solution may be pursued.

Problems that client's might experience can be boiled down to either they cannot get an IP address to begin with, or they cannot keep the IP address. Things that might cause these problems can be boiled down to problems with the client itself, problems with the DHCP server, or problems with the transport (ie: the service itself).

Client problems can be related to firewall settings, configuration problems (ie: the client is not setup for DHCP), software that does not function properly, or hardware that is not working properly (such as the ethernet card).

Server problems can be related to the DHCP server configuration, or the DHCP server actually being down or unreachable. This is typically not going to be the case unless several clients are down. Problems that are related to only one client would be limited to not being a standard known client or not having a standard static assignment when one of these is necessary on the network the client is connected to.

Transport problems could be related to a wiring problems (anywhere from the back of the client device all the way to the DHCP server), signaling problems with the service, a

 This document © 2011 First Network Group Inc. All Rights Reserved

configuration problem with the service, or the service actually being down. Isolating these problems may require the involvement of network administrators.

When a customer cannot get or keep an IP address, the first step should be obtaining a MAC address from them, then accessing the DHCP log search (Auth/Standard DHCP Reports -> Search DHCP Logs). Input the MAC address into the appropriate search field and click on Commit. The results shown will show what type of DHCP activity (if any) has occurred between the client and the server. If no DHCP activity is shown, have the user turn the device off and turn it back on again (power cycle). After the device boots, see if there is DHCP activity by performing the search again.

Normal DHCP activity should be similar to what appears in figure 12.3 and 12.4 which are the obtaining of a new lease and renewing an existing lease respectively. The first step in the process is the communication from figure 12.3 when the client obtains a new lease from the DHCP server. As can be seen from the example, both DHCPatriot devices should receive the DHCPDISCOVER (which comes from the client). The next step is the DHCPOFFER from the server. This should only come from one of the servers, but may come from both under certain circumstances. The client should send a DHCPREQUEST for the offered address. The server should respond with DHCPACK. This packet should come from the offering server.

0	2011-07-11 12:05:03 EDT (-0400) patriot-1 dhcpd: DHCPREQUEST for 74.115.183.254 (74.115.183.227) from 00:a0:cc:d9:96:a2 via 74.115.183.241: lease owned by peer
1	2011-07-11 12:05:03 EDT (-0400) patriot-1 dhcpd: DHCPDISCOVER from 00:a0:cc:d9:96:a2 via 74.115.183.241: load balance to peer patriot
2	2011-07-11 12:05:03 EDT (-0400) patriot-2 dhcpd: DHCPACK on 74.115.183.254 to 00:a0:cc:d9:96:a2 (windowstest) via 74.115.183.241
3	2011-07-11 12:05:03 EDT (-0400) patriot-2 dhcpd: DHCPREQUEST for 74.115.183.254 (74.115.183.227) from 00:a0:cc:d9:96:a2 (windowstest) via 74.115.183.241
4	2011-07-11 12:05:03 EDT (-0400) patriot-2 dhcpd: DHCPOFFER on 74.115.183.254 to 00:a0:cc:d9:96:a2 (windowstest) via 74.115.183.241
5	2011-07-11 12:05:03 EDT (-0400) patriot-2 dhcpd: DHCPDISCOVER from 00:a0:cc:d9:96:a2 via 74.115.183.241

Figure 12.3

16	2011-07-11 10:17:01 EDT (-0400) patriot-1 dhcpd: DHCPACK on 74.115.183.248 to 00:00:89:0c:51:57 (Cayman-2E703627) via eth0
17	2011-07-11 10:17:01 EDT (-0400) patriot-1 dhcpd: DHCPREQUEST for 74.115.183.248 from 00:00:89:0c:51:57 (Cayman-2E703627) via eth0

Figure 12.4

None of that conversation may happen, which could mean several things. The client could have a configuration problem, broken hardware or broken software. It also could be that the service is down, there is a configuration issue with the service or there is a wiring problem. Have the customer hook up some other equipment configured for DHCP. If that equipment functions properly, then the problem is likely with their device, if not, then there may be a service problem.

It could be that only part of it such as DHCPDISCOVER / DHCPOFFER which may repeat over and over with no DHCPREQUEST and DHCPACK. This usually means that there is a firewall problem on the client or that there is a service or wiring problem of some kind. Ensure that the client has UDP ports 67 and 68 open so that DHCP communication can occur. Have the customer try a different device. If that device won't work, then it is likely a wiring problem or service problem.

 This document © 2011 First Network Group Inc. All Rights Reserved

The client should renew the lease every half lease length, or at least before the end of the lease. A typical conversation is shown in figure 12.4. The client sends a DHCPREQUEST and the server responds with DHCPACK. At that point, the lease is good for another lease period (default is 8 hours).

A typical problem that may be encountered would be that this renew conversation doesn't happen at all. If this is the case, and the customer is able to use the Internet, it may be that a firewall is preventing proper operation or that there is some software problem with the client. Ensure that the client has UDP ports 67 and 68 open so that DHCP communication can occur. If the customer cannot browse, there may be a problem with the service. Have the customer try a different device to see if that resolves the problem.

Renews can also happen more frequently than expected. Frequent renews usually aren't a problem unless the client doesn't seem to realize that it was successful and drops the lease at the end of the original lease period. This could indicate a firewall problem or some sort of software problem on the client end, or a transport problem of some kind when accompanied by the client not being able to go anywhere when they clearly have a lease (ie: the client knows about the lease and so does the server). Be sure that the client has UDP ports 67 and 68 open so that DHCP communication can occur. Have the customer try a different device to see if that resolves the problem.

As noted previously, the above is not a comprehensive list, nor does it give instruction of how to perform these operations on the client. If there are unknown situations encountered, or there are questions, please contact your network administrator. Your network administrator may elect to call First Network Group for support.

Authentication Problems

If the DHCPatriot system is setup to perform authentication of users using the Captive Portal screen, users could have trouble with this process. Basically, this type of problem falls into two categories. The user may not be getting the authentication page. The user gets the authentication page, but cannot authenticate. Resolving these problems is fairly simple.

If the user does not get the authentication page when they open their web browser, find out if the user has gotten an IP address from the DHCPatriot system, and that the IP address is an unauthenticated IP address. Have them browse directly to one of the IP addresses of the DHCPatriot system. If they receive the captive portal login screen, then there is likely a problem with the "policy routing" and the network administrator should be notified. If they do NOT get the login screen, then it becomes a bit more complicated. The problem may lie with the customer equipment, or there could be a routing problem. The customer can be manually authenticated by going to Auth DHCP Actions -> Authorize Customer.

 This document © 2011 First Network Group Inc. All Rights Reserved

If the user gets the authentication page, but cannot authenticate, it may be a problem with their username and password, or it could be some other problem. Be sure and get the error message from the user. The list provided here will correlate the error message with possible causes and remedies.

1. **You are already authenticated on MAC Address <MAC>. There is no need to authenticate again at this time. Please restart your connected equipment and visit another site such as: Sony.com or Wikipedia.org**
   1.1. The MAC address is already known to the DHCPatriot system and is not suspended.
   1.2. Have the user reboot their connected equipment. Have them try again.
2. **Cannot authenticate <MAC> registering to user <USER> at this time. It is currently online. The current session will expire at <TIME>.**
   2.1. This means that the MAC address is already seen as online by the DHCPatriot system.
   2.2. This situation should resolve itself automatically, if it does not after a few minutes, First Network Group should be contacted as there may be a problem with the DHCPatriot system.
3. **Access was rejected for user: <USER>.**
   3.1. This means the username or password is incorrect.
   3.2. Verify the username and password.
4. **Authentication server failed to respond. Please try to authenticate again.**
   4.1. This means the authentication server may be down.
   4.2. Contact Network Administrator.

 This document © 2011 First Network Group Inc. All Rights Reserved

Chapter 13: User Based Tasks for Customer Service

Customer service personnel will need to interact with certain processes on the DHCPatriot system. Most will at least use Suspend User for monthly non-pay disconnects. If Built-in Authentication is used on the DHCPatriot system, they will also need to add users with Built-in Authentication: User Maintenance. These procedures are detailed below.

Suspend User

From time to time, it may be necessary to suspend one or more users. The DHCPatriot system contains a suspend user interface where one or more users can be suspended. The users may be suspended by username or by MAC address. A note may be left for the user indicating some action that should be taken, such as contacting the billing office. This note will be displayed on the Captive Portal screen when the user's device displays it.

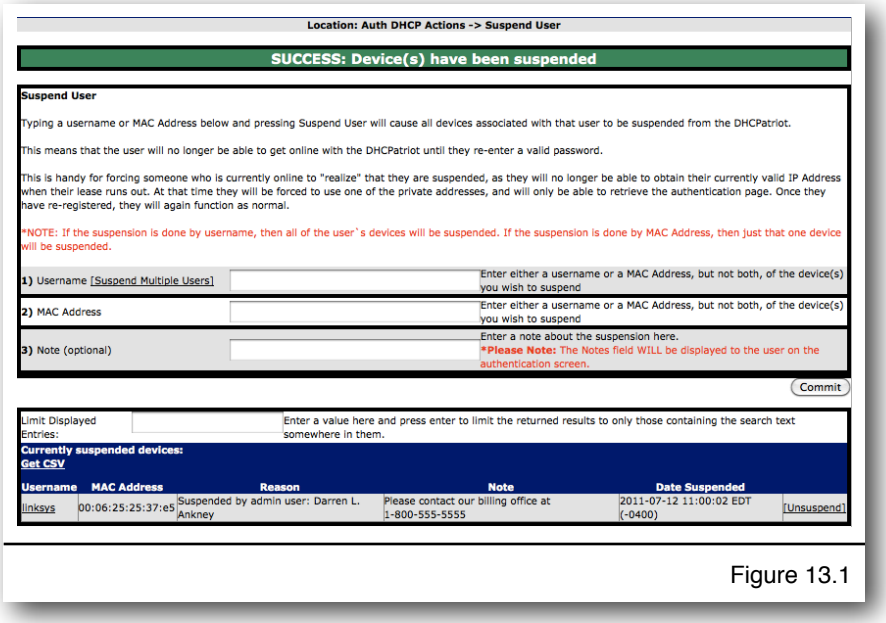


Figure 13.1

To access Suspend User, expand the Auth DHCP Actions menu and click on Suspend User. A screen similar to figure 13.1 will be shown. A username or MAC address as well as optional note may be entered here and then click on Commit. At that point, the user device(s) will be suspended and added to the list at the bottom. Multiple users may be suspended by clicking on the Suspend Multiple Users link in the username field. The username box will change to a text box. Enter as many users as necessary one per line. A note may be entered and will be applied to all users. Click on Commit. Summary messages will appear at the top warning you of any users that were not found.

If the users are only suspended on the DHCPatriot system, and not in the Built-in Authentication or external RADIUS server, it is considered a temporary suspend. The user will be able to get back on immediately by entering their username and password. This can be useful when attempting to warn a user of something, such as a virus. Include a note when doing this, and the user will see the note prior to logging on. If the user is suspended in both places, they will not be able to log back on until they are re-enabled in the external RADIUS server or the Built-in Authentication (whichever is in use). It should be noted that if a user is suspended in the Built-in Authentication that

 This document © 2011 First Network Group Inc. All Rights Reserved

they are also suspended here simultaneously, and there is no need to suspend them here as well.

Built-in Authentication: User Maintenance

If the DHCPatriot system is using authenticated DHCP, and not using an external RADIUS server, then Built-in Authentication is in use. This allows users to be added edited, suspended (singly or en-masse), and deleted. Static IP addresses can be assigned to users in this interface as well. Some sort of identifier may be added as well, such as a customer id or simply the customer's name.

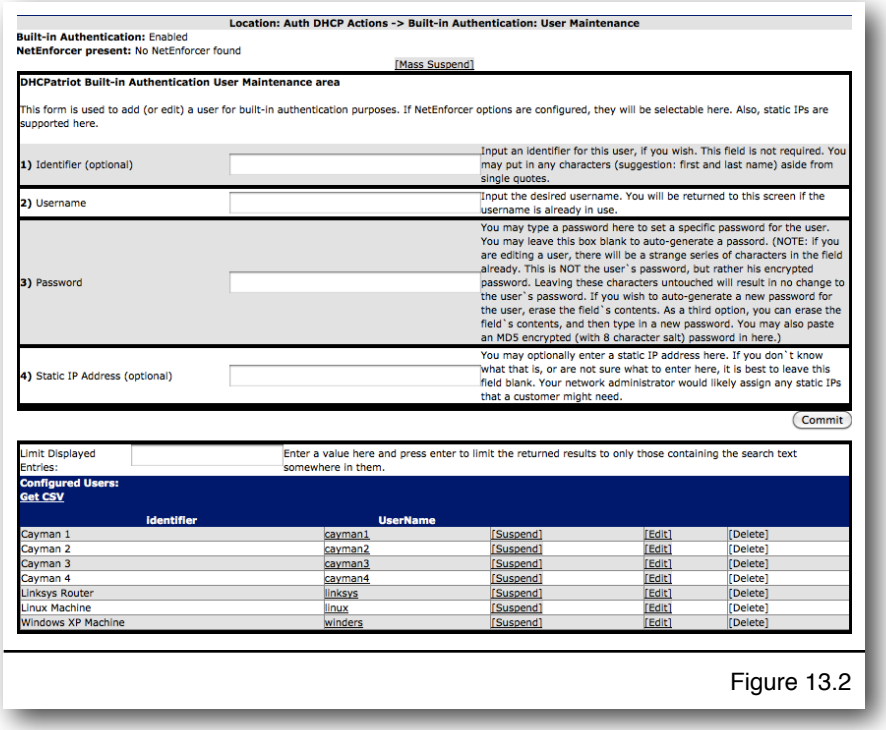


Figure 13.2

To access the user maintenance area, expand the Auth DHCP Actions menu and click on Built-in Authentication: User Maintenance. A screen similar to that shown in figure 13.2 should appear. From this screen, using the form, a user can be added. A user can be suspended, edited and deleted from the list at the bottom. A mass suspend of users can also be performed.

Adding a User

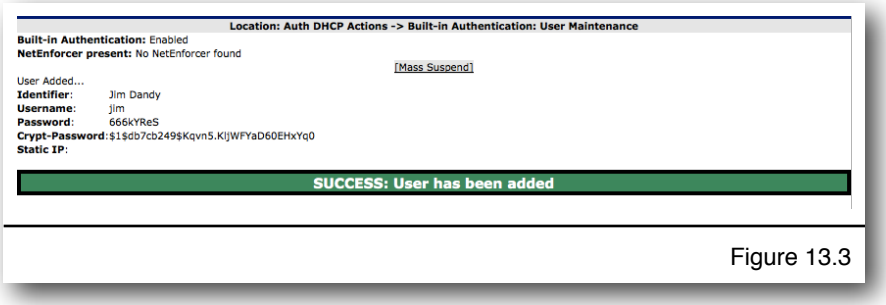


Figure 13.3

To add a user, complete the form similar to the one shown in figure 13.2. Identifier is an optional field and should be used for the customer's name or some other identifying information such as a customer billing ID. Both username and password are required fields. Please note that password may be left blank to auto-generate a password. Static IP Address is an optional field that should only be completed if your network administrator has advised that the customer will be receiving a static or fixed IP address. Simultaneous use restriction restricts the user to the number of simultaneous IP addresses chosen here. This overrides the General Settings default setting (even if it is not set). After completing the form, click on Commit. Figure 13.3 shows the resulting information that will appear at the top of the screen. The user information, including password, can be confirmed here.

 This document © 2011 First Network Group Inc. All Rights Reserved

Editing a User

To edit a user, locate the desired user in the list at the bottom. Click on the edit link. The add form will then be filled out with the user's current information. Make the necessary changes and click on Commit. A summary screen similar to that in figure 13.3 will appear so that the changes may be confirmed.

Suspending One or More Users / Enabling suspended users

To suspend a user, locate the desired use in the list at the bottom. Click on the suspend link for that user. Confirm that you really desire to suspend the user. A message will appear confirming that the user has been suspended.

To suspend multiple users, click on the Mass Suspend link at the top of the screen. A screen similar to that in figure 13.4 will appear. Enter the users to suspend one username per line as shown in the figure 13.4 example. A note may also be entered here as these users will be suspended in the Auth DHCP Actions -> Suspend User area. This note will be applied there and will be shown to the user on the Captive Portal screen. Contact our Billing office at <phone #>, for example, would be an appropriate note. Click the Commit button.

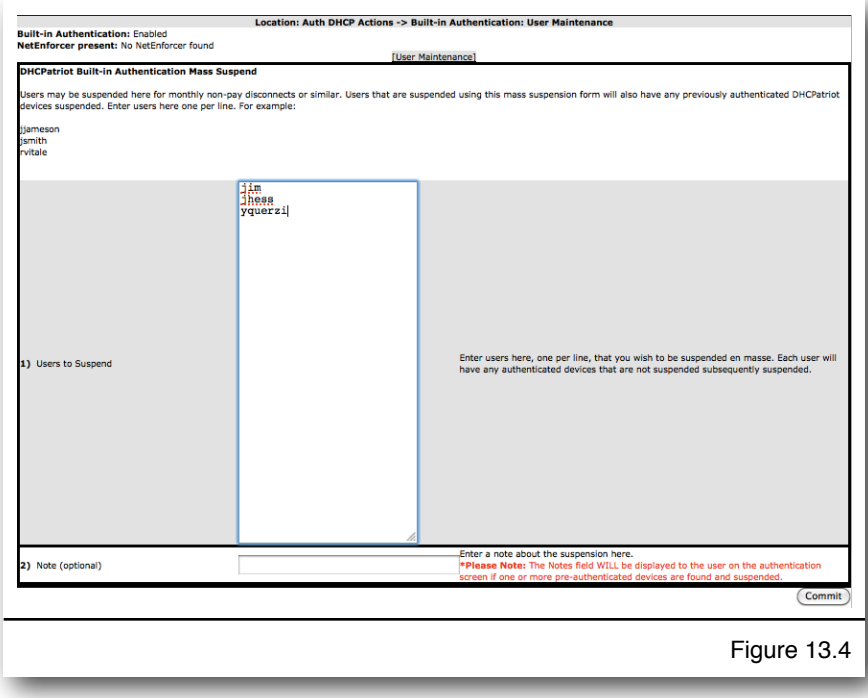


Figure 13.4

Two return messages will be displayed. The first refers to the suspending the user in Auth DHCP Actions -> Suspend User. This suspension may fail for one or more users if they have not registered a device, or are already suspended there. The second message refers to suspending the users in Built-in Authentication: User Maintenance. Unless one of the users entered here is already suspended, or not found, this should succeed. To return to normal user maintenance, click the User Maintenance link at the top of the screen.

To enable a user, locate the user in the list. Click on the Unsuspend link. Click OK on the resulting confirmation dialogue box.

 This document © 2011 First Network Group Inc. All Rights Reserved

Deleting a User

To delete a user, locate the user in the bottom list. Click the Delete link for that user. Please note that the Delete link will not be active unless the user is suspended. After clicking the Delete link, a confirmation box will appear. Answer OK and the user will be deleted.

Built-in Authentication: User Import

New in version 5.4.0, the DHCPatriot system now supports importation of a list of users to the built-in authentication interface via a Comma Separated Value (CSV) file. This file requires that the first two columns be username and password. Three optional columns are also allowed which are identifier, static IP address, and simultaneous use Restriction.

The username column should contain only the username for the user. The password should contain only the plain text/unencrypted password for the user. The optional identifier column should contain some sort of identifier such as a name or account number. Static IP address column should contain a standard IPv4 address that you wish to be assigned to the customer's device. The simultaneous use restriction column should contain a numeric value that would denote how many times the user can get online (overriding the global setting). Valid values for this column are 1,2,3,4,5,10,15,20,25,30,40, and 50.

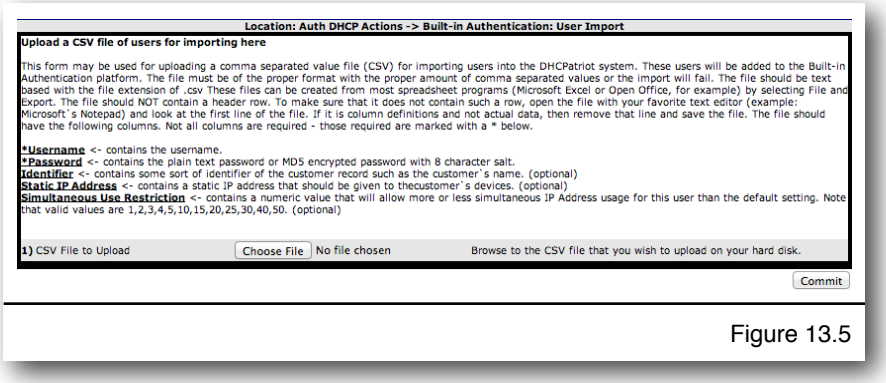


Figure 13.5

Please note that the .csv file MUST NOT contain a column header row. The row will seem to the system like it is user data to be entered and so MUST NOT exist.

The content of a properly formated .csv file might look something like this:
lisa,eddie01,Lisa Walker,1.2.3.4,3
centreclean,walleye,Jim Bob,,
actrisco,efy9?qr.,Adam Truebond,,2
bbwessel,BB.w3ss3l,Brent Bond,,
westsidesauk,azaz,Jim's Gas Station,,
clarsue,8d?y3cnw,Clark Clarkson,,
philp,8wnb!s5y,Phillip D Larson,,
armitchell,LOOdan22,Mitchell Allenson,4.3.2.1,50

 This document © 2011 First Network Group Inc. All Rights Reserved

To access this function, expand the Auth DHCP Actions menu and click on Built-in Authentication: User Import. A screen similar to that in figure 13.5 should appear. Click on the “choose File” button and navigate to the place on your hard drive that contains the .csv file to import. Choose the file and click OK. Click on the Commit button. The DHCPatriot will parse the file and display a preview of what it is going to import with an OK and Cancel button similar to that shown in figure 13.6. If there are errors that you need to correct, click cancel. If everything looks ok, click on OK. The import will occur and you will get a confirmation screen similar to figure 13.7. The imported users should now appear in Built-in Authentication: User Maintenance under the Auth DHCP Actions menu.

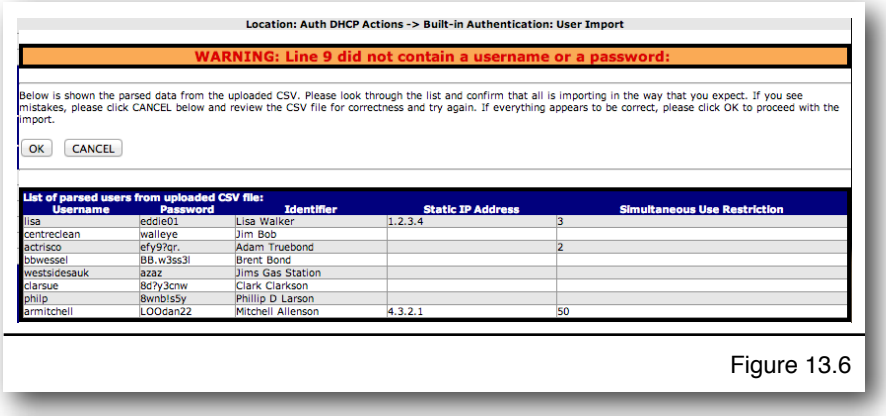


Figure 13.6

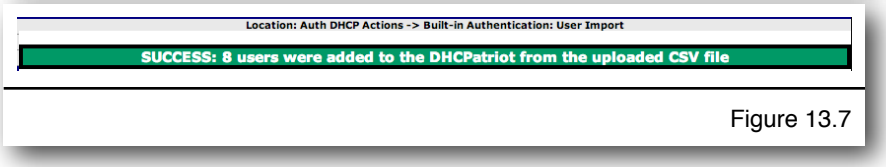


Figure 13.7

Device Import

As of version 5.4.0, the DHCPatriot system supports importing a list of devices with username and password for authentication through the use of a Comma Separated Value (CSV) file. The imported devices will be added in the same manner as if an administrator had authenticated them using Auth DHCP Actions -> Authorize Customer.

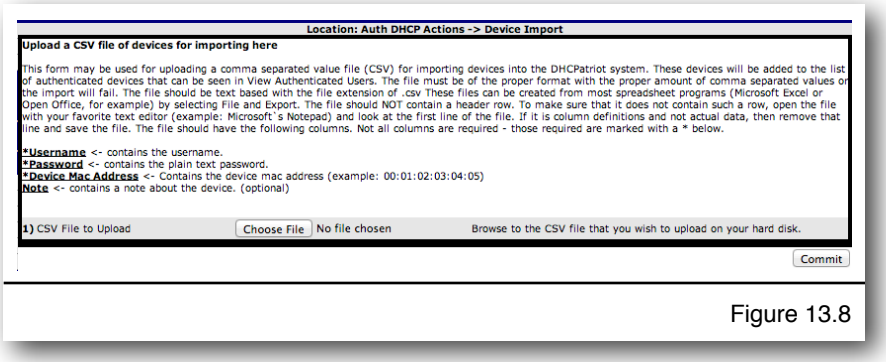


Figure 13.8

There are four possible fields in the the CSV file. The first three fields are required and the fourth is optional. The fields are: username, password, MAC address, and note which is optional. The password shall be unencrypted/plain text. The MAC address can be in any format that is supported on the DHCPatriot web interface (xx:xx:xx:xx:xx:xx, xx-xx-xx-xx-xx-xx, xxxx.xxxx.xxxx, xxxxxxxxxxxx).

Please note that the .csv file MUST NOT contain a column header row. The row will seem to the system like it is user data to be entered and so MUST NOT exist.

The content of a properly formated .csv file might look something like this:

```
lisa,eddie01,00:01:36:11:2A:50,This has a static ip
centreclean,walleye,00:01:6C:52:8E:96,
```

 This document © 2011 First Network Group Inc. All Rights Reserved

```
actrisco,efy9?qr7,00:01:6C:67:5A:97,
bbwessel,BB.w3ss3l,00:03:47:D1:C4:F0,
westsidesauk,azaz,00:03:6D:1A:64:F4,
clarsue,8d?y3cnw,00:04:5A:42:12:18,
philp,8wnb!s5y,00:04:5A:EF:7D:7C,
armitchell,LOOdan22,00:04:5A:F6:61:A1,This has a static ip
```

To access this function, expand the Auth DHCP Actions menu and click on Device Import. A screen similar to that in figure 13.8 should appear. Click on the “choose File” button and navigate to the place on your hard drive that contains the .csv file to import. Choose the file and click OK. Click on the Commit button. The DHCPatriot will parse the file and display a preview of what it is going to import with an OK and Cancel button similar to that shown in figure 13.9. If there are errors that you need to correct, click cancel. If everything looks ok, click on OK. The import will occur and you will get a confirmation screen similar to figure 13.10. If there are any errors, they will be displayed on this screen. The imported user devices should appear in Auth DHCP Reports -> View Authenticated Devices.

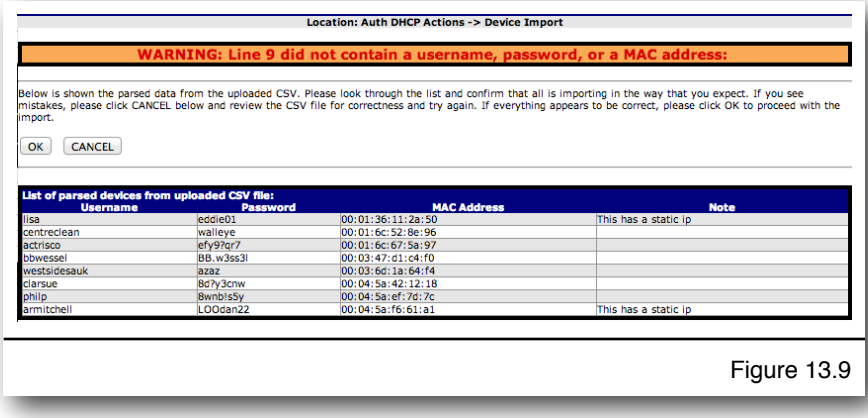


Figure 13.9

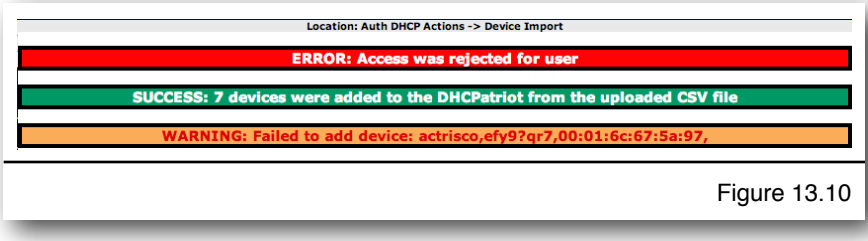


Figure 13.10

 This document © 2011 First Network Group Inc. All Rights Reserved

© Copyright 2002-2011
First Network Group Inc
4-6 Perry St.
PO Box 1662
Wapakoneta, OH 45895
DHCPatriot@network1.net
800-578-6381 opt. 3

DHCPatriot™ is a trademark of First Network Group Inc. (http://www.network1.net)
All other names and brands are protected by their respective companies.