



Total DHCP

The version 4.2.0 Total DHCP edition update to the DHCPPatriot™ system software includes a new configuration area for the configuration of standard/non-authenticated DHCP clients. This is useful in situations where a standard method of DHCP is required (ie: without authentication). Examples of use would be providing DHCP services to cable modems, set-top boxes, fiber termination devices at the customer premise, or simply providing DHCP services to the corporate network. These would be configured in addition to authenticated networks for use by the customer devices such as consumer routers or computers.

Features included are as follows:

- Shared network support for linking multiple subnets to the same interface.
- Dynamic subnets.
 - With both non-restricted and restricted leasing to only known-clients.
- Static subnets.
 - With assignment via either MAC address or Option 82 information.
- Maintenance subnets for defining DHCP Relay Agent source IP Addresses (if different from configured dynamic or static subnets).
- TFTP configuration for defining files that need to be delivered to the clients at boot.
 - This includes a built-in TFTP server.
 - External TFTP servers may also be defined.
- Viewing address usage and graphs for the defined networks and subnets on the DHCPPatriot™ is available.
 - Data regarding network utilization is also available via SNMP.

The following excerpt from Appendix L of the DHCPPatriot™ Version 4.2.x Operations Manual demonstrates how easy it is to setup the standard DHCP server.

Example configuration using a simple network

The example network consists of the following kinds of service and devices:

- Cable modem service
 - About 200 cable modem customers.
 - Cable modems require TFTP configuration file.
 - Only allow those cable modems on the network which were distributed by the ISP.
- Fiber to the home (FTTH) service

- About 200 FTTH customers.
- Each FTTH outside CP termination device must remain at the same IP address regardless of the devices MAC address.
- The FTTH DHCP Relay Agents reside in subnet 10.69.254.0/24 which is not part of the static subnet. A maintenance network must be configured to identify the source.

Main States

User States

User Management

Authenticated DHCP

Standard DHCP

Location: Standard DHCP -> Shared Network Config (NEW)					
Currently configured shared networks:					
Shared Network Name	TFTP Server	Lease Length	Dynamic Subnets	Static Subnets	Maintenance Subnets
FNCI-TEST	48 hours	0	0	1	[Edit]
TEST-RESTRICTIONS	local	48 hours	2	1	[Edit]

Shared Network Config (NEW)

Dynamic Subnet Config (NEW)

Known Client Config (NEW)

Static Subnet Config (NEW)

Static IP Assignment (NEW)

Maintenance Subnet Config (NEW)

View Address Usage (NEW)

tftp config (NEW)

System Configuration

Define new or modify existing shared networks here:
A Shared Network defines a group of subnets that all live on the same physical network or interface. Defining a Shared Network here allows you to add dynamic or static subnets to it in the other sections under Standard DHCP Configuration. Defining a network here is only the first step. One or more dynamic, static and/or maintenance subnets will need to be configured before any IP address assignments will be made to customers.

1) Shared Network Name: Example-Cable-Modem-Service [An Arbitrary name for the above Shared Network (DO NOT use special characters ...'-s are ok) (ex: FNCI-ATM)]

2) TFTP Server (optional): local [This is an optional setting allowing the specification of a TFTP server that will tell a device where to get a boot file. If you wish to use the built in TFTP server on the DHCP Patriot system, enter the word 'local' here. If you wish, you may enter an external TFTP server by IP address here.]

3) Lease Length: 8 hours [Set the length of the lease for this network here]

Add/Edit Network

Add a Network for the cable modems

Begin by defining each network under Standard DHCP → Shared Network Config. The Networks that are currently configured are shown at the top of the screen. Each network can be edited and deleted from

this screen as well, but only if it is not in use. Statistics regarding if it is in use, and by what types of subnets are shown here as well. The network must be named, and optionally have a TFTP server assigned to it. Also, lease time is chosen here.

If the local TFTP server is to be used, then Upload the file(s) that will be needed for the TFTP server to distribute to the clients.

Any type of file may be uploaded that may be needed by the client device. The file may be up to 2GB in size. Files that have already been uploaded are displayed above. If the filename is clicked on, a copy of the file may be downloaded

from this page for inspection. The size of the file, MD5sum and the date last modified are displayed here as well so that it may be confirmed that the file has not been changed. If the file is in use (ie: is configured for one or more subnets or clients) it cannot be deleted. If no clients or subnets are configured to use the file, it may be deleted from this area.

Main States

User States

User Management

Authenticated DHCP

Standard DHCP

Location: Standard DHCP -> tftp config (NEW)					
Successfully deleted TFTP file					
These are the TFTP files currently on the system:					
Name	Size	md5sum	Last Modified	In Use By	
test.txt	10 bytes	5afbf0e1bdcc8ea7fb3d071053ef778	2008-01-10 15:04:41 UTC (+0000)	1	
test2.txt	5 bytes	e4439267203fb5277d347eecd6e4a0b5	2008-01-10 20:30:20 UTC (+0000)	2	
test3.txt	177 bytes	571a0922dd07c7888459b1456001df	2008-01-10 21:21:16 UTC (+0000)	2	
test5.txt	625664 bytes	5b9213343e7fb2644677686305e29e81	2008-06-26 19:20:22 UTC (+0000)	1	

Shared Network Config (NEW)

Dynamic Subnet Config (NEW)

Known Client Config (NEW)

Static Subnet Config (NEW)

Static IP Assignment (NEW)

Maintenance Subnet Config (NEW)

View Address Usage (NEW)

tftp config (NEW)

System Configuration

Upload new TFTP files here:
This section is where new TFTP boot files are uploaded. Once uploaded, they will appear in the list above and may be selected for use with any of the Standard DHCP networks. Indicate the desired filename, and browse to the location of the file on your computer below then click upload.

1) Filename: Modern-Config-1.txt [Enter a name for the file you are uploading here.]

2) File to Upload: Desktop/ModemExample.txt [Browse...]

Browse to the file that you wish to upload on your hard disk. Please note that filename is not important here as the name on the server will be set by item number 1 above.

Upload

Upload a TFTP file for use by the cable modems.

Define a dynamic subnet for the cable modem network. Only allow known clients to use this network. A global TFTP file may be configured here. Or a TFTP file may be configured in the known clients, or both. If both are configured, the known client configuration will take precedence. The top of this screen shows the currently configured subnets. These networks may be edited or deleted from this screen.

Main

User States

User Management

Authenticated DHCP

Standard DHCP

Shared Network Config (NEW)

Dynamic Subnet Config (NEW)

Known Client Config (NEW)

Static Subnet Config (NEW)

Static IP Assignment (NEW)

Maintenance Subnet Config (NEW)

View Address Usage (NEW)

tftp config (NEW)

System Configuration

Currently configured dynamic subnets:						
Shared Network Name	CIDR	Gateway	Start Address	Stop Address	TFTP File	Allow only known clients
TEST-RESTRICTIONS	10.100.100.0/24	10.100.100.1	10.100.100.2	10.100.100.254	test3.txt	Yes
TEST-RESTRICTIONS	74.219.83.0/24	74.219.83.1	74.219.83.2	74.219.83.254	test3.txt	No

Location: Standard DHCP -> Dynamic Subnet Config (NEW)

Define new or modify existing Standard Dynamic Subnets here:
A Shared Network defines a group of subnets that all live on the same physical network or interface. Defining a Shared Network allows you to add dynamic or static subnets to it in the other sections under Standard DHCP Configuration. In this area, dynamic subnets can be configured that are attached to a specific Shared Network. It is required that you first have a Shared Network configured to attach the dynamic subnet.

1) Shared Network Example-Cable-Modem-Service Select the Shared Network that this dynamic subnet will be a part of.

2) Wire Address 192.168.254.0 Enter the Wire address of the dynamic subnet here. This is sometimes referred to as the network address. For example: The network 192.168.1.0/24 has wire address: 192.168.1.0 which is the first unusable address in the subnet.

3) Subnet Mask 255.255.255.0 Enter the Subnet Mask, which is sometimes referred to as the netmask of the dynamic subnet here. For example: The subnet mask of 192.168.1.0/24 is 255.255.255.0

4) Gateway Address 192.168.254.1 Enter the gateway address of the dynamic subnet here. The gateway address is the address that is configured on the router interface that the customers are connected to. It can be any usable address in the subnet that will not fall into the range of IPs specified by the pool start and stop addresses below. Most of the time, it is either .1 or .254. For example: The network 192.168.1.0/24 might have: 192.168.1.1 as the gateway address.

5) Pool Start Address 192.168.254.2 Enter the Pool Start Address of the dynamic subnet here. The pool start address can be any usable IP from the subnet provided it is less than or equal too the pool stop address and is not the gateway address. For example: The network 192.168.1.0/24 might have: 192.168.1.1 as the gateway address and 192.168.1.2 as the pool start address.

6) Pool Stop Address 192.168.254.254 Enter the Pool Stop Address of the dynamic subnet here. The pool stop address can be any usable IP from the subnet provided it is greater than or equal too the pool start address and is not the gateway address. For example: The network 192.168.1.0/24 might have: 192.168.1.1 as the gateway address and 192.168.1.2 as the pool start address.

7) TFTP File (optional) Modern-Config-1.txt You may optionally specify a TFTP boot file for the connected clients here. You can only do this if the shared network chosen above has a TFTP server specified. You will receive an error message otherwise.

8) Allow only known clients Yes No Choose whether to only allow known clients. If this option is set to yes, only those MAC addresses that you add to the system via the Known Client Config section will be allowed to get an address from this dynamic subnet. This type of configuration is typically used in a cable modem network.

Add/Edit Dynamic Subnet

Configure the dynamic subnet for the cable modems

Add known client(s) that may use the dynamic subnet that was added to the network. In this example, specifying a different TFTP file for this known client is shown. On the known clients configuration screen,

Main

User States

User Management

Authenticated DHCP

Standard DHCP

Shared Network Config (NEW)

Dynamic Subnet Config (NEW)

Known Client Config (NEW)

Static Subnet Config (NEW)

Static IP Assignment (NEW)

Maintenance Subnet Config (NEW)

View Address Usage (NEW)

tftp config (NEW)

System Configuration

Currently configured Known Clients:						
Show All Known Clients: <input checked="" type="checkbox"/>						
Limit matches shown:						
Match Identifier: <input type="text"/> MAC Address: <input type="text"/>						
Limit Entries Displayed						
Identifier	MAC Address	TFTP File	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>		
0006252537e5	00:06:25:37:e5		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>		
000625EEF4AC	00:06:25:ef:4ac		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>		
Cayman-2E703592	00:06:89:0c:s1:11		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>		
Cayman-2E703593	00:06:89:0c:s1:13	test2.txt	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>		
Cayman-2E703627	00:06:89:0c:s1:37		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>		
Cayman-2E703628	00:06:89:0c:s1:38	test3.txt	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>		
test	00:01:02:03:04:08		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>		
testing	00:02:03:04:05:08		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>		
windows-test1	00:00:cc:39:96:a6	test1.txt	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>		

Location: Standard DHCP -> Known Client Config (NEW)

Successfully deleted known client entry

Define new or modify a new or existing known client definition here:
A Shared Network defines a group of subnets that all live on the same physical network or interface. Defining a Shared Network allows you to add dynamic, static or maintenance subnets to it in the other sections under Standard DHCP Configuration. In this section, known client definitions are made. This allows clients to receive IP addresses from dynamic subnets that have 'Allow only known clients' marked. The only required parameter is the MAC Address. Optionally, an identifier may be specified that will identify the client in some way (such as a customer name, account number or similar). A TFTP file may also be specified. Please note that since this configuration is global for all standard DHCP dynamic subnets that have 'Allow only known clients' marked, it is not possible to do the usual verification of the TFTP file. The TFTP file specification will only have an effect if the dynamic subnet(s) that the customer is connected to have appropriate TFTP server parameters and if the file actually exists on the TFTP server.

1) Identifier Cable-Modem-1 You may optionally specify some sort of text string here that helps you identify this entry.

2) MAC Address 00:00:00:cc:cc:11 Enter the MAC Address of the client here.

3) TFTP File test.txt You may optionally specify a TFTP boot file for the connected clients here.

Add/Edit Known Client

Adding known clients

used to limit the entries displayed. The list of entries shows the identifier entered for each entry along with the MAC address and the TFTP file specified (if any). Editing and deleting may be done from this screen as well. Filling out the form allows the entry of new known clients.

On the known clients configuration screen, there are three main areas. Limiting displayed entries, entries that are actually displayed, and the form for adding more entries. Limiting displayed entries may either show all entries, if show all is checked. Otherwise, matching by identifier or mac address may be

Configuring a static subnet for the FTTH network is similarly done in the Static Subnet Config under Standard DHCP. A network called FTTH-Service was added under Shared Network Config for this example, as the FTTH service is a separate network from the cable modem

service. The top of this screen shows the currently configured subnets. These subnets may be edited or deleted from this screen. Specification of a global TFTP file is not possible for the static network.

Main

User States

User Management

Authenticated DHCP

Standard DHCP

Shared Network Config (NEW)

Dynamic Subnet Config (NEW)

Known Client Config (NEW)

Static Subnet Config (NEW)

Static IP Assignment (NEW)

Maintaince Subnet Config (NEW)

View Address Usage (NEW)

tftp config (NEW)

System Configuration

Currently configured static subnets:

Shared Network Name	CIDR	Gateway	Start Address	Stop Address	In Use
TEST-RESTRICTIONS	10.219.83.0/24	10.219.83.1	10.219.83.2	10.219.83.254	2

Define new or modify existing Standard Static Subnets here:

A Shared Network defines a group of subnets that all live on the same physical network or interface. Defining a Shared Network allows you to add dynamic, static or maintenance subnets to it in the other sections under Standard DHCP Configuration. In this area, static subnets can be configured that are attached to a specific Shared Network. It is required that you first have a Shared Network configured to attach the static subnet. You may assign static IPs from these subnets to individual customer devices using the Static IP Config under Standard DHCP Configuration.

1) Shared Network: FTTH-Service Select the Shared Network that this static subnet will be a part of.

Enter the gateway address of the static subnet here. This is sometimes referred to as the network address. For example: The network 192.168.1.0/24 has a gateway address: 192.168.1.0 which is the first unusable address in the subnet.

2) Wire Address: 172.16.254.0

Enter the Subnet Mask of the static subnet here. The subnet mask of 192.168.1.0/24 is 255.255.255.0

3) Subnet Mask: 255.255.255.0

Enter the Gateway Address of the static subnet here. The gateway address is the address that is configured on the router interface that the customers are connected to. It can be any unusable address in the subnet that will not fall into the range of IPs specified by the pool start and stop addresses below. Most of the time, it is either 1 or 254. For example: The network 192.168.1.0/24 might have 192.168.1.1 as the gateway address.

4) Gateway Address: 172.16.254.1

Enter the Pool Start Address of the static subnet here. The pool start address can be any unusable IP from the subnet provided it is less than or equal to the pool stop address and is not the gateway address. For example: The network 192.168.1.0/24 might have 192.168.1.1 as the gateway address and 192.168.1.2 as the pool start address.

5) Pool Start Address: 172.16.254.2

Enter the Pool Stop Address of the static subnet here. The pool stop address can be any unusable IP from the subnet provided it is greater than or equal to the pool start address and is not the gateway address. For example: The network 192.168.1.0/24 might have 192.168.1.1 as the gateway address and 192.168.1.254 as the pool stop address.

6) Pool Stop Address: 172.16.254.254

Add/Edit static Subnet

Configuring a static subnet

In order for addresses to be assigned to FTTH termination equipment statically on this example network, each device or circuit must be defined in the Static IP Assignment area under Standard DHCP. Possible ways of identifying devices are via MAC address, option 82 Agent-ID (Circuit ID) or option 82 remote ID. In

this example MAC address is used. In the static configuration, TFTP files must be assigned individually, there is no global definition. This example does not specify a TFTP file. On the Static IP Assignment screen, there are three main areas. Limiting displayed entries, entries that are actually displayed, and the form for adding more entries.

Main

User States

User Management

Authenticated DHCP

Standard DHCP

Shared Network Config (NEW)

Dynamic Subnet Config (NEW)

Known Client Config (NEW)

Static Subnet Config (NEW)

Static IP Assignment (NEW)

Maintaince Subnet Config (NEW)

View Address Usage (NEW)

tftp config (NEW)

System Configuration

Currently configured static IP assignments:

Show All Static IP Assignments:

Limit matches shown:

Match type: Select Limiter Type Match string:

Match Shared Network: Select Shared Network Match Static Subnet: Select Standard Static Subnet

Limit Entries Displayed

Shared Network Name **Static Subnet** **IP Address** **Type of Match** **Match String** **TFTP File**

TEST-RESTRICTIONS	10.219.83.0/24	10.219.83.10	MAC Address	00:00:03:04:05:06	test5.txt	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
TEST-RESTRICTIONS	10.219.83.0/24	10.219.83.11	MAC Address	00:00:03:04:05:14		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

Define new or modify existing Standard Static IP Assignments here:

A Shared Network defines a group of subnets that all live on the same physical network or interface. Defining a Shared Network allows you to add dynamic, static or maintenance subnets to it in the other sections under Standard DHCP Configuration. A static subnet is a subnet that will have addresses assigned to customers in a known manner by matching some type of information from the customer equipment. In this section static IP assignments may be made from the static subnets that have already been configured. At least one static subnet must be configured before you will be able to add static IP assignments here.

1) Standard Static Subnet: 172.16.254.0/24 Select the Standard Static Subnet that this static IP assignment will be allocated from.

2) IP Address Assignment: 172.16.254.2 Enter the IP Address that you wish to assign here.

3) Match Type: MAC Address Select the match type for the string that will be entered in question 4. MAC Address would be the MAC address of the customer equipment. Circuit ID is the Option 82 agent circuit-suboption. Remote ID is the Option 82 agent remote id suboption.

4) Match String: 00:01:02:03:04:05 Enter the string to match so that the DHCP server can correctly identify the customer equipment and therefore hand out the desired static IP assignment. Remember that the correct match type must be chosen above, or the assignment will not work. Limited checking is done on these two fields as it is largely unknown what type of string you may need to enter, so be sure to be careful. Please note that match strings are case sensitive.

5) TFTP File: You may optionally specify a TFTP boot file for the customer equipment to receive here. You can only do this if the static subnet chosen above is part of a shared network that has a TFTP server specified. You will receive an error message otherwise.

Add/Edit static Subnet

Assigning a static IP to a client

Limiting displayed entries may either show all entries, if show all is checked. Otherwise, matching by limiter type (mac address, circuit ID or remote ID), Shared Network, or Static Subnet may be used to limit the entries displayed. The list of entries shows the shared network, the static subnet, IP address, how the match will be done, along with the match string and the TFTP file specified (if any). Editing and deleting may be done from this screen as well. Filling out the form allows the entry of new static assignments.

The FTTH DHCP Relay agent(s) source of the DHCP traffic will be in the 10.69.254.0/24 subnet. The DHCP server must be told this so that it can correctly identify the proper network to assign an IP address to the client. This is done by specifying the aforementioned subnet as a maintenance subnet. Multiple maintenance subnets

may be configured as needed. This allows the use of large networks with many DHCP Relay agents in the case that the DHCP Relay agents are layer 2 devices such as DSLAMs or other such concentrator devices in networks where numerous devices are required to service the amount of clients on the network. It should be noted that separate networks should NOT be tied together in this manner as the client device may receive address assignments that are not routable on the network the device resides upon.

Location: Standard DHCP -> Maintenance Subnet Config ()

Currently configured maintenance subnets:	
Shared Network Name	CIDR
FNGI-TEST	10.128.128.0/24
TEST-RESTRICTIONS	10.0.1.0/24
<small>Define new or modify existing Standard maintenance Subnets here!</small>	
<small>A Shared Network defines a group of subnets that all live on the same physical network or interface. Defining a Shared Network allows you to add dynamic, static or maintenance subnets to it in the other sections under Standard DHCP Configuration. In this area, maintenance subnets can be configured that are attached to a specific Shared Network. It is required that you first have a Shared Network configured to attach the maintenance subnet. A maintenance subnet is a subnet that will not be allocated via DHCP but may be the subnet that the router(s) will communicate from when relaying DHCP messages. This allows the DHCPPatrol system to know which network an address should be allocated from in the case that the router(s) (relay agents) do not live in one of the static or dynamic subnets. For example: A router may have a different subnet configured as the primary subnet than any of the configured static or dynamic DHCP pools on the interface that has the relay agent configured upon it. The DHCP server still needs to know what interface the DHCP requests are regarding, so the addition of the maintenance subnet gives it that information.</small>	
1) Shared Network	FTTH-Service
<small>Select the Shared Network that this maintenance subnet will be a part of.</small>	
2) Wire Address	10.69.254.0
<small>Enter the Wire address of the maintenance subnet here. This is sometimes referred to as the network address. For example: The network 192.168.1.0/24 has wire address: 192.168.1.0 which is the first unusable address in the subnet.</small>	
3) Subnet Mask	255.255.255.0
<small>Enter the Subnet Mask, which is sometimes referred to as the netmask of the maintenance subnet here. For example: The subnet mask of 192.168.1.0/24 is 255.255.255.0</small>	

[Add/Edit maintenance Subnet](#)

Defining a Maintenance Subnet

Location: Standard DHCP -> View Address Usage ()

IP usage statistics

[1] Network: Example-Cable-Modem-Service					
Subnet	Type	Leased	Total	% in use	
192.168.254.0/24	Dynamic	1	253	0.4%	
Total Dynamic: 1 253 0.4%					
Totals: 1 253 0.4%					
[2] Network: FNGI-TEST					
Subnet	Type	Leased	Total	% in use	
10.128.128.0/24	Maintenance	0	0	0%	
Totals: 0 0 0%					
[3] Network: FTTH-Service					
Subnet	Type	Leased	Total	% in use	
172.16.254.0/24	Static	1	253	0.4%	
10.69.254.0/24	Maintenance	0	0	0%	
Totals: 1 253 0.4%					
[4] Network: TEST-RESTRICTIONS					
Subnet	Type	Leased	Total	% in use	
10.100.100.0/24	Dynamic	0	253	0%	
74.219.83.0/24	Dynamic	0	253	0%	
10.219.83.0/24	Static	0	253	0%	
10.0.1.0/24	Maintenance	0	0	0%	
Totals: 0 759 0%					
Totals (ALL): 2 1265 0.16%					

The View Address Usage report

list of currently used addresses, and which client is using them are available by clicking the subnet.

Checking client and network status is easily accomplished using the Standard DHCP → View Address Usage report. With this report, current leases used, as well as a percentage of utilization are available on a per subnet and network basis. Graphs are also available by clicking the green graph icons showing usage with a configurable time period with data up to one year in the past. Further, a

GUI Enhancements

Special User Reports

The DHCPPatriot™ system includes three special reports for use with authenticated DHCP as follows:

- View Static

Assignment:

Allows an administrator to verify whether the DHCPPatriot™ system has received a static IP assignment from RADIUS for a particular user.

The administrator can

search by username, MAC Address and/or IP address. The output from this report contains the username which, when clicked, brings up a list of all sessions by that username. The MAC address, when clicked, will bring up an IETF site specifying who the manufacturer may be (if the MAC address of the device has not been altered). The IP Address that is assigned statically is also displayed here.

Currently configured static IP assignments:		
Username	MAC Address	Assigned Static IP Address
cayman-1	00:01:02:03:04:05	192.168.10.85
cayman-1	11:01:02:03:04:05	192.168.10.85
cayman-1	11:01:02:03:04:06	192.168.10.85
cayman-1	11:01:02:03:04:07	192.168.10.85
cayman-1	00:00:89:0c:51:11	192.168.10.85

Search for static ip assignments using the limiters below:

Username: *(may be omitted to show a snapshot of all static assignments)
Use an Asterisk (*) in the username box to do a wildcard search of users.

MAC Address: *(may be omitted to show a snapshot of all online IPs/Users)
all or part of IP Address: *(may be omitted to show a snapshot of all online IPs/Users)

Show Exact match of IP address only!

Viewing Static IP Address Assignment for Authenticated Devices

- View Authenticated Users: Allows an administrator to search through a list of authenticated user devices to verify

that a particular

user or users

have been

authenticated

properly and

what their

current status is.

The

administrator can

search by

username and

MAC address.

The results shown consist of the username which, when clicked, brings up a list of all sessions by that username. The MAC address, when clicked, will bring up an IETF site specifying who the manufacturer may be (if the MAC address of the device has not been altered). The device's current IP address is displayed here, or OFFLINE if the device does not currently have an IP Address. The type of address that the device should get is shown here, as well, either STATIC, DYNAMIC or

Currently authenticated devices:						
Username	MAC Address	Current IP Address	IP Address Type	Assigned IP Address type	Account Status	
cayman-1	00:00:89:0c:51:11	192.168.10.85	STATIC	STATIC	ACTIVE	
cayman-1	11:01:02:03:04:06	OFFLINE	OFFLINE	STATIC	ACTIVE	
cayman-1	11:01:02:03:04:05	OFFLINE	OFFLINE	STATIC	ACTIVE	
cayman-1	00:01:02:03:04:05	OFFLINE	OFFLINE	STATIC	ACTIVE	
cayman-1	11:01:02:03:04:07	OFFLINE	OFFLINE	STATIC	ACTIVE	
cayman-2	00:00:89:0c:51:13	208.45.199.118	DYNAMIC	DYNAMIC	ACTIVE	
cayman-2	11:01:02:03:04:08	OFFLINE	OFFLINE	DYNAMIC	ACTIVE	
cayman-3	00:00:89:0c:51:59	208.45.199.116	DYNAMIC	DYNAMIC	ACTIVE	
cayman-3	11:01:02:03:04:08	OFFLINE	OFFLINE	DYNAMIC	ACTIVE	
cayman-4	00:00:89:0c:51:57	208.45.199.117	DYNAMIC	DYNAMIC	ACTIVE	

Search for authenticated users and devices using the limiters below:

Username: *(may be omitted to show a snapshot of authenticated users and devices)
Use an Asterisk (*) in the username box to do a wildcard search of users.

MAC Address: *(may be omitted to show a snapshot of all authenticated MACs/Users)

Viewing Authenticated user devices

STICKY. The last column gives the account status for the user device. Possible values are **ACTIVE** and **SUSPENDED**.

- Users using more than one IP: Allows an administrator to locate users who are using more than one IP address currently and thusly to find users that may be violating simultaneous use restrictions. This report merely presents a list. No searching is available here. The output of this report will have 2

or more lines per username equal to the amount of devices that are currently using an IP address that were authenticated by that user.

Location: User Management -> Users Using more than 1 IP()						
Users who have multiple devices using more than one IP address simultaneously (current):						
Username	MAC Address	Current IP Address	IP Address Type	Assigned IP Address type	Account Status	# of IPs in use
caveman-1	00:00:89:0c:51:11	192.168.10.85	STATIC	STATIC	ACTIVE	4
caveman-1	11:01:02:03:04:05	208.45.199.119	DYNAMIC	STATIC	ACTIVE	4
caveman-1	11:01:02:03:04:06	208.45.199.121	DYNAMIC	STATIC	ACTIVE	4
caveman-1	11:01:02:03:04:07	208.45.199.122	STICKY	STATIC	ACTIVE	4
caveman-2	00:00:89:0c:51:13	208.45.199.118	DYNAMIC	DYNAMIC	ACTIVE	2
caveman-2	11:01:02:03:04:08	208.45.199.123	DYNAMIC	DYNAMIC	ACTIVE	2
caveman-3	00:00:89:0c:51:59	208.45.199.116	DYNAMIC	DYNAMIC	ACTIVE	2
caveman-3	11:01:02:03:04:09	208.45.199.125	STICKY	DYNAMIC	ACTIVE	2

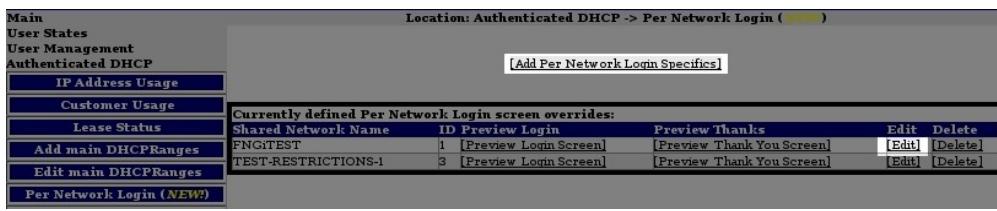
Viewing Authenticated users that have more than one device using an IP address

Columns

displayed are username which, when clicked, brings up a list of all sessions by that username. The MAC address, when clicked, will bring up an IETF site specifying who the manufacturer may be (if the MAC address of the device has not been altered). The device's current IP address is displayed here. The type of address that the device should get is shown here, as well, either **STATIC**, **DYNAMIC** or **STICKY**. The last column gives the account status for the user device. Possible values are **ACTIVE** and **SUSPENDED**.

Customization of Authentication Screens Per Network

The look of the login and thank you screens can be changed on a per network basis. Small tweaks may be made to the global look of the screens, or the screens can be made to look completely different. This is useful in situations where perhaps the ISP has multiple kinds of networks, or



Currently defined Per Network Login screen overrides:						
Shared Network Name	ID	Preview Login	Preview Thanks	Edit	Delete	
FNGITEST	1	[Preview Login Screen]	[Preview Thank You Screen]	[Edit]	[Delete]	
TEST-RESTRICTIONS-1	3	[Preview Login Screen]	[Preview Thank You Screen]	[Edit]	[Delete]	

Choose to add or edit a per network login definition

perhaps multiple ISPs are sharing a single DCHPatriot™ system.

Configuration of the custom screens is simple and similar to the configuration of the global login screen. Merely access Per Network Login under the Authenticated DHCP menu. Click on Add Per Network Login Specifics, or select Edit to change an existing per network login setting.

When configuring the per network login parameters, as many or as few parameters as desired may be overridden from the default login and thank you screens. If a setting in the per network login is left blank, then the value from the global setting will be used. Even the image may be overridden displaying a different image at the top of the login and thank you screens than is shown on the global login and thank you screens.

Main

User States

User Management

Authenticated DHCP

IP Address Usage

Customer Usage

Lease Status

Add main DHCPRanges

Edit main DHCPRanges

Per Network Login (NEW)

Add/Edit Additional DHCPRanges

Add/Edit Static DHCPRanges

Add/Edit Maintenance Subnet (NEW)

Assign Sticky IP

Exclude IP address

Standard DHCP

System Configuration

Location: Authenticated DHCP -> Per Network Login (NEW)

Per Network Login / Thank you screen definitions
This allows you to define a custom login and thank you screen on a per network basis. Enter information only in those fields that you wish to override default values of.

0) Select Network: FNGiTEST Select the network for which you want to define custom values.

1) ISP Name: Testing ISP per Network Login Enter your complete ISP Name here.

2) ISP Logo Graphic: [Click Here to Edit Logo Graphic] Click on the link to select the graphic file from your hard drive. Please make sure its file size is suitable for the web.

3) Service Type: DSL Select your Service Type from the drop down box.

4) Maximum Username Length: Enter a number here representing the largest character length for usernames on the system.

5) Background Color: Enter the Hex value for the background color the customer will see on the login screen. We suggest a primary color from your logo.

6) Support Phone Number: Enter in the full telephone number that a customer can use to reach your technical support center.

7) Authentication Page Text: Please login to this ISP per network login screen. This text will be displayed to the users on the Authentication (login) page. You may use all HTML tags, save table related tags. Table related tags will be removed from the text at the time of display to the user. If you do not wish to customize the login screen, you can leave this blank.

8) Thank you Page Text: TESTING the ISP Per network login This text will be displayed to the users on the Thank you (Authenticated) page. You may use all HTML tags, save table related tags. Table related tags will be removed from the text at the time of display to the user. If you do not wish to customize the Thank you screen, you can leave this blank.

9) Show/Hide FNGi and DHCPIpatriot logo: Show Powered By section Hide Powered By section This allows those who do not want their customers to see the FNGi and DHCPIpatriot logos on the authentication page to hide the "powered by" section entirely.

10) Show/Hide Mac Address on Thank You screen: Show MAC Hide MAC This option allows you to show or hide the MAC Address display on the Thank You screen. The MAC Address display shows the user what MAC Address they just registered on the DHCPIpatriot.

11) Override default 23) Authentication Page Text: This text will be displayed to the users on the Authentication (login) page instead of the default text normally displayed on the login page. You may use all HTML tags, save table related tags. Table related tags will be removed from the text at the time of display to the user. If you do not wish to customize the login screen, you can leave this blank.

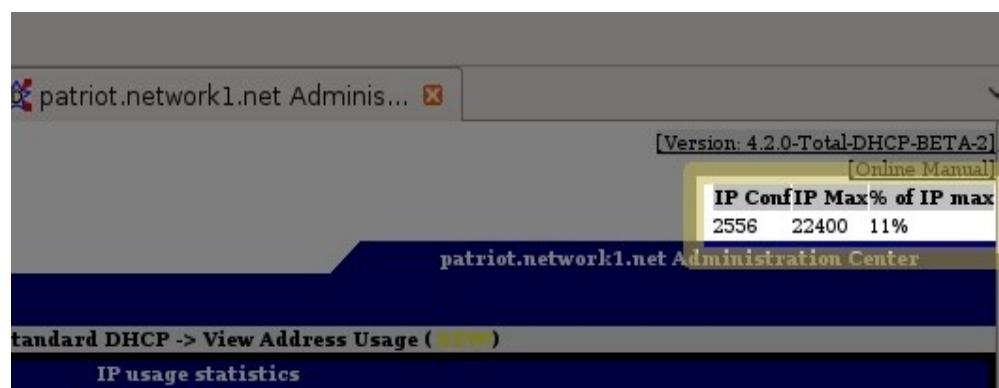
12) Override default 24) Thank you Page Text: This text will be displayed to the users on the Thank you (Authenticated) page instead of the default text normally displayed on the thank you page. You may use all HTML tags, save table related tags. Table related tags will be removed from the text at the time of display to the user. If you do not wish to customize the Thank you screen, you can leave this blank.

Cancel **Submit**

Fill the form out as desired and submit the changes.

IP Address Used vs Maximum

The IP address maximum usage table is scheduled to be added in version 4.2.0. This table is important for monitoring the existence on the DHCPIpatriot™ system of possible performance degrading configurations, or when it may be time to add additional DHCPIpatriot™ systems. The DHCPIpatriot™ system includes a small table in the upper right corner of



IP Addresses configured vs. Maximum

the administration interface that shows current IP usage, maximum recommended IP usage and the percentage of the maximum. The maximum IP Addresses that the DHCPPatriot™ can support is decided by hardware resources available, which varies by model, and the average lease length per IP on the system. The DHCPPatriot™ system computes this moving target and presents the results in the upper right hand corner of the DHCPPatriot™ administration interface. This is not to say that the DHCPPatriot™ will not allow more IP Addresses than the maximum shown to be configured, but rather that the system COULD become unstable if this number is exceeded.