DHCPatriot™ v.4.2.0 Total DHCP
Scheduled Feature
Implementation

Total DHCP

The version 4.2.0 Total DHCP edition update to the DHCPatriot™ 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 DHCPatriot™ is available.
  - Data regarding network utilization is also available via SNMP.

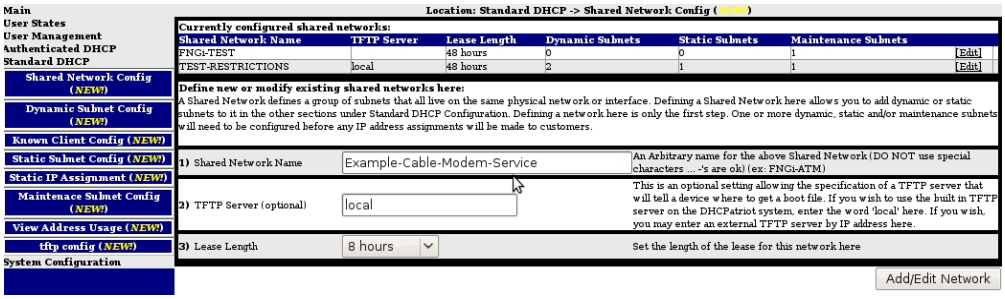
The following excerpt from Appendix L of the DHCPatriot™ Version 4.2.x Operations Manual demonstrates how easy it is to setup the standard DHCP server.

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

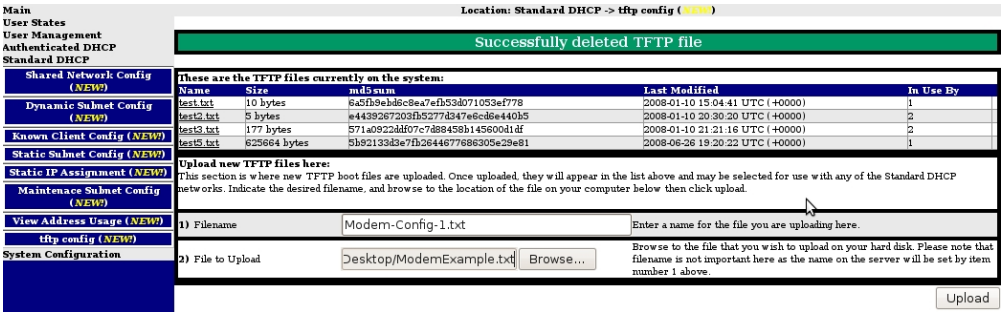
- About 200 FTTH customers.
- Each FTTH outside CP termination device must remain at the same IP address regardless of the devices MAC address.
- The FTTH DHCP Relay Agents reside in subnet 10.69.254.0/24 which is not part of the static subnet. A maintenance network must be configured to identify the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



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.

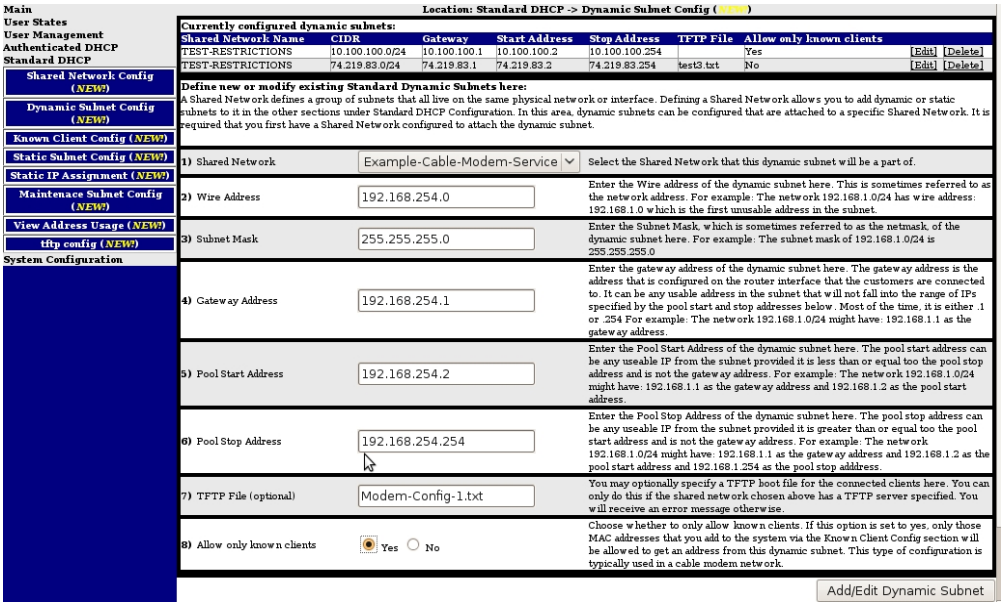
If the local TFTP server is to be used, then Upload the file(s) that will be needed for the TFTP server to distribute to the clients.



Upload a TFTP file for use by the cable modems.

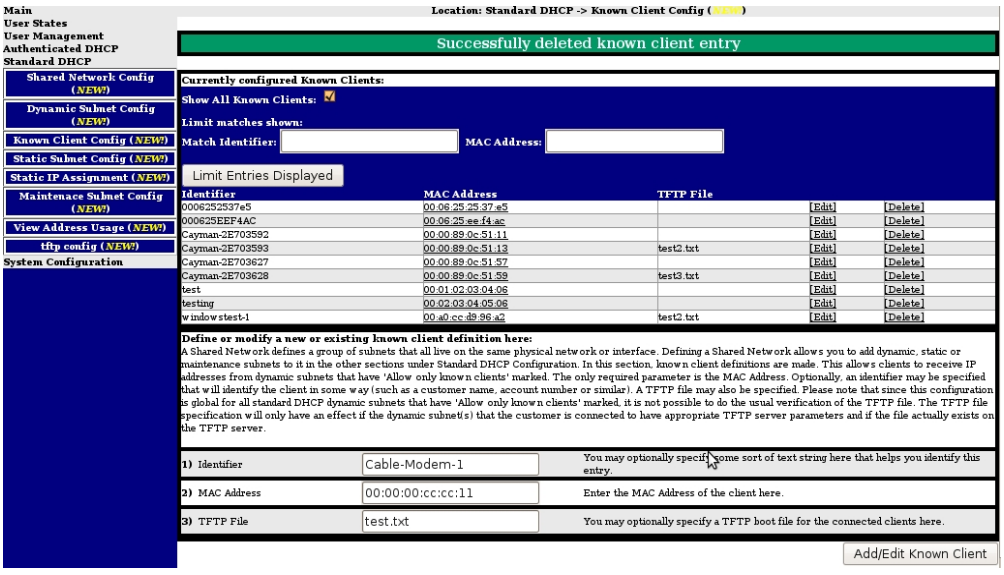
Any type of file may be uploaded that may be needed by the client device. The file may be up to 2GB in size. Files that have already been uploaded are displayed above. If the filename is clicked on, a copy of the file may be downloaded from this page for inspection. The size of the file, MD5sum and the 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.

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.



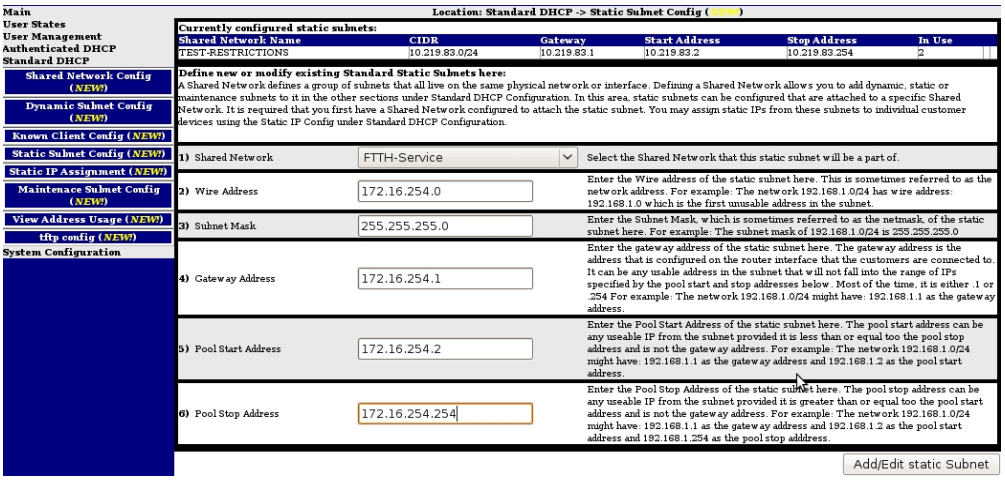
Configure the dynamic subnet for the cable modems

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, 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 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.



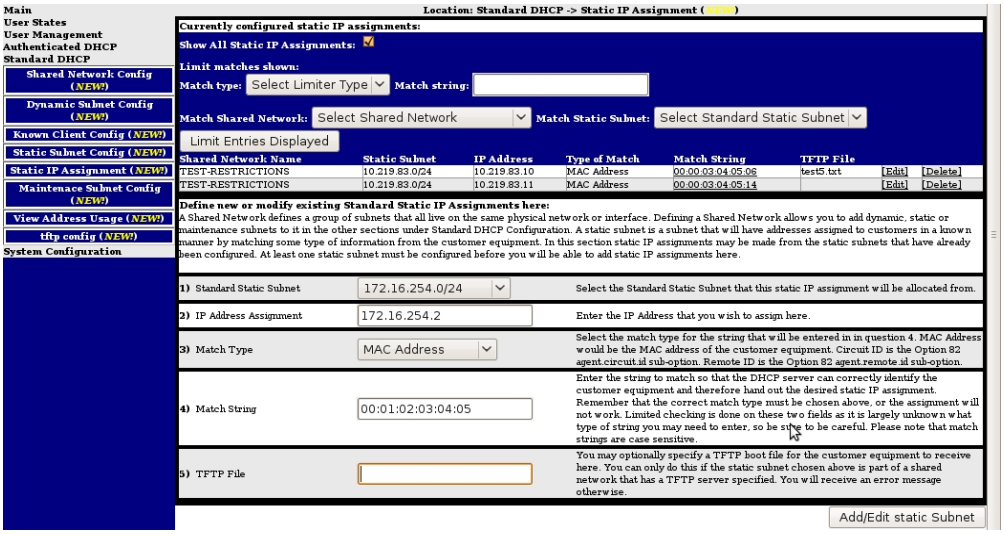
Adding known clients

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.



Configuring a static subnet

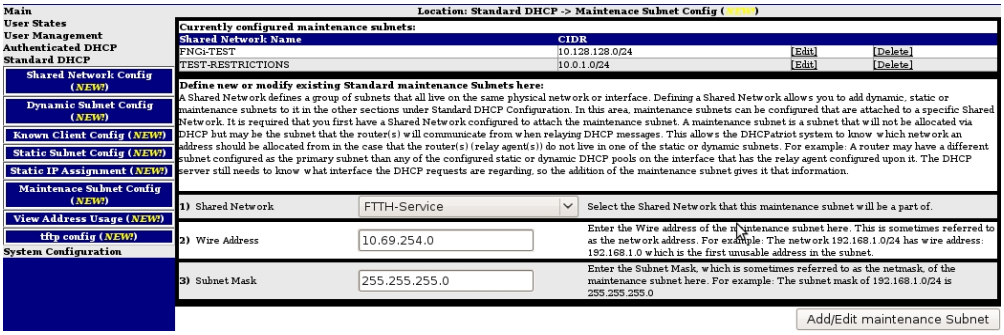
In order for addresses to be assigned to FTTH termination equipment statically on this example network, each device or circuit must be defined in the Static IP Assignment area under Standard DHCP. Possible ways of identifying devices are via MAC address, option 82 Agent-ID (Circuit ID) or option 82 remote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



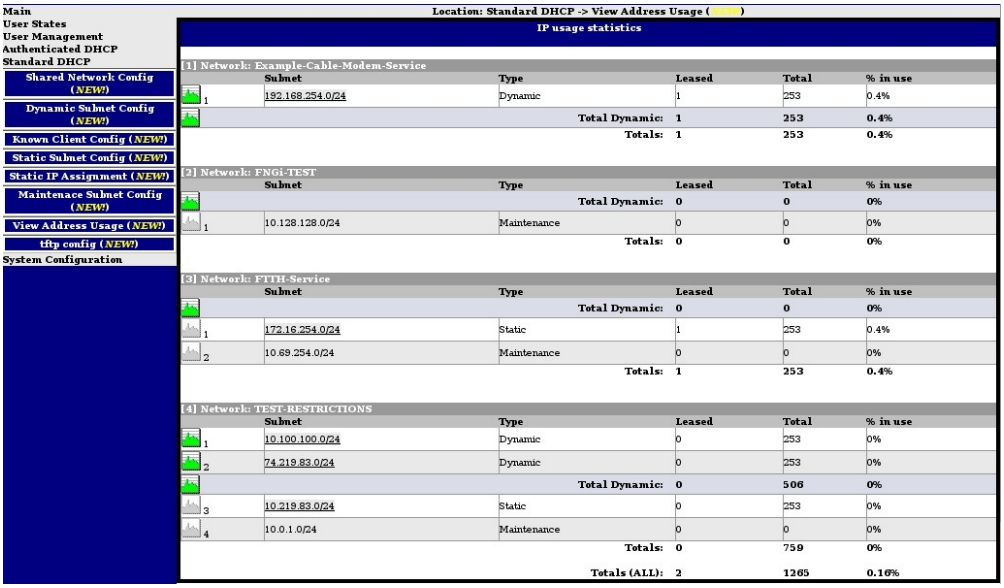
Assigning a static IP to a client

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.



Defining a Maintenance Subnet



The View Address Usage report

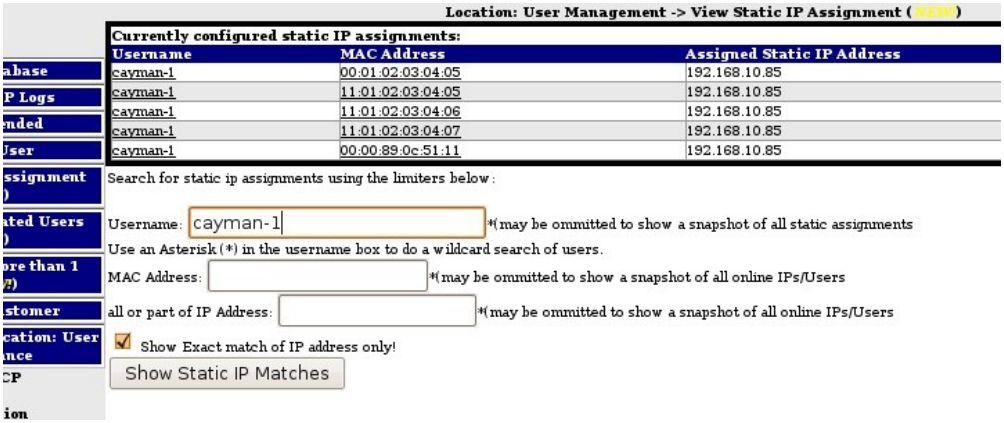
Checking client and network status is easily accomplished using the Standard DHCP → View Address Usage report. With this report, current leases used, as well as a percentage of utilization are available on a per subnet and network basis. Graphs are also available by clicking the green graph icons showing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

GUI Enhancements

Special User Reports

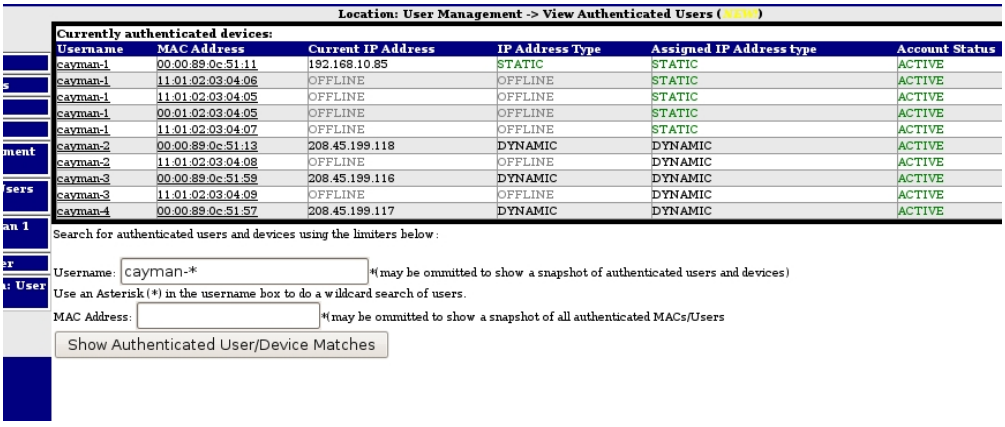
The DHCPatriot™ system includes three special reports for use with authenticated DHCP as follows:

- View Static Assignment: Allows an administrator to verify whether the DHCPatriot™ 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.



Viewing Static IP Address Assignment for Authenticated Devices

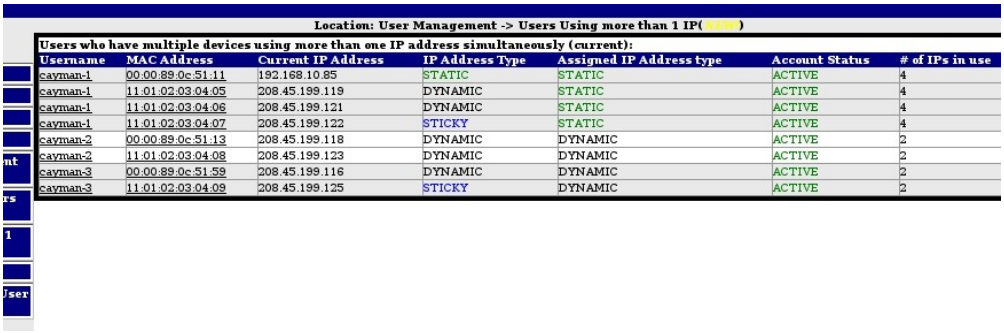
- View Authenticated Users: Allows an administrator to search through a list of authenticated user devices to verify that a particular user or users have been authenticated properly and what their current status is. The administrator can search by username and MAC address. The results shown consist of 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



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. 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.


Location: User Management -> Users Using more than 1 IP( )

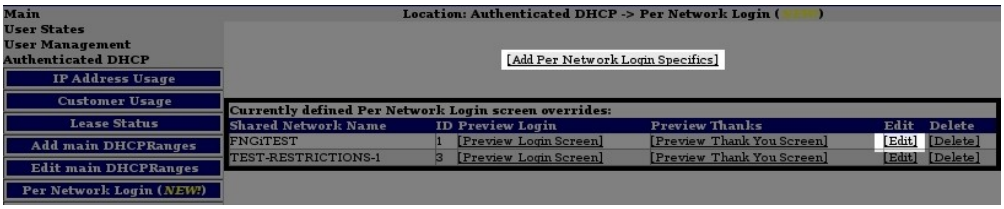
Users who have multiple devices using more than one IP address simultaneously (current):

Username	MAC Address	Current IP Address	IP Address Type	Assigned IP Address type	Account Status	# of IPs in use
cayman-1	00:00:89:0c:51:11	192.168.10.85	STATIC	STATIC	ACTIVE	4
cayman-1	11:01:02:03:04:05	208.45.199.119	DYNAMIC	STATIC	ACTIVE	4
cayman-1	11:01:02:03:04:06	208.45.199.121	DYNAMIC	STATIC	ACTIVE	4
cayman-1	11:01:02:03:04:07	208.45.199.122	STICKY	STATIC	ACTIVE	4
cayman-2	00:00:89:0c:51:13	208.45.199.118	DYNAMIC	DYNAMIC	ACTIVE	2
cayman-2	11:01:02:03:04:08	208.45.199.123	DYNAMIC	DYNAMIC	ACTIVE	2
cayman-3	00:00:89:0c:51:59	208.45.199.116	DYNAMIC	DYNAMIC	ACTIVE	2
cayman-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

Customization of Authentication Screens Per Network

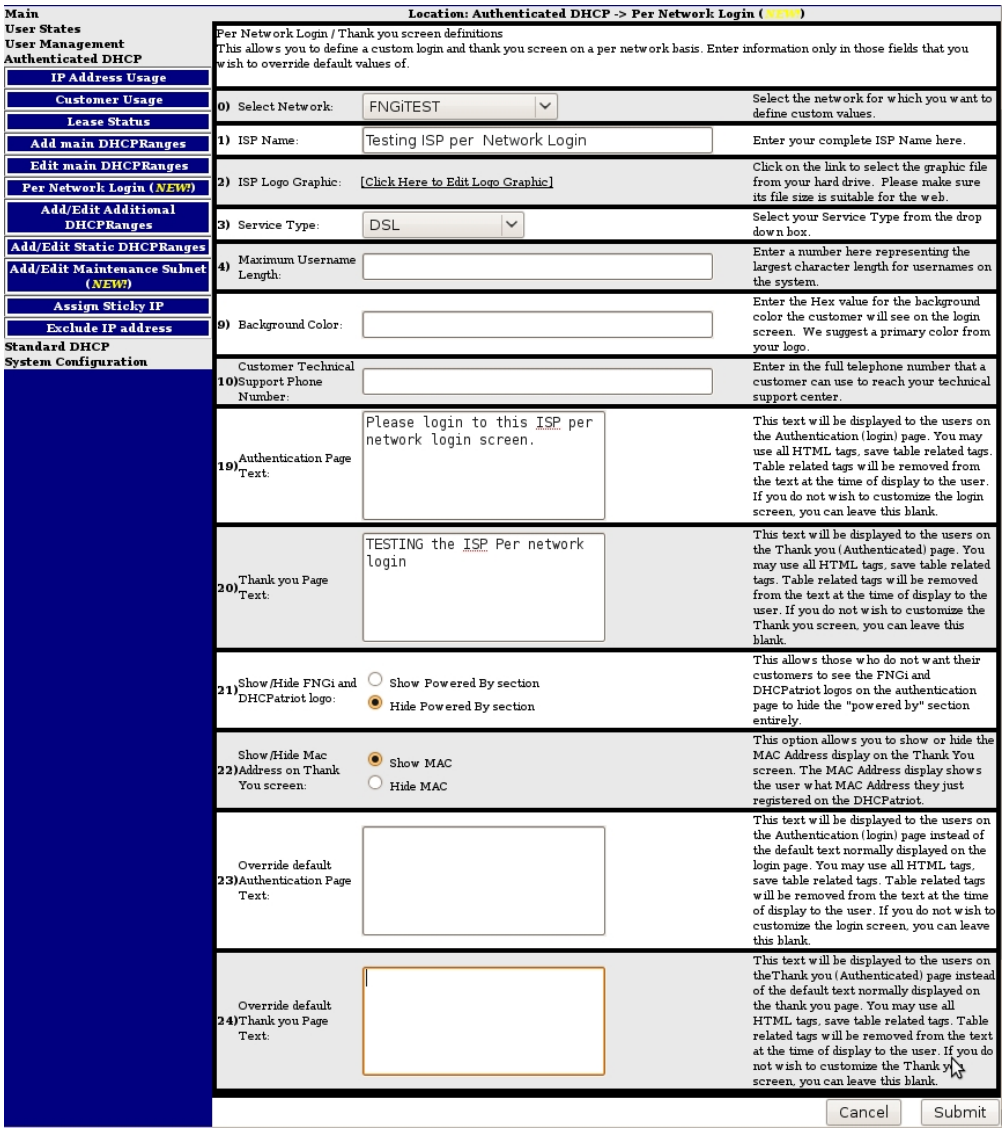
The look of the login and thank you screens can be changed on a per network basis. Small tweaks may be made to the global look of the screens, or the screens can be made to look completely different. This is useful in situations where perhaps the ISP has multiple kinds of networks, or perhaps multiple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



Choose to add or edit a per network login definition

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.

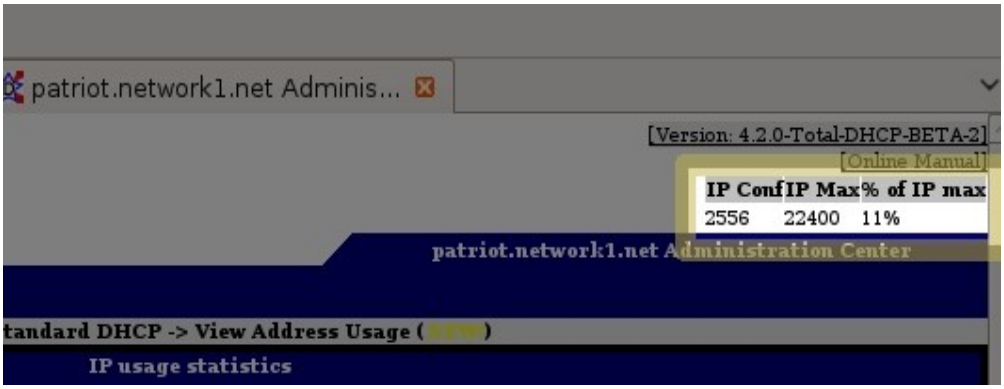
When configuring the per network login parameters, as many or as few parameters as desired may be overridden from the default login and thank you screens. If a setting in the per network login is left blank, then the value from the global setting will be used. Even the image may be overridden displaying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



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 DHCPatriot™ system of possible performance degrading configurations, or when it may be time to add additional DHCPatriot™ systems. The DHCPatriot™ 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 DHCPatriot™ can support is decided by hardware resources available, which varies by model, and the average lease length per IP on the system. The DHCPatriot™ system computes this moving target and presents the results in the upper right hand corner of the DHCPatriot™ administration interface. This is not to say that the DHCPatriot™ 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.