Features

First Network Group Inc
1-800-578-6381
www.DHCPatriot.com

The DHCPatriot™ is a broadband subscriber DHCP appliance with optional authentication designed to give network administrators the same visibility on DHCP networks they once had on dial networks.

At a Glance

- Fully RFC 1531/RFC 1533/RFC 1541/RFC 2131/RFC 2132 compliant DHCP server.
- Works with any broadband type that supports DHCP.
- Use the Built-in local customer authentication mechanism or an external RADIUS server for optional authentication and accounting of sessions.
  - The optional RADIUS client portion of the DHCPatriot complies with RFC 2138/RFC 2139/RFC 2865/RFC 2866.
- Local storage of session information on the DHCPatriot.
- Full white-list based firewall protection.
- Based on proven Linux® technology.
- High availability configuration.
- Easy for customers to use:
  - No software to install.
  - Only a standard DHCP configuration required.
  - Optional web based captive portal authentication.

- Easy for administrators, technical support or customer service personnel to use:
  - Web based system administration and server configuration.
  - System configuration via an easy menu interface available on serial console or an SSH session.
  - Advanced searching of system logs via the Web Administration Interface.
  - Authentication of individual MAC Addresses, for devices without a web browser, via the Web Administration Interface as part of the optional authentication.
  - Suspension/unsuspension by username, multiple usernames, or MAC Address all with customer messaging support via the Web Administration Interface as part of the optional authentication.
- Easy access to information via web based reporting.
  - Powerful reporting engines provide easy access to session data for abuse complaint resolution, subpoena response, CALEA compliance assistance, and acceptable use policy violations.
  - Access to IP address usage statistics and graphs for intelligent network management.
- Separate username/password/permissions for each administrator on the Web Administration Interface.
- Supports multiple subnets on the same interface, as well as multiple interfaces via standard DHCP/BOOTP Relay agent protocol.
  - Multiple subnets of varying types may be used on the same physical network.
  - Multiple physical networks are supported.
  - Static IP assignment via the Framed-IP-Address RADIUS Attribute, or via the Built-in local customer authentication mechanism in the optional authenticated DHCP.
  - Sticky IP assignment directly out of the dynamic pools.
  - Exclude any IP address from dynamic assignment.
  - Full featured DHCP server.
  - Built in TFTP server.

    - Configuration of external TFTP server also possible.
  - Dynamic address assignment (non-authenticated)
    - Optional TFTP server and file specification
    - Restrict to only known clients or leave open to all clients.
    - Optional global and/or per known client TFTP file assignment.
  - Static address assignment (non-authenticated)
    - Assign via option 82 or MAC address.
    - TFTP file assignment on a per static assignment basis.
- Web based remote access API for supporting comprehensive network administration programs.

Features and Benefits

The DHCPatriot is designed to be a secure, stable, simple to use/manage, flexible platform for management of broadband subscribers and general purpose DHCP. The DHCPatriot employs the proven firewall technology of Linux in a white-list-style configuration to protect from outside intrusion. With its CLI based system configuration menu interface, and web based administration interface, the DHCPatriot provides the network visibility and easy to use configuration options that administrators need without the burden to customers that comes with PPPoE or the time consuming task of assigning and maintaining static IP addresses. Any type of broadband may use the DHCPatriot so long as DHCP is supported. Easy access to both session data and IP address utilization information is standard.

Secure and Stable

In today's online world of hacking and denial of service attacks, its important that all systems be as security conscious as possible. The DHCPatriot, being Linux based, utilizes some of the best security features in the world. The firewall by default blocks all inbound traffic. It opens ports automatically for operation between itself and the broadband customers. A handy interface is also included on both the Web Administration Interface and the CLI based system configuration menu for adding IP addresses or subnets and port combinations to permit through the firewall for easy administration access. Coupling these features with a predictable software release schedule results in a very secure system.

In the early days of providing Internet access, customers were typically tolerant of needed maintenance related outages, or the occasional equipment failure. The rise of competition in the ISP market has reduced customer patience considerably. For this reason, the DHCPatriot employs a high availability design. It is actually comprised of two separate devices. Each device uses 1 unit of rack space. When both devices are available, they load balance between the two of them. If one of the devices fails, the other device handles the full operation. Even if several services fail across each device, they are still operating so long as the same service has not failed on both devices. As long as the secondary network is maintained between the two devices, it is even possible to locate each device in a separate data center. With this configuration, and the inherent stability of the Linux operating system, the DHCPatriot is able to maintain a high degree of uptime.

High Visibility

More people than ever before are using the Internet on a daily basis. This brings a level of responsibility to ISPs that did not exist in the 1990's. From locating abusers to answering subpoenas and maintaining CALEA compliance, it's imperative to maintain and track the user's identity, IP address and session information. Without the DHCPatriot, PPPoE or static IP addressing must be used to accomplish this task. PPPoE, in many cases, either does not operate with the customer's equipment, or requires the install of software applications on the customer's computer. Static IP addressing requires the ISP to maintain lists of what IP addresses are assigned to which customer.

Further, the customer must make configuration changes to his equipment. The DHCPatriot maintains session records of customer equipment IP address assignments with the ease and flexibility of DHCP. Customer interaction with the DHCPatriot is maintained at a minimal level. DHCP is the default configuration of many devices from the latest PC to home network routers. The DHCPatriot, in most cases, will require the customer login only once via the simple web interface. There is no software to install.

In order to meet ISP responsibilities, quick and easy access to customer session records is necessary. The DHCPatriot offers a powerful web based search mechanism to access this data. Furthermore, customer session records, in most cases, can be maintained as long as the DHCPatriot is in service. See figure 1 for an example of one type of report. As shown in figure 1, it is possible to search by username, MAC Address, IP address and time period. Any combination of these limiters can be used to refine the results.

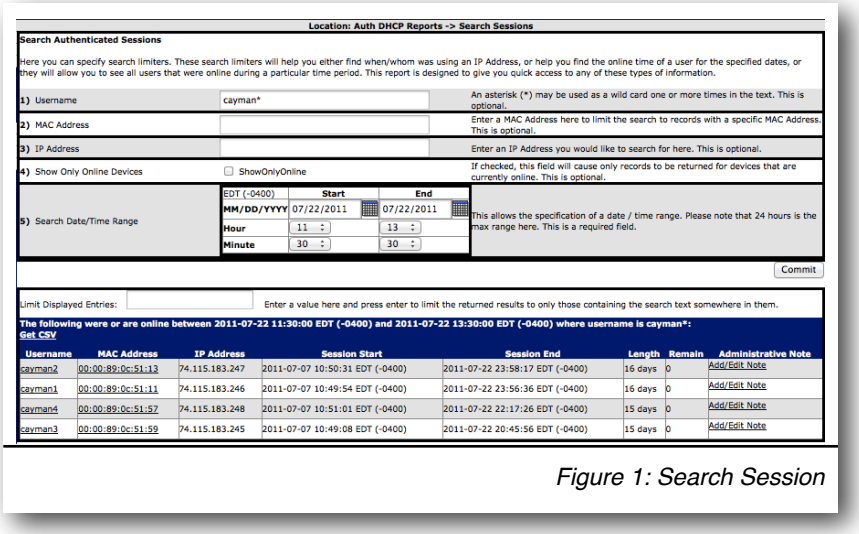

Figure 1: Search Session

With the explosion of the Internet, administration of networks has become increasingly complex. The DHCPatriot seeks to simplify the management of DHCP networks. Built-in reporting tools give network administrators all of the information they need. Figures 2 & 3 show an example report and graph. Figure 2 shows the output from the IP address usage report. This output is very informative, however administrators will likely need further information in order to forecast when additional network capacity will be needed. Figure 3 shows time based usage that may be viewed by clicking on one of the graph icons from figure 2. This graph allows the network administrator to quickly determine current information as well as trends over time, via the time based options, for an accurate overview of current network capacity and rate of growth.

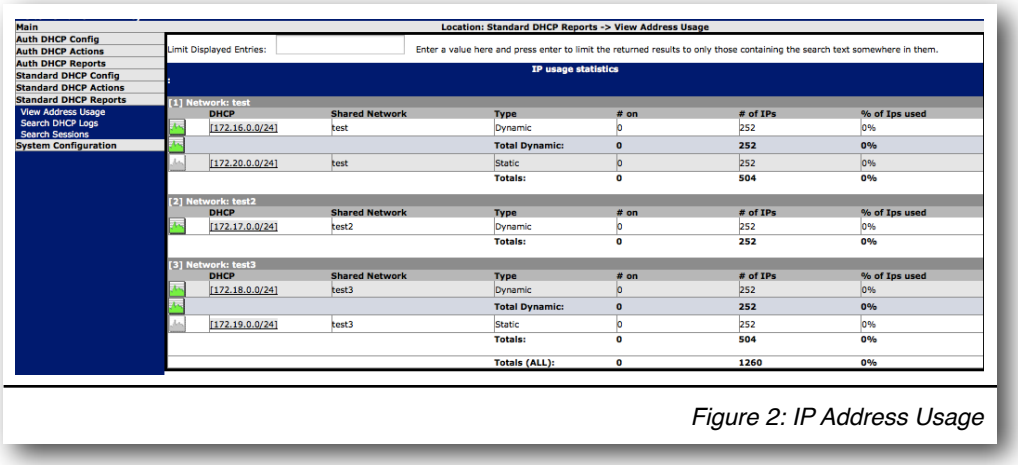

Figure 2: IP Address Usage

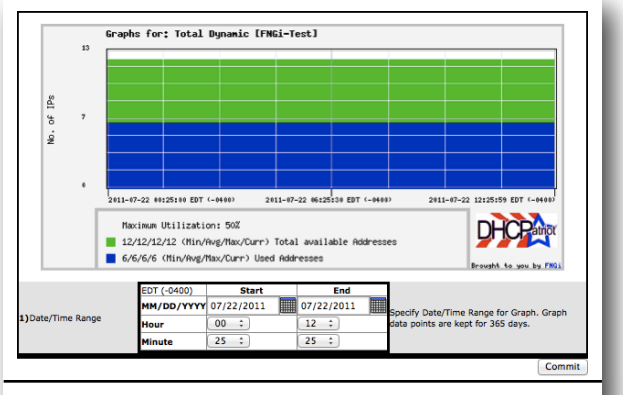

Figure 3: IP Usage Graphs

Example of Use

Perhaps the best method of describing the operation of the DHCPatriot is via example. In the following example, a customer with one computer connected via fiber to the home. The various processes from inception of service to leaving the service and their implications involving the DHCPatriot are described here. This example will create a clear picture of exactly what the DHCPatriot and optional equipment can do for a network and its subscribers.

The customer contacts the ISP to order service. The ISP dispatches a technician to install an ONT (Optical Network Termination) device on the exterior of the home and an Ethernet jack for accessing the network inside the customer's home. The customer will also be switched to VOIP service. The ONT device is installed, and the inside telephone wiring is connected for VOIP service. The technician installs the jack and connects the customer's computer to it via an Ethernet cable. The telephone service begins immediately working. Additional steps are required for the Internet to begin functioning for the customer.

The Standard DHCP on the DHCPatriot has been pre-configured to give the ONT device a static IP address based on the Option 82 Circuit ID of the fiber. Any ONT device installed at the customer premise will obtain the same IP address regardless of the MAC address involved. This is important as the particular brand of fiber equipment used assigns the VOIP telephone number based on the IP address that the ONT receives (This is typical with Occam equipment as well as other vendors). This IP address has nothing to do with the Internet service but rather is used for VOIP service. As such, it is usually a private IP address of some kind.

The customer is provided with a username and password for access to the network. The ISP has previously set this username and password for this customer on either their RADIUS server, or the Built-in Authentication on the DHCPatriot. The customer turns on the computer, and an IP address is obtained from the DHCPatriot via the default configured DHCP on the customer's computer. Since this computer is not known to the DHCPatriot yet, it receives an unauthenticated address. Unauthenticated addresses on the DHCPatriot are usually private addresses, as public addresses are not needed for this temporary purpose. This is configurable, however.

Figure 4: The login window

The customer attempts to browse the web, and is only able to obtain the 'Login' screen. The default 'Login' screen is shown in figure 4. This screen is, of course, highly customizable. The logo may be changed to a custom logo of your ISP. The background color may be changed. Nearly all of the text may be modified or completely replaced. Also, the 'Powered By' section can be hidden. If the customer attempts anything online, it will be declined. Only web browsing will work and only to the authentication page.

At this point, the customer enters the username and password that were provided to him. He clicks on Connect. The DHCPatriot will authenticate the customer either against an external RADIUS server, or use the Built-in Authentication.

Once the customer is successfully authenticated, he will be presented with the 'Thank You' screen. Figure 5 shows the default 'Thank You' screen. This screen is also highly customizable via the GUI. The logo may be changed. The background color may be changed. The text is heavily modifiable. The MAC Address can also be hidden.

Figure 5: Authentication Successful

The default 'Thank You' tells the customer to reboot his connected equipment. This is not strictly necessary as the default lease time for an unauthenticated lease is merely three minutes, at which point they will get an authenticated lease. Also, they could immediately release and renew and receive an authenticated lease. However, it is usually easier for the customer to merely restart his connected equipment than to wait three minutes or decipher the elusive release and renew ritual. The best method is likely for the customer to reboot.

Once the customer has authenticated the computer this initial time, he will not need to revisit this process unless the computer is suspended on the DHCPatriot for some reason, or the MAC Address changes.

After the customer reboots his computer, the computer will get an authenticated IP address. These are usually public IP addresses, but that is not required to use the DHCPatriot. The authenticated IP address ranges are fully configurable.

At this time, the DHCPatriot will authenticate the customer against either the external RADIUS server, if configured, or the Built-in Authentication. After the authentication process is completed successfully, an Accounting Start packet will be sent to the external RADIUS server, if configured. If the Accounting Start is not sent successfully, then the DHCPatriot will continue to try. The optional Accounting Start contains the following: the IP address of the DHCPatriot device that sent the packet, the customer's username, the customer's current IP address, the time the session started, and the MAC Address in the Calling-Station-Id RADIUS Accounting Attribute. If this entire process is successful, an open session will be created for the customer's computer in the DHCPatriot's internal database. This session record contains the customer's username, current IP address, MAC Address, and the session start time.

Some time later, the customer is finished using the Internet and shuts down his computer. Once the DHCP lease on the IP address that the customer's computer has expires, the DHCPatriot will send an accounting stop packet to the external RADIUS server, if configured. The DHCPatriot will also mark in it's own database that the customer is no longer online.

The next time the customer turns his computer on, the computer will immediately receive an authenticated address. The DHCPatriot will then authenticate the customer behind the scenes and perform the operations mentioned previously. All subsequent sessions will behave in this manner, as well. The customer will not receive the 'Login' screen again unless their computer is suspended or disabled on the DHCPatriot, which may be done by either MAC address or username.

Customer devices may become suspended due to RADIUS or built-in authentication failing, an administrator manually suspending them by either username or MAC address, or due to the auto-suspend user time period setting on the DHCPatriot. This setting allows an administrator to configure the DHCPatriot to automatically require the customer to login via the 'Login' screen periodically, to ensure that the MAC address/username correlation is still valid. There also exists a setting to automatically suspend devices that have not had an address in some time period. Devices that are being used or have been used in the intervening time period will not be suspended. This may be more desirable to some than forcing users to authenticate at intervals.

Suspension is not permanent unless the customer's username is also suspended on either the optional external RADIUS server, or the Built-in authentication, whichever is being used. If the customer is not suspended there, then it will be possible for him to immediately login again.

During the manual suspend process, a 'note' field is available. This allows an administrator to enter a note that will be displayed to the customer on the 'Login' screen. A temporary suspension may be performed using this 'note' field to alert the customer of some issue (that he has a virus, for example) that while it needs attention does not necessarily require the customer be prevented from accessing the Internet until the issue is resolved. This note may also be left in event of permanent suspension (such as the customer did not pay his bill, for example). It is also possible to suspend multiple customer's simultaneously leaving the same note, such as for a list of non-pay customers. This allows the customer to receive clear indication of the reason that Internet access is cut off, as opposed to other methods such as simply disconnecting service, and save a wasted call to technical support when the billing office should have been contacted.

At some point, the ONT device fails to work correctly. A technician is sent to the home to replace the ONT device. This can be done when the customer isn't even home as the device is on the exterior of the house. The technician does this. The phone service and Internet begin immediately working again with no further intervention needed. This is due to the Option 82 based address assignment to the ONT. The key to assigning the correct address for VOIP services to the ONT is based on the circuit ID, not the MAC address of the ONT. The customer returns home and the service is working.

The final life cycle of the customer would involve the optional purging from the DHCPatriot after some months of being disconnected for non-pay or similar. The DHCPatriot may be configured to automatically purge customer devices that have been suspended for some length of time. Coupled with the setting to automatically suspend customer devices that have not been online (ie: had no address via DHCP) for some specified period of time, this setting allows for automatic data upkeep. Entries in the database that are no longer needed will be removed based on these settings. This removal does not, however, remove the session history containing the list of IP addresses and times, correlated to the customer's username, that the customer device was online. These sessions remain. This purge mechanism is done at the MAC address level, meaning that old customer devices of still active customers will be cleaned also.

The DHCPatriot creates an environment where the network administrator is in control of network access. It does this without complicating the customer's experience and, at the same time, simplifying the administrator's experience. The DHCPatriot makes it easy for the network administrator to maintain any DHCP network with easy access to reports regarding utilization of network address resources thus enabling the network administrator to upgrade network capacity before it becomes an emergency. The network administrator can also easily manage abuse complaints, subpoenas, and

CALEA warrants using the DHCPatriot. Overall, the DHCPatriot can help in many areas, thusly freeing ISP resources for other tasks.

Implementation

The DHCPatriot is designed to be centrally deployed in your network. It is also designed to service any type of device that supports DHCP. The following figures illustrate the DHCPatriot centrally deployed and servicing various types of DHCP networks in various example network configurations.

In Figure 6, the DHCPatriot has been placed in the 'Server Farm' with other servers such as the mail server and web server. The border router in this example has two separate Ethernet ports. One for the 'Customer Network' and a second port for the 'Server Farm'. This is necessary as the DHCPatriot cannot live on the same LAN segment as the customers due to its central location design. This simple border router would only then need one other interface of whatever type is necessary to connect to the outside world depending on the type of connection.

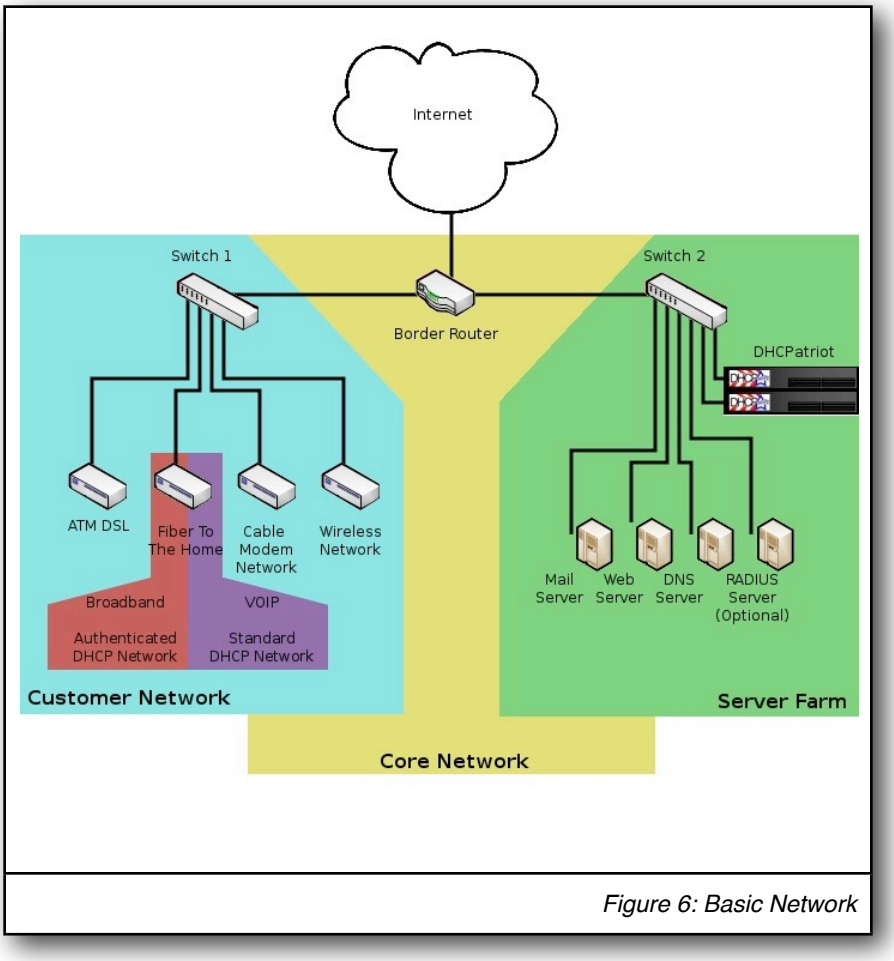

Figure 6: Basic Network

This very simple example of a small ISP network could support a great many customers with relatively low cost and easy management using the DHCPatriot. The DHCP packets from the customer would be relayed to the DHCPatriot via the Border router or the routers associated with the individual customer network types, such as the Cable modem network. The DHCPatriot requires source based policy routing to force unauthenticated customers to the DHCPatriot for authentication. The Border router in this scenario would be the only point in the network requiring this policy routing.

Figure 6 also shows how two distinct networks exist on the Fiber to the home service. The Broadband network being authenticated customer Internet access, and the VOIP network being DHCP based access for phones. The ONT device that exists on-site at the customer premise may need one or more IP Addresses for VOIP or television access as part of a triple play strategy. The Standard DHCP Server in the DHCPatriot can provide the DHCP and TFTP services necessary for these types of networks, as opposed to the Authenticated DHCP that the DHCPatriot must provide to the Broadband Internet network.

The DHCPatriot can also be deployed in more complex networks such as that shown in Figure 7. Here we have a fiber ring setup with remote POPS throughout the ring. This example ISP also has two data centers and two Internet backbone connections for redundancy purposes. The DHCPatriot

devices in this scenario can be separated between the two data centers. This provides redundancy of the DHCPatriot equipment without the need to purchase a second DHCPatriot set.

Each data center would be setup in a similar manner to the 'Core Network' and 'Server Farm' configuration shown in Figure 6. These data centers would basically be a mirror of each other. The only special requirement for the DHCPatriot is that the back plane Ethernet connection be maintained at the default addresses for purposes of the two devices communicating with each other. This back plane Ethernet does require Gigabit speeds as well. Traffic could flow in either direction and out either data center in this configuration. This offers optimal uptime for customers.

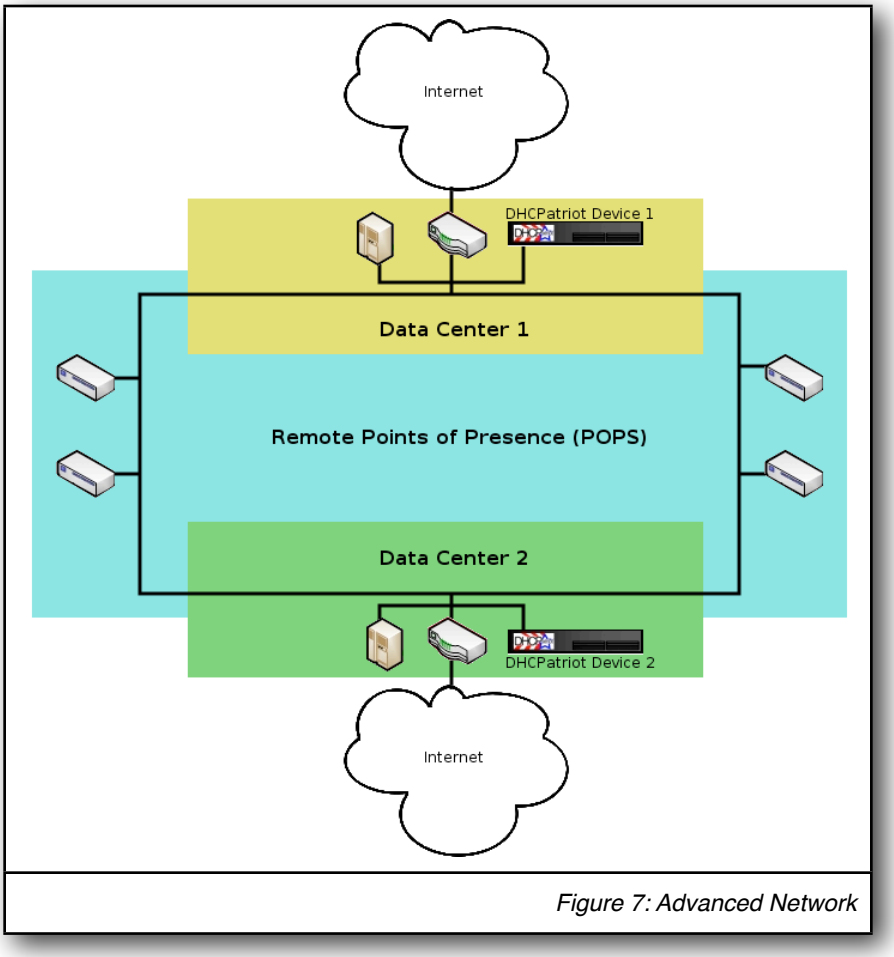

Figure 7: Advanced Network

Until this point, the discussion has centered around general placement of the DHCPatriot in various types of network configurations. This next section will describe what is necessary to integrate the DHCPatriot with existing equipment. In most cases, additional equipment purchase is not necessary to utilize a DHCPatriot system. Some configuration changes to existing routers are necessary, however.

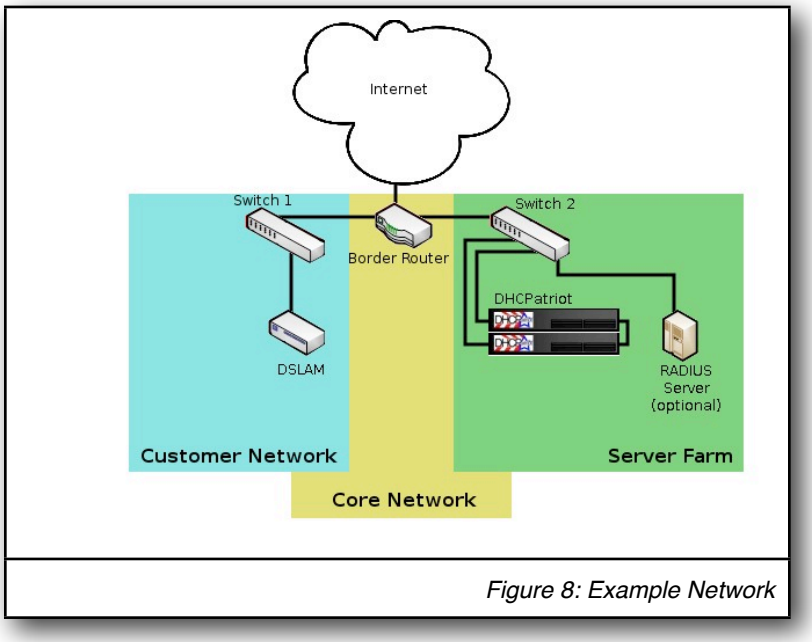

Figure 8: Example Network

This example of implementation will be framed in a very small network that consists of only an Ethernet based DSLAM, one border router, two switches, and a 'Server Farm'. Figure 8 gives an overview of this network. For clarity, the only server depicted in the figure is the RADIUS server. In this example, the 'Server Farm' exists on a separate Ethernet segment from the 'Customer Network'. The border router, in this example, has two Ethernet interfaces, as well as some type of interface to connect to the Internet backbone provider. Standard DHCP will not be discussed in this example.

Replacing an existing DHCP server in such a network would require configuration changes to only the border router. The

Ethernet interface connected to switch 1 would host these configurations. Other more complex networks may require configuration changes to several routers.

Since the initial process of discovery on a DHCP network is done via broadcast, this interface would need to act as a DHCP (BOOTP) Relay agent (Cisco® routers invoke this via the 'ip helper-address' syntax). This causes broadcasted DHCP packets on the 'Customer Network' to be forwarded to the DHCPatriot. The DHCPatriot is able to correctly hand out an IP address to a customer from the correct subnet for that network based on the source IP address that was used by the border router. Typically, this source IP address would be the same as the gateway that the customer will use once authenticated.

The DHCPatriot uses a configurable separate 'unauthenticated' subnet for forcing authentication. This subnet would be added to the interface on the border router that is attached to switch 1. In order to force authentication, the outbound traffic from this 'unauthenticated' subnet must be sent to the DHCPatriot. This requires what Cisco calls source based policy routing. This usually consists of some ACL rules that facilitate a modification in routing if the source IP address of an inbound packet is the 'unauthenticated' subnet. These ACL rules are applied to the border router Ethernet interface that is connected to switch 1. The rules usually set the next destination of the packet to be the DHCPatriot, instead of the default route, or other possible destinations. This forces the customer to authenticate so that they may receive an IP address from the configurable 'authenticated' subnet.

The DHCPatriot is also capable of handing out static IP addresses via DHCP that are assigned to the customer via RADIUS or its built-in authentication (mentioned previously). The DHCPatriot will assign these addresses to customers based on what RADIUS or the built-in authentication returns. If an external RADIUS server is used, the authentication response packet merely needs to contain the Framed-IP-Address reply attribute with a value of the static IP address that is to be assigned. The Built-in authentication provides a predefined place to enter the static IP address.

After a period of time, it may become necessary to provide more IP addresses for lease on a particular network segment due to subscriber growth. The DHCPatriot makes this easy. A network administrator will assign another subnet that will be configured on the border router Ethernet interface that is connected to switch 1. On the DHCPatriot, this subnet will be configured also. Once this is completed, the DHCPatriot will begin handing out these addresses. As many subnets as are required may be added.

CALEA Compliance

The DHCPatriot ties a username to each IP address in use on your dynamic network. It does this in real time satisfying CALEA requirements. Since the DHCPatriot optionally utilizes RADIUS authentication and accounting, it is ready to interface with the many mediation devices that are able to interface with a RADIUS server to receive information regarding a specific targets current status and IP address, collectively termed Call Data. The mediation device can then use this information to configure one or more probes to send a specific targets IP traffic, termed Call Content, to the mediation device. This requires no special configuration on the DHCPatriot as it is designed to force user authentication and accounting in a broadband environment. Figure 9 shows an example of this type of setup.

As shown in Figure 9, the DHCPatriot is authenticating DHCP users such as the target. This authentication and accounting is passed from the RADIUS server to the call data probe device (the probe on the right in figure 9). The probe then sends this information (of the Target only – other customers authentication is ignored by the probe) to the mediation device, a device that collects the

Lawful Intercept data and presents it to law enforcement in real time, at the Trusted Third Party. The mediation device uses the call data to configure the call content probe device (the probe on the left in figure 9) to send the target's call content to the mediation device at the Trusted Third Party. A RADIUS server is required in this scenario.

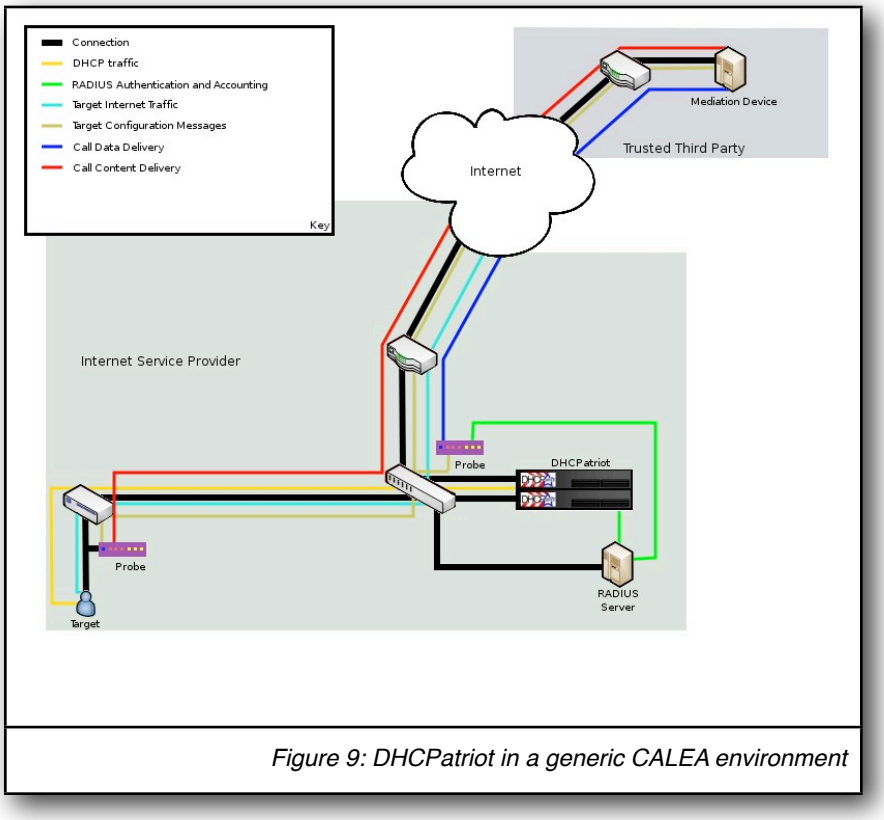

Figure 9: DHCPatriot in a generic CALEA environment

Clearly the DHCPatriot is an extremely flexible and powerful package that can help any ISP control their network. It is easy to integrate into existing networks. It provides powerful features with relatively few changes required to existing equipment. Further, it does not require the purchase of specialized equipment or software to integrate seamlessly into the network. The DHCPatriot is also flexible enough to be used in fully redundant network configurations. It can also support static IP addresses and multiple subnets on the same interface. The DHCPatriot provides an intelligent DHCP solution.

Requirements

- DHCP must be the method the customers will use to get an IP address.
- The gateway routers for the customers must support the BOOTP/DHCP Relay Agent protocol (helper address command on a Cisco router).
- The unauthenticated addresses must be routed to the DHCPatriot.
  - This is usually accomplished via source based policy routing.
    - Policy routing location is configured based on the network layout.
    - Most Cisco devices support policy based routing via ACL(s), as do many other types of routers.
- User authentication via either the Built-in Authentication, or an external RADIUS server.
  - External RADIUS server:
    - If an external RADIUS server is used, it should comply with RFC 2138/RFC 2139/RFC 2865/ RFC 2866.
    - The RADIUS server must at least send the Framed-IP-Address attribute in the authentication response packet.
    - A more complete response packet would contain:
      - Service-Type=Framed-User,Framed-Protocol=PPP,Framed-IP-Address=255.255.255.254,Framed-IP-Netmask=255.255.255.255,Framed-Compression=Van-Jacobsen-TCP-IP
- As of Version 4.2.0 Total DHCP Edition, the DHCPatriot can provide Authenticated DHCP services to CPE (Customer Premise Equipment) such as computers, routers or router/modems. The DHCPatriot can also provide non-authenticated (Standard) DHCP services as well as TFTP (Trivial File Transfer Protocol) services to other types of equipment such as FTTH (Fiber to the home) ONT (Optical Network Termination) devices, cable modems, or just simply to any network that doesn't require authentication. These networks need to be separated on separate relay agents.

How to Purchase

The DHCPatriot may be purchased direct, or through one of our reseller partners. If purchased direct, no discount from MSRP will be available.

To purchase through a reseller, please contact your reseller of choice. For a current list of resellers, with contact information, please visit https://www.dhcpatriot.com, email DHCPatriot@network1.net or call 800-578-6381 x7 (419-739-9240 if outside the United States of America) with your request.

To purchase direct or receive pre-sale support, please use the following contact information:

DHCPatriot@network1.net

800-578-6381 x7 (419-739-9240 x7 if outside the United States of America)

First Network Group, Inc.
P.O. Box 1662
4-6 Perry St.
Wapakoneta, OH 45895
United States of America