Version 4.2.2 fixed the following:
Release Month-Year: October 2009

1. Repaired issue where during auto suspension and auto deletion of devices, if a long list of devices was encountered, false alarms would be raised in DHCPatriot HEALTH stating that the auto-suspend was broken in some way.
2. Repaired an issue that caused the auto deletion of devices to ignore whether NetEnforcer disable VC creation was checked. It attempted to delete Fallback VCs that probably weren't there.
3. Some delete commands from auto deletion of devices would never complete on the NetEnforcer due to issues such as the user was already deleted at some point in the past on the NetEnforcer. The DHCPatriot will now only try these commands for 7 days, after which it will remove these stuck commands.
4. Added new First Network Group address range to the firewall.
5. Added new First Network Group address range to the DHCP monitoring.
6. Health detail via SNMP now works properly again.
7. ISC DHCP version 3.1.2p1 is now the underlying DHCP server used in the DHCPatriot system. This should greatly enhance failover support.
8. Database choice is now MUCH more intelligent and relies less on randomness. This will greatly enhance the speed of the software in the event that one database server is down.
9. Additional and Static DHCP range administration links now function properly from within edit main DHCP ranges.
10. The DHCPatriot now cleans its temporary file system at regular intervals. Previously, it did not do this which could lead to some stale data being presented via SNMP.
11. A problem causing it to be impossible to alter main dhcp ranges after they were configured was corrected.

Version 4.2.1 introduced/fixed the following:
Release Month-Year: June 2009

1. Adjusted the chart at the top right showing how loaded your DHCPatriot system is compared with max load. It now computes based on IPs in use, rather than IPs configured. This should give a more realistic value.
2. Repaired problem with editing of authenticated ranges (main, additional and static) that prevented submission of the changes with an incorrect error message about the gateway not being part of the subnet.
3. Repaired a problem with clicking on setup or editsetup when the other should have been clicked. Previously, Internet Explorer 7 could not properly navigate to the correct function. The function has been changed to accommodate limitations in Internet Explorer 7
4. Repaired a problem with disabling and deleting old devices. Previously, if many old devices were encountered, the process could consume enough system resources to affect the operation of the system as a whole. Now, it is not possible for the process to consume many resources at all.
5. Some older DHCPatriot systems have the storage column for the username of administrative users set to a maximum of 8 characters. This is no longer the case with this patch. Usernames and passwords can each be max 255 characters.
6. DHCP would sometimes attempt to run before the configuration files were completely committed to disk. Configuration file is now tested to be sure it is correct before DHCP attempts to run. This should eliminate certain race conditions.
7. Some minor enhancements to database troubleshooting abilities.
8. Decreased interval between writes of log data to database. This will allow more realtime access to current log data, as well as prevent large amounts of data from accumulating and being written at once.
9. Repaired a problem where the identifier for the users built in authentication would be erased upon editing a user.
10. Made start_stop only run from one device (device #2) and fail over to the other device in event of a problem. This should work much better than the previous way.
11. Made traffic_shaper_commands run only from one device (device #1) and fail over to the other device in event of a problem. This should alleviate problems with duplicate commands being run on the NetEnforcer device.

12. NEW! DHCPatriot system is now a time of day server for use by clients on the DHCP network. In particular, this is useful for devices such as cable modems that need to retrieve rfc868 time at boot according to docsis specifications.
13. IP Address Usage under Authenticated DHCP now shows maintenance networks that are configured for each shared network.
14. Static IP Assignment, under Standard DHCP, now has the ability to assign an identifier. This identifier will show up in the list of clients, as well as under the details in View Address Usage. You can use the asterisk (*) as a wildcard character.
15. Known Client Configuration, under Standard DHCP, now allows the use of the asterisk (*) as a wildcard character when limiting searches by identifier.
16. Viewing clients in a given subnet by clicking on the subnet in View Address Usage under the Standard DHCP menu now shows the identifier, if any, assigned to the client. This is the identifier that was entered by the administrator in Known Client Config, or Static IP Assignment under the Standard DHCP menu.
17. Usage data access via SNMP has received an overhaul. The original method still exists on the DHCPatriot. A new method of gathering both per subnet in use/total data, as well as dynamic subnet totals per network in use/total data is available. Additionally, it is now possible to list the available indexes for the appropriate graphs. Additional Object Identifiers (OID) have been added:

    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:
    1. 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

18. 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:
    1. 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*

2. 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*

19. 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

    For example:
    1. 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]"

20. 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:

    1. 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*
    2. 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*

21. NEW! Administrative notes upon authentication are now supported! These notes will not be seen by the customer. These are used to note what type of device, or any other kind of information when manually authenticating a device. These notes are visible in the view static ip assignment, view authenticated users, and users using more than one ip reports under the user management menu. Further, these notes are editable under the view authenticated users report.
22. Repaired longstanding issue with prompt and window title in both ssh and console. The command prompt will now operate correctly.
23. It is now possible to add the note while using the suspend via API. This is the same note that is specified on the suspend user screen. This note **WILL** be visible to the customer. An extra parameter is added to the GET string: note. Example:

    1. https://patriot.network1.net/cli/remotesuspend.php?username=apiuser&password=apipass&user=linux&action=suspend&note=Call%20our%20billing%20department
24. NEW! A new edition to the API allows remote access to authorize a MAC address using the customer's username, password and MAC address. The new note feature is also supported so that the device may be noted in some way, such as that it's an Xbox360, for example. The API user may be the same as for other CLI/API tasks. Admin level required is 5. Here is the format of the API call (via secure URL):
    1. https://patriot.[domain]/cli/remoteauthorization.php?username=[API username]&password=[API Password]&user=[username for device]&pass=[password for device]&MAC=[MAC address of device]&note=[optional note]
25. And here is an example of what a properly formatted URL might look like for the authorize device API:
    1. https://patriot.network1.net/cli/remoteauthorization.php?username=apiuser&password=apipass&user=linux&pass=Geqp9t4k&MAC=00:a0:cc:d9:96:a2&note=Jim+Smith's+Xbox360
26. The "chattiness" of the PerNetworkLogin information display for the user login page has been "quieted".
27. Daemons that were not previously being monitored with DHCPatriot health are now being monitored via the facility.
28. The programs tcpdump and jnettop and the pcap library are now included in the DHCPatriot OS for use by FNGi personnel.

Version 4.2.0 introduced the following:
Release Month-Year: January 2009

1. NEW! This DHCPatriot software revision features the addition of a standard DHCP server. Standard DHCP server refers to the ability to create DHCP Networks that do not require authentication. Additionally, these Networks may contain a TFTP server specification. A TFTP server has been added to the DHCPatriot system. Each DHCPatriot device contains a running TFTP server for full redundancy. Also, a separate TFTP server may be specified instead. The standard DHCP server also supports full dynamic subnets with optional TFTP file specification, as well as static subnets with optional specification of a TFTP file with the addition of a statically configured device in that subnet. By statically here, we mean that the client will still get their address via DHCP, but will always get the same IP address based on MAC address or some option 82 information. The standard DHCP server is meant to be used with cable modems, customer premise fiber interface equipment, TV set-top boxes, or any other non customer accessible device that needs to access a DHCP server for address allocation. The standard DHCP server could be used for the ISP's LAN or other non-customer purposes as well. It is recommended that it NOT be used for customer-access as the customers would not be easily track-able in that event.
2. Added TFTP server on each DHCPatriot device to be used with Standard DHCP. The firewall will automatically open for any Standard DHCP subnet that needs to utilize the TFTP server.
3. Added Standard DHCP Configuration sub-menu. This section allows an administrator to setup DHCP subnets that do not require authentication, and can hand out files via TFTP using either the DHCPatriot built-in TFTP server or an external TFTP server.
4. Modified DHCP Configuration menu to be Authenticated DHCP.
5. Added TFTP configuration under the Standard DHCP menu. This allows an administrator to upload and delete previously uploaded TFTP files.
6. Added Shared Network configuration area under the Standard DHCP menu. This section allows the administrator to define, edit, or delete a Shared Network for use with the Standard DHCP configuration. A shared network is required before any standard dynamic, static, or maintenance subnets may be added. The DHCPatriot knows that the subsequently configured subnets are all on the same network because they belong to a shared network. Multiple shared networks may be added. This is also where the TFTP sever is specified.
7. Modified add and edit of main DHCP ranges under Authenticated DHCP menu so that they won't allow multiple networks with the same shared network name as this is not possible in the DHCP server.

8. Modified subnet-in-use routine to check the new Standard DHCP subnets also so that an administrator cannot accidentally configure a subnet in two different places thus breaking things.
9. Speed enhancements made to process of DHCP configuration adding, editing and deleting greatly speeding up the process of configuration changes.
10. Added configuration of standard dynamic subnets under Standard DHCP menu. A global TFTP file may be configured here for the entire subnet. Also, allow only known clients may be specified here indicating that only clients that have been entered with 'Add Known Client' may receive an IP address. Others will be ignored.
11. Added area to add known clients for standard dynamic subnets that are configured to only allow known clients. A TFTP file may be specified here on a per user basis.
12. Added configuration of standard static subnets under Standard DHCP menu. Devices can be assigned static IP addresses via static IP assignment in the same area.
13. Added configuration of standard maintenance subnets under Standard DHCP menu. 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 DHCPatriot system to know which network an address should be allocated from in the case that the router(s) (relay agent(s)) do not live in one of the static or dynamic subnets.
14. Added static IP assignment option to Standard DHCP menu. This allows a static IP assignment to a DHCP client using the Standard DHCP server. The client may be matched by MAC address, the option 82 circuit ID sub-option, or the option 82 remote ID sub-option. Additionally, previous assignments can be viewed, edited and deleted in this area. A TFTP file may optionally be specified on a per-client basis also.
15. Firewall now will automatically allow standard subnets that have TFTP configuration set to the DHCPatriot and TFTP files specified to connect to the built-in TFTP server.
16. Repaired problem where sometimes DNS service would fail to start properly after a change in settings and subsequent restart.
17. Added Known Client Config for the configuration of known clients for use with standard dynamic subnets that have allow only known clients marked.
18. Added view address usage which shows the current usage level of addresses in the standard DHCP networks. This also includes a click-able list for a list of those clients currently using IP Addresses, as well as graphs for each dynamic subnet.
19. NEW! Added table showing IP usage, max IP usage and percent of max. The maximum IP Addresses that the DHCPatriot can support is decided by hardware resources available (varies by model) and the average lease length per IP on the system. This table 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 max to be configured, but rather that the system COULD become unstable if this number is exceeded.
20. SNMP access of IP used/available is now computed on a per subnet basis instead of on a per network basis. Numbers for each dynamic subnet are now available at the subnets gateway address. Previously, only total dynamic counts were available. These totals must now be computed on the client side.
21. In the interest of simplicity, the menu called IP Management has been removed. There are now two new menus called Authenticated DHCP and Standard DHCP. Each of these accesses their respective areas instead of having a third menu (IP Management) which displayed statistics that belong to Authenticated DHCP. The reports from the menu called IP Management are now in Authenticated DHCP.
22. Queries against the DHCP or system logs that returned more than 100k results have been disallowed. An error message advising you to narrow your search parameters will be displayed if more than 100k results would be returned. This will eliminate some load problems which occur due to large result sets from log queries.
23. Suspending users now takes you back to the suspend user screen instead of the view suspended screen.
24. Authorizing customers now takes you back to the authorize customer screen instead of to the home page.
25. Added success feedback to all configuration functions. Previously, most of them had no feedback on success and only feedback on error messages.

26. Domain name configuration now strips patriot-1. and patriot-2. in case an administrator accidentally adds that to the domain portion. Previously, it could cause problems having this host-name in the domain field.
27. You can now enter mac addresses in the manner that they are usually displayed on Cisco, Windows or other devices. These four formats are now supported:
    1. 00b0646208c1
    2. 00b0.6462.08c1
    3. 00-b0-64-62-08-c1
    4. 00:b0:64:62:08:c1
28. in all entry boxes for MAC addresses throughout the DHCPatriot GUI.
29. Repaired an issue where it was possible that a session with some missing data could cause the DHCPatriot to not report any further sessions to RADIUS until this issue was repaired. This problem has been rectified.
30. Performance enhancement: all graph entry cleaning (entries older than one year) and cleaning of log entries (entries older than 30 days) have been moved to a central location with more control over the consumed resources.
31. Performance enhancement: Old lease entries are now cleaned after they have been expired for 30 days. This will likely only apply to networks that are no longer configured on the DHCPatriot system.
32. Repaired problem where DNS would report down on the server status screen on the GUI even though it was operating properly.
33. Administrator user-names and passwords can now be 254 characters long. Previously, they could only be 8 characters.
34. Administrator add and edit will now correctly detect duplicate user-names. Previously, it was possible to accidentally add a duplicate administrator user-name.
35. Edit setup will now execute initial setup if it has not yet been run.
36. The timezone selection has been removed from all setup screens as it could inadvertently re-execute the last run operation if someone were to change the timezone after completing changes at the setup screen.
37. NEW! Added a report that shows the static IP assignments from RADIUS. The report is called view static IP assignment and can be found under User Management. These results can be searched via user-name, mac address, or static IP address.
38. NEW! Added a report that allows the viewing of authenticated users/devices. These results can be searched via user-name or mac address. The report is called View Authenticated Users and can be found under User Management.
39. NEW! Clicking a MAC Address within the DHCPatriot Administration interface will bring up http://standards.ieee.org/regauth/oui/index.shtml (OUI search) with the result of what company probably manufactured the device. Keep in mind that MAC Addresses are very easily changed on most equipment, and therefore an incorrect manufacturer may be displayed.
40. NEW! DHCPatriot license status is now available via SNMP. The OID is: 1.3.6.1.4.1.2021.51.12.101.1 and returns output like this: LIMITED:[EPOCH TIME] for an expiring license, and output like this: FULL:0 for a full license (non-expiring).
41. NEW! DHCPatriot device current time (expressed as UNIX EPOCH) is now available via SNMP. The OID is: 1.3.6.1.4.1.2021.51.13.101.1
42. NEW! View Server Status under System Configuration now shows the current time on each server.
43. Repaired problem with add and edit administrator where the encrypted password box would remain filled out if an encrypted password was pasted in there during adding or editing a user. The administrator would literally have to clear the box to continue adding users... Edit user was not quite as affected as clicking on a new user to edit would empty the box.
44. NEW! Radius test program is available on the DHCPatriot system.
45. The Built-in Authentication: User Maintenance now allows the addition of an identifier that is free form text. This could be a customer name or a billing ID or something of that nature. The search box also displays results matched by either identifier or user-name. The Identifier is not required.
46. Default DNS server entries corrected to match new FNGi IP Addresses.
47. Additional information given on authentication web page in event of failure.

48. Manual authentication password box changed to type text. This should alleviate problems with user/pass combos being saved in browser. In general, the hidden typing is not necessary here as these will be entered in a controlled CSR or support work environment.
49. Corrected instructions regarding adding additional and static DHCP subnets.
50. Added support for a tertiary DNS server. This server can optionally be configured along with the primary and secondary DNS servers in the basic settings.
51. Currently Online result set can now be downloaded as a CSV file.
52. The configuration of main DHCP range, additional DHCP range and static DHCP range can now be viewed for an existing network even if customers are currently online. Editing is still not possible unless all customers are not using that network. This applies only to the Authenticated DHCP, as Standard DHCP does not need to concern itself with such things as RADIUS is not used there. Standard DHCP configurations can be viewed, changed or removed at any time.
53. /etc/issue now contains the software version of the currently installed DHCPatriot software.
54. NEW! Users using more than 1 IP report located under user management. This report shows authenticated users who are currently using more than one device, and currently have more than one IP address in use.
55. NEW! Authenticated DHCP maintenance networks are now available. This allows the configuration of a subnet or subnets that will not be handed out via DHCP, but will contain the source address of one or more DHCP Relay Agents. This allows these agents to be associated with the correct network. Previously, only one maintenance subnet could be associated, and only at the time that the original subnet was added or edited.
56. NEW! Load testing program now available on DHCPatriot systems. This program allows FNGi personnel to simulate various amounts of authenticated DHCP traffic. It also allows lease churn (people coming and going) to be simulated. Please contact us if you would like to run any of these tests. These tests are NOT recommended for production machines.
57. NEW! Auto suspend old devices function added. This allows you to configure the DHCPatriot to automatically suspend old devices that have not been online in some chosen period of time. In conjunction with the auto delete of suspended devices already available in the DHCPatriot system, the database of authenticated devices can be kept fresh with only those currently being used on the network. This is an optional feature, and not necessary for the proper operation of the DHCPatriot system.
58. Changed message displayed on end-user authentication page to make more sense. Message is now as follows:
    1. We are unable to authenticate your account at this time. Please type your user-name and password above and click connect. If you are still not able to connect, please contact the [ISP name] Support Department for details.
59. This is the message that appears to customers who are suspended on the DHCPatriot system. This message does not appear if the customer has not previously authenticated the current mac address.
60. Fixed bug with interface which caused the administration interface to be rendered improperly in both Google Chrome and Apple Safari. Both browsers are now able to correctly render the interface.
61. NEW! It is now possible to specify override parameters to change the look of the login screen on a per-network basis! This allows either small tweaks for each network, or a total change in the case of sharing a single DHCPatriot system among multiple Internet Service Providers. Access this new feature under Authenticated DHCP -> Per Network Login.
62. NEW! It is now possible to suspend multiple users simultaneously in the built-in authentication. The users must be entered one user-name per line.
63. Built-in authentication disabling and enabling of users now causes the user devices to also be disabled and enabled.
64. Built-in Authentication Limit Displayed Users now remembers your limitation until you unset it with Display All Users or change it to some other limitation.
65. A new restriction on displayed networks was added to the add and edit administrators areas. If either the authenticated or standard network have networks checked within them for a particular administrator, that administrator will ONLY be able to view statistics for networks that are check-marked regardless if they be Authenticated or Standard networks. Please note also that this is not meant to be a security measure, and therefore only serves to clean up the display of some of the reports. If the administrator has sufficiently high

enough credentials to make changes to networks, these limitations will not be active in the setup screens.

66. Added start and stop time restrictions to CLI session access. This allows the limitation of returned results based on start and end date/time. Two new parameters are to be added to the end of the URL as in this example:
https://patriot.network1.net/cli/remotelist.php?username=*hidden*&password=*hidden*&action=search&user=jsmith&mac=&ip=&online=1&start=1222796365&stop=1225388388
The important addition to note is at the end:
    1. &start=1222796365&stop=1225388388
    where start=EPOCH&stop=EPOCH
67. NEW! Remote Access API foundation laid for built-in authentication! Currently it is possible only to change a user password remotely. Future features will allow full control so that some sort of customer management/billing system can add and remove users from the built-in authentication. This API works in the same fashion as the others. Here is an example URL that will change the user jsmith's password:
    1. https://patriot.network1.net/cli/BuiltInAuthAPI.php?username=*hidden*&password=*hidden*&action=changepass&user=jsmith&newpass=123abc
68. Tweaks made to operation of NTPD. Synchronization should be lost much less often now.
69. Repaired display bug which caused Hide MAC address to always follow the Hide Powered By setting in the basic settings.

```
# Version 4.1.4 fixes the following:
# Release Month-Year: September 2008 (HOTFIX)
# 1) Problem: When adding/removing customers from a hostgroup on the NetEnforcer,
        if the hostgroup name contains a - then some of the commands may fail.
        This software release addresses that problem.


# Version 4.1.3 fixes the following:
# Release Month-Year: February 2008 (HOTFIX)
# 1) Repaired logic problem that prevented users whose authentication had failed
        during subsequent online sessions from being suspended.  Please note that this
        DID NOT affect the web based authentication.  This only affected people who
        were suspended, had a password change, or username change on the RADIUS server
        and were NOT suspended on the DHCPatriot system and who had already authenticated
        at the web page.  These users would have been able to continue to use the
            internet
        indefinately with verison 4.1.2.
# 2) Performance enhancement to log gathering.  DHCP and system logs are now only
            inserted
        every 15 seconds.  This should greatly enhance performance on systems with
            abusive
        DHCP users.  This feature was set to emerge in version 4.2.0, but due to the
            above
        hotfix was rolled into this version.
# 3) System log viewer performance issue was corrected also.


# Version 4.1.2 fixes the following:
# Release Month-Year: December 2007
# 1) Disabled the gathering of lease details that were displayed in search database.
        This gathering and storage was creating significant load on the DHCPatriot
        for little gain.  We may revisit this feature at a later time.
# 2) Repaired a problem where a customer with an invalid all 0 mac address would see
        Warning! 'Your mac address is  ...etc'  This was thought to have been
        fixed in a previous version.
# 3) Repaired an issue with auto delete users after x months where users were deleted
```

but their suspension entries were not. This caused it to be impossible for them to re-authenticate any device that had been deleted.
4) Firewall_setup now does not run under certain configuration change situations where it is not necessary to.
5) Increased available resources to database server.
6) Wireless Internet has been added as a selectable Service Type under basic information.
7) The DHCPatriot now uses ISC DHCP 3.0.6 as the underlying DHCP server.
8) Repaired a problem where the web service would not always restart properly when recovering from a DOS style attack post blocking the offending IP.
9) Improved health monitoring of NetEnforcer processes to generate less false alarms.
#10) NetEnforcer commands will now auto-resume at almost exactly an hour after being paused if not unpaused after 60 minutes. Previously it may or may not have unpaused after an hour.
#11) Repaired a problem where address usage graphs were not always available via snmp. They were unavailable while the next round of graphs were being generated.
#12) Illegal characters are now: \|\'_"\%\`\\~\<\>\:\;\,\/*\?\!\@\#$\& as this is the new list for the NetEnforcer.
#13) It is now possible to set a separate accounting or authorization RADIUS host even while using the built-in authentication for the other type of RADIUS host. Previously, if localhost was selected for either one, it used both for authentication. Please note that you still must keep the secret the same on both RADIUS servers if using a separate auth and accounting RADIUS host.
#14) The DHCPatriot now responds with its own IP address to all DNS queries from the unauthenticated addresses (the only hosts that should be using the DHCPatriot as their DNS server). Please note that this does NOT remove the requirement of the policy routing as the DNS server(s) handed to the customer are still the configured ISP name server(s).
#15) The DHCPatriot now strips @domain.com from any NetEnforcer command usernames. The @ character is invalid on the NetEnforcer and some ISPs need to use the @domain.com in their usernames for RADIUS realms.
#16) The DHCPatriot now provides some detailed health data about running processes via SNMP by accessing the OID: 1.3.6.1.4.1.2021.51.10.101.
#17) The DHCPatriot now responds with its version number via SNMP to the OID: 1.3.6.1.4.1.2021.51.11.101.1.
#18) NTP now quickly re-establishes sync with the chosen remote time servers upon a stop and start or reboot. Previously it could take 15 to 20 minutes for sync to be re-established.
#19) Speed of displaying daemon choices on System Logs has been greatly increased.
#20) NetEnforcer pause will now unpause correctly. Previously, under certain circumstances, clicking un-pause had no effect.
#21) Problem deleting entries from excluded ips has been corrected.
#22) Excluded ips at the end of a range were not previously excluded. This situation has been remedied.
#23) Further speed/resource enhancements have been made to the firewall control mechanism.
#24) Repaired a problem where a user would be removed from a host group on the NetEnforcer if only one of his devices had gone offline instead of waiting for all devices to have gone offline. This bug would have been introduced several versions ago.
#25) The web server has been patched to the latest stable version to close security holes.
#26) The libraries used for RADIUS communication were found to not be completely RFC compliant. A new set of libraries are now used that accurately follow RFC. The non-compliance was related specifically to adding multiple instances of

certain attributes to a packet as specified in RFC rfc2866.

Version 4.1.1 fixes the following:
Release Month-Year: July 2007
1) Repaired problem with the firewall and DHCPatriot controlled routing which caused commands to accumulate even if DHCPatriot controlled routing was disabled. This made it impossible to update the firewall to allow administrators into the machines, or to revoke their firewall access privileges.

Version 4.1.0 introduced the following:
Release Month-Year: June 2007
1) Repaired issue that allowed database tables to 'fill up' at 4.0 GB. The limit has been raised to 1.0 TB.
2) Repaired issue that allowed database sync errors to not cause an error condition under certain circumstances. All database sync errors should now cause an error condition.
3) Increased the maximum simultaneous HTTP connections available to 120.
4) Repaired issue that would keep the web server from restarting properly under certain conditions.
5) Repaired issue that allowed an all uppercase mac address to be entered during the manual authorization. This was a problem as the system expects the mac addresses to be all lowercase. A repair program will fix currently erroneous MAC addresses upon upgrade to version 4.1.0 CALEA edition.
6) Repaired issue that allowed users to enter user@domain.com when registering if their mac address was brand new. If it was existing, the stripping of @domain.com worked correctly. It works correctly now no matter the status of the mac address.
7) Repaired issue that caused setup to not work correctly when certain characters were placed in the login/thank you/override login/override thank you settings.
8) The 8 hour lease choice was inadvertently left out of the possible lease choices in version 4.0.2 AAA This choice has been returned to the list.
9) The U.S. is implementing Daylight Savings Time changes in 2007. The DHCPatriot has been tested and has been found to comply with these changes that have been known since 2005.
#10) NEW! The DHCPatriot can now support the Allot Communications NetEnforcer CALEA module!
It supports multiple NetEnforcers with this module. This requires purchase of the DHCPatriot CALEA module. Contact First Network Group Inc. for details.
#11) The DHCPatriot now reports the lease start_time and lease stop_time rather than the start_time and stop_time that the AAA messages were generated.
#12) The DHCPatriot now generates the AAA session id early in the process and will use the
same session id even if RADIUS has fatal errors. It will use the session id regardless
of how long it takes for RADIUS to respond properly and regardless of failures across
the devices in the DHCPatriot system.
#13) A bug was encountered that allowed certain situations to cause a duplicate start record
to be generated. This has been repaired!
#14) NEW! A new CLI feature has been added! This feature allows a remote search of the session data using several parameters with a result set in xml format for easy integration. Results are limitable by one or more usernames, MAC addresses, and IP addresses. They are further limitable by whether currently open sessions, closed sessions, or both are desired. Accessing this CLI feature is done in the same manner as the remote suspension/unsuspension utility. A cli user is required with admin level 6. The URL is as follows:

https://patriot.example.com/cli/remotelist.php?username=someadmin&password=somepassword&action=search&user=jim,jane&mac=00:00:00:00:00:00,00:00:00:00:00:01&ip=192.168.0.4,192.168.0.5&online=0

As can be seen from this example URL, commas are used to separate multiple limiters.

#15) Offsite backup of the database now no longer contains the system or dhcp logs as these were quite large. It was taking several hours to transfer the db backup from some sites. Certainly, several network administrators will be pleased by the reduction in traffic load.

#16) Added a maximum lease length when DHCPatriot system is in failover mode (ie: one of the devices is down). A 30 minute lease is the max lease that will be handed out by the non-authoritative server for a particular mac. This will make recovery from an outage take a maximum of 30 minutes rather than the length of the lease.

#17) Added support for the NetExplorer. Some minor logic additions were required to the NetEnforcer interface to support those NetEnforcer devices with NetExplorer support.

#18) Repaired bug that made it nearly impossible to add a NetEnforcer into the mix without first knocking all users offline. The configuration of users can now be done on an ongoing basis. If you wish to drop all traffic from non-configured users, you will still need to suspend all subnets so all users go offline, or suspend all online users or so forth so that entries will be created for them on the NetEnforcer when they come online after falling offline.

#19) Repaired bug that caused some configuration changes to be overlooked in the short run by the backend. These changes would be overlooked when the backend was already processing earlier changes and more changes were subsequently made. The backend now checks to be sure that no new changes have been made prior to assuming that all changes have been implemented.

#20) The DHCPatriot now does a better job of detecting software lockups and recovering from the situation on its own.

#21) NEW! A new type of binding between IP and MAC address has been added! Sticky IP addresses are assigned out of dynamic pools rather than special static pools like the static IP addresses that are assigned via RADIUS. Very little sanity checking is done when assigning these IP addresses. Be sure that the IP address exists in the appropriate dynamic pool. Further, the statistical counts for available IP Addresses are not affected by assigning these IP addresses, so be aware that the number of available addresses will only be decreased if someone is actually using the assigned address. The menu for assigning the sticky IP addresses is available under the DHCP Configuration menu.

#22) NEW! It is now possible to add dynamic IP addresses for exclusion from assignment by the DHCP server. Addresses added to the exclusion list will be ignored by the DHCP server when assigning addresses out of dynamic pools. Very little sanity checking is done when accepting

these additions, so be sure you are entering the IP address that you mean to. Further,
the statistical counts for available IP Addresses are not affected by adding them to the
exclusion list, so be aware that the number of available addresses will not be decreased.
The menu for adding an excluded IP address is available under the DHCP Configuration menu.

#23) NEW! We are now remotely monitoring the health of more of the software. Any error condition
that exists in the software that cannot be automatically recovered from will generate an error
condition that we can detect remotely, and respond to (for those that have the maintenance
contract).

#24) Support for the NetEnforcer CALEA module disabled as they are not releasing the product.

#25) NEW! Lease details including option 82 information (if applicable) is now available by clicking on
lease detail at the end of each line of search results in the search database report under
the User Management menu. The link will only appear if lease details are available. Not
all leases will have lease details available for various reasons.

#26) Added the DHCP lease start and end, if available, to the xml return from the remote search API.

#27) Corrected an issue where a web process could use a tremendous amount of system resources if no
database connection is available.

#28) Repaired issue that caused the error message to show up as:
Warning your mac address is
when their MAC address is 00:00:00:00:00:00
it will now show up correctly. All 0 MAC addresses are not permitted on the system.

#29) Moved usage graphs to a separate process as some large installs with many networks configured
caused the process to not get done in a reasonable amount of time holding other things up.

#30) Graphing/health processes spawned as their own process at regular intervals now check to see that
the last round of polls is complete. If a previous process is found, it is killed.

#31) The NetEnforcer hostgroup support has been changed. Hostlists are now removed from hostgroups
upon logoff. They are readded to the hostgroup at login if they are supposed to be a member
of the hostgroup. Previously, hostlists would remain a member of a hostgroup until the RADIUS
server or built in authentication no longer configured them as a member at login. This could
leave orphaned entries as members of hostgroups.

#32) NEW! It is now possible to delete individual pending NetEnforcer commands from the pending NetEnforcer
commands interface accessible from IP Address Usage. The command must be at least 60 seconds old
before it can be deleted. Please be sure that the command is an erroneous command before deleting,
such as improper parameters sent by RADIUS or the like.

#33) Repaired bug that prevented the DHCPatriot from utilizing all of the available RAM in model 2007-1.

It previously would only utilize 884MB of RAM. It now utilizes all 1024MB of RAM.
#34) Usage graph via snmp data spawn has been streamlined to work inline and in the separate process mentioned
in # 29.
#35) Graph data will now be kept for a maximum of 1 year.
#36) Graph data is now no longer included in the offsite backup.
#37) The NetEnforcer lockfile will now stay locked until all of the commands are run, even if it takes longer
than 3 minutes. Previously, many backed up commands could cause some lock stealing from the other
device.
#38) The instructions for placing the rsa keys on the NetEnforcer have been clarified.
#29) At time of upgrade any DHCPatriot devices that were set to not allow the @ sign in usernames
will automatically clean any extraneous @domain.com entries from the user database.
#30) DHCPatriot systems which are configured to control routing will now allow each gateway address
through the firewall. Previously, only the customers were allowed through which led to some
wierdness with diagnosing certain network problems.
#31) A problem was encountered that caused the web authentication mechanism to crash if the RADIUS Reply-Message
contained binary or control characters. The Reply-Message is now stripped of any non-word, non-number,
non-whitespace characters before use.
#32) Repaired a problem that somtimes prevented a DHCPatriot device from booting when connected to a noisy console
cable.
#33) Reduced load on database servers by making some processes more efficiently use the data result sets.
#34) Log messages added that record radius communication including the username, IP address, and MAC address.
These messages appear for both initial web authentication as well as background authentication.
#35) Database dumps no longer occur on the primary device, but only on the secondary device. These database dumps
from the secondary device are copied offsite (as always) if you have the maintenance contract. This will
further address load concerns from database backups.
#36) The DHCPatriot will no longer get hung on a particular user if RADIUS will not respond to authentication or
accounting packets for that user. It will move on to someone else and try that user again later.
#38) The DHCPatriot will now forget older queued lease updates if a new lease update is received for the same
mac address.
#39) The graph generation process has been optimized to use less resources.
#40) The Framed-IP-Address attribute is now included in RADIUS Access-Request packets when the user's IP address is known.
#41) The Service-Type attribute is now set to Login-User in the web based authentication to match the setting elsewhere.
previously it was set to Framed which caused problems with some RADIUS implementations.
#42) Graphs have been further optimized to use less CPU during the data point gathering process.

Version 4.0.2 (Maintenance release) introduced the following:
Release Month-Year: January 2007

```
# 1) Version 3.0.5 of dhcpd now included.
# 2) DHCPatriot logo updated to include trademark symbol.
# 3) Added more choices to the authenticated and non-authenticated lease length
        selection.
      Choices available between 3 minutes and 48 hours.
# 4) Re-worked lease length selection so that the currently chosen value is inline with
        the
      rest of the values instead of at the bottom as was previously the case.
# 5) Increased the number of simultaneous HTTP connections available from 30 to 60.
# 6) Implemented maximum simultaneous HTTP connection limit.  The limit is currently set
        to 20.
      If an IP address opens more than 20 simultaneous HTTP connections, that offending
      IP will be blocked from all access to the DHCPatriot for a period of 300 seconds.
      After the 300 second time period expires, access is again allowed.  Log entries
        are
      generated by dhcpd_conf_daemon corresponding to these events.  These can be viewed
      via the system log function in the System Configuration menu.
# 7) Updated licensing support to repair a few issues.


# Version 4.0.1 (Maintenance release) introduced the following:
# Release Month-Year: November 2006
# 1) Repaired issue that prevented speed and duplex settings from being applied properly
      upon bootup.
# 2) Repaired issue that allowed improper MAC addresses to be entered during the
      manual authentication process. (example: 00-08-00-c0-8e-c1)  The DHCPatriot
      now properly checks that the MAC addresses really are MAC addresses before
      accepting them.
# 3) Clarified on-screen instructions during IP change.  Previously, when the domain name
      was still set to the default example.com, the IP would remain set to the default
      IP that the devices use before configuration is made (10.1.1.2 and 10.1.1.3).
      The on-screen instructions now alert the user that they must change the domain
      name away from example.com in order to have the IP change occur.
# 4) Fixed issue where ntpd may not update time properly if the DHCPatriot was left
      powered on but unable to reach the internet for a long period of time and then
      was not subsequently rebooted.  The DHCPatriot devices now monitor the health
      of ntpd and attempt to recover from problems on their own at regular intervals.
# 5) Corrected entry in manual that showed the usage of the Framed-Filter-Id erroneously
      containing a registered trademark symbol for NetEnforcer.  Although NetEnforcer
      is a registered trademark of Allot Communications, the Framed-Filter-Id attribute
      must not contain this symbol.
# 6) Corrected problem with the setup process that prevented the firewall being opened
      properly when configured to do so via the CLI based menu interface.  New entries
      would not be allowed through the firewall until after the complete setup was done
      via the web interface.  This created an unrecoverable situation that required
      First Network Group intervention.  This has been corrected.
# 7) Updated ethernet driver support to include support for the new Gigabit Ethernet
      interfaces in DHCPatriot model 2007-1.
# 8) Corrected problem that caused ssh sessions to hang on initial authentication when
      setting up the DHCPatriot from the default IP Addresses (10.1.1.2 and 10.1.1.3).
# 9) Corrected problem that caused ntp startup to hang when setting up the DHCPatriot
        from
      the default IP Addresses (10.1.1.2 and 10.1.1.3).


# Version 4.0.0 introduced the following:
# Release Month-Year: October 2006
# 1) NetEnforcer Support: Radius attribute #11 Framed-Filter, Filter-Id, or Framed-
        Filter-Id
      can now be used instead of Radius attribute #25 Class when sending the NetEnforcer
```

information. The structure of the data in the string remains unchanged. Also, the DHCPatriot™ still accepts the Class attribute if you prefer to use that.
2) NetEnforcer Support: Changes are now made on the NetEnforcer on a more real-time basis. Previously, they were run periodically.
3) Start_stop function processor utilization made more efficient.
4) Add_DHCP_Range function - repaired bug that prevented adding DHCP ranges with with no error message.
5) Version number now stored globally.
6) New FNGi developed linux distro now platform that the DHCPatriot™ runs on. All DHCPatriot™ devices will run this as of this version. Previously, they ran Fedora Core 1, 2, or 3.
7) Start_stop now sets SIG{ALARM} instead of forking to wait for a hung radius server.
8) auth_hardware either by user or by csr (manual) now same program. Previously, there were two: auth_hardware and auth_hardware-manual. Many performance enhancements have been added to auth_hardware.
9) Repaired potential expliot allowing a user to use auth_hardware-manual instead of auth_hardware to simulate being authenticated by customer service. auth_hardware now checks to make sure that the admin user is logged on to the admin interface before 'believing' that they are an admin user. This potential exploit was discovered during an internal security audit.
#10) Most console messages from the DHCPatriot™ software have been removed. These messages
are now located in /var/log/DHCPatriot.log
#11) NEW! Console access is finally here! Administrators of the DHCPatriot™ can now login to a nice GUI system for configuring the OS related items (such as IP Address)
from console. Merely use the admin username and password (contact FNGi for the password if you do not have a v.4.0.0+ manual). We STRONGLY urge you to change the admin password upon successful login to the console configuration interface.
#12) NEW! Ping and Traceroute are now available on both the console GUI system as well as on the web administration interface! This should greatly help troubleshooting new networks that are added for DHCP, as well as configuring the actual IP Addresses on
the actual DHCPatriot™ devices.
#13) Corrected odd and various spelling and gramatical errors.
#14) changed view_suspended to be a search type viewer, instead of just displaying a list.
That will make it much easier for the administrators to locate users in the list.
#15) Added a dynamically generated title to the top of each DHCPatriot™ function on the web administration page.
#16) Adjusted load-balancing and failover parameters to a bit more sane values.
#17) Log-facility changed on the DHCPd.
#18) /etc/hosts is now auto-generated so that the DHCPatriot™ devicess will always be fully aware
of each other.
#19) firewall_setup now blocks ALL forward traffic instead of just by router. It still specifically allows traffic that it should. This cuts down on the amount of firewall rules needed.
#20) firewall_setup now adds the drop INPUT traffic rule before moving on to the forward traffic rules to speed up the setup of protection type firewall rules before setting up the customer firewall rules that are only present if the DHCPatriot™ has 'DHCPatriot™ controlled routing' option set.
#21) firewall_setup now generates all the rules before applying them all at once instead of as before on-the-fly.
#22) Web administration: setup screen #3 (add/edit) repaired bug that prevented an administrator from adding or editing a dhcp range.
#23) Repaired bug where it was impossible to choose a 'blank' service type when editing or adding the basic info on the web administration interface.
#24) Consolidated several functions into one daemon, therefore greatly reducing RAM

usage of the backend. This should allow the DHCPatriot™ to handle more IPs after the completion of some other things in a future revision.

#25) Database backup now MUCH more efficient than previously.

#26) Made changes to isp image upload commensorate with new OS and methods.

#27) May have fixed long standing cache issue. Customers who have authenticated and then rebooted should no longer see the authentication page as their homepage until they change their cache settings to 'every visit to page (IE)' instead of their real homepage.

#28) NEW: Licensing support now enabled in the DHCPatriot™. This protects all parties from misuse of the product.

#29) Fixed bug that caused some users to not be un-suspended when using the new un-suspend function available in the view_suspended function.

#30) More visual enhancements added to the DHCPatriot™ to provide a more consistant appearance amoung the various functions.

#31) The DHCPatriot™ devices now share information about each other's IP Address so that they
can be moved to different subnets and still have correct host entries about each other in a single system.

#32) Logo file now stored in generic location for better compatibility across upgrades.

#33) NEW! Search database function now has a csv download option for downloading the search
results as a comma separated file for viewing in Microsoft Excel or OpenOffice.org Calc.

#34) Repaired issue that prevented ISP logos from being accepted for upload and/or displaying
if the filename contained spaces.

#35) Repaired issue that sometimes prevented the dhcp daemon from running when there were multiple superscopes.

#36) Enhanced security of product as relates to php includes.

#37) Enhanced security of product as relates to the underlying daemons. Protected these daemons from prying eyes.

#38) Interface has been cleaned up and special attention has been given to the ease of reading data displayed on the screen.

#39) auth_hardware now syslogs instead of writing directly to a log file. This coincides with
the new ability to view DHCPatriot™ specific syslogs from the web interface.

#40) Customer login screen modified so that errors/note from administrator/cant auth you at this
time messages appear just below the login button. Previously, it was possible that
users running under a lower resolution (800x600 or 640x480) may not have been able to see those messages.

#41) Corrected some issues with the licensing support.

#42) New text appears on screen if a non-suspended user happens to get the login screen again
for some reason:
Notice: You are already authenticated and do not need to authenticate at this time...

#43) All screens that show the Authenticated CIDR now also display the shared_network setting so that easy identification of networks may be done.

#44) Repaired HTML issue in detail that caused the page to display blank on IE6.

#45) Reapired issue in detail that caused it to display the wrong title.

#46) NEW! Usability of the Web Admin Interface enhanced through the introduction of a new category based menu system. This should allow users to quickly find the functions
that they are looking for. This menu system has been tested under the following browsers:
70. FireFox 1.0.7 (Gentoo Linux)
71. Konquerer 3.4.3 (KDE 3.4.3) (Gentoo Linux)
72. Opera 8.54 (Windows XP SP2)

73. * Note: The menu items take up two lines instead of one.
74. * Note: The CSV downloads will need to be renamed .csv
75. Netscape 8.1 (Based on FireFox) (Windows XP SP2)
76. Internet Explorer 6.0.2900.2180.xpsp_sp2_rtm.040803-2158

#47) NEW! Search Database now displays the remaining lease time (0 for offline users).
#48) Setup now correctly detects what portion of the process you are on, and returns you there.
If you are done with the initial setup, it takes you to the EditSetup screen.
#49) Add Main DHCP range now is separate in the DHCP Configuration menu category.
#50) Edit Main DHCP range is now separate in the DHCP Configuration menu category.
#51) Repaired isssue that prevented the proper re-config/re-start of DHCPd in some cases.
#52) IP Address Usage has been re-ordered and re-organized so that the shared-networks are all
together. This should make more sense (with a total dynamic for easily identifying
networks that need an additional subnet added).
#53) Lease status was also re-organized in much the same way as IP Address Usage.
#54) Changes were required to continue using the ability to change fonts. A survey was performed and the level of interest in the ability to change fonts on the end-user login screen was determined to be low. Therefore, the option was simply removed.
#55) DHCPatriot™ Web Administration errors are now logged via syslog.
#56) NEW! dhcp logs are now stored in the database.
#57) NEW! DHCPatriot™ software logs are now stored in the database.
#58) dhcp and DHCPatriot™ software logs are now deleted every 30 days.
#59) Administrator passwords can now be of any length.
#60) Administrators can paste an MD5 encrypted password into the add/edit user screens instead of having to type the users password in. This allows existing *nix passwords to be used when setting up new Administrators (NOTE: The password MUST be MD5 encrypted - older methods such as DES are not supported).
#61) Repaired issue where login errors upon failed logins to the Web Administration of the DHCPatriot™ would sometimes be hidden from view at the bottom of the screen. These errors now display just below the Enter button.
#62) Repaired issue where table tags were not properly being disabled/removed from the override text on the login and thank you screens for the End Users.
#63) The Radius attribute Calling-Station-Id now is sent with both Start and Stop. It contains the user`s MAC Address.
#64) Auto delete users now deletes after the specified time period only if the user has been suspended for that period of time.
#65) Search dhcp logs. These logs are now stored in the database for an indefinate period
of time. A future version may offer the ability to delete the logs after a specified period of time. The search DHCP logs feature has been updated to allow the specification of a time period, as well as limiters such as IP Address and MAC Address. The logs from each server are now shown in line instead of as two separate blocks. This should make troubleshooting far easier.
#66) System logs added. The software logs are now viewable from the admin section. These can be searched using limiters such as time/date, daemon and host.
#67) Repaired bug in Additional DHCP Range that allowed a network to be deleted if the one above it was empty.
#68) Repaired bug in Static DHCP Range that allowed a network to be deleted if the one above it was empty.
#69) It is now possible to edit a main DHCP Range if there are no users online in it even if there are additional/static subnets tied to it.
#70) It is now impossible to delete a main DHCP Range until there are no users online and there are no additional/static subnets tied to it.
#71) It is now possible to disable a main DHCP Range in order to 'knock' people out of a particular set of IP Addresses. This has the effect of allowing a main DHCP range to be cleared out so that edits can be made on it and then it can be

re-enabled.
#72) Pause NetEnforcer Communication function added to Pending NetEnforcer Commands function. Pausing the NetEnforcer Communication can allow an administrator to make changes on the NetEnforcer without fear of the DHCPatriot™ revoking the administrator`s write privileges. The pause feature has a max-duration of one hour. At the end of that time period, the communication will be restored. While the communication is paused, commands will continue to queue. When the communication is restored, the queue of commands will be executed.
#73) Added length check to the is_ip function to ensure that the length of each part is less than 4.
#74) All date/time are now stored as EPOCH. This will eliminate problems that result from dst changes and the like. A conversion program has been created that will convert current data to the new format. No data will be lost during this conversion process.
#75) A timezone selection box now appears at the bottom right corner of the web administration interface for the DHCPatriot™. This allows a timezone to be selected and merely left alone, or the timezone may be changed on the fly to assist with resolution of abuse complaints. This timezone selector only modifies the display of data. Each administrator may have their own timezone setting. Change of the timezone setting by one administrator will not affect any other administrator's timezone setting.
#76) NEW! The DHCPatriot™ is now gathering stats about numbers of dynamic customers online versus total IP Addresses available on an ongoing basis. It gathers these stats every 5 minutes. The stats are available for the following types of networks: Main DHCP Ranges, Additional DHCP Ranges, and total Dynamic usage (per Main DHCP Range).
#77) Found and repaired long-standing bug that caused start_stop to miss the rest of the user base after sending a start or stop. It would have to cycle by again to check the rest of the userbase. It was long suspected that there was some problem, but the problem could not be duplicated in testing. The bug manifested itself in the field recently which helped in isolation.
#78) NEW! Graphs of address usage are now available on the DHCPatriot™. These are accessable in the IP Address Usage report by clicking on the graph icon.
#79) NEW! Usage data is now available via SNMP. Currently, only totals are available with the
OID: .1.3.6.1.4.1.2021.50.60.3.0.
Example: .1.3.6.1.4.1.2021.50.60.3.0.208.45.199.113
These numbers contain all dynamic (main and additional) addresses for that particular main range.
#80) All system logs are now available in the System Logs function under System Configuration.
Previously, only DHCPatriot™ software specific logs were available in that report.
#81) Customer Usage function now notes the type of network and the status (ie: disabled) of the network. This should keep users from having to remember this information from the Address Usage function.
#82) It is now possible to manually authenticate a user who has not received a private IP address using the Authorize Customer function under User Management. The MAC Address of the customer equipment MUST be supplied to use this functionality. This can be useful for pre-authorizing existing customers during a cut to the DHCPatriot™, or merely to make the Tech Support job easier.
#83) Enhanced security on backplane interface.

#84) NetEnforcer host modification procedure altered. Previously, it was only possible to
add 4 IP addresses to a host using the DHCPatriot™. Now, the number is only limited
by any limit to entries within a host on the NetEnforcer.
#85) NEW! It is now possible to disable the auto-creation of VCs by the DHCPatriot™ in the
Fallback Pipe on the NetEnforcer. This setting is located located in General Setup.
It is item number 12, just below the NetEnforcer IP setting.
#86) NEW! It is now possible to have 2 or more DHCPatriot™ systems communicate with a single
NetEnforcer. The DHCPatriot™ systems will not step on each other, and all commands
will be run in a linear fashion as specified by Allot Communications. No settings
are required to utilize this functionality.
#87) NEW! Usernames can now be rejected at the login screen if they contain any of these
characters: \|\'_"\%\`\\~\<\>\:\;\,\/*\? anywhere in the username. This setting
is available System Configuration->under setup/edit setup->basic information.
This setting is especially useful for NetEnforcer owners, as those characters are
not permitted in Hosts and Virtual Channels on the NetEnforcer.
#88) NEW! A setting that allows the stripping of @ signs and everything following them
from the username as a user attempts to login. This will make it easier for
administrators to locate users on the DHCPatriot™ who tend to login with:
user@domain.com instead of just their username. This setting is available under
System Configuration->under setup/edit setup->basic information.
#89) NEW! A setting now exists that allows the administrator to force all usernames to
be in lowercase letters. This will make it easier for administrators to locate
users on the DHCPatriot™ who tend to login with: user@domain.com instead of just
their username. This setting is available under
System Configuration->under setup/edit setup->basic information.
#90) Repaired bug that allowed multiple non-unique usernames to be entered into the
administrator table. This would have rendered one or more administrators unable
to login. This was found during an internal audit, to our knowledge, no one
has experienced the effects of this bug.
#91) NEW! It is now possible to remotely suspend and un-suspend users via a Web based CLI
interface. An administrative user must be added with cli_user privileges and an
appropriate admin level (remote suspend currently requires admin level 5). CLI
users will not be able to access the administrative web interface, but rather, only
the CLI interface. Also, normal users cannot access the CLI interface, regardless
of admin level. This interface is meant for use with automated scripts that control
user access on-the-fly. Usage instructions:
Suspend user:
https://patriot.[domain]/cli/remotesuspend.php?username=[username]&password=
[password]&action=suspend&user=[username to suspend]
Un-Suspend user:
https://patriot.[domain]/cli/remotesuspend.php?username=[username]&password=
[password]&action=unsuspend&user=[username to un-suspend]
#92) NEW! The DHCPatriot™ now supports local authentication via a built-in authentication module!
Users can be maintained using the new User Maintenance function located under User Management.
The built-in authentication also supports static IP addressing and NetEnforcer options
in the same manner as a separate radius server. Available NetEnforcer options may
be setup using the Configure Built-in Authentication Options function located under
System Configuration.

#93) ISC DHCP updated to version 3.0.4.
#94) NEW! The DHCPatriot™ now displays a list, and provides a CSV download of a list of users
on a per subnet basis. Click the network address in IP Address usage to bring up a list of users in this manner.
#95) NEW! Reply-Message support. If the Radius server returns Reply-Message in event of login
failure, this message will be displayed to the user on the failure screen.
From RFC 2058 section 4.3:
If any value of the received Attributes is not acceptable, then the
RADIUS server MUST transmit a packet with the Code field set to 3
(Access-Reject). It MAY include one or more Reply-Message
Attributes with a text message which the NAS MAY display to the user.
#96) View Server Status has been reworked to give more meaningful information.
#97) Found bug during internal audit that allowed a network to step on another network so-to-speak. It was possible to add a network like this one: 192.168.1.0/24 and then add another network like this: 192.168.0.0/22.
The DHCPatriot™ will now return an error when the above situation is encountered.
#98) Maximum character length on administrator usernames has been upped to 255. It was a bug that the maximum length was set to 8.
#99) NEW! Lease length settings > 1 hour have been added. Lease lengths from 2 hours to 24 hours (in one hour increments) can now be configured. The actual available lease length settings are as follows:
10 minutes
15 minutes
30 minutes
45 minutes
1 hour
2 hours
3 hours
4 hours
5 hours
6 hours
7 hours
8 hours
9 hours
10 hours
11 hours
12 hours
13 hours
14 hours
15 hours
16 hours
17 hours
18 hours
19 hours
20 hours
21 hours
22 hours
23 hours
24 hours
#100)NEW! DHCPRELEASE now destroys the lease. If a customer performs this action on his device,
the IP Address is freed, a stop accounting packet is sent to RADIUS and the DHCPatriot™
closes their online session.
#101)NEW! If a device is suspended and ends up with an unauthenticated address prior to the expiry of his authenticated address, the authenticated address lease is destroyed,

the IP Address is freed, a stop accounting packet is sent to RADIUS and the DHCPatriot™
closes their online session. This allows the customer to authenticate once the above
action is completed rather than when the authenticated lease would have expired as was previously the case.
#102)NEW! If a device somehow receives a different authenticated lease when his previous
authenticated lease has not yet expired, the prior authenticated lease is destroyed,
the IP Address is freed, a stop accounting packet is sent to RADIUS and the DHCPatriot™
closes their online session. Subsequently, the start process will ensue for the new authenticated lease.
#103)Repaired bug where it was possible for users to slip through the cracks when registering
under certain situations. They may not have shown as online for several days.
#104)Repaired a bug that caused the actual stop address of a DHCP pool to be ignored and .254
to be used instead when the network was larger than a /24.
#105)High Availability behavior changed: The system no longer assumes that a particular peer is
down based upon the status of the actual DHCP process. Heartbeats of some service(s) are
now used instead.
#106)NEW! DHCPDECLINE support. If a dhcp client detects that an IP that has been offered by the
server is in use via arp or some other means, the client sends a DHCPDECLINE message.
This message is now recognized, and the client can immediately DHCPDISCOVER and receive
a new address.
#107)NEW! An online manual has been added. A link to this manual appears in the upper right
corner of the DHCPatriot™ Web Administration Interface. A new window will appear
containing the PDF version of the manual for v.4.0.0 AAA.
--- Beta 1 patches ---
#108)Reduced the number of logs produced when the firewall rules are maintained.
#109)Repaired several bugs with lease_updater that occured when certain rare conditions were
encountered that required re-initialization of its internal db.
--- Beta 2 patches ---
#110)Visual enhancements made to the following reports: IP Address Usage, Customer Usage,
Lease Status.
#111)Several repairs made to the NetEnforcer communication backend.

Version 3.4.0 introduced the following:
Release Month-Year: August-2005
1) installed version 3.0.2rc2 of the ISC DHCP server.
2) corrected a problem with monitor where $time was being reset preventing
proper monitoring of the lease_updater process
3) removed 'Pending NetEnforcer Commands' button from address usage page when
no NetEnforcer is configured.
4) removed debug output from the 'Pending NetEnforcer Commands' screen.
5) added IP Address to text only view of the user detail screen.
6) removed debug output from security.
7) repaired an issue where customer_usage would not show all additional ip usage stats.
8) added 'CSV download of data' option to detail.
9) added the ability to search by MAC Address in the search area.
10)it is now possible to add global DHCP configs in the radius setup area. This is

probably not a feature that most customers will need, but some may need it for specific situations.
11)changed behavior of start_stop-wrapper so that it only restarts procs if the actual patriot it resides on calls for it.
12)It is now possible to disable an additional dynamic network. This allows you to empty an additional dynamic network for reclamation purposes. There are other more standard methods of emptying main and static networks.
13)DHCPD is now able to recover from another DHCP robbing situation. This error: 'lease in transition state expired' is now automatically recovered from.
14)it is now possible to set an auto suspend and auto delete time in months for the users (MAC Addresses). This will cause them to either get suspended after the set number of months since they last authenticated on the webpage or delete them after the set number of months since the last time they were online, or both.
15)repaired issue where leases would still be written to the database with the old year stamp on the culmination of a new year. lease_updater should now realize that a new year has come upon us (Happy New Year!).
16)monitor now logs errors instead of mailing them to the administrator.
17)the new auto delete functionality added this patch now also deletes the users entries on the NetEnforcer if so configured.
18)Fixed a problem where the initial setup did not function due to some fields not being inserted into the DB.
19)Removed password box length restriction from the nonsecure side. some folks apparently have longer than 8 character passwords :)
20)Repaired issue where the background color chosen was not properly being displayed on the the thank you screen as it was on the login screen.
21)Reversed the sort order of the detail.php It now sorts from newest to oldest by start_time.
22)It is now possible to search by MAC Address on the Search Database screen.
23)Disabled SNMP/ARP selections from the DHCPatriot™ setup screens, as this mode is no longer supported.
24)Blank log messages no longer crash the syslog mechanism.
25)Fixed situation where start_stop wouldnt always receive settings changes requiring manual intervention. This is now repaired.
26)Fixed issue where if the FNGi network was down, the patriot news would hang for 3 minutes and then timeout. I have instituted a 5 second timeout using fsockopen ()
27)Movied version text above the blue area so that the blue area appears correctly, per web developer.
28)NTPD now uses some random servers from ntp.pool.org so that we are more sure that the time is up-to-date. Previously, it used network1.net ntp servers... Now, it uses the following Addresses:
77. us.pool.ntp.org
78. north-america.pool.ntp.org
79. europe.pool.ntp.org
80. south-america.pool.ntp.org
81. asia.pool.ntp.org

The above addresses return random server IPs ... Most of them are stratum 2 or 1.

```
# 29)It is now possible to suspend multiple users at once using the manual_suspend the
        usernames MUST be separated by a CRLF in order to have the list built properly.
        Notification will appear on screen for those users that do not exist.  The
        rest of the users in the list will be suspended.
# 30)start_stop is now a linear process that (should/will) run much more efficiently.
# 31)start_stop and traffic_shaper_commands will now restart much more sanely using a
        SIGHUP on config change...
# 32)fixed problem where add administrator caused passwords to not be md5 encrypted and
        had to subsequently be edited so that they would be encrypted and usable.
# 33)Disclaimer added to credits that Microsoft Internet Explorer is required for credits
        to work properly.
# 34)fixed a problem where it was possible to put improperly formatted IP Addresses into
        the DHCPatriot™ configs causing the unit to not work properly.  All IP Addresses
        are now checked to see if they are valid IP Addresses.
# 35)added user_purge to the distrubiton.  This allows a software administrator to accept
        a list of users (one user per line) and suspend them.  Later they can be deleted
        as well...
# 36)security now properly limits access to functions even if the actual URL was typed.
        Previously, users who were logged in properly could access functiosn they werent
        meant to access by typing the URL directly.
# 37)Databased firewall added.  Rules may be modified from the web admin interface.  Some
        rules are generated automatically based on configured networks.  The firewall is a
        whitelist.  FNGi netblock is added automatically to the database at time of
            install
        (or upgrade on previously installed DHCPatriot™ systems).
# 38)Changed cryptic 'Server Problem: Unable Authenticate you at this time. Try again in
            5
        minutes' error on login screen to: 'Server Problem: Unable Authenticate you at
            this
        time. Try again in  minutes'
# 39)Plugged security hole in dhcp_log allowing remote users to gain access to the DHCP
            log
        file.  This was discovered during a security audit.  To our knowledge, there have
        been no violations at this time.


# Version 3.3.1 (bug fix release) introduced the following:
# Release Month-Year: November-2004
# 1) Fixed a problem with auth_hardware-manual.pl that caused Internet Explorer
        to report 'Page cannot be displayed' after either unsuccessful or successful
        manual authentication.
# 2) Added more logging detail to auth_hardware-manual.pl and auth_hardware.pl
# 3) Fixed an issue where an incorrect main subnet could be added or edited into the
        dhcp range.  This had the effect of dropping DHCPD out.
# 4) Fixed an issue with the static IP addition where the DHCPatriot™ could get into
        a state where it was no longer possible to add static ranges to the DHCPatriot™.
# 5) Fixed an issue with the additional IP Addition where the DHCPatriot™ could get into
        a state where it was no longer possible to add static ranges to the DHCPatriot™.
# 6) Repaired an issue that could cause the redirect to not work after manual
            authentication
        on patriots where more than one patriot system was present.
# 7) Changed undesireable behavior of the session db - the username is now stored in the
        session db so that if a REMOTE_MAC is reassigned to another username, it no longer
        changes past sessions to the new username.
# 8) Enhanced NetEnforcer (and other bandwidth management tools) interoperation by adding
        separate process to specifically handle the command actions.
# 9) fixed next and back button functionality in the search function.
# 10)changed behavior of search function so that it now remembers which limiter boxes you
        had checked after submitting and using back and next.
# 11)fixed the link colors on the detail function so that they could more easily be seen.
```

```
# 12)fixed an issue where auto-restarting of DHCP failed under certain circumstances.
# 13)changed behavior of firewall maintenance to only occur if DHCPatriot™ controlled
            routing
        is enabled.


# Version 3.3.0 introduced the following:
# Release Month-Year: November-2004
# 1) Administrator passwords are now stored MD5 encrypted in the Database.
# 2) The DHCPatriot™ now detects stale auth_hardware_lock and NULL it.  This eliminates
        a situation where the DHCPatriot™ could no longer process new login attempts.
# 3) repaired a problem where blank hostnames would sometimes enter server_status.
# 4) repaired a problem where the auto-restarting of DHCPD from lease_updater would
        sometimes get into a loop.
# 5) added auto-generation of /etc/hosts in preperation for a menu driven DHCPatriot™
        system configuration (IP Address; hostname; gateway address)
# 6) added auto-generation of /etc/resolv.conf in preperation for a menu driven
            DHCPatriot™
        system configuration (IP Address; hostname; gateway address)


# Version 3.2.1 (bug fix release) introduced the following:
# Release Month-Year: August-2004
# 1) fixed a problem where lease_updater would hang under certain conditions.
# 2) fixed a problem where NetEnforcer updates where happening too fast for the
        NetEnforcer to handle.
# 3) fixed two different situations where DHCPD could hang.  DHCPD will now auto-restart.


# Version 3.2.0 introduced the following:
# Release Month-Year: August-2004
# 1) repaired bug that prevented the thank you page custom texts from showing up
            correctly
        (it used the login page instead).
# 2) repaired problem where the ISP logo, if placed on patriot-2, would disappear after
        a time.  The logo now automatically copies itself to patriot-1 if placed
        on patriot-2.
# 3) repaired a problem where using a  tag would backfire in the basic setup
        screens, as the web browser would think that the  tag was meant to
        end the current text box and not part of the data.  This has been repaired.
# 4) Three new options added to the Service Type specification: a blank option,
        a Broadband option, and a Wireless Ethernet option.
# 5) The ability to preview the login and thank you screens has been added to the
        edit_basic_setup  This allows an administrator to preview the changes that
        were made on that screen.
# 6) it is now possible to hide the 'powered by' section on the login page so that
        ISPs who do not want their customers to see where or what the login page
        comes from can now hide the brand name/company name if so desired.
# 7) it is now possible to hide the user's MAC Address that he just registered on the
        DHCPatriot™ from his sight on the 'thank you' page.
# 8) Repaired a problem with start_stop where alot of CPU was chewed up by larger
        networks ... The process has been throttled.  Very large networks such
        as /20s take a couple minutes for the start_stop to complete, but this
        still functions better than it did with the old method.
# 9) all users who have permission to authorize customer now have permission to do it
        via MAC Address.  It was discovered that this was no more a problem than doing
        it by IP Address.  So there was no reason to limit the access to that feature
        separately.
#10) added optional overriding text to the basic_setup.  This text will override the
            default
```

```
        text on that screen allowing an administrator to completely change the wording on
        the login screen to suit their ISP.


# Version 3.1.5 (bug fix release) introduced the following:
# Release Month-Year: August-2004
# 1) fixed a bug where the MAC address would show up as all 0's 00:00:00:00:00:00
        on the thank you page after login.
# 2) fixed and optimized start_stop - as of version 3.1.4 radius errors were occuring
        sometimes when talking to radius.  The error involved the DHCPatriot™ thinking
        there were blank packets in response to accounting start.  This was, infact,
        not the case as tcpdump has shown.  This 'blank' packets still crop up from
        time to time, but the start_stop retries 10 times before giving up and moving
        on to the next user.  This appears to emulate router behaviour.  I cannot
        be completely certain that this hasnt always been a problem and the stepped
        up logging in version 3.1.4 is just now showing it.  It also may be some
        weird problem with Fedora Core 2.  This workaround is the best that can be
        managed at this time.


# Version 3.1.4 (bug fix release) introduced the following:
# Release Month-Year: July-2004
# 1) fixed incompatibility between NetEnforcer 5.1.1 and DHCPatriot™ ac(go) command
        format.
# 2) removed instances of 1.1.1.1 being set for last_ip at time of user login
        when they had logged in previously and therefore may receive the same
        ip again...
# 3) changed lease_updater.pl to key on MAC instead of IP therefore not missing
        anyone's IP changes...
# 4) changed start_stop.pl to daemon form.  One daemon runs for each main subnet.
        this has greatly enhanced the speed of which the users are accounted for.


# Version 3.1.3 (bug fix release) introduced the following:
# Release Month-Year: July-2004
# 1) further tweaks made to lease_updater.  It now no longer
        has to restart and gives detailed output in
        /var/log/messages
# 2) Bug discovered in the DHCP server config.  This bug caused
        failover to work improperly.  It has been repaired.


# Version 3.1.2 (bug fix release) introduced the following:
# Release Month-Year: June-2004
# 1) installed dhcpd version 3.0.1rc14 as 3.0.1rc13 has a serious
        buffer overflow vulnerability
# 2) repaired logrotate issue that was causing problems with proper
        logging of the DHCPD activity after a logrotate occured.


# Version 3.1.1 (bug fix release) introduced the following:
# Release Month-Year: June-2004
# 1) temporarily fixed serious problems with lease_updater.pl  Will be looking
        into more permanent fixes for version 3.1.0


# Version 3.1.0 introduced the following:
# Release Month-Year: May-2004
# 1) removed 15 minute database backup due to load concerns.  Data now is backed
```

up once per hour.
2) fixed bug with start_stop-wrapper.pl which was causing multiple scripts to run
on top of each other.
3) fixed a bug where the DHCPatriot™ would not block routing for static or
additional networks when in router mode.
4) Fixed a bug where the additional DHCP Range Add/Edit screen had the
incorrect link on the Edit Main DHCP Range screen.
5) fixed many bugs related to lease tracking on more heavily trafficed servers.
6) streamlined speed and processor utilization for more heavily trafficed
servers.
7) installed latest release of DHCP.
8) installed latest release of RedHat Linux.
9) repaired start-stop hang problem...
#10) search_dhcp.php now searches both patriots' logs at the same time.
#11) Lease times for authenticated and non-authenticated are now configureable.
#12) Fixed situation where static_ip could be historically assigned to
multiple MAC Addresses.
#13) Added the ability to suspend a single device by MAC Address even if you don't
know the username.
#14) Fixed search.php error with start and end date display.
#15) Fixed display error with the text-only view of the detail window
involving the zeroing and rounding of current_interval.
#16) Added the ability to do */% searches in search.php for username_
#17) lease_updater now uses /var/log/dhcp.log to populate the database.
#18) dhcp now writes logs to /var/log/dhcp.log instead of /var/log/messages
#19) firewall now blocks and allows mysql access properly.
#20) Added 00:e0:06:09:55:66 to the unacceptable MAC list due to the vendor
not following RFCs.
#21) A four hour login timeout is now included.
#22) Fixed various GUI issues and typographical errors in the GUI.
#23) Fixed the page code on the news and known issues etc...
#24) Added disk space as a category in server_status.
#25) Lease Status now shows Static/Additional dhcp.
#26) IP Usage over time now shows Static/Additional dhcp.
#27) Calanders are now updated to the functional calander.
#28) IP Usage over time now has link to show graphs on each CIDR.
#29) Enabled change password option on the admin interface for administrators.
#30) Notes field added for suspension that a user will see upon receiving the
authentication page.
#31) It is now possible to insert some customized text (or HTML) into the login
and thank you screens.
#32) Specifying the snmp string is no longer necessary. A simple router
selection box has been implemented instead...
#33) NetEnforcer enhancements are implemented. The following is now possible:

Enhanced NetEnforcer Support: It is now possible to assign users to
pre-existing hostgroups on the NetEnforcer. This allows an
administrator to automatically assign a particular template of
restrictions on, or enhancements to the flow of traffic on a per-user basis.
This applies to all the devices that the user logs on with. The application
of the user to the group occurs upon authentication, so it would be
advisable to suspend all the user's devices upon a change in the groups, or
other pre-defined per user NetEnforcer rules in radius. This forces
authentication, which subsequently causes the application of the speed
package and hostgroup associations. For more information on hostgroups and
what they are useful for, please consult your NetEnforcer user's guide, or
contact support@allot.com

The radius class attribute for the NetEnforcer now consists
of: class="NetEnforcer:[speed package]:[Group1],[Group2],...[Group10],...."

The class attribute must appear in the radius users file. Consult your radius documentation for further information on the users file. (example: class="NetEnforcer:Gold:FastToLAN,SlowKazaa,WideOpenWeb" (note: The speed packages, in this case: Gold, need to be pre-defined on the NetEnforcer, along with the groups. I suggest creating a "PlaceHolder" host with IP information of 1.1.1.1 to place in each hostgroup so that these may be pre-defined as they require at least 1 host for creation.)

Further information about the DHCPatriot™'s support of the NetEnforcer is available below, or in your DHCPatriot™ user's guide, or by contacting First Network Group:
Email: DHCPatriot™@network1.net Phone: 800-578-6381 x7

Version 3.0.1 (bug fix release) introduced the following:
Release Month-Year: September-2003

1) repaired issues with config file: patriot-1.crontab.root in the installer.
2) repaired bug in: NetEnforcer.pm
3) repaired various issues in: start_stop.pl
4) added some notes about the customer_usage.php screen.
5) changed start_stop-wrapper.pl to daemon mode. All debug from start_stop related scripts now prints to /var/log/messages via syslog.

Version 3.0 introduced the following:
Release Month-Year: September-2003

1) Support for both Radius versions of IP address configurations added: Framed-IP-Address, Framed-Address.
2) firewall_setup and lease_updater.pl throttled to use less of the Processor.
3) Added Network name (shared network) to the following: ip address usage, private ip usage, customer usage, lease status, ip usage over time
4) investigated bug with search database as in the IP address specified was not retained across clicking next-> bug did not exist.
5) Search page: now can specify exact match of IP address as well as partial match. exact match is now the default.
6) fixed bug with static IPs where some static IP users may not have been shown as online.
7) Added unique customer count to customer usage page.
8) Fixed bug where adding static ip ranges added the values to the table in the wrong order requiring manual db repair.
9) Search Database: Username / or IP now stay in the box after searching.
#10) Various: Date ranges that were selected now stay after running a command.
#11) Search DHCP Logs: added ability to search /var/log/messages for DHCP logs of a certain MAC Address
#12) Made routing through the patriot optional via the web interface.
#13) Domain name and ISP name are no longer one and the same on the web setup -> allows ISP name to be set to 'joe's just good ISP' example.
#14) detail: An optional text only view has been added.
#15) Made release notes viewable from HTML interface.
#16) lease_updater.pl has been optimized for I/O purposes.
#17) simusecheck and simuse are now optional via the radius server options on the web.
#18) fixed an issue where users requesting HTTPS:// instead of HTTP:// from a private address would be presented with the administration interface login page rather than the user login page.
#19) Hickory-tech-specific/hourly_password_check.pl now interfaces directly

with the broadsword database rather than verifying via radius.
#20) lease_updater.pl no longer sleeps 30 seconds between runs. Rather
it usleeps 100 microseconds between each record check.
#21) Added support for more than one public dynamic pool. No longer will
the pool have to be of a large size in order to accomidate the Patriot.
You can now have several small pools, such as 4 /26's instead of a /24.
#22) Updated edit/delete main DHCP. Statics and additional must also be deleted
as well as no users online before you can edit or delete the main DHCP range.
#23) on all reports with page breaks, you can now jump directly to a given number of 50
users by typing a number in the box labeled: "Jump to specific starting number"
and pressing enter.
#24) Updated instructions/interface/font sizes on the Administration interface.
#25) Added ability for deletion of Administrators.
#26) Added ability of Administrators to change their own password.
#27) Shortened log.auth_hardware.pl in /var/log/auth_dhcp messages to one line only.
#28) Removed ability to enter all CAPS MAC Addresses via
/var/www/cgi-bin/auth_hardware-manual.pl This bug in effect would allow
a user to be online and not acrue sessions on the DHCPatriot™ as
the all CAPS Mac Address did not match the Mac Address from the router.
caps_mac.fix will be executed at time of upgrade to DHCPatriot™ 3.0 to
translate any all CAPS Mac Addresses to lower case.
#29) Added NetEnforcer support for the DHCPatriot™ as detailed below:

Require: ssh keys from both the primary and secondary patriot be
installed in /root/.ssh/authorized_keys2 on the NetEnforcer.
Require: Configuration of the NetEnforcer's IP Address in the Basic
Information setup on the DHCPatriot™.

I. The user turns on his computer
a. the patriot (at the appointed time - every 1 minute most
places - this is a variable, as some customers routers are
very busy (5000+ subscribers) and it requires every 5 minutes
be the interval) attempts to update the user's host record on
the NetEnforcer with the current public IP.
1) if this fails, it is assumed that the host entry does not
yet exist on the NetEnforcer, and subsequently adds a host
entry for that user on the NetEnforcer.
If it fails, it also attempts to add a VC for it at
82. this time. The VC addition may contain -qos
83. option or not depended on whether
84. radius responded with the Class attribute of
85. the following: NetEnforcer:Gold <- or some other
86. package... The patriot can work with almost any
87. package name including one with spaces in it.
b. If the patriot received a -qos setting via the Class attribute of:
NetEnforcer:Gold or similar, it will at this point attempt to update
the VC with the correct -qos setting.
1) if that fails, it will assume there is no VC in existance for this
host, and attempt to add one.
II. The user is no longer online anymore (ie: their arp entry disappears)
a. The patriot follows the same procedure as outlined in I. with
the exception that 1.1.1.1 is used as the IP address.

#30) Server Status now displays the Last Updated time.
#31) Server Status now represents server load in a more accurate manner.
#32) You can now view this version txt by clicking the version number
on the patriot GUI interface.
#33) fixed URL redirection problem in auth_hardware-manual
#34) start_stop.pl now monitors itself via the currently running copy. It
no longer is killed by the next script in line if Radius hangs. This

facilitates a new set of features that will enhance the start_stop.pl
#35) start_stop.pl now runs separately and concurrently for each router. This facilitates more users, as well as better downed router handling. Some enhancements have also been made to the start_stop.pl.
#36) Fixed ARP entry bug in the DHCPatriot™. This caused some Mac Addresses to be undecodable. This has been repaired, and all users will now be accounted for.
#37) currently_online.php has received a speed inhancement. It now loads quickly and correctly.
#38) Added news/information center to index2.php. I will now be able to easily pass on information to patriot owners.
#39) New version of Net::SNMP installed (4.1.0).
#40) New version of Crypt::CBC installed (2.08).
#41) New version of Date::EzDate installed (1.08).
#42) New version of Digest::SHA1 installed (2.04).
#43) New version of Net::Radius installed (1.44).
#44) added 65.222.44.0 subnet to be used for DHCP monitoring by FNGi.
#45) Version of ISC DHCP upped from dhcp-3.0.1rc11 to dhcp-3.0.1rc12.
#46) reordered columns in a more intelligent way in customer_usage.php

Version 2.3 introduced the following:
Release Month-Year: May-2003

1) ISC DHCP v3.0.1RC11 is now being used as the core dhcp server.
2) lease_updater.pl now load balances across the 2 patriots.
3) made some important changes to the dhcpd.conf file that facilitate the failover and dhcpd.leases file working better.

Version 2.2 introduced the following:
Release Month-Year: May-2003

1) Disallow the mac address of either patriot from a remote customer for DHCP - this needs to be manually configured in /var/www/cgi-bin/*
2) delete bad encrypted password entries after 1 month - this is a hickorytech specific change in /usr/local/auth_dhcp... etc...

Version 2.1 introduced the following:
Release Month-Year: April-2003

1) Certain passwords when encrypted would cause problems - this behavior has been fixed...
2) Hickory-tech-specific/hourly_password_check.pl had a problem with writing to the database - this has been fixed...

Version 2.0 introduced the following:
Release Month-Year: April-2003

1) The Patriot Software now load balances between the two units that comprise the Patriot. This will increase the number of customers that the DHCPatriot™ can support.
2) Failover now is instantaneous, as either Patriot can handle the load of the other in event of systems or hardware failure.
3) Long searches, or other web interface operations that previously took several seconds to complete should now be faster as the results per page have been limited. A next and/or a back link will appear at the top of results that span multiple pages.
4) Server health can now be viewed from the web interface under: View

Server Status