DHCPatriot™ version 4.0.0 AAA is currently scheduled for release during the month of August 2006. This version of software has been over a year in development. Many new features and performance enhancements will appear on the DHCPatriot™ with the release of this software. Due to the sweeping scope of the differences from v.3.4.0 to v.4.0.0, we felt that a preview of some of the major features and enhancements was in order. What follows is a list of features that are scheduled to be included in the pending release.

1 AAA Enhanced

1.1 Local authentication via a built-in authentication module has been added! This gives the DHCPatriot™ even greater flexibility by making an external RADIUS server optional! The built-in authentication also supports static IP addressing and NetEnforcer® options in the same manner as a separate radius server.

1.2 Adding and configuring customers on the DHCPatriot™ to utilize the built-in authentication is quick and easy. Modifying/disabling/deleting previously added users can be done quickly. This interface is very intuitive which allows customer service personnel to be comfortable using it in a very short amount of time, further easing the integration of the DHCPatriot™ into your network.

1.3 Configuration of the DHCPatriot™ to use the built-in authentication is also a breeze. Setting up NetEnforcer® options, that can be chosen by customer service personnel for each customer as necessary, is fast and simple. Everything is streamlined to accelerate the configuration of the built-in authentication.

2 Performance Enhancements

2.1 The DHCPatriot™ v.4.0.0 AAA includes a new custom Linux® based core. This greatly enhances performance on the DHCPatriot™. It also enhances stability and uniformity across deployed DHCPatriot™ systems.

2.2 All time storage in the database is now EPOCH based. This will resolve issues that typically occurred when daylight savings time states changed.

2.3 A conversion process will occur for existing customers upon install of v.4.0.0 AAA. It may take several days for the conversion process to update all previous records. Not all records may be available during this process. The conversion process will quickly port all active sessions and then continue, in reverse chronological order, until all records have been converted.

2.4 The DHCPatriot™ will begin requiring a valid license in order to operate in v.4.0.0 AAA. Demo units will receive a 30-day license for the current version of software. Purchased units receive a lifetime license for the current version of software. Upgrades to the software will require a new lifetime license. Customers with current and active maintenance contracts will receive a new lifetime license when they receive a new version of software. Customers without a maintenance contract will need to purchase the new lifetime license in order to use new versions of the DHCPatriot™ software.

3 Administration Interface enhancements

3.1 Console access is coming to the DHCPatriot™! This feature allows access to the DHCPatriot™ via either serial console or standard secure shell (ssh). It features a menu driven interface with various functions that will help administrators configure the DHCPatriot™. Some of these features include:

- View current system settings displays settings such as IP Address, configured domain name and current Ethernet link status.
- Configure IP Address allows an administrator to set IP information.
- Configure Domain Name allows the configuration of the domain name.
- Configure speed and duplex allows the modification of speed and duplex settings for the primary Ethernet interface.
- Change admin password allows the configuration of the admin user password for access to the console.
- Firewall administration allows the configuration of the built-in firewall.
- Web admin account setup allows configuration of user accounts for access to the web administration interface.
- Restart and Shutdown of the DHCPatriot™.

3.2 The search database function now supports exporting to a CSV file. This allows the download of the results of the search that was performed. A CSV file can be imported into Microsoft Excel or OpenOffice.org Calc for data manipulation purposes.

3.3 To greatly help troubleshooting, the search database function displays the remaining lease time in version 4.0.0 (or 0 if the user is offline).

3.4 A new menu system has been introduced on the Web Administration interface. This is a category based menu system, to allow easier and faster location of needed functions.

3.5 The view suspended users feature is now a searchable list, instead of a display of all suspended users. The suspended users may be searched by username. In addition to this new functionality, an unsuspend option has been added for each suspended MAC Address. A button appears next to each listing allowing unsuspension at a single click.

3.6 The Address Usage function has been reordered and reorganized for easier viewing of information. All portions of the network information (Main, Additional, Static, and Unauthenticated) have been grouped together by Shared Network title. It is now much easier to discern the current status of IP usage and whether new address space should be added.

3.7 In order to enhance access to network and user information, the DHCPatriot™ now displays a list, and provides a CSV download of a list of users on a per subnet basis.

3.8 DHCP messages are now stored in the database. The View DHCP Logs feature has been updated to take advantage of this functionality. Historical logs can now be searched and viewed on a page basis. Additionally, the Hosts logs are intermingled so that it is easier to understand the DHCP conversations. Previously, the logs for only the current day were available, were shown all at once, and with the two host's logs separated. This will make troubleshooting customer problems much easier, as a time period may be looked up limited by MAC Address, IP Address, and date/time ranges. Additionally, MAC Address and IP Address limiters may be left blank for real time or historical viewing of all DHCP logs.

3.9 All DHCPatriot™ software logs and system logs are now stored in the database as well. These logs are also searchable with several limiting factors to display only the needed

results. They may be limited by daemon, host and date/time ranges. Additionally, the two Host's logs are displayed together (provided they are not limited) so that a clearer picture may be developed. Here again, any combination of search limiters may be used or not used to allow real time or historical viewing of logs.

3.10 It is possible to paste an MD5 encrypted password into the appropriate box when entering a new administrator, or editing an existing administrator. This eliminates the need for the use of an initial password that the new Administrator changes upon login.

3.11 Several changes have been made to the editing of Main, Additional, and Static subnets. The Main and Additional subnets may be disabled to force users to other Additional subnets, or to lock them out all together so that changes may be made. Additionally, you can now edit a Main subnet once all users are offline even if it has Additional and Static subnets attached to it (and even if those Static and Additional subnets do have users logged into them).

3.12 A timezone selection feature has been added to the Web Administration interface. This selection can be done on the fly, providing quick access to other timezones when displaying records. The default setting is UTC (GMT+0000). This setting may be changed once, and then left at the chosen setting, or it may be changed whenever desired. A change while viewing a report will cause that report to immediately reflect the new timezone selection. A persistent cookie is created upon selection of a timezone. This allows the Web Administration interface to display the correct timezone on an ongoing basis. Selections by one administrator will not affect another administrator's selection unless they share the same computer and cookie information.

4 End user administration

4.1 The end user authentication screen displays a notice that the user is already authenticated and does not need to do so again. Some support callers have been repeatedly authenticating in an attempt to get rid of the cached page that displayed as a result of an Internet Explorer 6 default setting of check for new version of page: Automatic. Coupled with recent changes to browser cache settings that are received from the web server, there is a good chance that most of these would-be callers will never see the cached version, or will figure it out on their own.

4.2 It is now possible to authenticate a user who has not received an unauthenticated address. The MAC Address that the user will be using as well as the user's username and password will be required to complete the authentication process. This feature may be used to preauthorize users prior to moving existing customers to a DHCPatriot™ installation, as well as, to allow for easier authentication of Playstation 2 customers. The Playstation 2 does not initiate a DHCP lease until a user attempts to connect to an online gaming network. Additionally, it does not maintain a DHCP lease if it fails to connect to the game servers. This causes problems when the Playstation 2 is using the Unauthenticated network, as this network is limited to communication with the DHCPatriot™.

4.3 Usernames can be rejected at the login screen if they contain any of these characters: |'_"%`\~<>::,/*? anywhere in the username. This setting is especially useful for NetEnforcer® owners, as those characters are not permitted in Hosts and Virtual Channels on the NetEnforcer®.

4.4 A setting that allows the stripping of @ signs and everything following them from the username as a user attempts to login has been added. 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.

4.5 It is now possible to remotely suspend and unsuspend users via a Web based CLI like interface. This opens up wide possibilities for network wide automated user maintenance, thus making management of large ISPs easier. This interface is meant for use with automated scripts that control user access on-the-fly.

5 RADIUS Communication

5.1 The DHCPatriot™ now sends the RADIUS Attribute Calling-Station-Id containing the user's MAC Address when sending an accounting start to the RADIUS server.

5.2 Reply-Message support is new. If the RADIUS server returns Reply-Message in event of login failure, this message will be displayed to the user on the failure screen.

6 NetEnforcer® Functionality changes

6.1 The 'Pause NetEnforcer® Communication' function is now available! This allows an Administrator to pause the NetEnforcer® Communication so that a NetEnforcer® may be logged into with write permissions without fear that the DHCPatriot™ would revoke the write permissions by making changes on the NetEnforcer®. The paused communication will automatically be restored after a one hour period to safeguard against an Administrator failing to restore communication when the edits are complete. While the communication is paused, needed changes to the NetEnforcer® will still queue. When the communication is restored, these queued changes will be executed as quickly as possible.

6.2 The host modification procedure has been altered. Previously, it was only possible to add four 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®.

6.3 It is now possible to disable the auto-creation of Virtual Channels by the DHCPatriot™ in the Fall Back Pipe on the NetEnforcer®. This allows even more flexibility in the auto-configuration of the NetEnforcer®.

6.4 Multiple DHCPatriot™ systems can now communicate with a single NetEnforcer®. All commands will be run in a linear fashion as specified by Allot Communications.

7 Data and Graphing

7.1 The DHCPatriot™ now gathers statistics about network utilization on an ongoing basis. This data is computed and stored every five minutes. Data is gathered for Main, Additional, and Total Dynamic utilization.

7.2 User graphs are now accessible using the aforementioned data on the Address Usage function. Graphs can be displayed for Main, Additional, and Total Dynamic utilization. The time period used to compute and display the graph may be adjusted as well allowing the viewing of long-term trends.

7.3 This data is also available via SNMP, see release notes, and v.4.0.0 manual for further information.