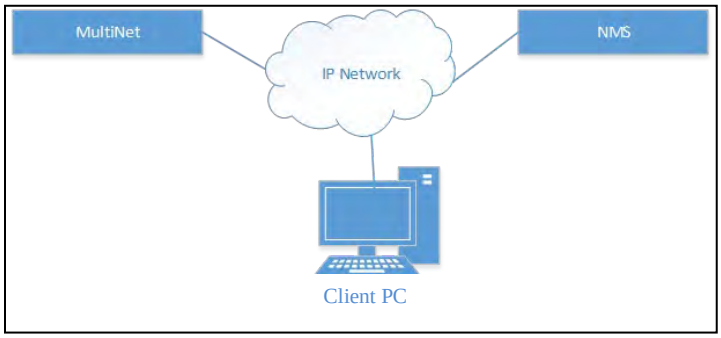
7275
AES-*Network Management System* (NMS) 5.0

User Manual

Table of Contents

1 Product Overview

The AES-*Network Management System* (NMS) is a complete end-to-end *IntelliNet* Mesh Radio Network monitoring and management platform. NMS provides real-time performance data and an interactive visualization of network service using Google Earth to assure that alarm and other critical signals are communicated quickly and reliably. The NMS platform can also drive down overall network management costs while supporting efficient and profitable network growth as additional *IntelliNet* subscribers are deployed. NMS monitors all network subsystems which includes *MultiNet* servers, IP Links, Burglary and Fire Subscribers and delivers real-time notifications of system events. The NMS software platform was designed with flexibility in mind, providing the ability to add enhancements and new functionality with future releases.



NOTE: Closely follow the entire contents of this User Manual as it contains information that is essential to successfully completing the installation of the AES-*Network Management System* (NMS).

1.1 NMS Product Description

The NMS offers the following features:

- Multi-level Intelligent Network Dashboards
- Radio Network Interactive Visualization of each Business Unit
- 24/7 Notifications via email or SMS of network events to key personnel

1.1.1 Multi-level Intelligent Network Dashboards

NMS features multi-level browser based dashboard architecture for system configuration, maintenance, and operation. The *Administrator Dashboard* is designed for the *MultiNe*t owner and provides real time status of *MultiNet* connectivity and the NMS server once the system is set up and operating. Through the *Administrator Dashboard*, the *MultiNet* owner sets up and supports:

- Configuration of *MultiNet* server parameters
- Configuration of NMS server parameters
- Edit user credentials for access to the *Operator Dashboards* - one for each Business Units
- Edit user credentials for access to the *Dealer Dashboards* – one for each dealer
- Remote software upgrade of NMS server
- Reset to factory defaults for NMS server
- Overall appliance Status

Each *MultiNet* Business Unit is set up with a separate *Operator Dashboard* that provides visibility into radio signal traffic and overall operation. This dashboard displays critical Business Unit information in a dynamic and intuitive format to enable a quick assessment of the network's performance and to quickly identify events that could affect network operation. For example, the *Network Pulse* dynamically tracks key performance indicators including

subscriber Check-Ins and Ack Delays over the most recent ten day period. The *Network Health Score* quantifies overall network operational quality on a scale between 0 - 100. Below is a list of Business Unit specific data displayed in a user-friendly format on the *Operator Dashboard:*

- List of Subscribers needing service
- List of IP Links needing service
- Network performance charts
- Total received packets
- IP Link Load
- List of Top Talking Subscribers
- List of Top Repeater Subscribers
- List of Subscribers with Late Check-Ins
- List of Subscribers with Check-Ins more than once per 24 hrs.
- Subscriber Security – Quarantine mode
- List of Subscribers with high number of Hops
- List of Subscribers sending Ack Delay signals
- List of Subscribers sending a NetCon signal
- IP Link Equipment List
- Subscriber Equipment List
- Link for Google Earth for interactive visualization of network
- List of Non - AES unit

1.1.2 Interactive Radio Network Visualization

Radio Network Visualization is a feature accessed through the *Operator Dashboards* that presents an interactive geographical layout of the *IntelliNet* network and Non-AES units using Google Earth. It will show Business Unit specific information such as the following:

- Subscriber positions
- Subscriber status
- IP Link positions
- IP Link status
- Most Used Route
- Most Recent Route
- Route and distance information
- Subscribers requiring service
- IP Links requiring service
- Subscriber utilization
- IP Link utilization
- Non - AES unit location

1.1.3 24/7 Notification

The Notification function enables users to monitor their *IntelliNet* network from anyplace at any time. Through the *Operator Dashboard*, users can configure automatic alerts based on the system-wide *Network Health Score* to send alerts by both SMS and email to key personnel. Triggers can also be set up for alerts due to many types of subsystem fault with any Subscriber or IP Links. The user can create the list of personnel to be notified, define the fault criteria to be reported, and create associations between the alerts and personnel to optimize responses.

1.2 NMS Server Specifications

Server Appliance Hardware Specifications

Processor	SL-1U-LL6412J-GC-1
Mainboard	MinilTX
Chipset	Intel Pentium SoC
System Memory	1x DDR4 2666MHz SO-DIMM RAM, up to 4GB
Ethernet	Realtek RTL8111E,10/100/1000Mbps, 2x LAN
Storage	4x SATA III
Expansion	1x PCI, 1x Mini PCIe
Cooling System	CPU Fan <2>
Power Supply Form Factor	Standard ATX 20 Pin
Graphic Controller	Supported by CPU
Display Resolution	Supported by CPU
PS/2 Port	1x Keyboard, 1x Mouse
Digital I/O	8bit GPIO header
Rear Panel	USB 2.0 (2), USB 3.2 Gen 1 (2), Audio on IO, LAN (2), Serial Ports 232/422/485 (2)
Front LED/Control	Power LED, HDD LED, Power Button, Reset Button, 2x USB

Features and Options	Short-Depth 1U Chassis
Enclosure Materials	Aluminum
Coating Processes	Powder Coating
Mounting Option	19” Rackmount (1 U Height)
Color	Black
Operating Temperature	0 - 60 °C (32 - 140 °F)
Dimensions	11” x 19.10” x 1.75” D x W x H
Weight	Approx. 2.7 kg (6 lb.)
Power Requirements	DC Power: 12 V DC-in

Server Appliance Software Specifications
Dashboard, Visualization, and Notification applications are implemented over an industry standard Linux environment.

1.3 NMS Software and Hardware Requirements

- Windows client PC for accessing NMS *Administrator Dashboard* and Google Earth
    - Google Earth application
    - Internet access for Google Earth during operation
    - Network Access for NMS Dashboard
    - Internet Browser such as Firefox, Chrome etc.
- NMS Server (Included with NMS)
- NMS Server Ethernet cable (Included with NMS)
- NMS Server AC power cord (Included with NMS)
- Uninterrupted Power Supply
- AES-*MultiNet* Receiver version 467 or later is required. For optimal performance the most current version is recommended. **NOTE:** *MultiNet* Receiver Version 467 will not display NetCon faults.

2 Installation and Configuration

2.1 Installation Preparation

It is recommended to collect all configuration information prior to starting installation to reduce installation time.

2.1.1 NMS Server

Take a note of the NMS factory default addresses as they will be needed when connecting with the NMS Server for the first time:

Default Ethernet Connection 1:

1. Default IP: 192.168.1.254
2. Default NM: 255.255.255.0
3. Default GW: 192.168.1.1
4. Default DNS1: 8.8.8.8
5. Default DNS2: "blank"

Default Ethernet Connection 2:

1. Default IP: 169.254.66.66
2. Default NM: 255.255.0.0
3. Default GW: 0.0.0.0

The following information will be required for setting up the NMS Server with your preferred settings.

1. Private IP address
2. Subnet Mask
3. Default Gateway
4. DNS Server 1
5. DNS Server 2 (optional)
6. Public IP address (optional)
    a. TCP port 1194, 1195 for AES VPN

2.1.2 *MultiNet* Receiver

Only one *MultiNet* Receiver can be monitored at a time so identify which *MultiNet* (usually the Primary *MultiNet*) is to be monitored by the NMS and collect the information below.

1. *MultiNet* IP address
2. *MultiNet* password

2.2 Connect and Power up NMS Server

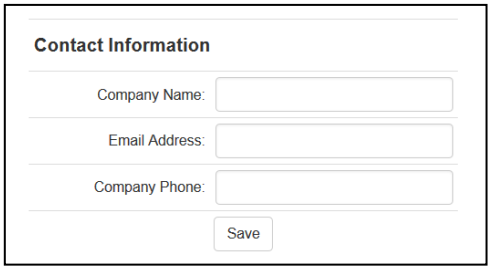
1. Connect the power cord to NMS and plug into an outlet, NMS server will power up right away
2. Connect NMS Server (Ethernet port labeled 1) to an IP network or PC where it can be reached with the factory IP address (192.168.1.254) from a PC for configuration purposes

2.3 Access the Administrator Dashboard

1. Open a web browser on a PC on the same network as NMS server
2. Enter the default IP address: *https://192.168.1.254* in the browser URL
3. This will open the Administrator log on Window
4. Login as administrator - type "admin" in Business Unit and use the password "admin"

NOTE: Password can be changed later

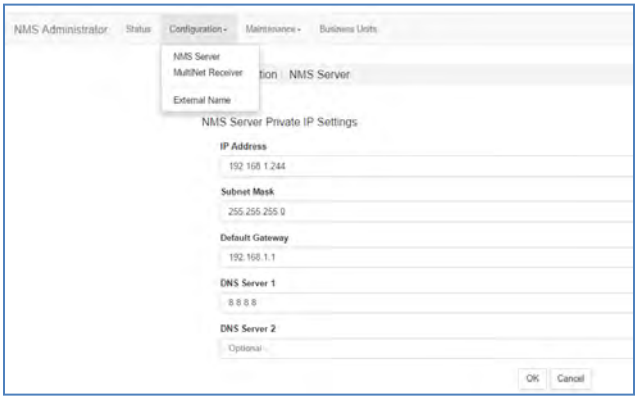
2.3.1 Enter Contact Information



1. Click on **Maintenance**
2. Then **Contact**
3. Enter contact information
4. Click **Save**

2.3.2 Configure the NMS Server IP settings

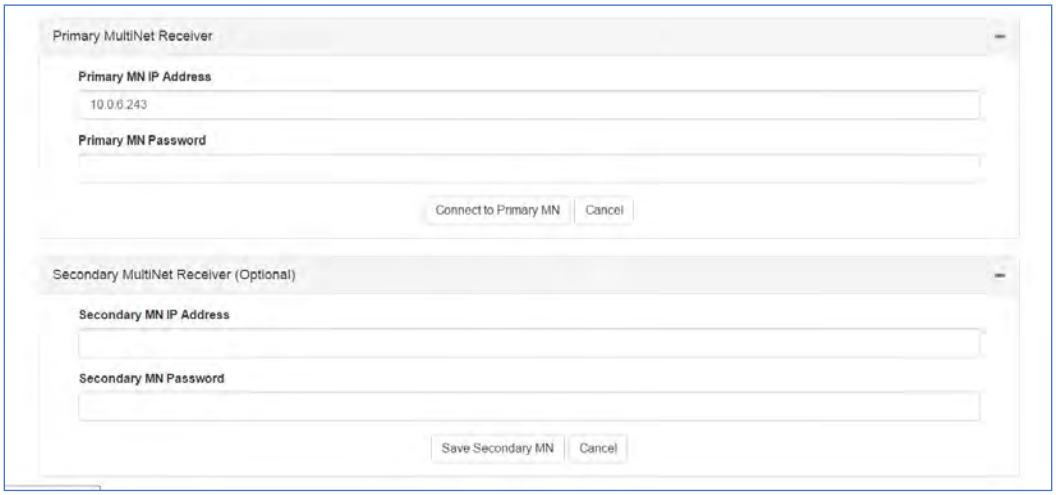
1. In the *Administrator Dashboard* click on **Configuration**>**NMS Server** to change the NMS IP settings.
2. Change the NMS IP settings to the prefered network settings - on the same network as *MultiNet*
3. Click **OK**.
4. Power down the NMS server by briefly pushing and releasing the power button. The NMS will power down within 10 seconds.



NMS Server IP Settings

2.3.3 Enter *MultiNet* Receiver parameters

1. Disconnect NMS sever from the initial network if not the same IP network as the *MultiNet* receiver.
2. Move the server to the permanent rack location - use the rack mount brackets included
3. Connect server to same IP network as *MultiNet* receiver (Ethernet port labeled 1)
4. Access the *Admin Dashboard* - enter *https://new NMS IP address* - and log in as before as administrator.
5. Click on **Configuration**>***MultiNet* Receiver**.
6. Enter the *MultiNet* receiver IP Address and password
7. Click **Connect to Primary MN** and NMS will restart and begin communication with *MultiNet*
8. If preferred you can also configure the Secondary receiver when the NMS reboots.

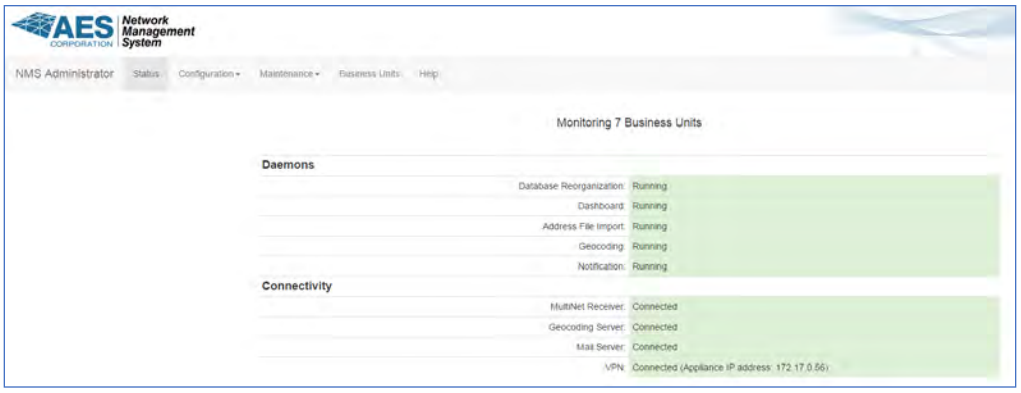


***MultiNet* Receiver Parameters**

2.3.4 Verify that the NMS is communicating with the *MultiNet* receiver

1. After the NMS server restarts, access the *Administrator Dashboard* by entering the new IP address - *https://new NMS IP address*.
2. Within a few minutes verify that you see the number of Business Units monitored at the top of the *Status screen*. The number might change as information is retrieved from the *MultiNet.* This could take between 15 minutes and a few hours depending upon the size of the database.

Note that *MultiNet* operation is never affected in any way by the operation of NMS.



Administrator Dashboard Status screen - Verify number of Business Units monitored.

The AES-*Network Management System* is now ready for operation. The next sections provide additional information and operational instructions.

3 System Operation Summary

NMS features multi-level browser based dashboard architecture for system configuration, management, and operation. The *Administrator Dashboard* is designed for the *MultiNe*t receiver owner. The *Operator Dashboard* is designed for each Business Unit (one user per Business Unit). The Administrator and the Operator Dashboards can both be accessed at http://your_NMS_IP_Addess but they have different capabilities and different login credentials. Below are some capabilities of the *Administrator* and *Operator Dashboards*.

Administrator Dashboard - Monitoring and Configuration Capabilities:

- NMS system and *MultiNet* connectivity status
- NMS private and public IP settings
- Settings for communication with *MultiNet*
- NMS factory reset and restart
- NMS software upgrade
- User credential configuration
- Dealer configuration

Operator Dashboard Monitoring Capabilities:

- Network Health Score
- Subscriber and IP Link service requirements
- Network Pulse
- IP Link load
- List IP Link Service Log
- List Top Talker Subscribers
- List Top Repeater Subscribers
- List Late Check-In Subscribers
- List Frequent Check-In subscribers
- List Subscriber Service Log
- Subscriber Security – Quarantine mode
- List Subscribers with 4 or more Hops
- List Subscribers with Ack Delays
- List Subscribers with NetCon trouble
- List of IP Links and Subscribers with model and revision numbers
- Subscriber and IP Link addresses import for Google Earth
- Google Earth access
- Set up 24/7 Notifications or network events
- Operator password change
- List Non-AES units
- List of Inactive Subscribers
- Dashboard custom logo
- List of NCT units

Dealer Dashboard Monitoring Capabilities:

- Network Health Score
- List Non-AES units
- List IP Link Service Log
- List Subscriber Service Log
- Dashboard custom logo

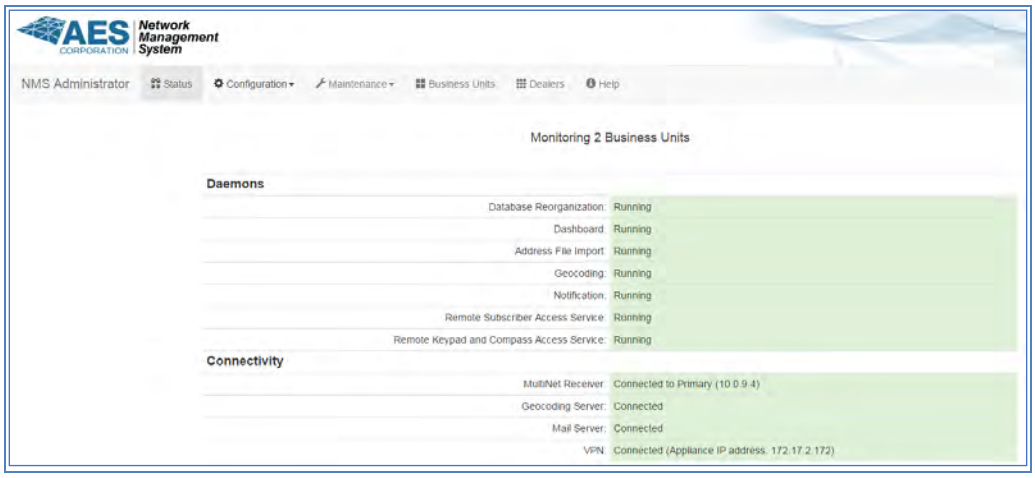
4 Administrator Dashboard

4.1 Login

If you are a *MultiNet* Owner, you can access your *Administrator Dashboard* by signing in at the following URL: http://your_NMS_IP_address to launch the sign in screen. The username will be “admin” and the password “admin”. **NOTE**: Password can be changed later.

4.2 Administrator Dashboard - Status

The *Administrator Dashboard* displays the status of the *MultiNet* receiver and the NMS server as detailed in the screen below followed by an explanation of each of the sections on the status screen. Click on **Status** to return to the Status screen.



Administrator Dashboard - Status Screen

Database Reorganization
Indicates proper optimization of databases and gathering of data from the *MultiNet* receiver and reorganizing in NMS

Dashboard
Indicates that Dashboard calculations and preparation of data for presentation on the Dashboards are operating properly

Address File Import
Indicates status of importing addresses from a .csv file in to the NMS

Geocoding
Indicates status of geocoding when finding GPS coordinates for the provided addresses

Notification
Indicates status of Notification function - NMS monitoring for trigger conditions configured by users

Remote Subscriber Access Service
Indicates status of feature used to access the subscribers remotely

Remote Keypad and Compass Access Service
Indicates status of service used to access (1) Virtual keypad through subscribers and (2) Used to connect remotely via Compass

***MultiNet* Receiver**
Indicates connectivity to the *MultiNet* receiver

Geocoding Server
Indicates connectivity to the Geocoding server

Mail Server
Indicates connectivity to the Mail server

VPN
VPN for remote support from AES Tech Support team and remote system upgrade

4.3 NMS Server Configuration

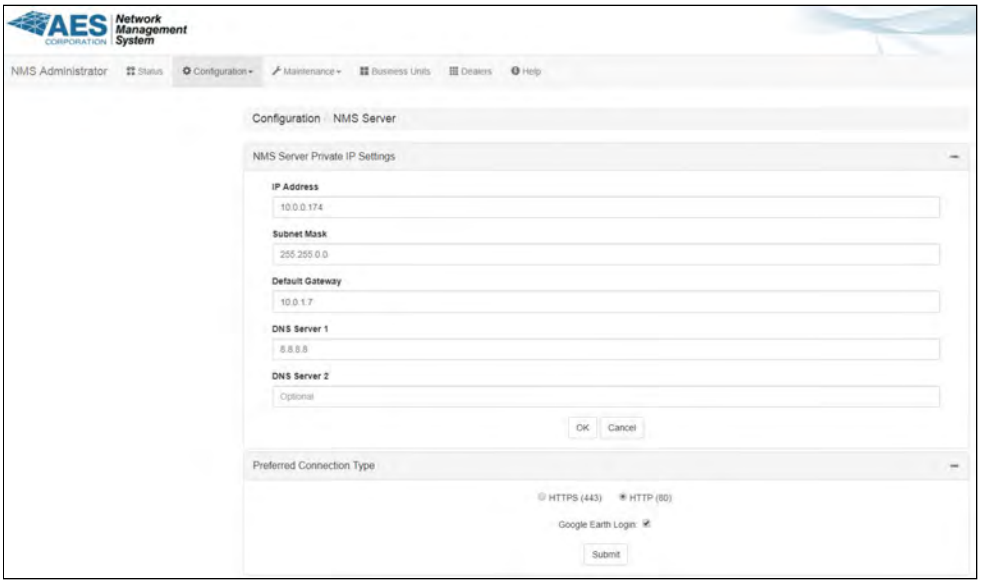
The view below will be displayed after clicking on **Configuration** then selecting **NMS Server**. This allows you to enter and change NMS private IP setting.

Configuration>NMS Server

Enter NMS server IP settings and click **OK**

Select Preferred Connection Type and Click Submit

Select Google Earth Login preference if you'd like to enable or disable Google Earth login request.



Configure NMS Server Screen

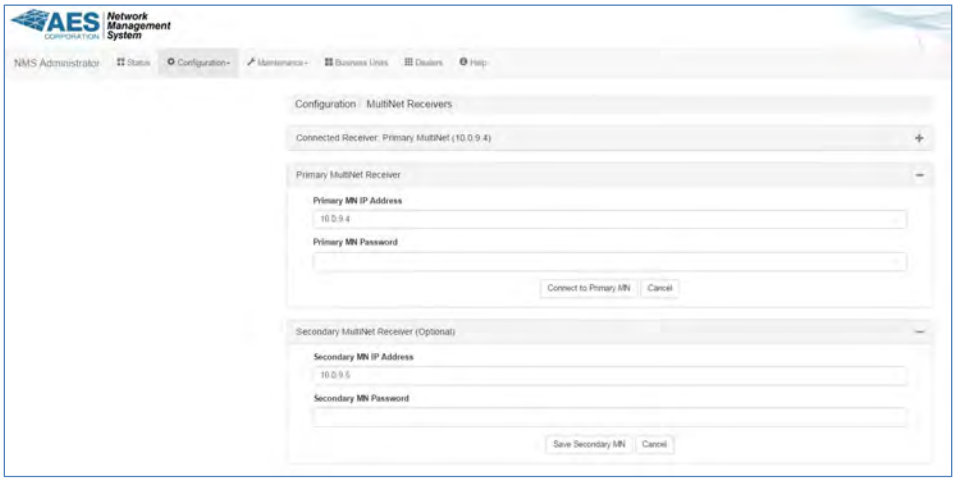
4.3.1 *MultiNet* Receiver Configuration

The view below will be displayed after clicking on **Configuration** then selecting ***MultiNet* Receiver**. This allows you to change *MultiNet* Receiver settings.

Configuration>MultiNet Receiver

Enter Secondary *MultiNet* IP address and password and click Save Secondary MN

Enter Primary *MultiNet* IP address and password and click Connect to Primary MN



NOTE: Entering a new IP address after initial setup will result in loss of current data in the system including address and GPS data.

4.3.2 External Name Configuration

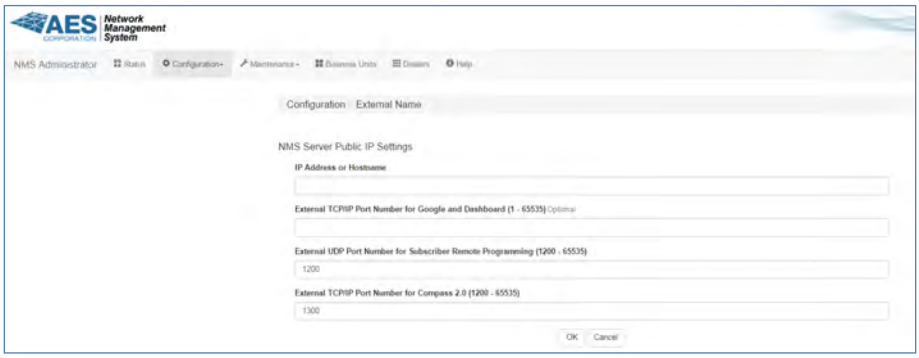
The view below will be displayed after clicking on **Configuration** then selecting **External Name**. This allows you to change NMS public IP settings for communication from outside the LAN.

Configuration>External Name

Enter a public IP address or host name and port number if needed for access from outside the LAN

Enter UDP port number for Subscriber Remote Programming

Enter TCP/IP port number for Compass 2.0 programming



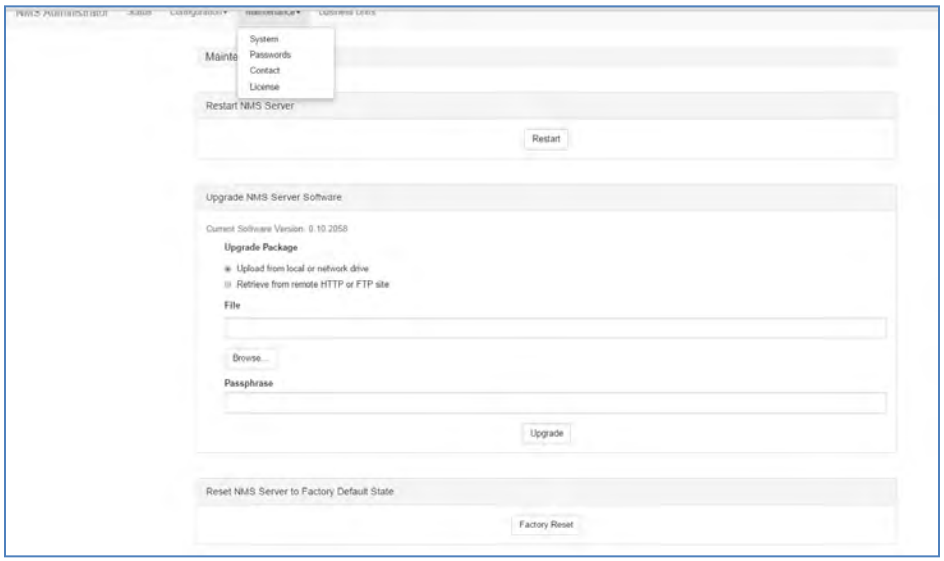
4.4 Maintenance - Administrator Dashboard

The view below will be displayed after clicking on **Maintenance** then selecting **System**. This allows you to do the following:

1. Restart the NMS server - when you click on **Restart** the NMS system will restart. If the NMS server is restarted, contact information, and NMS server IP settings will not be affected.

2. Upgrade NMS software using an upgrade package or URL. The new upgrade package and passphrase will be provided by AES. Upgrading the NMS software will cause a restart to the NMS appliance.

3. Reset NMS to Factory Default State - this will reset the system to original status. All passwords will be reset to default and all Business Unit data will be lost. The NMS private IP address and customer contact information will not be lost.



System Section

4.4.1 Passwords

The view below will be displayed after clicking on **Maintenance** then selecting **Password**. This allows you to set and/or change the *Administrator Dashboard* password as well as the *Operator Dashboard* passwords for all Business Units. The factory default log in and password for access to the *Operator Dashboard* at start up is *admin* (enter into Business Unit field) and *admin* for password.

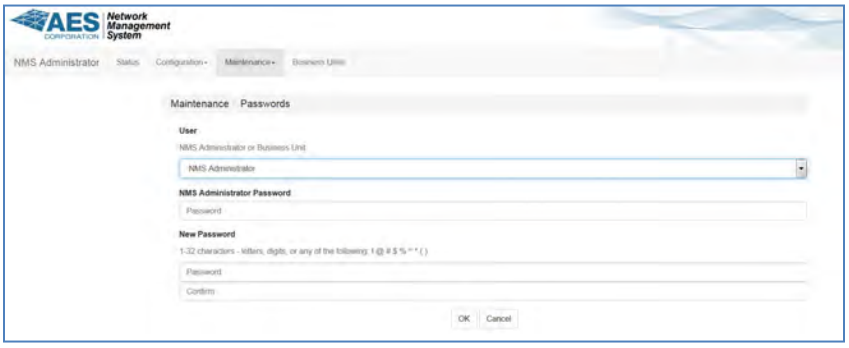
Maintenance>Password

Select either administrator or a Business Unit

Enter current Admin password

Enter new password twice

Click **OK** to save



Password Section

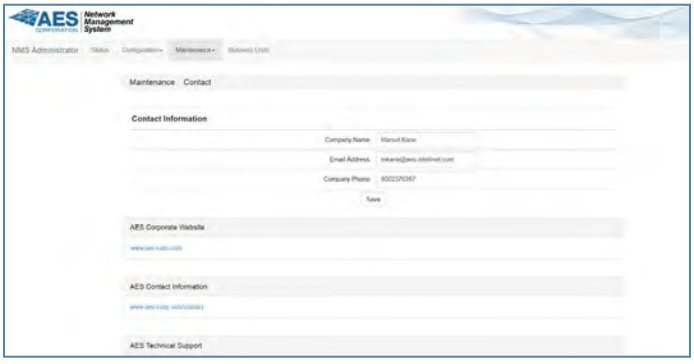
4.4.2 Contact Section

The view below will be displayed after clicking on **Maintenance** then selecting **Contact**. This screen allows the *MultiNet* owners to input contact information. The contact section is not affected by a system restart.

Maintenance>Contact

Enter Administrator contact information including email and phone

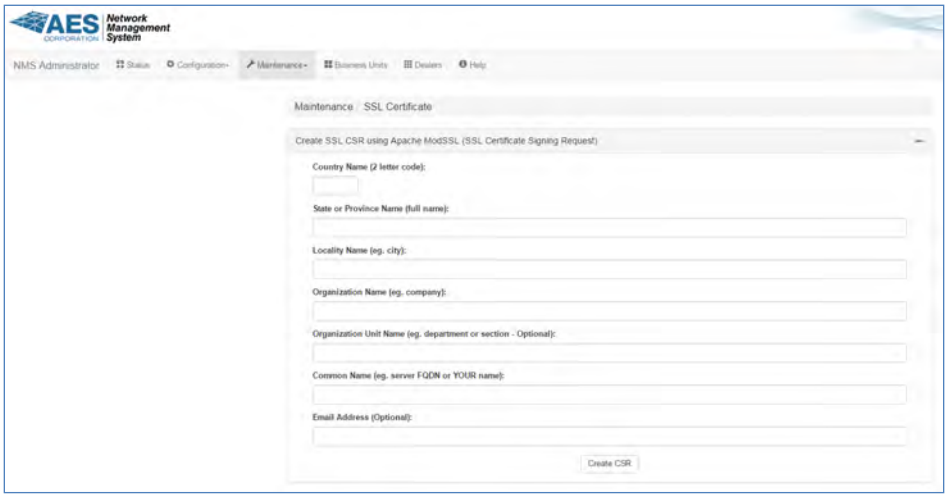
Click **Save**



Contact Section

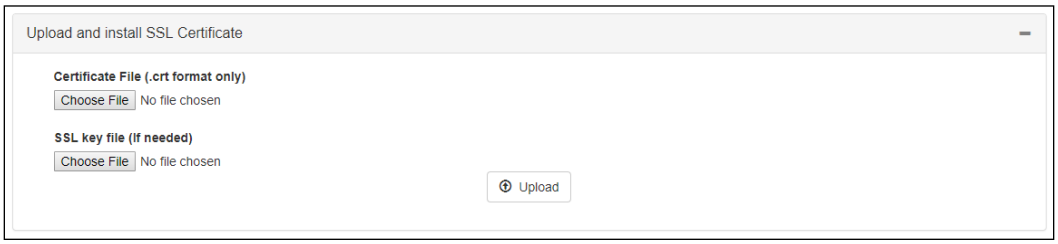
4.4.3 SSL Certificate

The view below will be displayed after clicking on **Maintenance** then selecting **SSL Certificate**. This feature helps you create and SSL CSR using Apache ModSSL. Enter all the relevant information asked for in the form on this page and click on Create CSR to generate a SSL certificate.



SSL Certificate Section

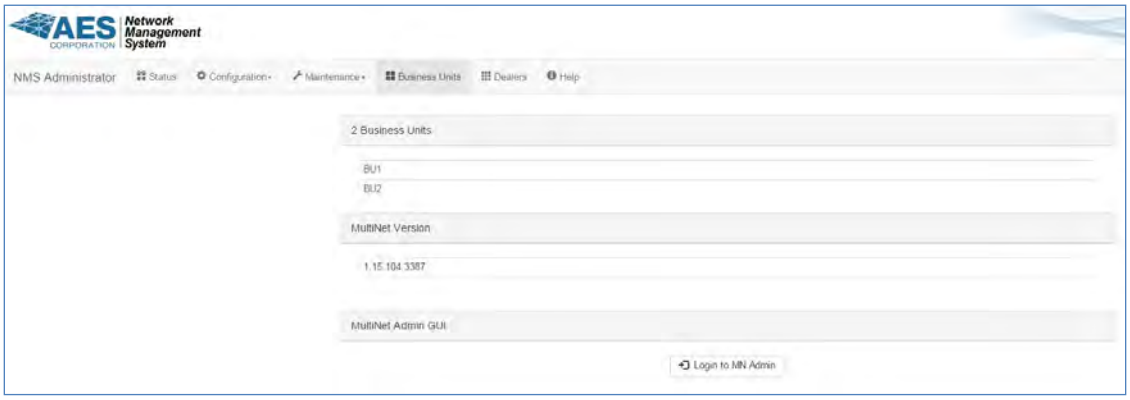
If you prefer, you can install your own key and SSL certificate at the bottom of the page.



Upload and Install SSL Certification

4.5 Business Units

If you are the *MultiNet* owner and have access to the *Administrator Dashboard*, you can access the *Operator Dashboard* for any Business Unit by clicking on **Business Units** then click on any Business Unit listed. This will launch the *Operator Dashboard* for that Business Unit in a separate tab. The *Administrator Dashboard* remains open. The Administrator can open multiple Business Unit *Operator Dashboards*. This window also provides information about the version number of the *MultiNet* to which the NMS is connected. You can also access the *MultiNet* GUI page from NMS. Click on Login to MN Admin and enter the username and password of MN to get access to MN GUI.

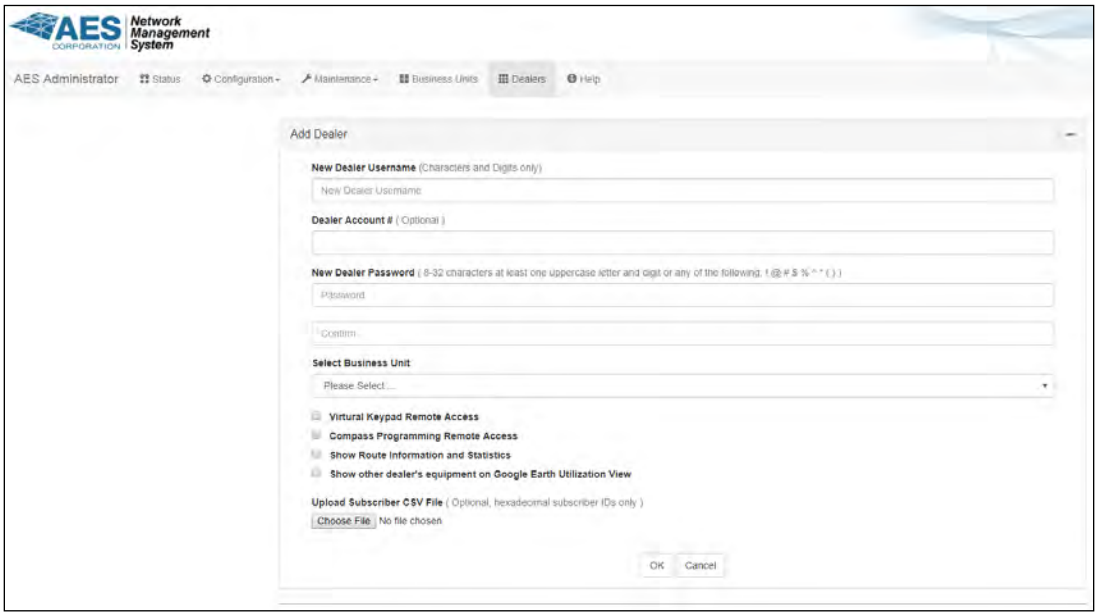


Business Units Section

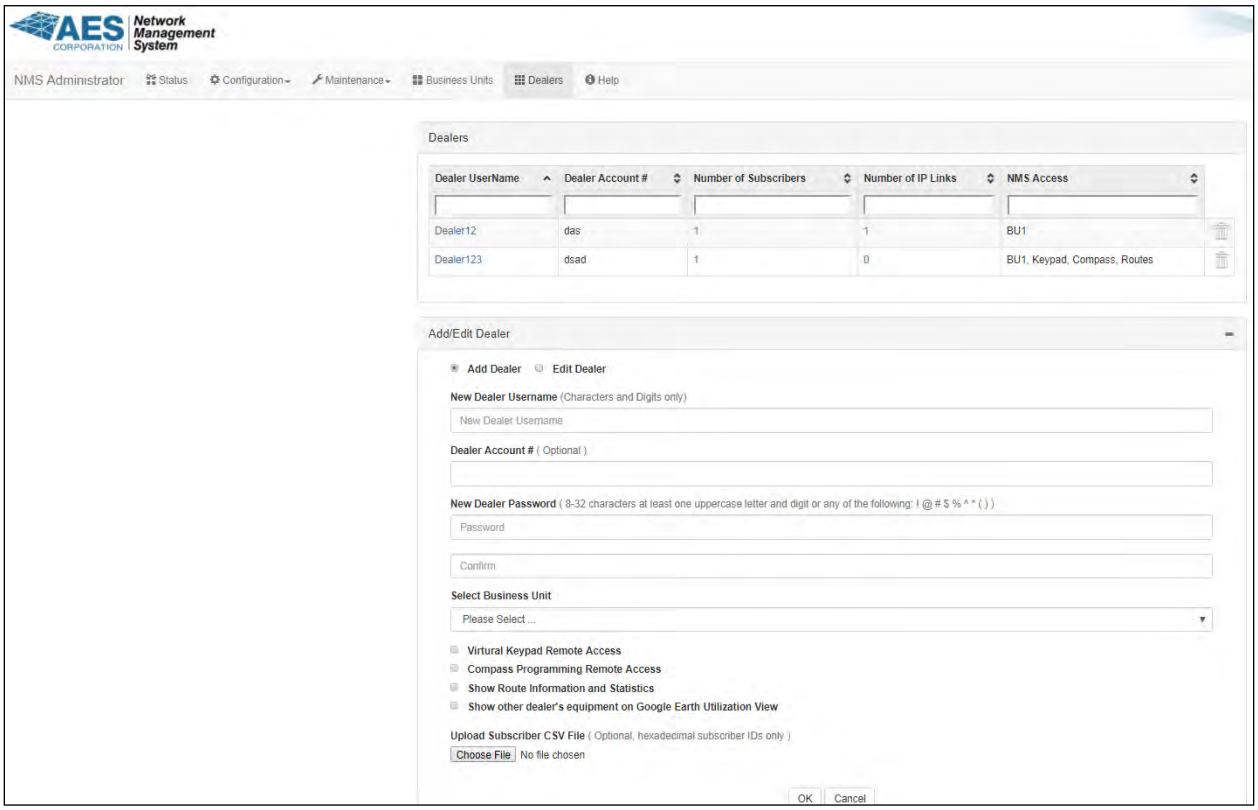
4.6 Dealers

The view below will be displayed after clicking on **Dealers** for the first time. This allows you add new and maintain existing Dealers. You can change password for the dealer, select which Business unit they can have access to, also select whether they can have access to Virtual keypad Remote Access and/or Compass Programming Remote Access.

You can also choose whether you want to show Route information and Statistic on a Subscriber Unit View for a certain dealer.
You can also choose whether you want to show subscribers on Google Earth that belong to other dealers for each specific dealer.



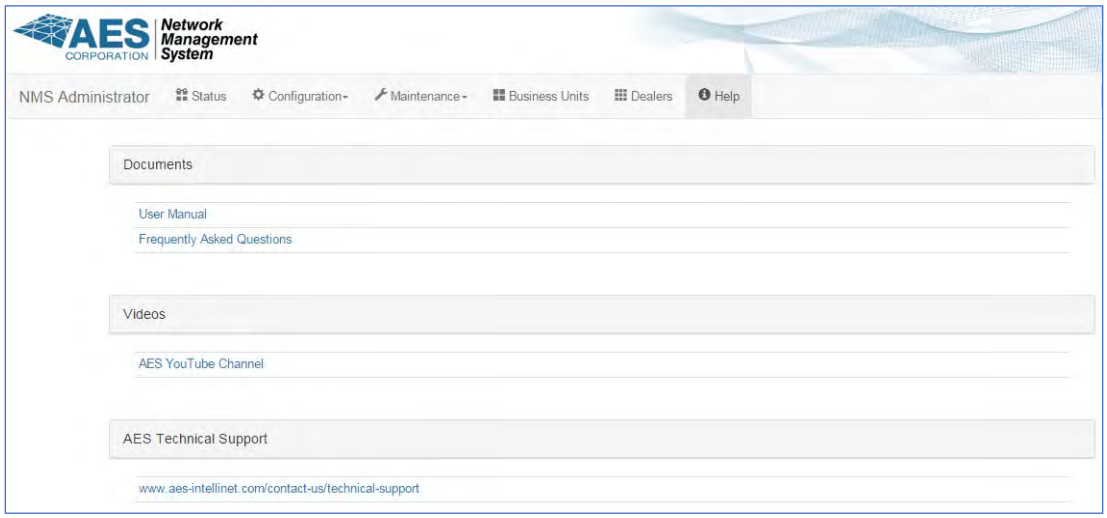
After you add a Dealer you will see thes following when you click on **Dealers**



Once the dealer is created, you can click on dealer username to access the Dealer Dashboard. You can also click on the number below the *Number of Subscriber and Numbers of IP Link* and select the list of subscribers and/or IP Links which you want to add/delete to that dealer.

4.7 Help - Administrator Dashboard

Through the help tab on the *Administrator Dashboard*, users can easily access additional information for help, such as manual, FAQ and videos.



4.8 Web API

The NMS has a Web API which allows users to add, remote or update subscriber information form a program or other device without having to log into the GUI.

The form looks similar to the example below:
https://nms_server_ip/nmsapi.html?request=url_encoded_json_string
Note that API item names are low cases

request string format {"name":"value", "name2":"value2", ...}

For Example:
{"pwd":"admin", "bu":"BU1", “dealer”:”Dealer1”, “action”: “add”, “subid”:”1234”, “address”:”310 Main St” ....}
{"pwd":"admin", "bu":"BU1", “dealer”:”Dealer12”, “action”: “add”, “subid”:”23F0”}

API requests must be contain:
pwd --> admin user's password
bu --> Business Unit name (case sensitive)
subid --> Subscriber ID (aes hex number)

If you include the **dealer**, then you must provide action too.
dealer --> dealer name
action --> add, delete or update (all low cases)

All of the fields below are optional:
address --> subscriber geography address
address2
city
state
zip
country
latitude --> for example 40.7486
longitude --> for example -77.8786

5 Operator Dashboard

5.1 Overview

The *Operator Dashboard* displays all information available from the *MultiNet* receiver for that Business Unit for the last 10 days. Each *Operator Dashboard* provides the following important information to the operator to help manage, monitor, and maintain the AES-*IntelliNet* network.

5.2 Login

If you are a Business Unit Owner, you can access your *Operator Dashboard* by signing in at the following URL: http://your_NMS_IP_address to launch the sign on screen below. The username will be the *MultiNet* Business Unit name and the initial password is "oper". Each Business Unit has its own username but the password is the same for all Business Units, "oper". This can be changed after login. Business Unit users should coordinate *Operator Dashboard* password management with the *MultiNet* owner.

Business Unit Sign on Screen

Enter name of Business Unit

Password (default password is "oper")

5.3 IP Link and Subscriber Status Monitoring

If IP Link and Subscriber faults occur, these faults are highlighted on the left and right panels of the Dashboard to indicate new service requirements in real time do that they can be scheduled in the normal workflow. The green color indicates that there are no faults with any Subscribers or IP Links.

5.3.1 IP Link Status Monitoring

New IP Link faults will flash red-white for 10 seconds then remain red. These faults can flash again red-white when the browser is refreshed but if you click on any of the faults to view them, they will remain red.

5.3.2 Subscriber Status Monitoring

New Subscriber faults will flash orange-white for 10 seconds then stay orange. If a new Subscriber is added to a fault, the fault will flash red-white for 10 seconds then remain red.

5.3.3 View Fault Detail Windows

Each fault is described by name and in parentheses next to the name is the number of IP Links or Subscribers on the network experiencing that fault. To view a list of IP Link or Subscribers with the fault, click on the red button for

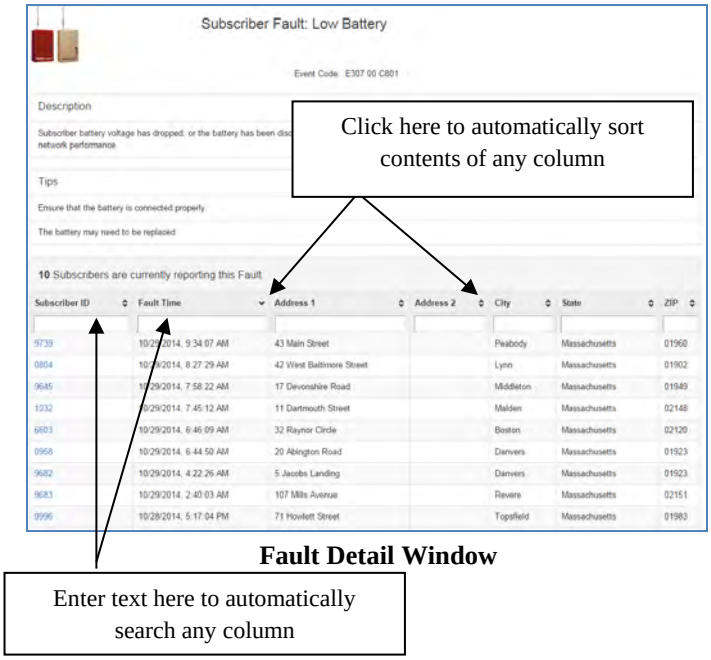
that fault to open a Fault Detail Window. An example is below - a list of Subscribers with a low battery fault condition.

To access Fault Detail Window, Click on a fault. This is an example of Subscriber Battery Fault Detail Window - on right.

The IP Link and Subscriber fault detail windows privide the following:

- Name of the fault and Event code
- A description of the fault and what causes it
- Tips for resolving this fault
- Total number of IP Links or Subscribers experiencing this fault
- Sortable list of IP Links or Subscribers experiencing this fault and the time stamp

Filters at the top of each column permit easy search and sort of the contents of the column.

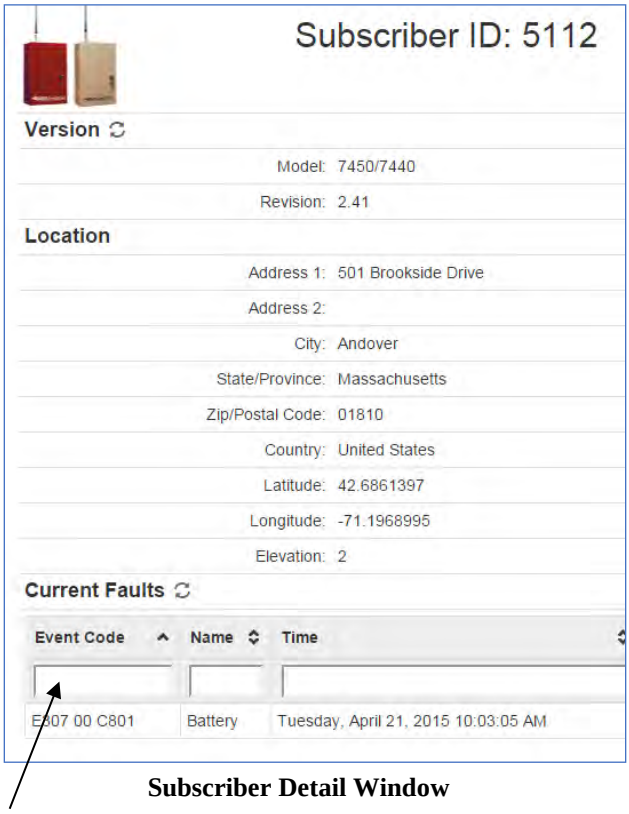


Fault Detail Window

Next, One-click detail information is available for any specific Subscriber. Click on and Subscriber ID to open the **Subscriber Detail Window** that provides:

- Type of Subscriber - model and revision
- Location including address and longitude and latitude
- Current faults if any including CID codes
- Routes and time stamps
- Peers and time stamps
- Number of repeat dependent Subscribers
- Number of generated messages over last 10 days
- Subscriber Programmed Settings
- 10 day event history including CID codes.

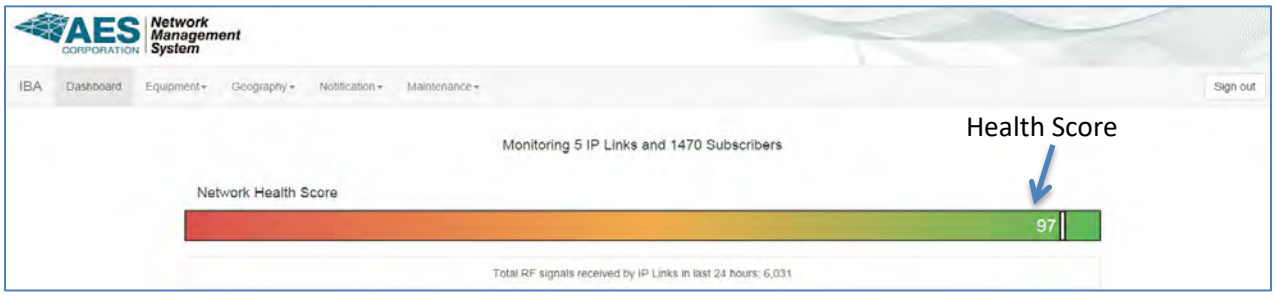
One-click detail information is also available for any specific IP Link.

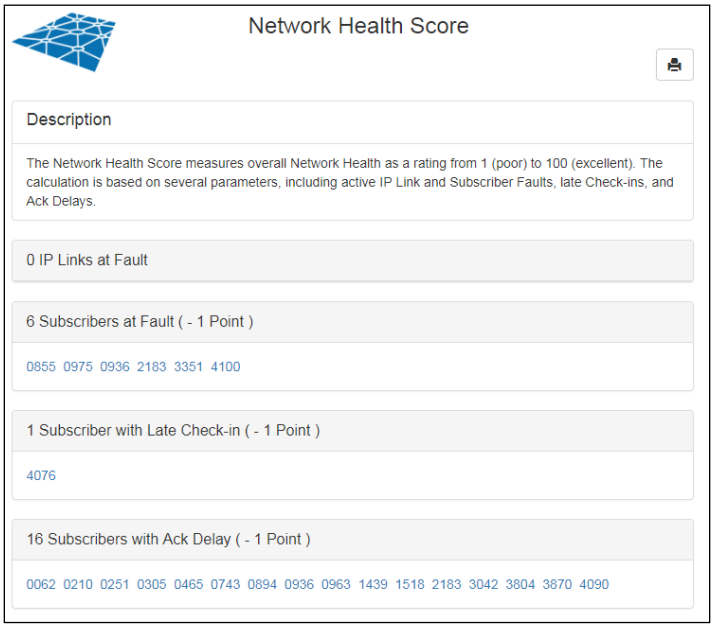


Subscriber Detail Window

5.4 Network Health Score

The Network Health Score is a quick indicator of network performance. The score is calculated based on the number of Ack Delays, IP Link and Subscriber faults as well as the number of late check-in messages. The Health Score range is a number from 1 to 100. A higher score suggests a healthy network and a lower score suggests that improvements can be made to the network.



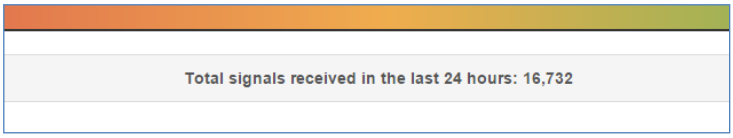


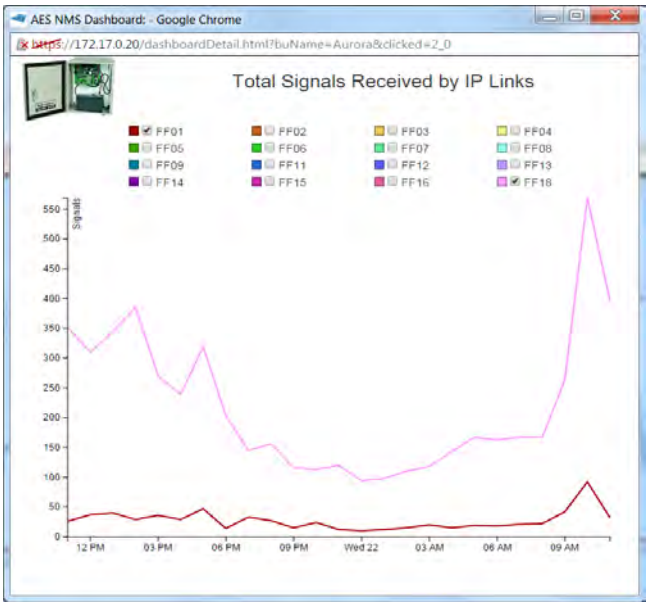
Click on the Network Health Score bar to view more details about the Subscribers and IP Links that are affecting your Network Score.

5.5 Total Signals Received

"Total signals received in the last 24 hours" indicates how much inbound RF traffic has been received in the last 24 hours. This includes all events that originate from the AES Subscribers and also the alarm panels.

Click on the "Total signals received in the last 24 hours" to see additional details about the amount of traffic from all IP Links in the Business Unit.



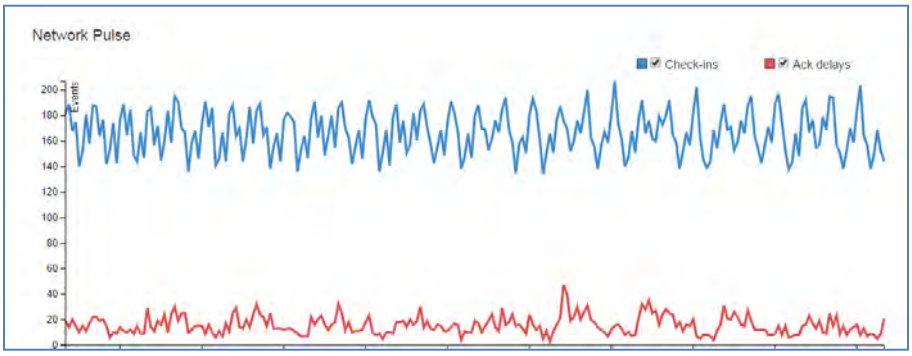


5.6 Network Pulse

The Network Pulse is a dynamic 10 day historical view of leading network health indicators. Network Pulse at the Dashboard level presents the number of Check-Ins and Ack Delays in a way such that any change in network performance will be quickly visible. A consistent pattern to the Network Pulse indicates consistent network operation. If an issue develops with network performance, the number of Check-Ins will decrease and the number of Ack Delays will increase. This change in performance will be quickly visible because the 10 day pattern will change. Additional one-click detail is available by clicking on the **Network Pulse** Chart which will open a window with a 10 day history of all events.

Network Pulse - Dashboard view
Blue line section details 10 day history of all Subscriber Check-Ins

Red line section details 10 day history of all Subscriber Ack Delays
Click on the chart to open detail view window of all events

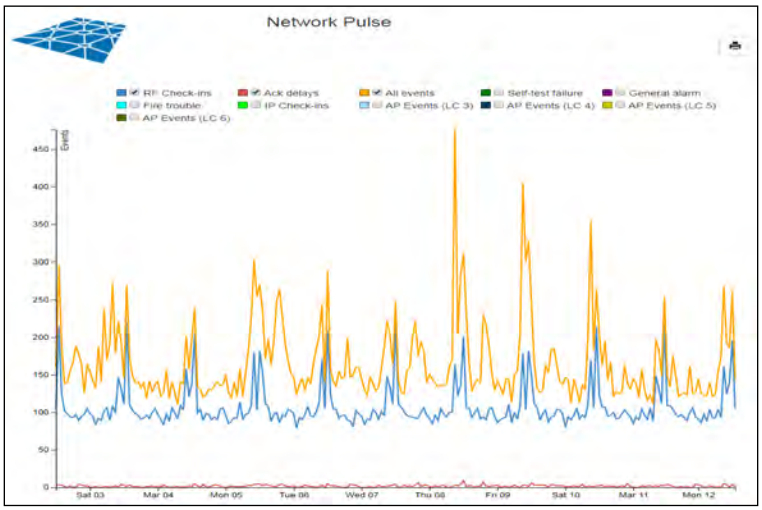


Network Pulse Dashboard View

Network Pulse - Detail view

Detail View shows a 10 day history of all events depending on check boxes at top. Includes:

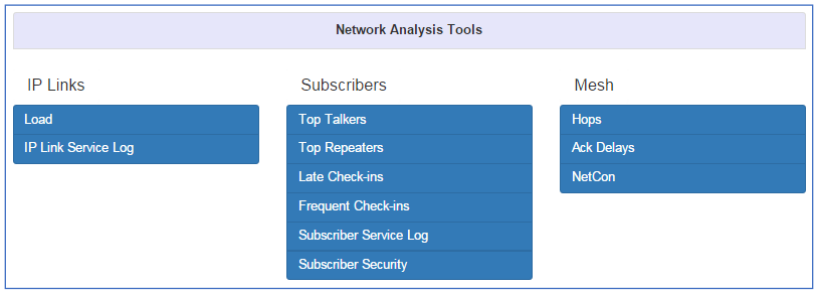
- RF Check-Ins
- IP Check-ins
- Ack Delays
- All events
- Self-test failure
- General alarm
- Fire trouble
- Alarm Panel Events on Line card 3 (RF)
- Alarm Panel Events on Line card 4 (RF)
- Alarm Panel Events on Line card 5 (IP)
- Alarm Panel Events on Line card 6 (IP)



Network Pulse Detail View

5.7 Network Analysis Tools

Under the Network Pulse are a set of Network Analysis tools for 3 critical network subsystem categories - IP Links, Subscribers and Mesh. Clicking down on each link opens another window which provides analytical information related to network performance. Note that these windows update automatically.



***IntelliNet* Network Analysis Tools**

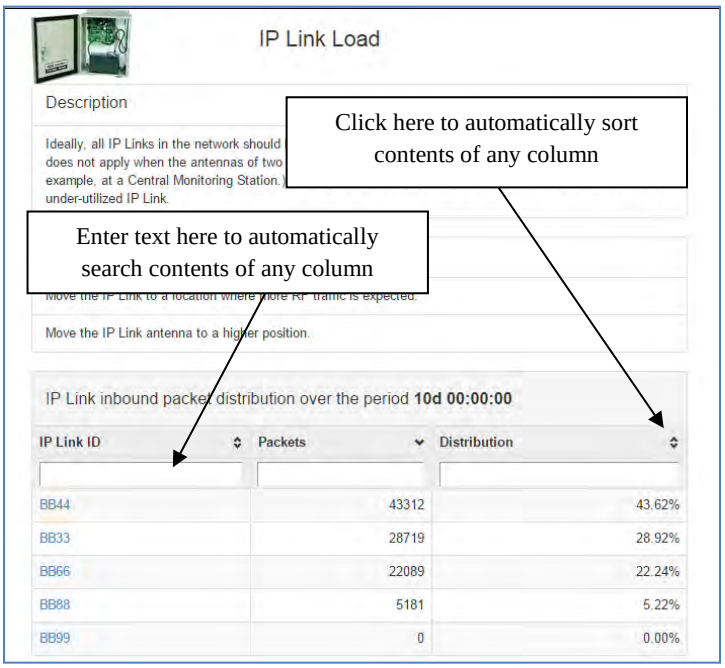
5.7.1 IP Links Load

Click down here to see a 10 day history of total signals and relative distribution across IP Links on the network. An example of the IP Link Load is illustrated below. Ideally, all IP Links in the network should handle roughly equal volumes of RF traffic. This generalization does not apply when the antennas of two IP Links are deliberately placed within RF range of each other such as at a Central Monitoring Station. See the Tips section describing how to increase RF traffic handled by an under-utilized IP Link.

Click on **Load** to open new window with the following information relating to the IP Links on the network:

- A description of IP Links load concept
- A number of tips are offered to generally improve network performance
- A list of the IP Links is presented at the bottom
- Additional analytical details including number of packets received by each IP Link and the distribution of packets among all of the IP Links on the network

Filters at the top of each column permit easy search and sort of the contents of the column.



IP Link Load

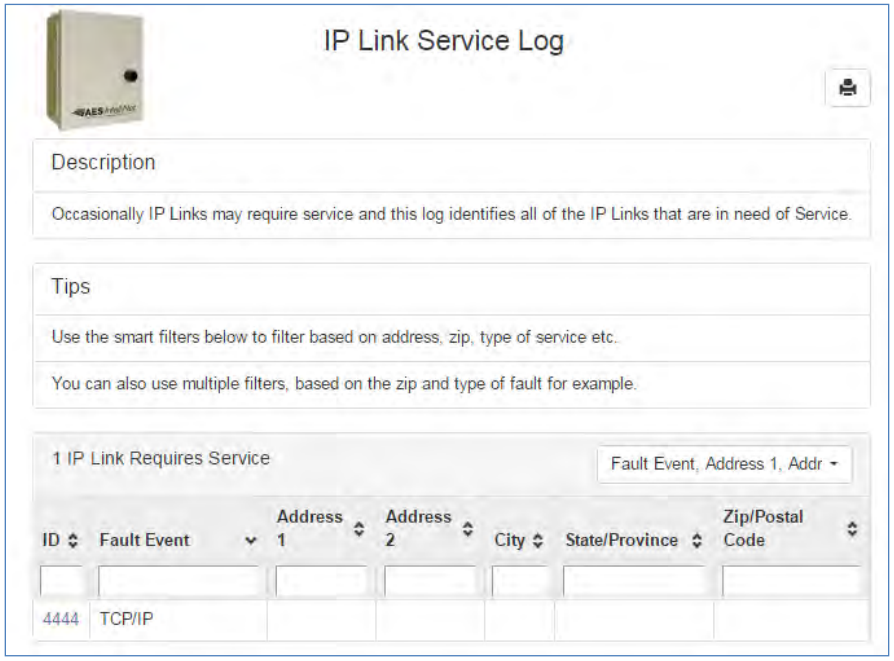
Next, One-click detail information is available for any specific IP Link. Click on any IP Link ID to open the **IP Link Detail Window** that provides:

- Version of IP Link - model and revision
- Location including address and longitude and latitude
- Current faults if any including CID codes
- Number of repeat dependent Subscribers
- Number of generated messages over last 10 days
- A section for Notes
- 10 day event history

IP Link Detail View

5.7.2 IP Link Service Log

Click here for a list of all IP Links which may require service. This window will give you quick information about what kind of Fault the IP Link is experiencing and its location. You can also click on the IP Link ID and this will open the IP Link Detailed window as explained before.



5.7.3 Top Talkers

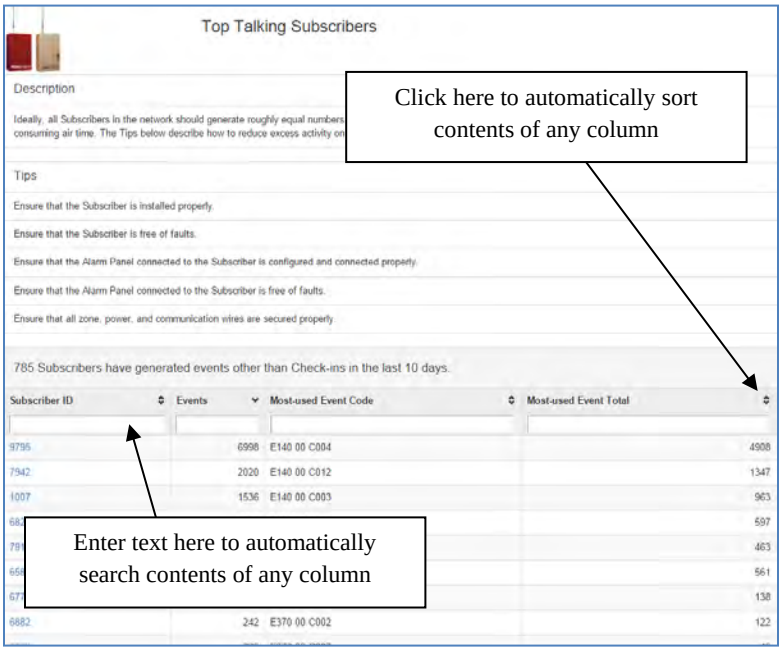
Click down here for a list of all Subscribers that have sent any signal other than Check-In during last 10 days. For each of these Subscribers, this list also includes total signals transmitted, the events most sent, and the number of times this event was sent.

Click on **Top Talkers** to open a new window with the following information relating the Subscribers on the network:

- A description of the Top Talker Concept
- Tips for generally improving network performance.
- A list of the Subscribers that generated the largest amounts of events in the last 10 days.
- The total number of events generated by each of these Subscribers
- The most used Event Code and the most used Event Code occurrence total

Filters at the top of each column permit easy search and sort of the contents of the column.

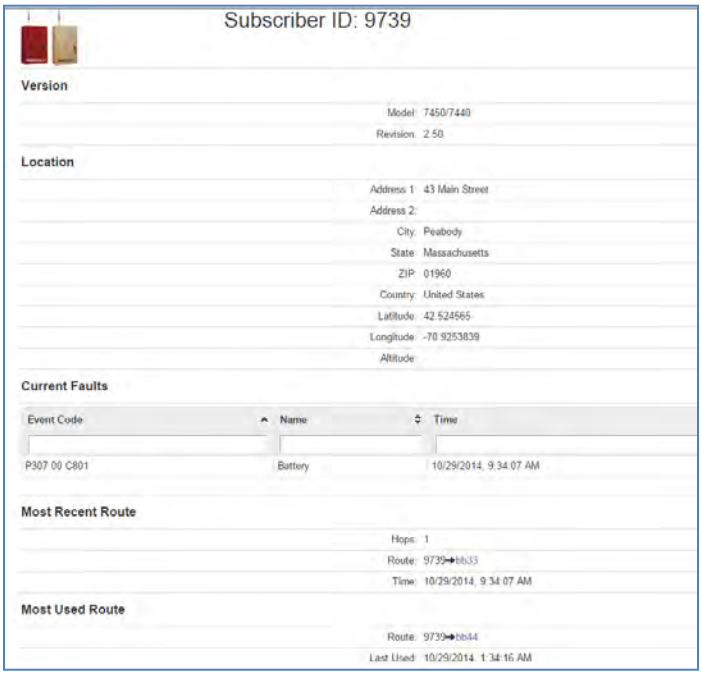
Click on any Subscriber ID to open **Subscriber Detail Window**



Top Talkers - Subscribers

One-click detail information is available for any specific Subscriber. Click on and Subscriber ID to open the **Subscriber Detail Window** that provides:

- Type of Subscriber - model and revision
- Location including address and longitude and latitude
- Current faults if any including CID codes
- Most Recent Route
- Most Used Route
- Number of repeat dependent Subscribers
- Number of generated messages over last 10 days
- Subscriber Programmed Settings
- 10 day event history including CID codes



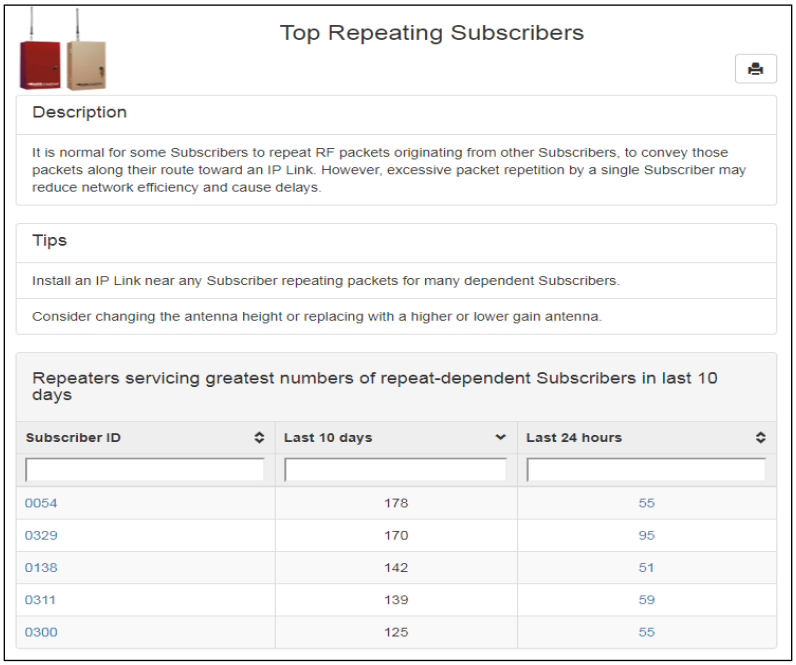
Subscriber Detail View

5.7.4 Top Repeaters

Click here for a list of the top 5% largest repeater Subscribers. Repeating the packets of other Subscribers is a normal function of the mesh network. Excessive packet forwarding by a single Subscriber may reduce network efficiency and cause delays though it is unlikely. It may be advisable to locate or install an additional IP Link near Subscribers forwarding RF packets from a high percentage of other Subscribers.

Click on **Top Repeaters** to open a new window with the following information relating the Subscribers on the network:

- A description of the Top Repeater Concept
- Tips for generally improving



Top Repeating Subscribers

Description

It is normal for some Subscribers to repeat RF packets originating from other Subscribers, to convey those packets along their route toward an IP Link. However, excessive packet repetition by a single Subscriber may reduce network efficiency and cause delays.

Tips

Install an IP Link near any Subscriber repeating packets for many dependent Subscribers.

Consider changing the antenna height or replacing with a higher or lower gain antenna.

Repeaters servicing greatest numbers of repeat-dependent Subscribers in last 10 days

Subscriber ID	Last 10 days	Last 24 hours
0054	178	55
0329	170	95
0138	142	51
0311	139	59
0300	125	55

Top Repeating Subscribers

5.7.5 Late Check-Ins

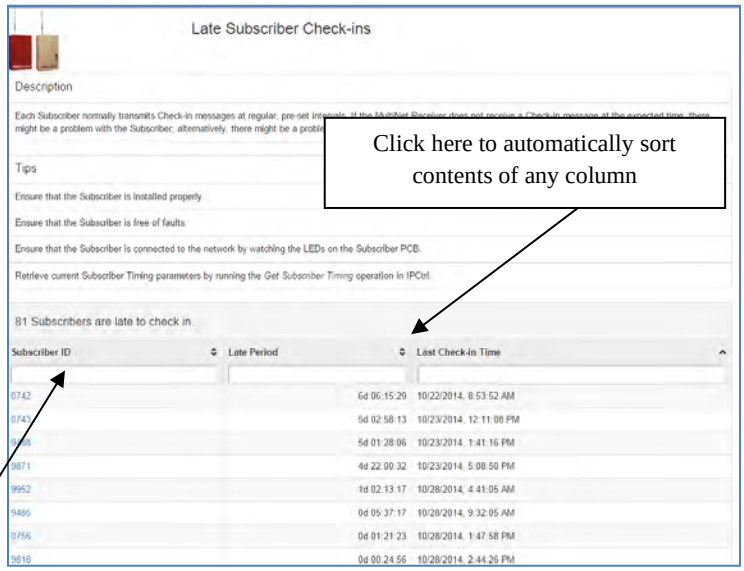
Click here for list of Subscribers from which the *MultiNet* Receiver has not received a Check-In message at the expected time (as configured on the *MultiNet* receiver). This could indicate a service requirements for this Subscriber or may be explained by some environmental factor such as the weather. In order to come off this list, the Subscriber must transmit 3 Check-Ins on schedule.

Click on **Late Check-Ins** to open a new window with the following information relating the Subscribers on the network:

- A description of the Late Check-In Concept
- Tips for generally improving network performance.
- A list of the Subscribers that currently are late to Check-In, length of time each is late, and last time each checked in.

Filters at the top of each column permit easy search and sort of the contents of the column

Click on any Subscriber ID to open **Subscriber Detail Window**



Enter text here to automatically search contents of any column

Late Subscriber Check-Ins

5.7.6 Frequent Check-Ins

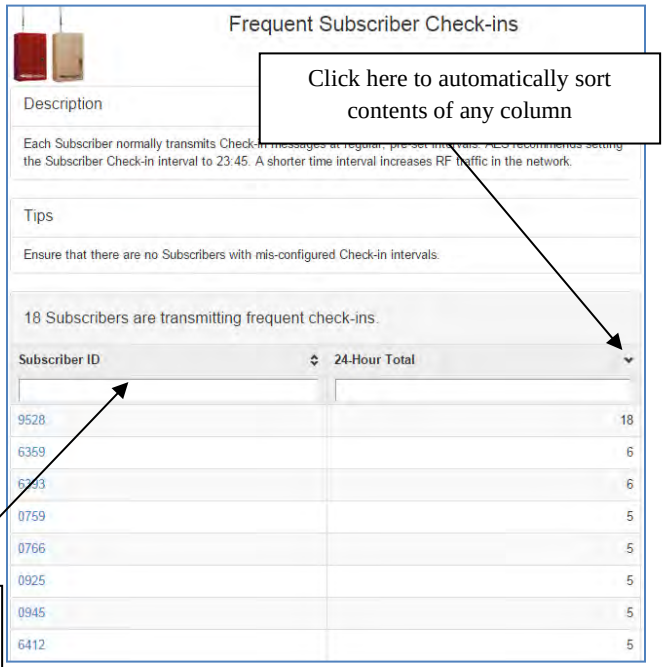
Click here for list of Subscribers transmitting more than one Check-In during a 24 hour period. The list shows the number of Check-Ins each Subscriber transmits per 24 hour period. The recommended number of Check-Ins per 24 hours is one. This meets the requirements of UL 864 for Commercial Fire and is appropriate for virtually all applications. A higher number of Check-Ins per 24 hour period can unneccessarily increase RF traffic on network.

Click on **Frequent Check-Ins** to open a new window with the following information relating the Subscribers on the network:

- A description of the Frequent Check-In Concept
- Tips for generally improving network performance.
- List of the Subscribers that currently are transmitting frequent check-ins and the number of check-ins per 24 hour period.

Filters at the top of each column permit easy search and sort of the contents of the column

Click on any Subscriber ID to open **Subscriber Detail Window**

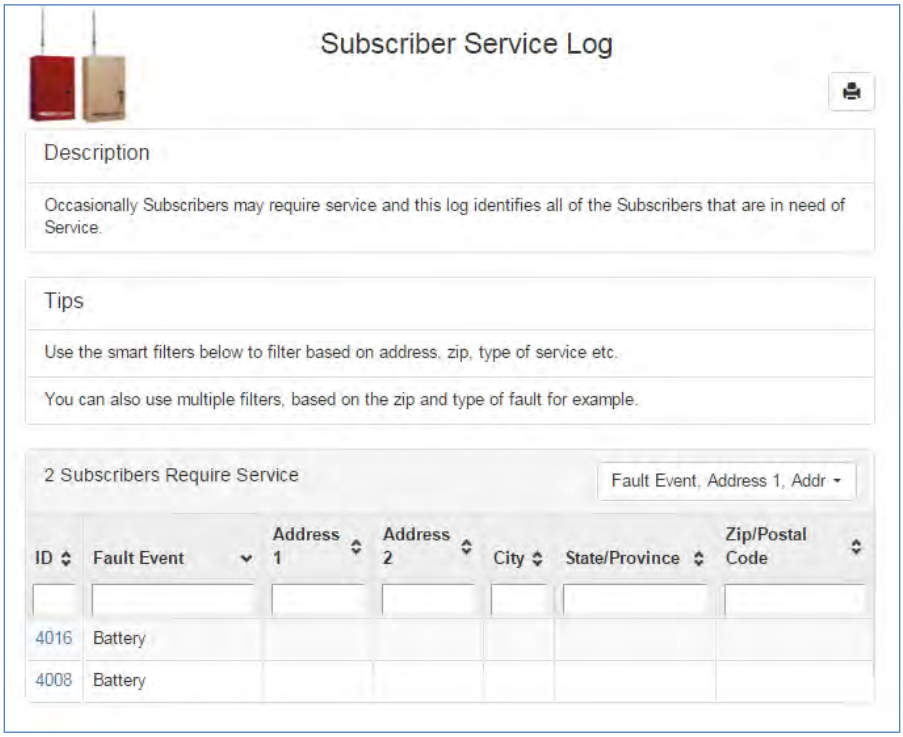


Enter text here to automatically search contents of any column

Frequent Check-Ins

5.7.7 Subscriber Service Log

Click here for a list of all Subscribers which may require service. This window will give you quick information about what kind of Fault different subscribers are experiencing and there location. You can also click on the Subscriber ID and this will open the Subscriber Detailed window as explained before.



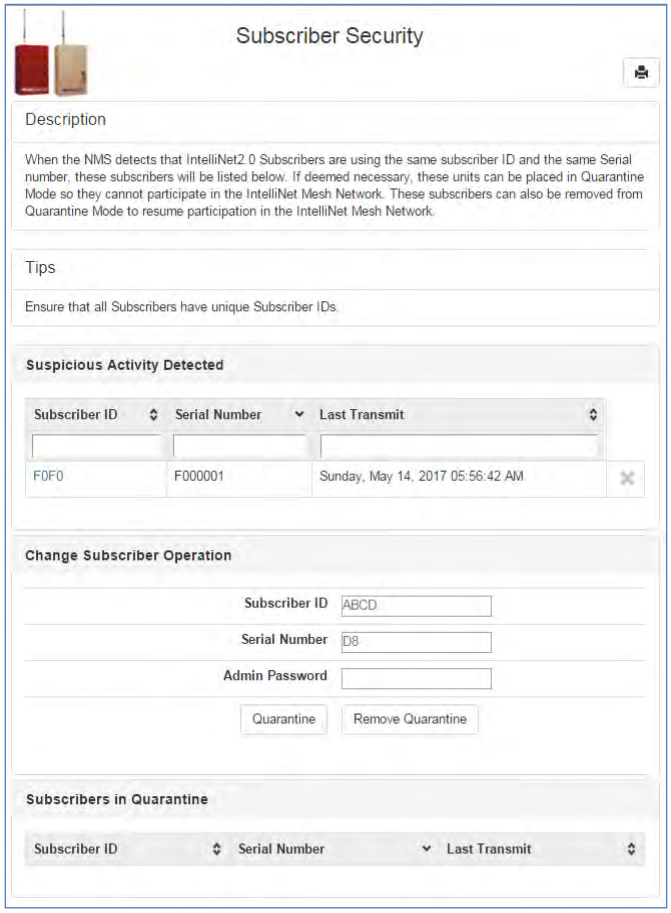
5.7.8 Subscriber Security

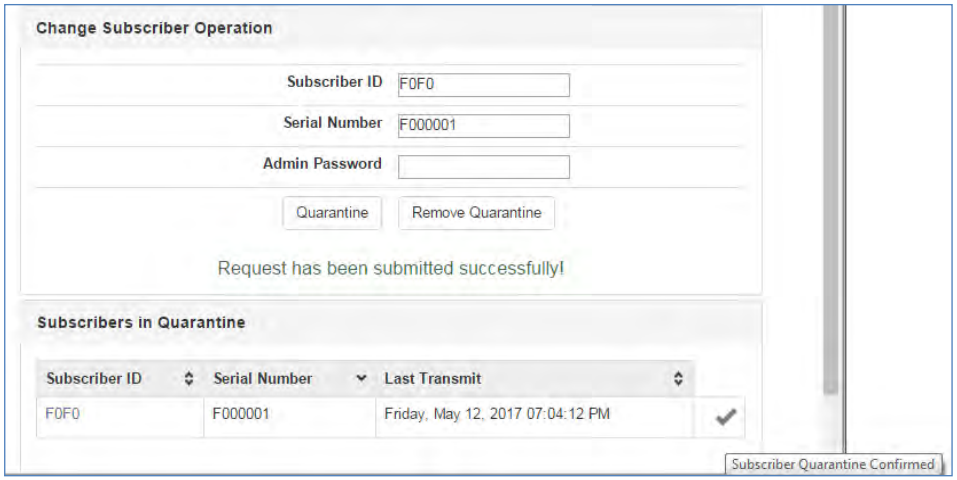
Click here to manage the subscribers with suspicious activities by placing them in Quarantine mode. When the NMS detects that IntelliNet2.0 Subscribers are using the same subscriber ID and the same Serial number, these subscribers will be listed here. If deemed necessary, these units can be placed in Quarantine Mode so they cannot participate in the IntelliNet Mesh Network. These subscribers can also be removed from Quarantine Mode to resume participation in the IntelliNet Mesh Network.

Hover over the Subscriber IP from the Suspicious Activity detected subscriber and the Subscriber ID and Serial number will be automatically populated under the Change Subscriber Operation section.

Enter the Admin password for the subscriber and click on Quarantine or Remove Quarantine depending on the state of subscriber.

If you select Quarantine, then once successful, a checkmark will appear in the Subscriber in Quarantine tab next to that particular subscriber.





5.7.9 Hops

Click here for a list of Subscribers with 4 or more hops to reach an IP Link in either the most recent transmission and/or the most used route to an IP Link over the past 10 day period. It may be advisable to locate or install an additional IP Link near Subscribers on the list with 4 or more Hops.

Click on **Hops** to open a new window with the following information relating the Subscribers on the network:

- A description of the Hops Concept
- Tips for generally improving network performance.
- List of the Subscribers that are located 4 or more Hops from an IP Link, number of Hops in most recent route, and number of Hops in most used route - over past 10 days.

Filters at the top of each column permit easy search and sort of the contents of the column

Click on any Subscriber ID to open **Subscriber Detail Window**

Analytic Tools – Hops

5.7.10 Ack Delays

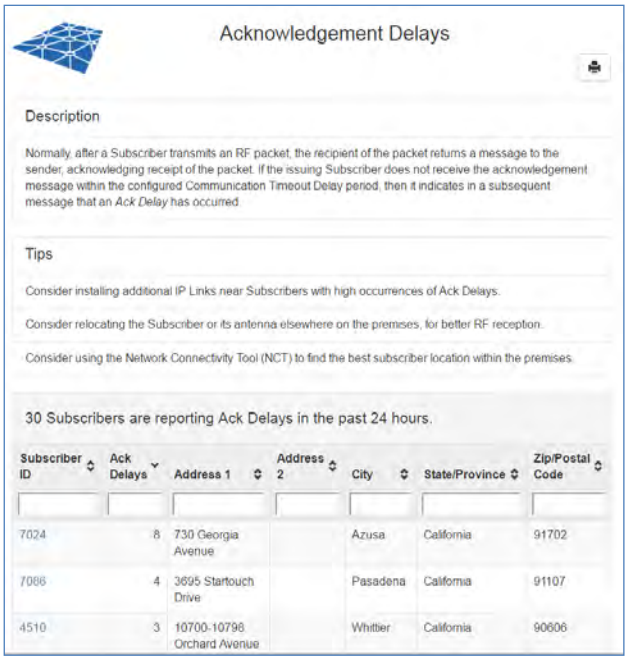
Click here for a list of all Subscribers that have transmitted an *Ack Delay* in the past 24 hours as well as the quantity of *Ack Delays* over that period. When any Subscriber transmits an RF packet, the Subscriber recipient of the packet returns a message to the sender acknowledging receipt of the packet. An *Ack Delay* is triggered if a Subscriber does not receive an acknowledgement message of a transmitted signal within the configured Communication Timeout Delay period. *Ack Delays* could indicate a service requirements for a Subscriber or may be explainined by some environmental factor such as the weather. It may be advisable to locate or install additional IP Links near Subscribers that remain on the list for extended periods.

Click on **Ack delays** to open a new window with the following information relating the Subscribers on the network:

- A description of the Ack delay Concept
- Tips for generally improving network performance.
- List of the Subscribers that have reported an Ack delay over past 24 hours and quantity over that period.

Filters at the top of each column permit easy search and sort of the contents of the column

Click on any Subscriber ID to open **Subscriber Detail Window**



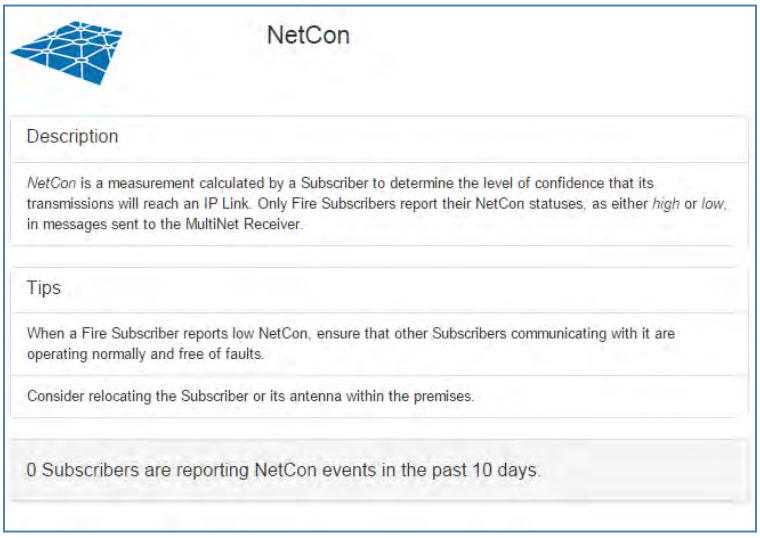
5.7.11 NetCon

Click here for a list of all Fire Subscribers that have reported a *NetCon* fault in the last 10 days. *NetCon* is a measurement calculated by a Subscriber to determine the level of confidence that its transmissions will reach an IP Link. When a Fire Subscriber reports NetCon fault, ensure that the other Subscribers communicating with it are operating normally and are free of faults. In may be advisable to relocate the Subscriber or to relocate or change its antenna.

Click on **Netcon** to open a new window with the following information relating the Subscribers on the network:

- A description of the Netcon Concept
- Tips for generally improving network performance.
- List of the Subscribers that have reported a Netcon event over past 10 days and quantity over that period.

Click on any Subscriber ID to open **Subscriber Detail Window**



Analytic Tools - NetCon

5.8 Equipment List

Through the *Operator Dashboard*, users can obtain list of all Subscribers and all IP Links on the Business Unit Network. The Operator can sort each equipment list extensively and further click down into each Subscriber or IP Link for important information.

Click on **Equipment>IP Links** or **Equipment>Subscribers**

NOTE: Non-AES Units will show up only if Non-AES Unit addresses have been imported.

5.8.1 Equipment List, IP Links

A list of IP Links along with ID, Model, Revision and Location can be obtained by clicking on **Equipment** then IP Link**s** at the top of the Dashboard. If IP Links are removed from the *MultiNet*, they are automatically removed from this list and no longer monitored. These views can be sorted using the filters at the top of the list and can be easily printed.

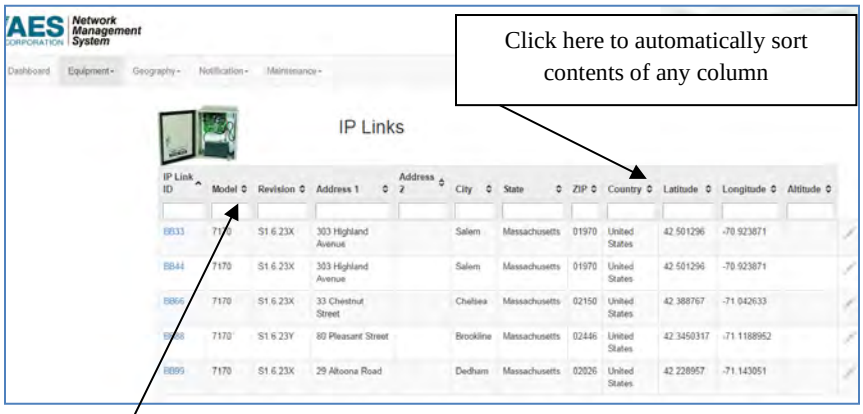
To access a list of all IP Links on a network:

Click on **Equipment>IP Links**

Information includes: IP Link ID, Model, Revision and Location

Filters at the top of each column permit easy search and sort of the contents of the column

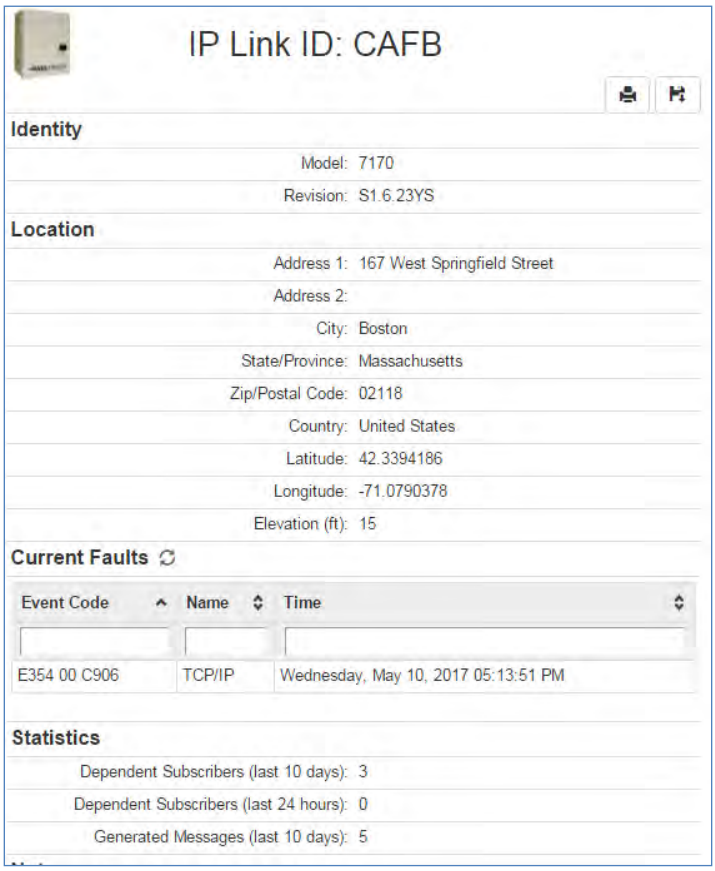
Click on IP Link ID to open **IP Links Detail Window**



Equipment List - IP Links

Next, One-click detail information is available for any specific IP Link. Click on any IP Link ID to open the **IP Link Detail Window** that provides:

- Version of IP Link - model and revision
- Location including address and longitude and latitude
- Current faults if any including CID codes
- Number of repeat dependent Subscribers
- Number of generated messages over last 10 days
- A section for Notes
- 10 day searchable and sortable event history



IP Link Detail View

5.8.2 Equipment List, Subscribers

A list of Subscribers along with ID, Model, Revision and Location can be obtained by clicking on **Equipment** then **Subscribers** at the top of the Dashboard. If Subscribers are removed from the *MultiNet*, they are automatically removed from this list and no longer monitored. These views can be sorted using the filters at the top of the list and easily printed.

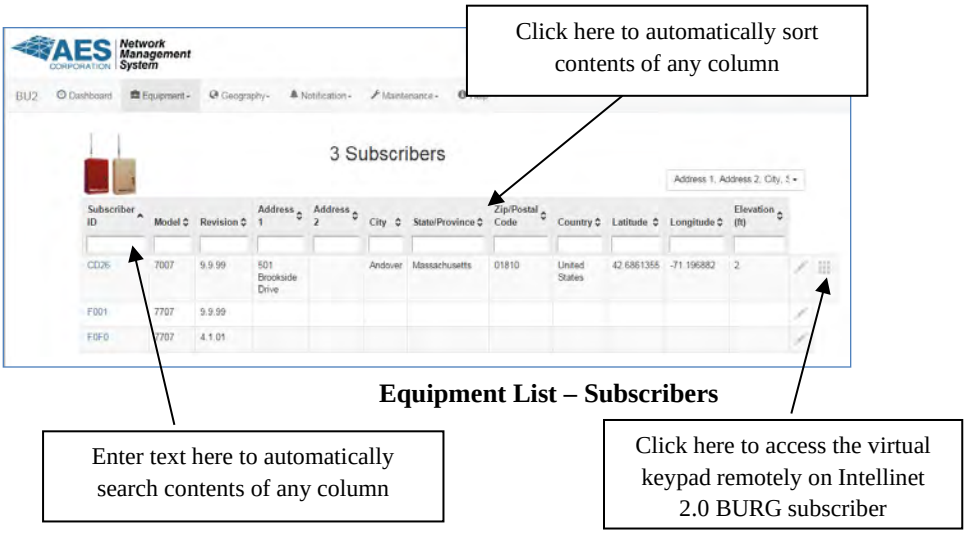
To access a list of all Subscribers on a network:

Click on **Equipment>Subscribers**

Information includes: ID, Model, Revision and Location

Filters at the top of each column permit easy search and sort of the contents of the column

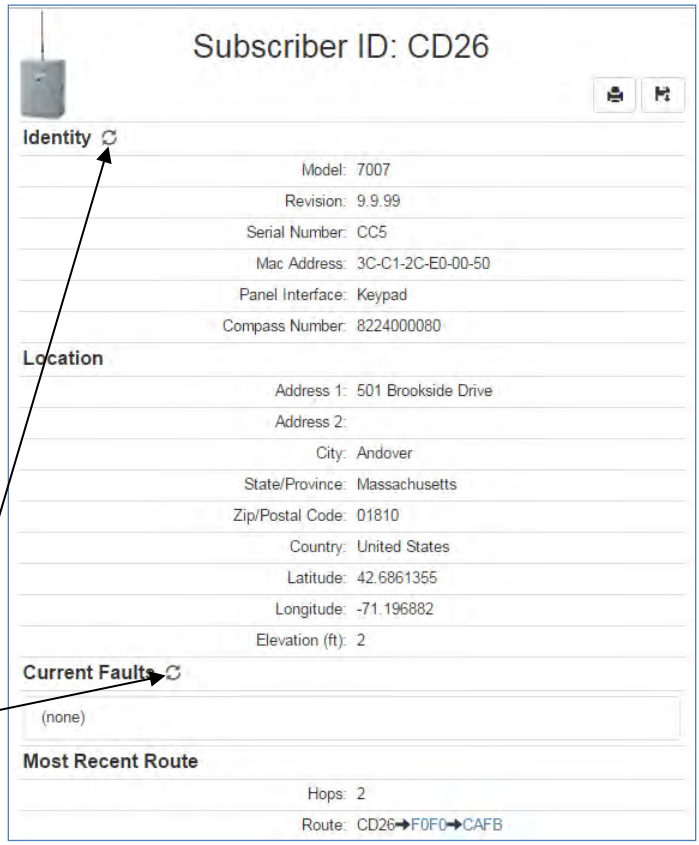
Click on Subscriber ID to open **Subscriber Detail Window**



Equipment List – Subscribers

One-click detail information is available for any specific Subscriber. Click on and Subscriber ID to open the **Subscriber Detail Window** that provides:

- Type of Subscriber – model, revision, serial number, Mac Address, Panel Interface and Compass Number. On those information which is applicable to a subscriber.
- Location including address and longitude and latitude
- Current faults if any including CID codes
- Most Recent Route
- Most Used Route
- Number of repeat dependent Subscribers
- Number of generated messages over last 10 days
- Subscriber Programmed Settings
- 10 day searchable and sortable event history including CID codes



Subscriber Detail View

5.8.3 Equipment List, Non-AES Units

A list of Non-AES Units along with ID and Location can be obtained by clicking on **Equipment** then **Non-AES Units** at the top of the Dashboard. Note that this link will show up only if Non-AES Units have been imported in the CSV file for Non-AES Units. The Non-AES Units list can be sorted using the filters at the top of the list and easily printed.

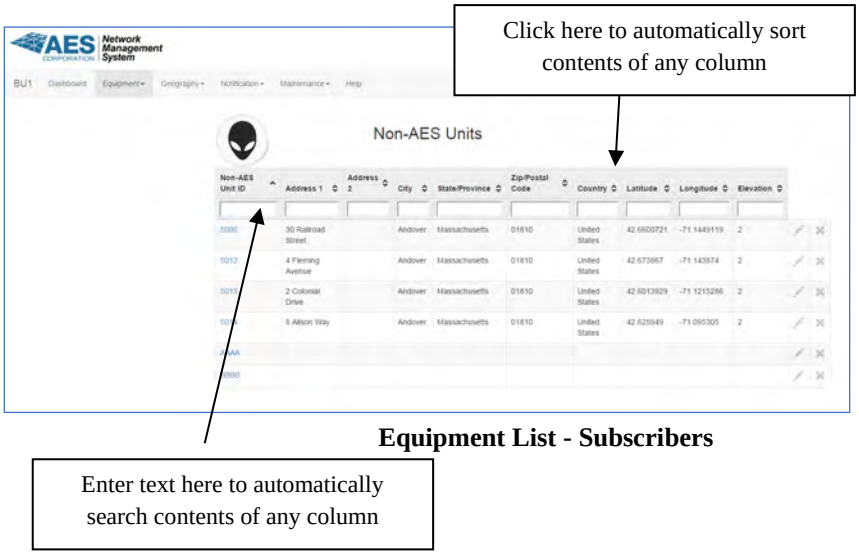
To access a list of all Non-AES Units on a network:

Click on **Equipment>Non-AES Units**

Information includes: ID and Location

Filters at the top of each column permit easy search and sort of the contents of the column

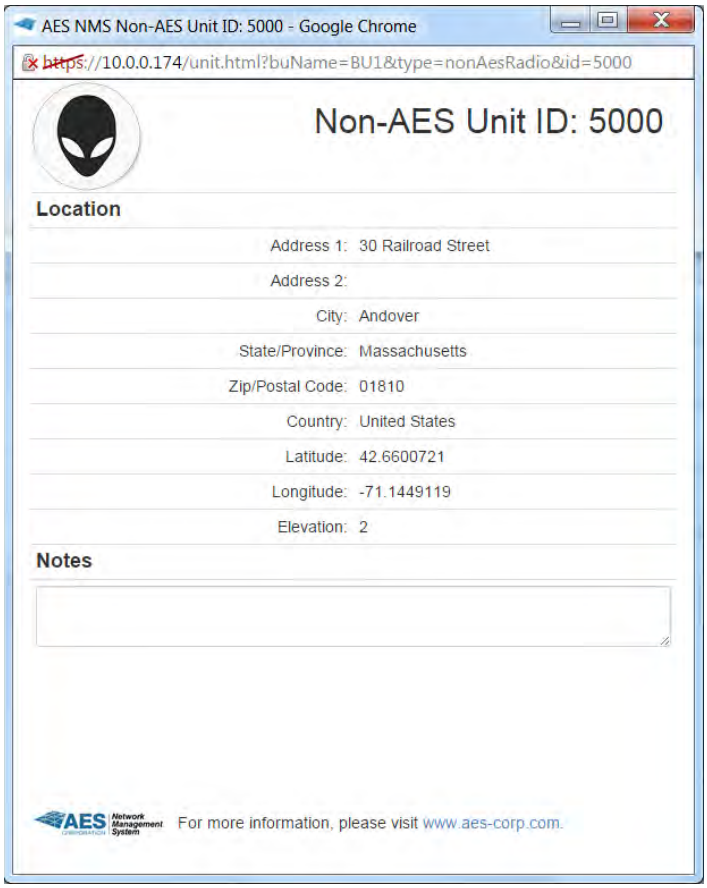
Click on Non-AES Unit ID to open **Non-AES Unit Detail Window**



Equipment List - Subscribers

One-click detail information is available for any specific Non-AES Unit. Click on and Non-AES Unit ID to open the **Non-AES Unit Detail Window** that provides:

- Location including address and longitude and latitude



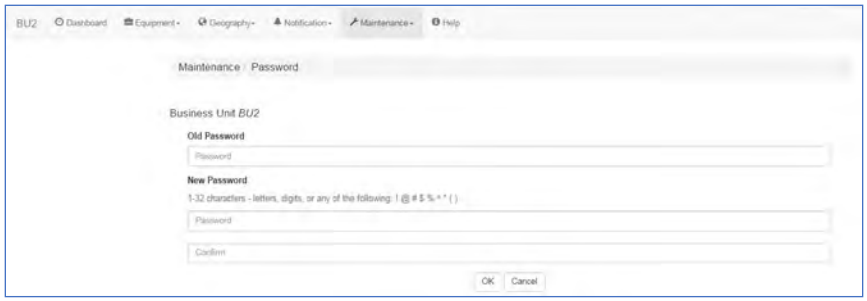
Non-AES Unit Detail View

5.9 Maintenance - Operator Dashboard

Through the Maintenance dropdown on the *Operator Dashboard*, users can easily change the Business Unit password and contact information.

To change the Password Click on **Maintenance>Password** to launch the screen below

First, enter the current password and then the new password twice and click **OK** to save the new password

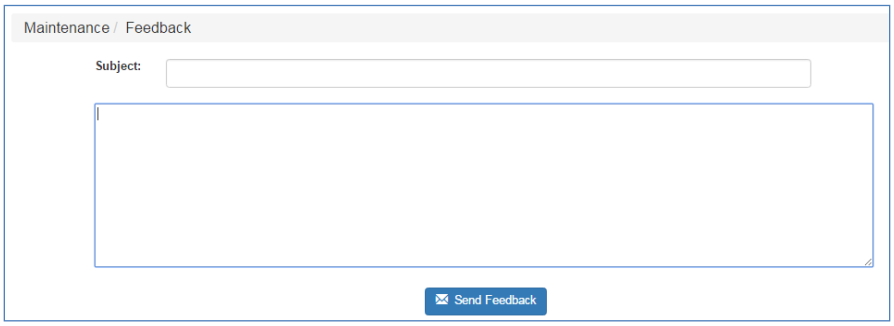


For a list of AES Contact Information, click on **Maintenance>Contact** to launch the screen below:

Click on **Maintenance>Contact**

To Send Maintenance Feedback, click on **Maintenance>Feedback** to launch the screen below:

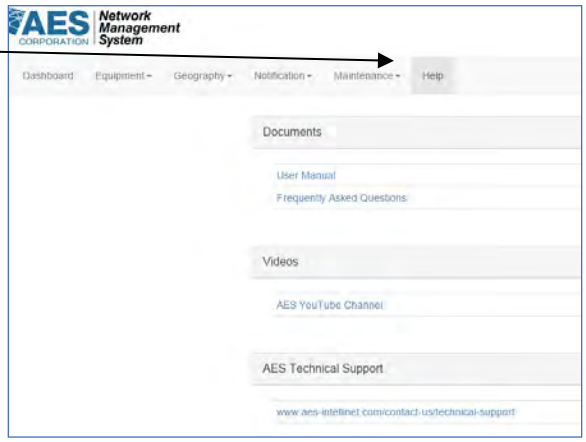
Enter the Subject and contain in the respective boxes and click on Send Feedback when done



5.10 Help - Operator Dashboard

Through the help tab on the *Operator Dashboard*, users can easily access additional information for help, such as manual, FAQ and videos.

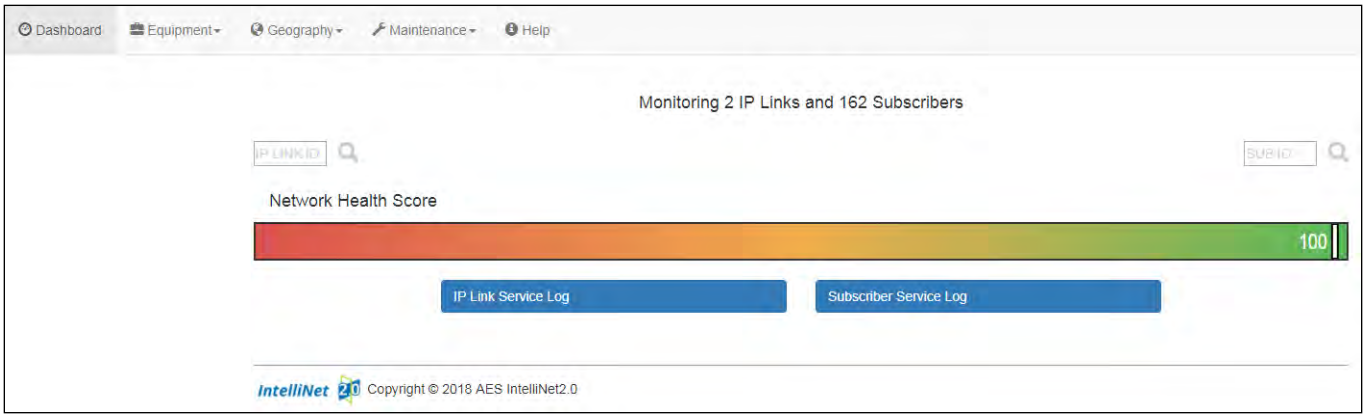
Click **Help**



6 Dealer Dashboard

6.1 Overview

The *Dealer Dashboard* displays all information available from the *MultiNet* receiver for that Dealer for the last 10 days. Each *Dealer Dashboard* provides the following important information to the operator to help manage, monitor, and maintain the AES-*IntelliNet* network.



6.2 Login

You can access your *Dealer Dashboard* by signing in at the following URL: http://your_NMS_IP_address to launch the sign on screen below. The username and password are generated by the administrator user of the NMS.

Dealer Sign on Screen

6.3 IP Link and Subscriber Status Monitoring

If IP Link and Subscriber faults occur, these faults are listed on the IP Link Service Log and Subscriber Service Log.

7 Interactive Visualization

7.1 Overview

Through the NMS *Operator Dashboard*, a user can launch an interactive satellite map of their *IntelliNet* network that uses Google Earth. The map shows the location and status of all IP Links and Subscribers and illustrates the multiple routes for RF signals across the network from each Subscriber over past 10 days.

All interactive satellite maps are refreshed automatically as new data is received. By clicking in any IP Link or Subscriber icon, the following information is accessible: ID, Version, Settings, Location, Current Faults, Communication Trends, editable Notes and Event History. By providing a comprehensive visualization of the

network and its subsystems, the network map helps with planning for network expansion. There are four discrete views the user can access for interactive visualization of their network. The four network views are **Utilization, Routes, Faults, and Topology**.

In order to view the visualization feature of NMS, Google Earth (www.earth.google.com) must be installed on the PC you plan to use.

7.2 Enter Subscriber and IP Link Addresses into NMS

In order to view the Visualization feature of the NMS on Google Earth you have to first load the addresses of the Subscribers and IP Links. To import the street addresses go to **Geography** then **Import AES Units**. You can download a template which can be used to import all the addresses. After the addresses are imported, the NMS server will resolve to latitude and longitude and display progress.

7.3 Enter Non-AES Unit Addresses into NMS

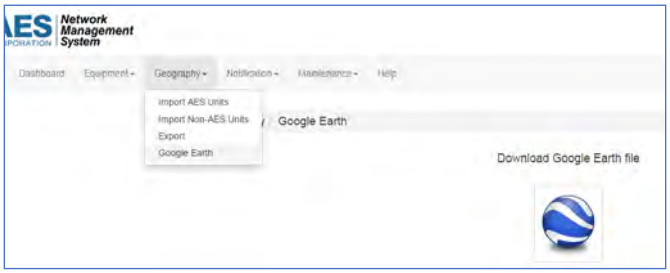
You can utilize the NMS Visualization features to place Non-AES units on Google Earth to get an idea where you Non-AES units are located in reference to AES Subscribers and IP Links. To import the Non-AES Unit street addresses go to **Geography** then **Import Non-AES Units**. You can download a template which can be used to import all the addresses. After the addresses are imported, the NMS server will resolve to latitude and longitude and display progress.

7.4 Export Addresses

The NMS also allows you to export already resolved or entered addresses of Subscribers, IP Links or Non-AES units. To export addresses go to **Geography** then **Export**. You can download the addresses and print them or save them and use them as an import file when importing addresses on a different NMS.

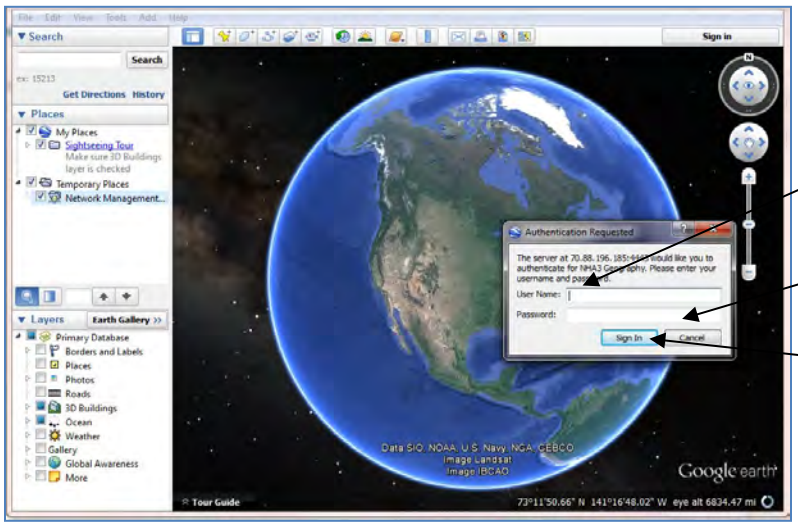
7.5 Launch Interactive Visualization

To launch the Visualization function, click on **Geography>Google Earth** to view the screen below



Click on the Google Earth icon to download the .kml file with the Business Unit map information. The Business Unit .kml file will download an icon to the bottom left of the screen.

Next click on he Business Unit .kml file. As Google Earth begins to launch, you will be asked to enter a User Name and password. The user name is the name of the Business Unit and the password is the same used for the *Operator Dashboard* password for that Business Unit. Next, enter user name and password and click **Sign In.**



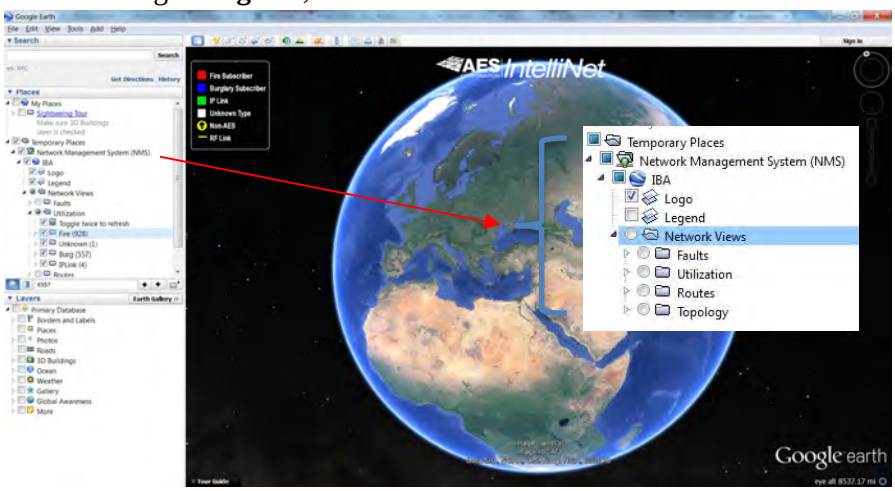
Enter the name of the Business Unit as the User Name and

Use *Operator Dashboard* password

Click **Sign In.**

NOTE: Administrator can sign in as "admin" and use the *Administrator Dashboard* password

After clicking on **Sign In**, the Business Unit data base will load which could take a few seconds.



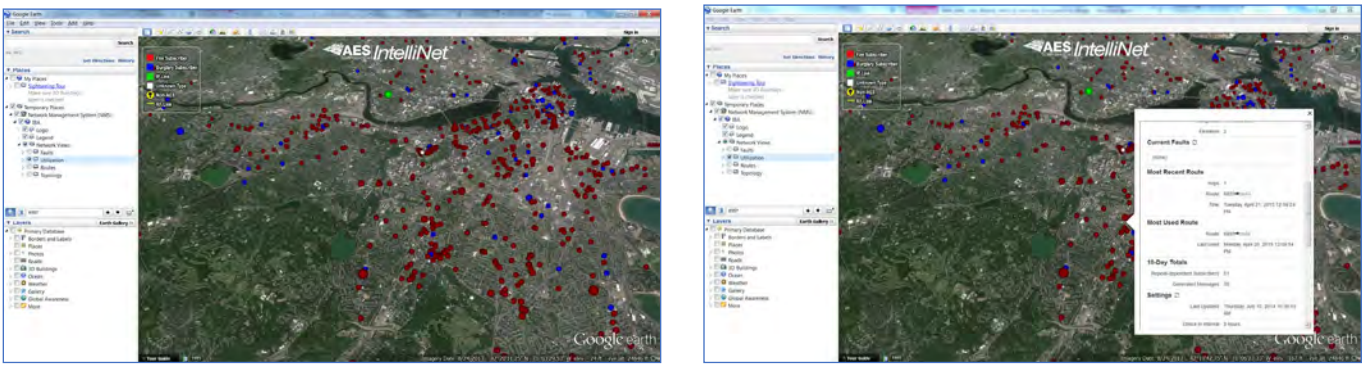
On the left of the screen will be the NMS Google Earth Summary as detailed above. At the top of the Summary under *Network Management System* is the name of the Business Unit - in this example the Business Unit name is IBA. Below the Business Unit name are check boxes that control whether the Legend and the AES *IntelliNet* logo are visible on screen. Note in the Legend that the AES Fire Subscribers are red, Burglary Subscribers are blue, and unknown Subscribers are white.

Next in the Google Earth Summary are the four Network views which present the interactive maps of the *IntelliNet* network from four different perspectives. The four network views are **Utilization, Routes, Faults, and Topology**.

Next, double click on the **Utilization** view to populate the map with the Subscribers and IP Links from this Business Unit network. The program will zoom into the network geography.

7.6 Utilization View

This view provides an interactive satellite map that highlights the most often used Subscribers for signal delivery across the network to IP Links. The graphical size of the Subscriber icon on the map illustrates relative utilization of each Subscriber as measured by the number of repeat dependent Subscribers.

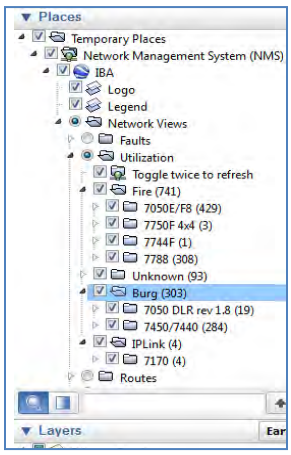


Utilization View - The larger the Subscriber icon indicates a higher number of repeat dependent Subscribers

One-click detailed information is available for all Subscribers. Click on any Subscriber icon to get a view of the following real time information: Type of Subscriber - model and revision, location including address and longitude and latitude, current faults if any including CID codes, Most Recent Route, Most Used Route, number of repeat dependent Subscribers and number of generated messages over last 10 days, Subscriber Programmed Settings, and a 10 day event history including CID codes.

The components of the network detailed on the interactive map can be modified using the Google Earth Summary. Expanding the check boxes below the **Utilization** view enables users to select, and limit if needed, the Subscribers and IP Links that are displayed based on Subscriber type and Subscriber model.

Utilization View - Google Earth Summary



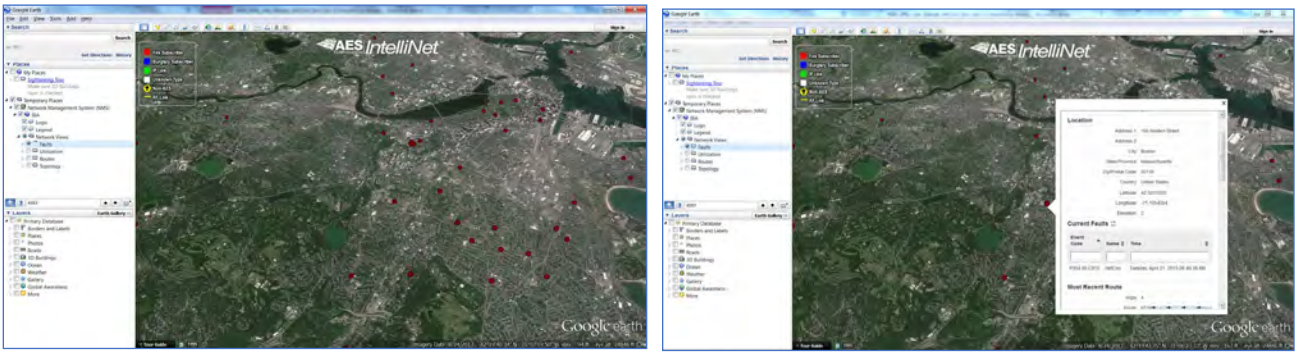
Users can select Subscribers and IP Links to view on the interactive map using Google Earth Summary

The value of the Utilization view for managing an *IntelliNet* Network is that it can identify potential network bottlenecks to enable proactive network management for optimal performance.

To return to the Utilization view, double click on **Utilization** in the Google Earth Summary.

7.7 Faults View

This view provides an interactive satellite map of all subscribers with a current fault condition. Subscribers with a new fault will automatically appear on the map. When a fault restores, the Subscriber will disappear from this view. To access the Faults view, double click on **Faults** in the Google Earth Summary.



Faults View - User can display Subscribers with a current fault real time and click down for details to plan service

One-click detailed information is available for all Subscribers in the Fault view. Click on any Subscriber icon to get information on the current fault and a view of the following real time information: Type of Subscriber - model and revision, location including address and longitude and latitude, current fault CID codes, Most Recent Route, Most Used Route, number of repeat dependent Subscribers and number of generated messages over last 10 days, Subscriber Program Settings, and a 10 day event history including CID codes.

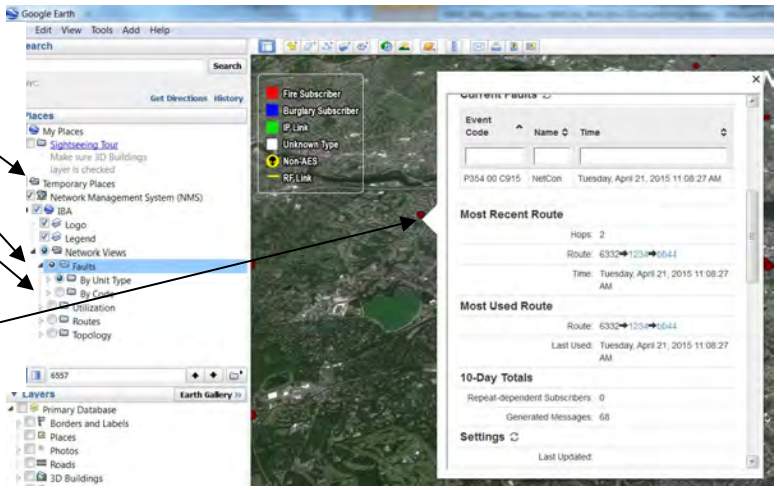
The Subscribers with a fault that are detailed on the interactive map can be modified using the Google Earth Summary. Expanding the check boxes below the **Faults** view enables users to select, and limit if needed, the Subscribers with a fault that are displayed based on Subscriber type, Subscriber model, or by event code. For example the illustration below details Subscribers with a fault sorted by event code - see the Google Earth Summary check boxes.

Google Earth Summary

For Faults view - check here

Control display by event code - Check here

Click on any Subscriber for Subscriber Detail View

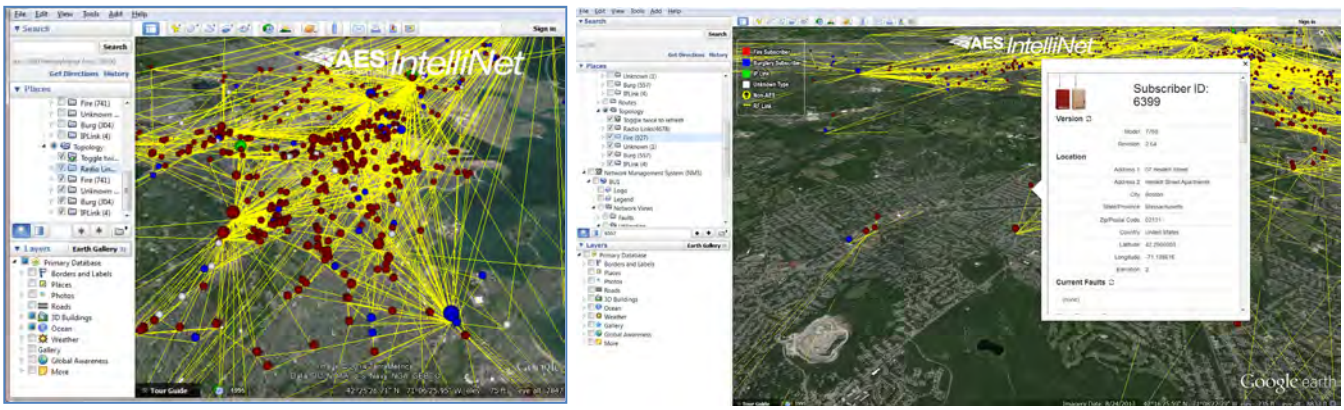


Users can select Subscribers to view by type and model or event code

The value of the **Faults** view is that it can simplify planning for routine service of Subscribers so that it can be scheduled cost effectively within normal workflows.

7.8 Mesh Topology View

This view provides an interactive satellite map of all Subscribers and illustrates on the map the RF paths between each Subscriber and the IP Links. In additional to detailed Subscriber information, user can click on any path and obtain RF Link data including the beginning and end nodes and the distance between the nodes.



Topology View - User can display RF paths between Subscribers and IP Links

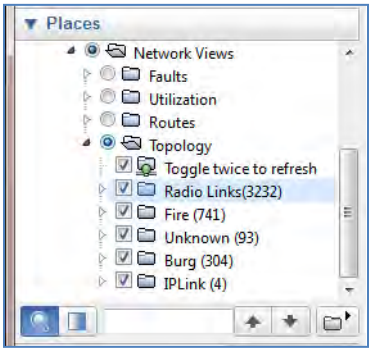
One-click detailed information is available for all Subscribers in the Topology view. Click on any Subscriber icon to get a view of the following real time information: Type of Subscriber - model and revision, location including address and longitude and latitude, current faults if any including CID codes, Most Recent Route, Most Used Route, number of repeat dependent Subscribers and number of generated messages over last 10 days, Subscriber Program Settings, and a 10 day event history including CID codes.

One-click information is also available on any of the RF paths between Subscribers and IP Links illustrated on the map. Click on a line representing an RF path to create a pop up box with the details of that particular RF Link that includes the distance of the link and ID of the beginning and end nodes of the link.

User can access the details of any RF path on the network

The components of the network detailed on the interactive map can be modified using the Google Earth Summary. Expanding the check boxes below the **Topology** view enables users to select, and limit if needed, the Subscribers and IP Links that are displayed on the map based on Subscriber type and Subscriber model.

Topology View - Google Earth Summary



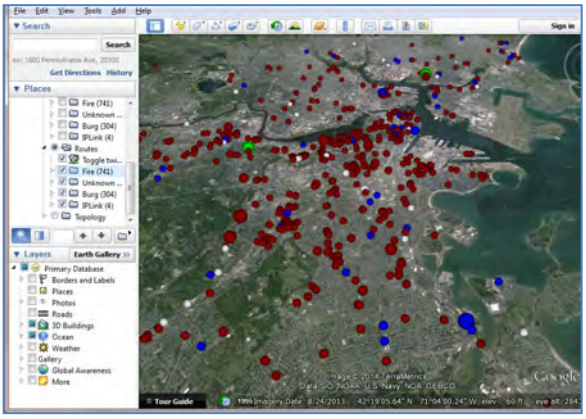
Users can select Subscribers to view by type and model

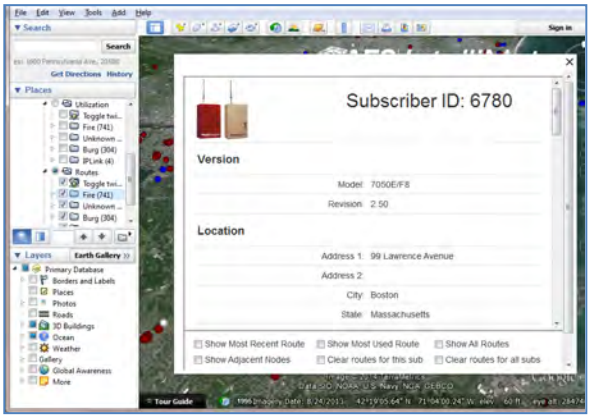
The value of the **Topology** view is that it is a powerful tool for planning network growth - detailing optimal locations for new Subscribers and the basis for planning expansion into new geographies.

7.9 Routes View

This view provides an interactive satellite map that enables users to view the historical RF paths, or routes, between Subscribers and other Subscribers, and Subscribers and IP Links over the past 10 day period. It shows route

information on the map that includes most recent route, most used route, as well as details on adjacent nodes and peers. To access the Routes view, double click on **Routes** in the Google Earth Summary.

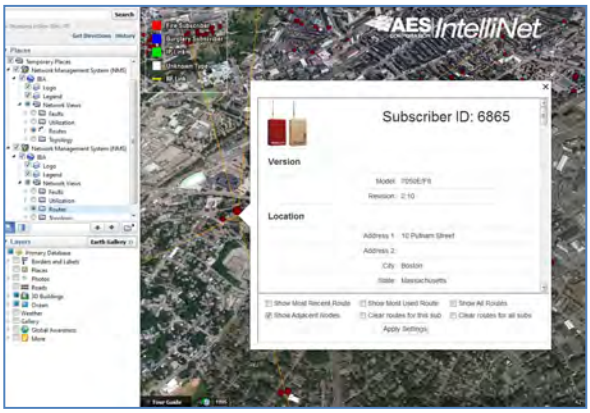




Routes View - Users can access historical RF path information for any Subscriber

One-click detailed information is available for all Subscribers in the Routes view. Click on any Subscriber icon to enable interactive access to route information. Use the check boxes at the bottom to generate specific route information on the map. This information includes most recent route, most used route, all routes used, and to identify adjacent nodes. Below is an example of detailed information generated in Visualization to identify the adjacent nodes for a Subscriber on the network.

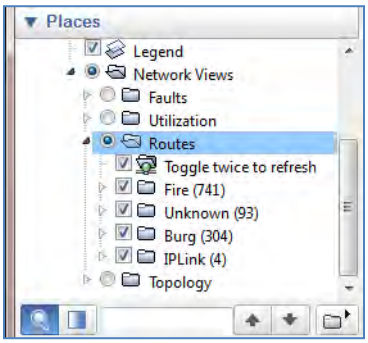
Routes View - Identifying Adjacent Nodes



Click on **Show Adjacent Nodes** and then click **Apply Settings** to illustrate on map all other Subscribers with which this Subscriber has exchanged RF communication in the past 10 days. One-click information is available for the RF paths illustrated on the map. Click on a line representing an RF path to create a pop up box (see above) with the details of that particular RF Link that includes the distance of the link and ID of the beginning and end nodes. You can perform the same request on any IP Link as well and see all Subscribers that have exchanged RF communication in the past 10 days with that IP Link.

The components of the network detailed on the interactive map can be modified using the Google Earth Summary. Expanding the check boxes below the **Routes** view enables users to select, and limit if needed, the Subscribers that are displayed based on Subscriber type and Subscriber model.

Routes View - Google Earth Summary

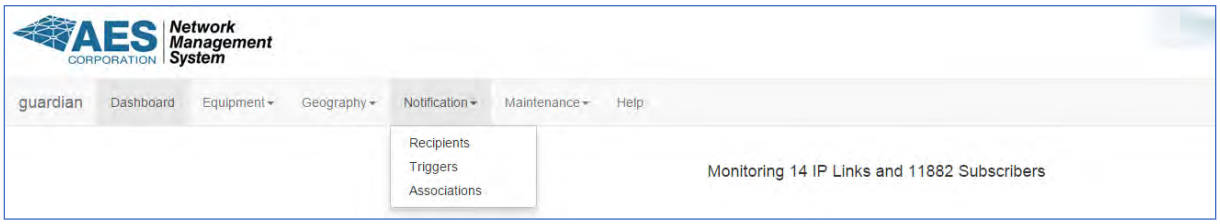


Users can select Subscribers to view on the interactive map by type and model

8 Notification

8.1 Notification Set-up

The Notification function enables users to monitor their *IntelliNet* network from anyplace at any time. Through the *Operator Dashboard*, users can configure automatic alerts based on a change to the *Network Health Score* or a fault with any Subscriber or IP Links. Separate drop down menus enable the user to easily create the list of personnel to be notified by both SMS and email, define the fault criteria to be reported, and create associations between the alert triggers and personnel to optimize response.



Set up Notifications

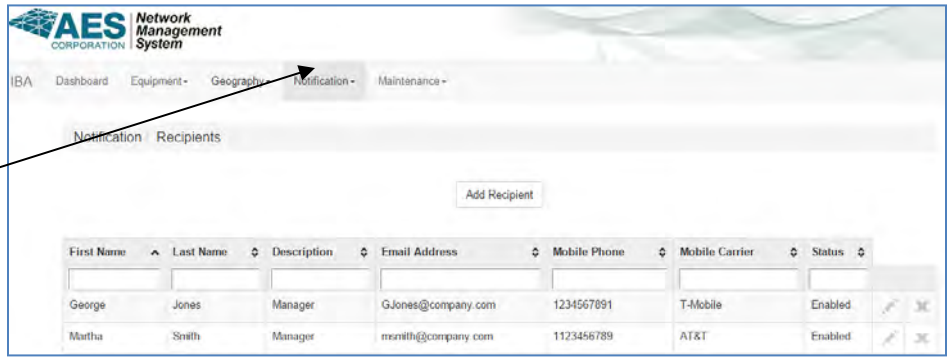
In order to set up and manage the Notification function, click on **Notification** and then on each of the following sections:

- **Recipients** - To identify personnel that receive one or more alerts
- **Triggers** - To define network events from which to generate alerts
- **Associations** - To map personnel or recipients to trigger events

8.2 Recipients

To add personnel to the alert list or to edit information about an existing Recipients, change the status of a Recipient, or delete a Recipient, click on **Notification** > **Recipients** to launch the screen below.

Click on
Notifications > **Recipients**



Recipient View

To edit an existing Recipient, click on the pencil icon to bring up the Edit Recipient screen. In this screen you can also change the status of a Recipient from Enabled to Disabled. SEE NEXT PAGE.

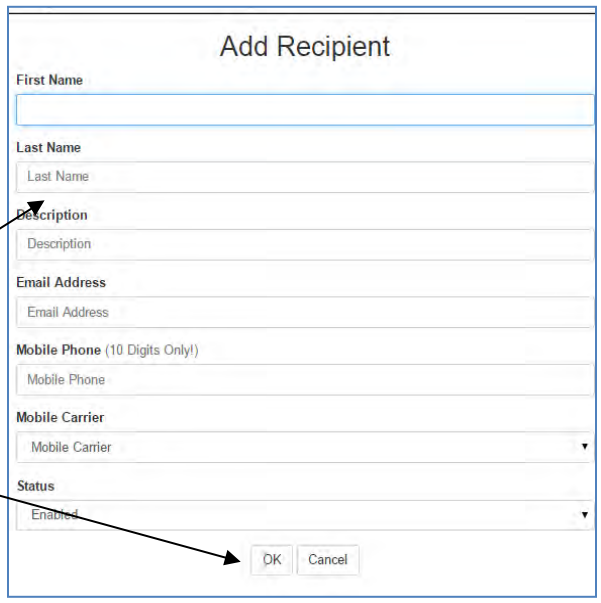
To delete a Recipient, click on the X icon to the far right. You will be asked to CONFIRM that you want to delete the Recipient.

To add a new Recipient, click on **Add Recipient** button at top. SEE NEXT PAGE.

To add a new Recipient, click on **Add Recipient** button at top of Recipient view

Input contact information including email address and mobile phone number

Click **OK** to complete and save the Recipient information**.**

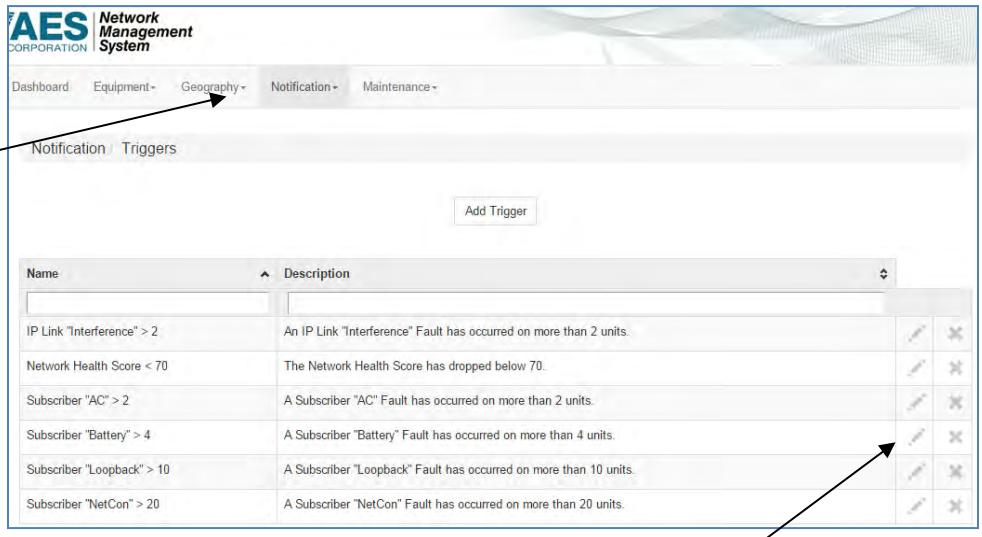


Add Recipient View

8.3 Triggers

To add a network events that will trigger an alert, click on **Notification >Triggers** to launch the Manager Triggers screen below - In this screen you can also edit or delete an existing Trigger.

Click on **Notifications > Triggers**



Manage Triggers Screen

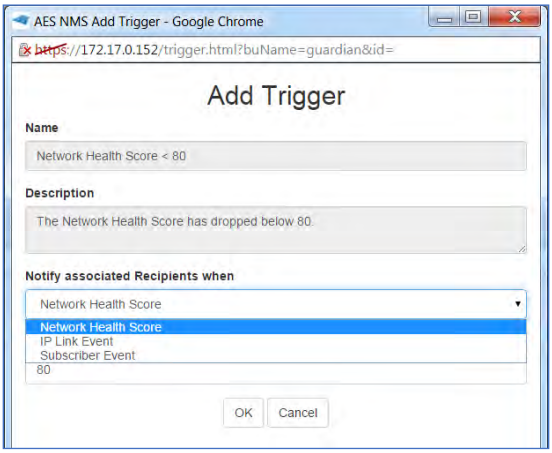
To edit an existing Trigger, click on the pencil icon to bring up the Edit Trigger screen.

To delete a Trigger, click on the X icon to the far right. You will be asked to CONFIRM that you want to delete the Trigger.

To add a new Trigger, click on **Add Trigger** button at top of Manage Triggers Screen

There are three criteria for triggers - see below.

Click **OK**
to complete and save the Trigger information**.**



Add Trigger View

There are three criteria for each alert Trigger event defined.

- Fault source - there are 3 possible fault sources - (1) a reduction in the Network Health Score below a set score, (2) an IP Link Fault, and (3) Subscriber Fault
- Fault type - These are defined in the drop down lists for Subscriber Fault and IP Link Fault
- Minimum events needed to alert - the number of occurrences requires to send the alert

Input your selections from the three criteria above then click **OK** to complete and save the Trigger**.**

8.4 Associations

To map Recipients to Triggers, click on **Notification** > **Associations** to launch the screen(s) below - In these screens you can view list of recipients and associated Triggers or a list of Triggers and associated Recipients depending which 'view by' box is checked at the top of the screen.

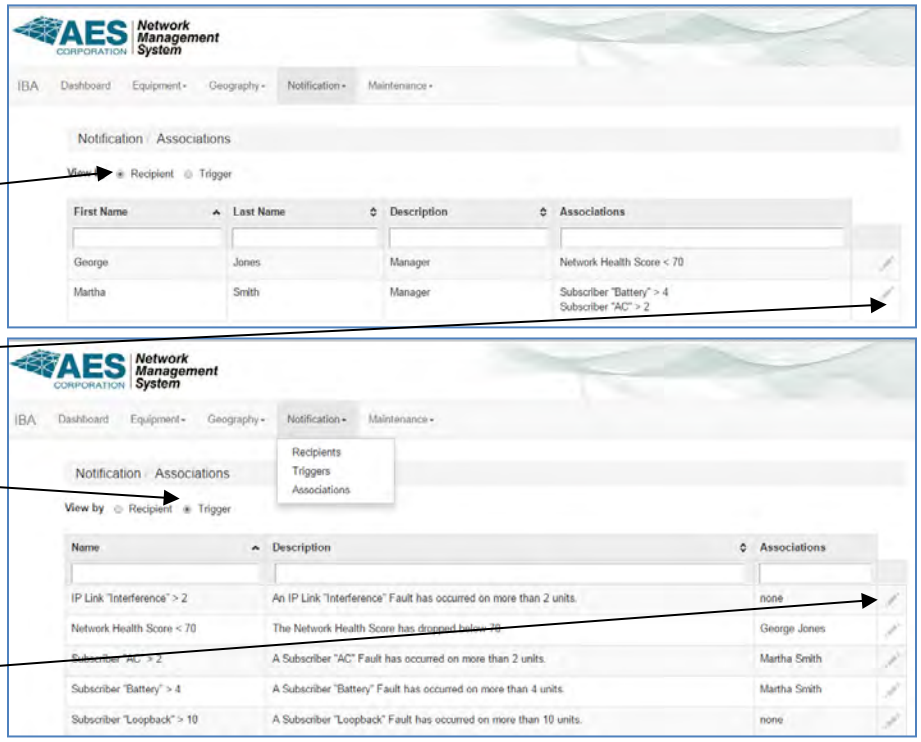
Click on **Notification** > **Associations**

Sorted by Recipients and associated Triggers

To add or edit an association
Click on the pencil icon

Sorted by Triggers and associated Recipients

To add or edit an association
Click on the pencil icon

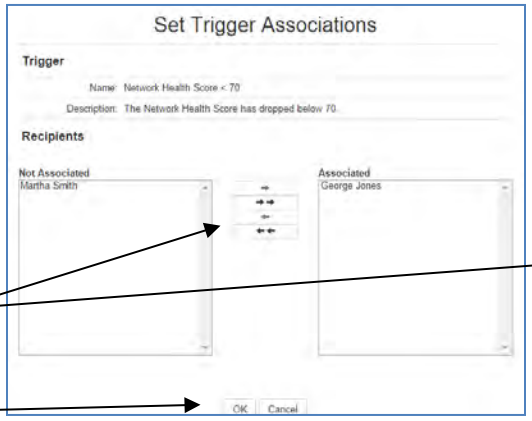


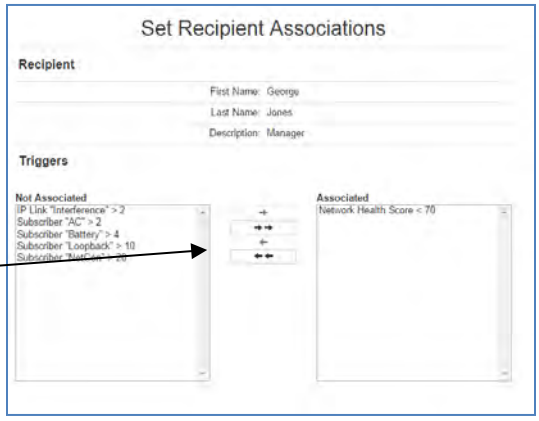
To set a new Association or edit an existing Association, click on the pencil icon on the right of the grid. See screens below. Use arrows as needed to manage Associations and click on **OK** to save.

Set a new or edit an existing Association

Use arrows to adjust Associations

Click **OK**





NOTE: If a notification has been already sent out to existing recipients, all new recipients added after this notification will not receive notifications until the status of the associated triggers drops below the threshold. Only after the trigger status is below the threshold will the new and existing recipients receive notifications when the threshold is surpassed. If a threshold condition remains the same or increased, the next notification will be sent after 24 hours.

9 Revision History

Revision	Date	Notes
1	3/16/2018	Initial document
2	1/24/2020	Update server specification information
2a	5/25/2022	Power consumption detail added
2b	11/18/2022	Added New Appliance and Spec & Changed NMS Photo of backplate

10 Warranty

OWNER WARRANTY - AES CORPORATION
LIMITED PRODUCT WARRANTY AND TECHNOLOGY LICENSE

LIMITED PRODUCT WARRANTY:

AES warrants to the original purchaser that the AES Subscriber Unit will be free from defects in material and workmanship under normal use and service for three (3) years from the date of original purchaser's purchase. Except as required by law, this Limited Warranty is only made to the original purchaser and may not be transferred to any third party.

This Limited Product Warranty is made in lieu of any other warranties, expressed or implied, it being understood that all other warranties, expressed or implied, including of merchantability or fitness for a particular purpose, are hereby expressly excluded.

AES assumes no liability for any personal injury, property damage, consequential damages, or any other loss or damage due, among other things, to this product's failure to operate or provide adequate warning. AES's sole responsibility is to repair or replace, at AES's sole option, the AES product that is judged defected by AES during the limited warranty period under the terms of its Limited Warranty.

TECHNOLOGY LICENSE:

Certain AES Products include software, protocols and other proprietary and confidential technology and trade secrets of AES which are incorporated in or provided with AES Products solely for use in conjunction with and in order to operate AES Products (“Licensed Technology”). AES grants the original purchaser a non-exclusive license to use such Licensed Technology solely in connection with the use and operation of AES Products and for no other purpose or use whatsoever. No title or ownership in or to any such Licensed Technology is conveyed by the sale or delivery of any AES Products; all such rights are retained by AES.

AES SERVICE PROCEDURE: Contact AES by Phone (978) 535-7310, Fax (978) 535-7313 or Email service@aes-intellinet.com, to receive a Return Material Authorization Number. Have the AES part number and serial number ready. Repack equipment in original or equivalent packaging. Inside the box, please include a contact name, telephone number, address and a brief description of the reason for return.

Ship items freight-prepaid to:

Repair Services, RMA#_____
AES Corporation,
285 Newbury Street
Peabody, MA 01960 USA

(Contact AES for Return Material Authorization number)