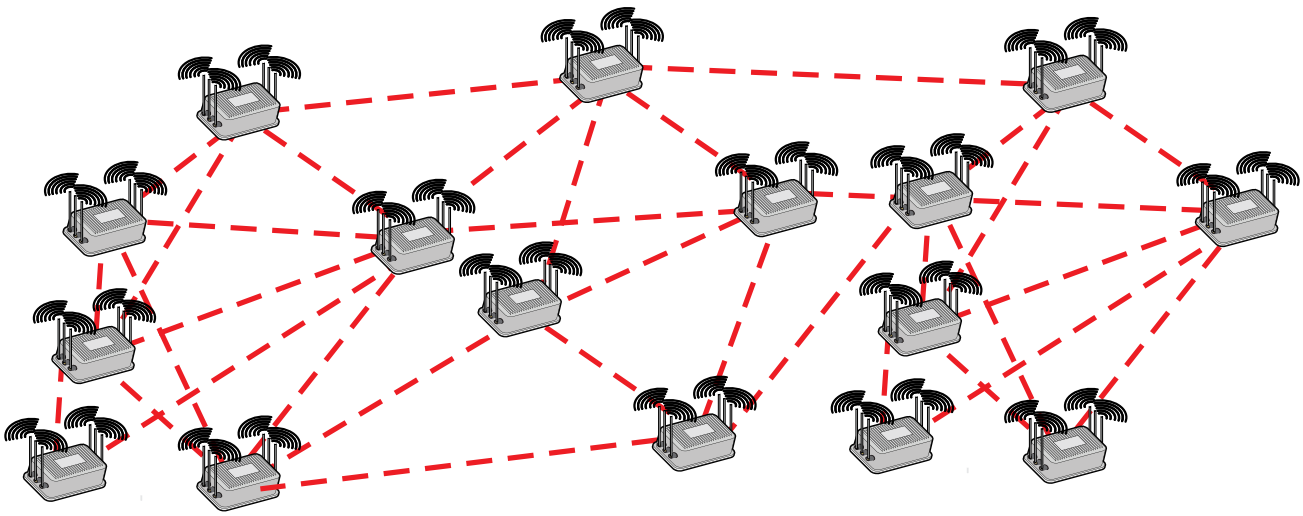
Reference Guide

Aclara 5900™ Software Operation

Software Version 0.1.3.7



Manual Version 1.0draft2. Release Date 2012-02-13. Please refer to the Firetide web site, www.firetide.com, for current versions.

Contents

List of Figures

1 Introduction

Aclara's STAR Network system is a meter reading solution that delivers comprehensive usage information through a secure, long-range wireless network. A portion of that network is implement using Firetide's patented AutoMesh™ wireless Ethernet system.

STAR Network Components

The STAR Network Meter Transmission Units (MTUs) are small, permanently sealed modules that are connected to water meters or are integrated into electric and gas meters. MTUs read the meter and forward the meter data. These messages are received by one of several Data Collector Units that cover the service area.

STAR Network Data Collector Units (DCUs) are intelligent network devices that receive, process, and store meter reading information transmitted from STAR Network MTUs. The DCUs forward this information to the STAR Network Control Computer (NCC) located at the utility. DCUs connect to the NCC by a variety of backhaul communication networks, including fiber optic, WiFi, and cellular. The WiFi method is implemented with products based on Firetide's technology, and engineered to meet the specific requirements of Aclara.

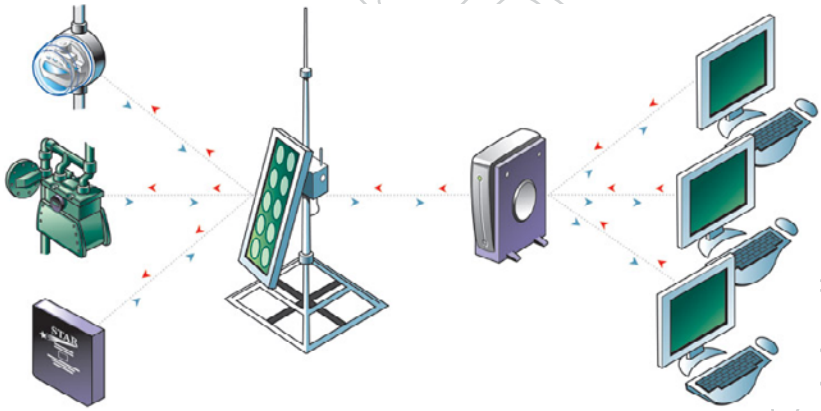


Figure 1.1 The Aclara STAR Network

The STAR Network Control Computer (NCC) collects, validates, processes, and stores data transmitted by the STAR Network DCUs. .

Note

This equipment emits RF energy and has received regulatory approval in its country of origin.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Please refer to the appendix for additional regulatory information.

Aclara 5900 Series units use Firetide's AutoMesh WiFi technology. Firetide's HotView Pro Network Management System is the control platform for these units. The version of HotView Pro you are using has been tailored to the requirements of Aclara's STAR system.

"Command Summary" on page 7 provides a summary of the commands available in HotView Pro, with a brief description of their function and purpose. Further information on the more complex commands may be found in later chapters.

2 HotView Pro Command Summary

This version of HotView Pro is tailored to the requirements of Aclara's STAR system. It is focussed on the 5900 family of products, but also shows other HotPort mesh nodes in some examples.

This chapter provides a summary of the commands available in HotView Pro, with a brief description of their function and purpose. Further information on the more complex commands may be found in later chapters.

Launching HotView Pro

The software is started via the desktop shortcut created by the installation process, shown in Figure 1.2. If this icon is not visible, the launcher application can be accessed via the Windows Start menu.

FIGURE 1.2 LAUNCHER ICON

Double-click to launch the software. Your version number may be different.

If you plan to connect to an already-deployed mesh, single-click on the client application icon in the launcher window, and enter the IP address of the server.

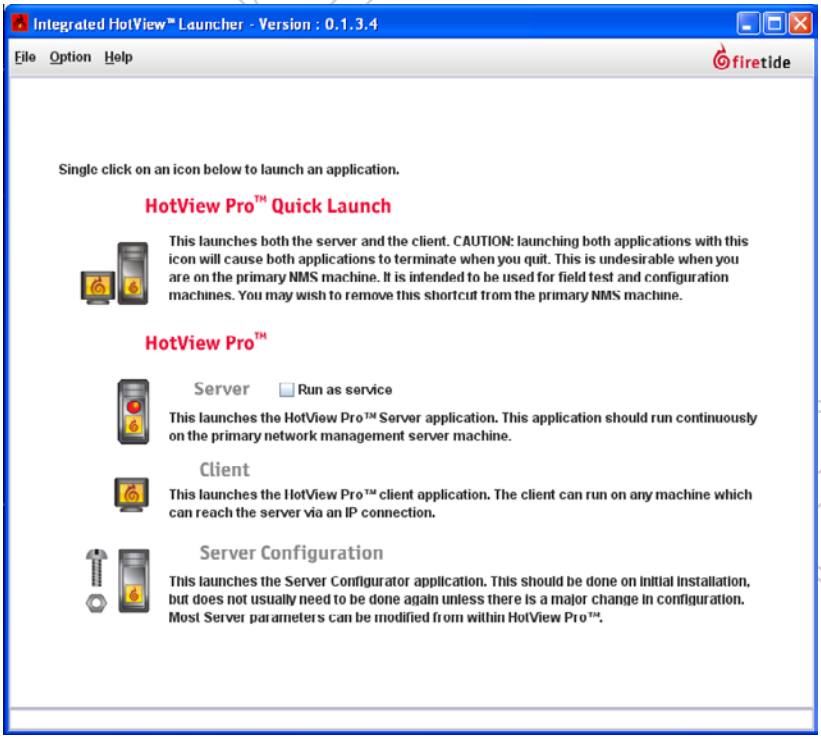


FIGURE 1.3 LAUNCHER WINDOW

Quick Launch is used in test and debug environments. It launches both the server application and the client application; when the client application is closed; the server application terminates.

The **Server** icon launches the server application; it will remain running until it is manually terminated. If the 'LED' is red, the server is not running; if it is green, the server is running.

The **Client** icon launches the client application.

Server Configuration is used for initial server setup, and also to manage users and other system-wide settings.

If you plan to test and configure units on the bench, use the quick launch icon. However, do not do this unless you are sure there is not another copy of the server application managing the mesh. A mesh cannot be managed by two different server applications simultaneously.

Figure 1.4 Initial Screen

When connecting for the first time, you will see a screen similar this. No mesh is visible because the server does not yet know which meshes to manage.

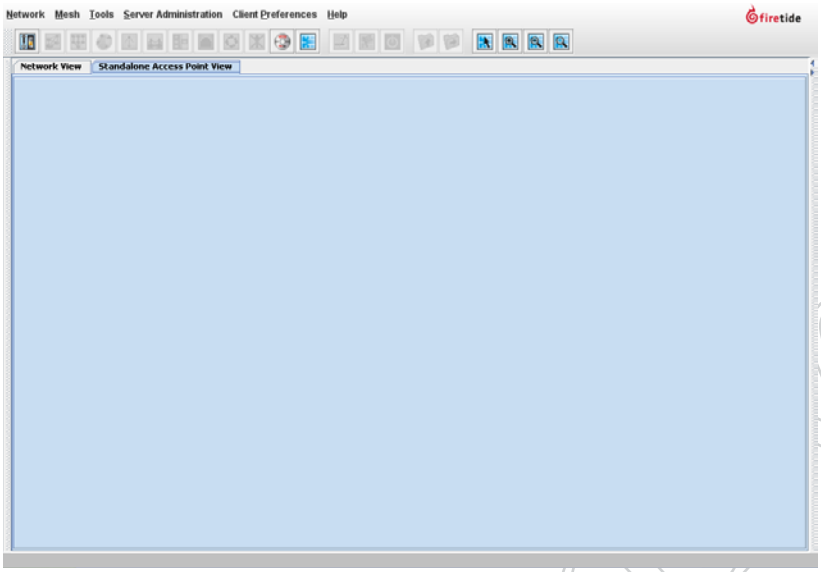


Figure 1.5 Adding a Mesh

To add a mesh, click on the mesh menu and select the Add Mesh command. Enter the mesh IP address. The default is 192.168.224.150. Enter the password. The default is firetide.

After about 30 seconds, the mesh should appear. If it does not, insure that the HotView Pro system is wired to a node on the mesh, and that you can 'ping' the mesh at its IP address.

You must use a wired connection to connect to the mesh; you cannot connect wirelessly.

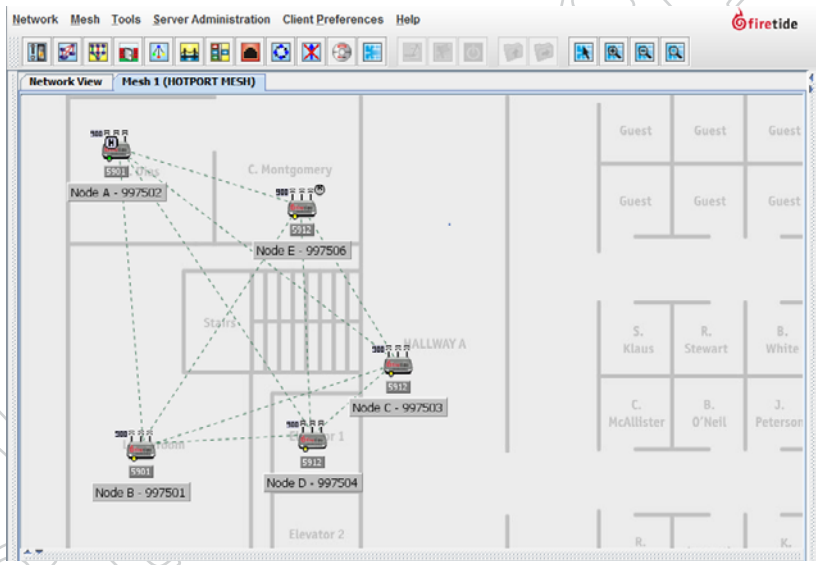


Figure 1.6 Menu Commands

The menu commands are at the top of the screen. Shortcut icons for many commands appear just below the menu commands

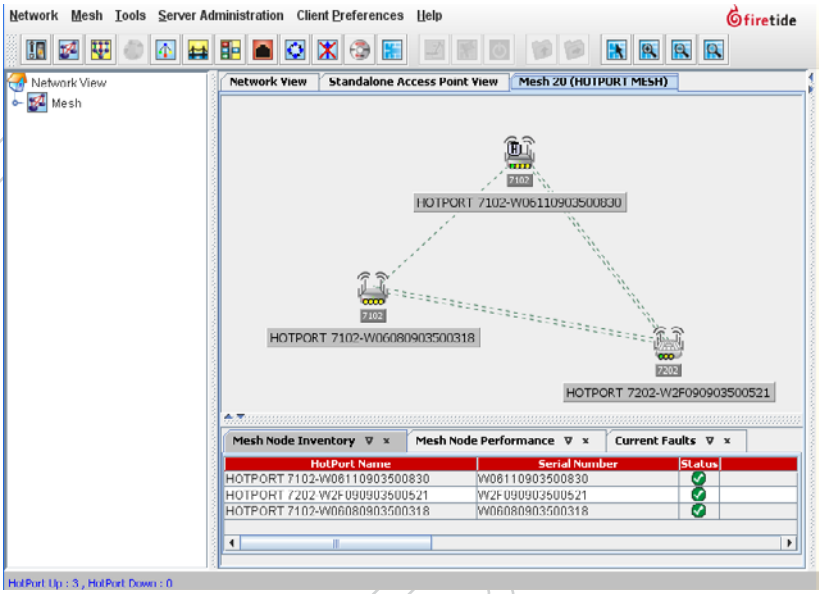
The menu commands are:

- Network: Used for certain network-wide functions, such as firmware upgrades.
- Mesh: Has most of the commands needed for mesh configuration and management.
- Tools: Provides certain tools for configuration and troubleshooting.
- Server Admin: Provides tools for configuring HotView Pro.
- Client Prefs: Affects the screen view.

These menu commands will be explained in more detail in the sections that follow.

Understand the Basic Screen Layout

The HotView Pro screen layout varies according to settings. It can look like Figure 1.4, the default view; Figure 1.5, the default view after adding a mesh; or Figure 1.7, a typically-customized view. This customized view has enabled the Explorer option, on the left of the screen. Along the bottom is the Inventory window. At the very bottom is the status bar.



The menu bar includes numerous shortcut icons; at the far right are ones for zooming in and out.

The nodes are in the central area, along with the background image of the topography of the mesh installation. Just above them are multiple tabs; a network view tab, one for access points, and as many mesh tabs as there are meshes. These tabs can be right-clicked to access certain commands.

Of particular interest is the **Logout of Mesh** command. This is the opposite of the **Add Mesh** command, and instructs HotView Pro to stop managing that particular mesh.

HotView Pro is a multi-user system. Write-access control commands are available via the mesh tab.

FIGURE 1.7 TYPICAL SCREEN IMAGE

This shows a typical screen view for a simple three-node mesh

FIGURE 1.9 NODE ICONS

A 7000-900 is shown on the left; a 5900 on the right.

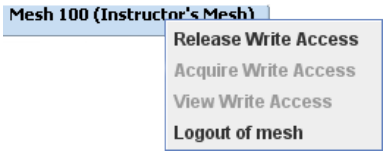


FIGURE 1.8 MESH TAB COMMANDS

Right-clicking on the mesh tab lets you log out of the mesh. It also controls which user has write access to that mesh.

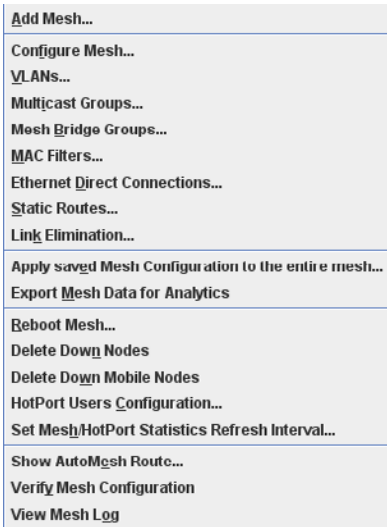


FIGURE 1.10 MESH MENU

This menu contains most of the commands you will need for configuring and managing a mesh. These commands can also be accessed by right-clicking on the mesh area of the display.

Mesh Menu Commands

Add Mesh causes HotView Pro to begin managing the mesh. The program will record performance and events until the mesh is explicitly removed from management control.

Configure Mesh displays a separate window which contains all of the key mesh configuration commands. This is described in more detail in Figure 1.13 and following sections.

VLANs allows you to configure VLANs, VLAN trunks, and hybrid VLANs.

Multicast Groups allow you to define and control IP multicast traffic.

Mesh Bridges are connections between meshes. The Mesh Bridge Group command creates these connections.

MAC Filters allow you to limit mesh access to a defined list of MAC addresses. Warning: careless use of this tool can lock you out of the mesh.

Ethernet Direct Connections are wired connections within a mesh. They are an efficient way to connect nodes which are relatively close, but not necessarily within radio range.

Static Routes can be used to steer traffic within the mesh. In most cases it is better to let the AutoMesh™ protocol make path decisions, but there are exceptions.

Link Elimination is used to force the mesh to ignore weak, marginal links that sometimes spring up, unplanned, between nodes.

Apply Saved Mesh Configuration to the Entire Mesh is used to apply a previously-saved configuration file to an entire group of nodes. (The configuration file is created from an individual node; the command can be found in the node-specific command section.)

Export Mesh Data for Analytics exports certain mesh performance data in an Excel-compatible format.

Reboot Mesh causes all nodes on the mesh to reboot, but does not affect any settings.

Delete Down Nodes (and Delete Down Mobile Nodes) removes 'old' nodes from HotView Pro's database of known hardware. The software normally remembers all hardware and reports it as down; this command overrides that.

HotPort Users Configuration lets you define and limit certain types of Telnet and SSH access to the individual nodes.

Set Mesh/HotPort Statistics Refresh Interval lets you define how often statistics are collection. The shortest interval is 300 seconds.

Show AutoMesh Route lets you examine the mesh's choices for traffic flows within the mesh.

Verify Mesh Configuration compares the mesh-wide settings on all nodes.

View Mesh Log displays a log of mesh events. It is searchable and filterable.

DCU Communication Configuration

The DCU Communication Configuration command is accessed by right-clicking in the mesh area of HotView Pro, NOT on any node. This brings up all mesh commands, plus the DCU-specific command.

The DCU expects to be able to communicate with the STAR Network Communications Controller. The Firetide mesh node acts as a proxy for the STAR NCC, and so it needs to know the IP addresses being used by that particular deployment. In some deployments, the DCU already knows the IP address, so the mesh can simply auto-detect it. In other cases, you must program the IP address yourself.

Other deployments use a domain name instead of an IP address. You should specify the address for a primary and secondary DNS. (Note that 8.8.8.8 and 4.4.4.4 are well-known DNS servers maintained by Google, and can be used if another DNS server is not available.)

You must also specify the exit node. In all cases, be sure to check the **Enable DCU Communication** checkbox. It can be turned off for certain debug operations, but should normally be on.

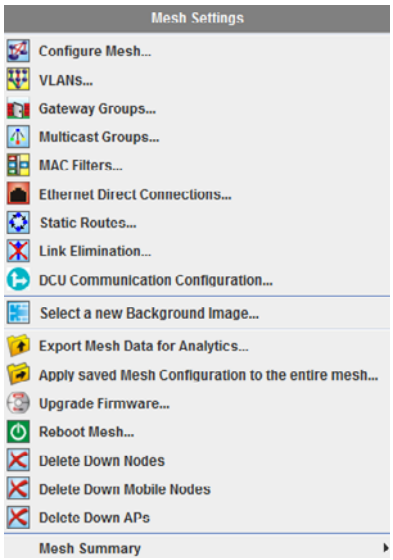
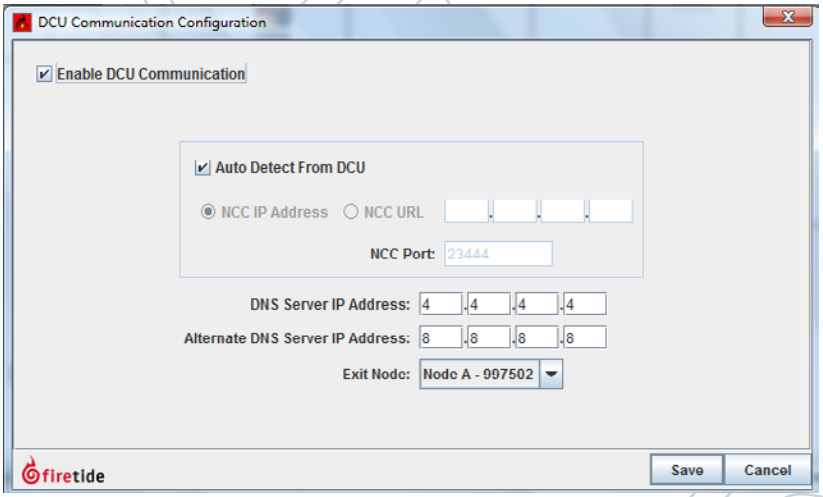


Figure 1.11 Right-Click Mesh Menu

This menu can be accessed by right-clicking on the mesh area of the display.



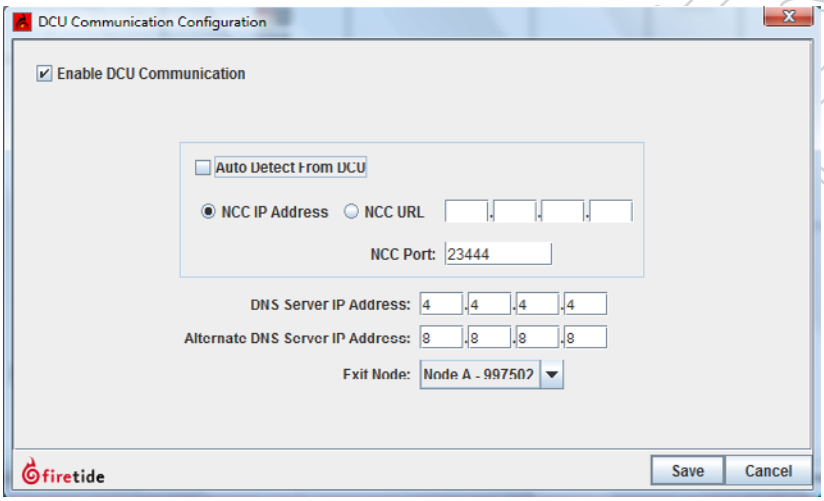


Figure 1.12 DCU Communication Configuration - Auto Detect vs Manual

In Auto-Detect mode, the system will detect and use as many IP addresses as the various DCUs might supply.

In Manual mode, you must supply a single IP address.

Mesh Configuration

Mesh configuration is the heart of overall mesh design. Mesh configuration includes network, wireless, security, and other key settings. There are five tabs:

- Network — This tab sets the IP address and related information, and allows you to specify a human-readable mesh name.
- Wireless — This tab controls most aspects of radio behavior. (Certain radio parameters, such as transmit power, are set on a per-node basis.)
- Security — This tab controls the encryption type and keys.
- User Accounts are the login credential used by the HotView Pro server to access the mesh. These are NOT human logins.
- Advanced — The advanced tab contains a number of configuration and tuning options for meshwide operation.

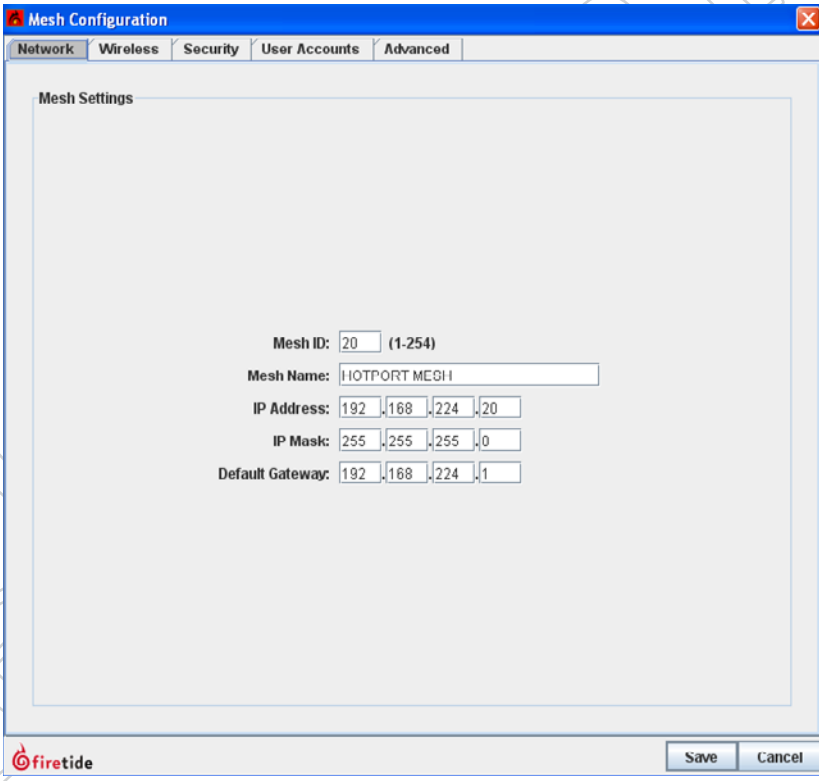
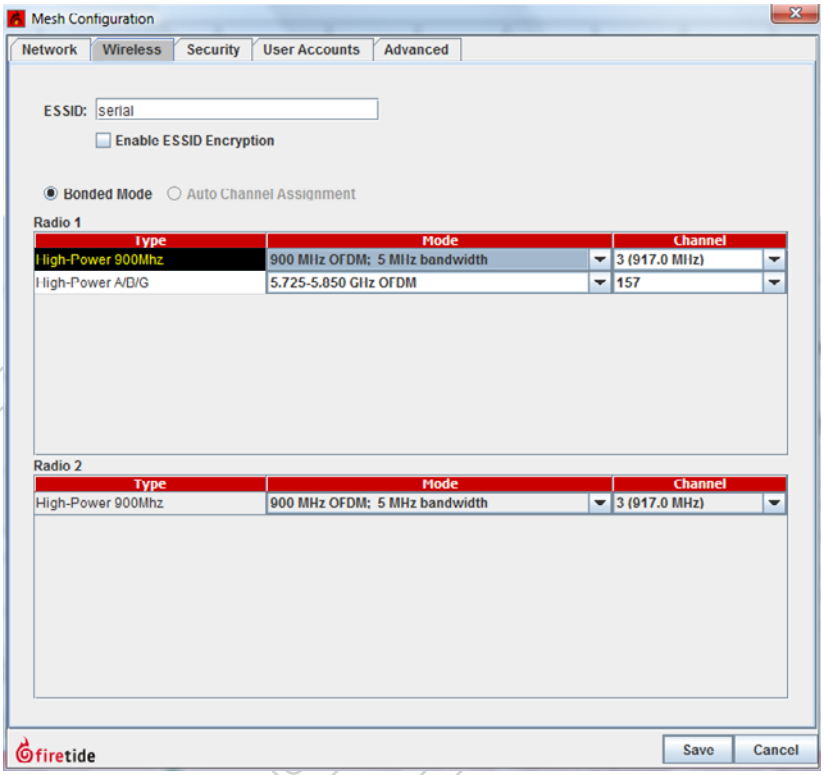


Figure 1.13 Mesh Configuration

The Mesh Configuration window has five tabs, each of which affects a different aspect of basic mesh configuration.

The Network tab allows you to assign a unique ID number for the mesh. The default is 1, legal values are 1-254. It also allows you to configure the management IP address. This can be anything.



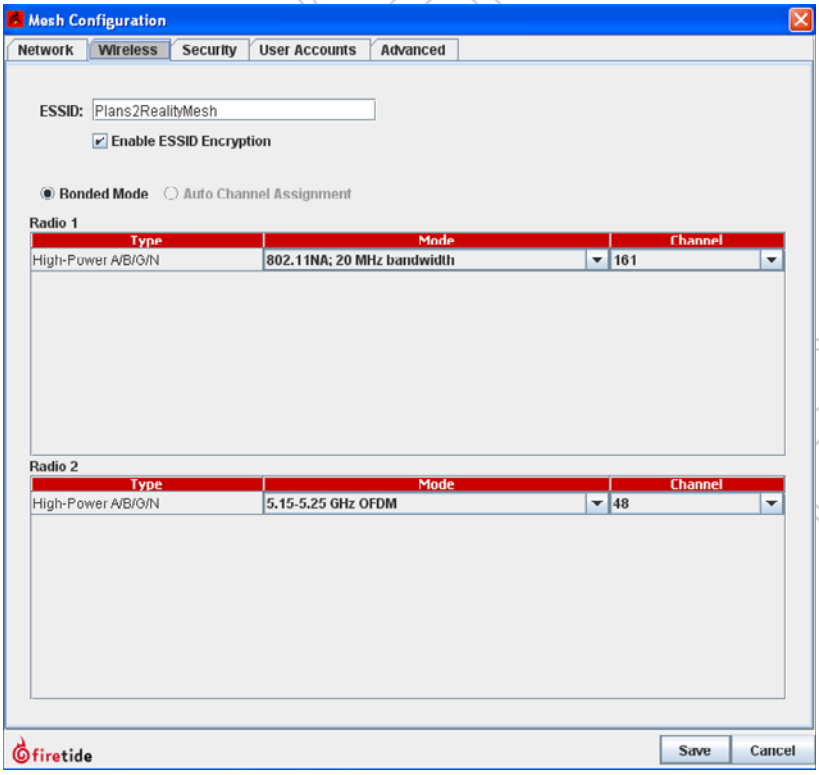


Figure 1.14 Wireless Settings

The Wireless tab lets you define (and encrypt) the ESSID. More importantly, it lets you set mesh-wide radio channels for all Radio 1 units in each node, and all Radio 2 units in each node. (Note: "Bonded" refers to the fact that all Radio 1 units will be tied together on one channel, and all Radio 2 units tied together on a second channel. It does NOT mean that Radio 1 and Radio 2 are tied together. The two radios ALWAYS operate independently.

Single-radio 5900 nodes have a 900 MHz radio for Radio 1. Dual-radio nodes place a 2.4/5 GHz node in the Radio 1 slot, and a 900 MHz radio in the radio 2 slot.

Thus,depending on the node type, Radio 1 can be a 900 MHz unit or a 2/4/5 GHz unit. This is why both frequency ranges are shown for Radio 1

For each radio, the Mode drop-down allows you to select frequency bands and operating modes (a/b/g/n). The choices available will vary with the node configuration - one radio or two, MIMO (802.11n) or non-MIMO, and 900 MHz.

The channel drop-down lets you select from the channels available within the chosen band.

The lower screen shows the wireless options for 2.4/% GHz radios.

Figure 1.15 Security

The Security tab lets you enable AES security on the RF links. This is implemented in hardware and does not impose a performance penalty. Its use is recommended.

End-to-End security provides a second layer of encryption, but imposes a small throughput penalty, about 15%.

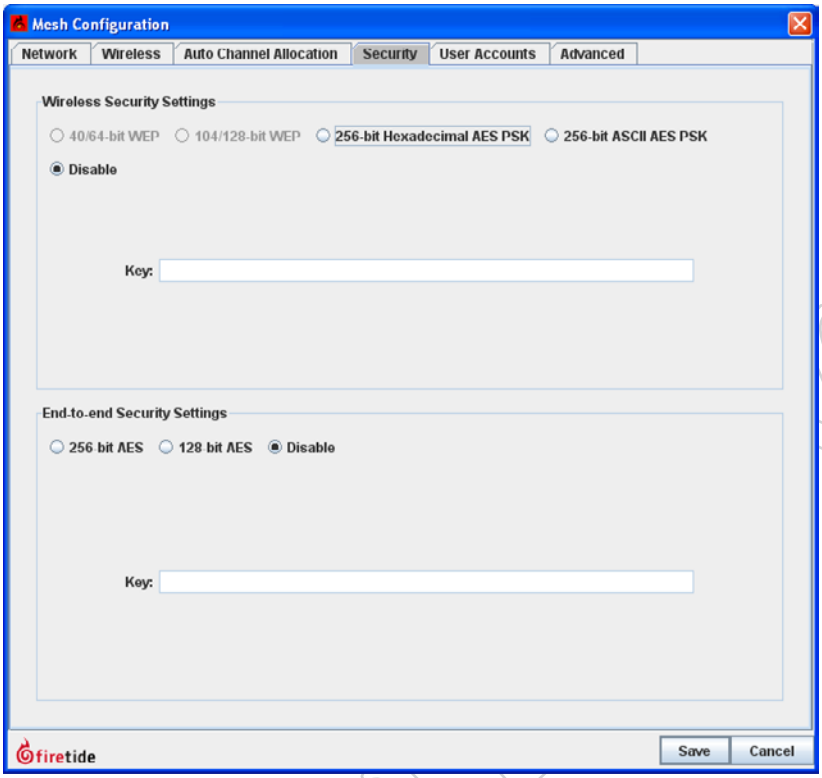


Figure 1.16 Advanced Tab

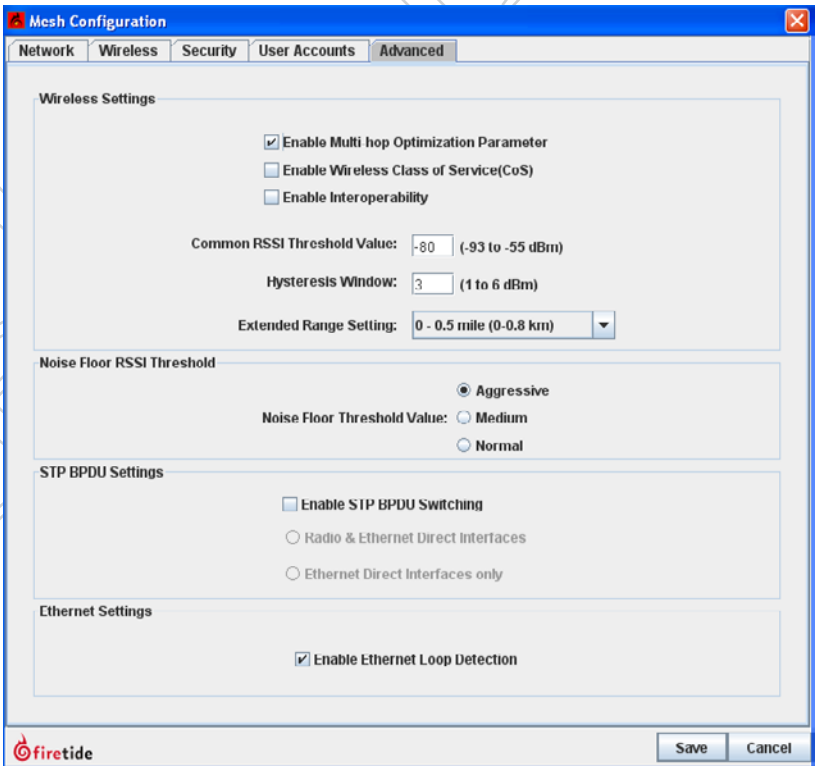
The Advanced tab controls several key features.

Multi-hop Optimization should be turned on for all meshes with more than two nodes.

Wireless Class-of-Service should be turned on if you plan to support either 802.1p or port-based traffic prioritization.

The RSSI Threshold Value and Hysteresis Window values can be used to keep weak links from “flapping” on and off, impacting mesh performance.

Ethernet Loop Detection is on by default. It can be disabled, but do not do so unless there is a good reason.



Node Commands

Rename HotPort lets you assign a name to each node for management purposes. This name can be up to 32 characters long. It is for the benefit of network managers; the software is not affected by this entry.

HotPort Location lets you enter a 256-character string describing the location of the node. You can also enter the latitude, longitude, and elevation of the node. This is used by the antenna alignment tool to assist in alignment.

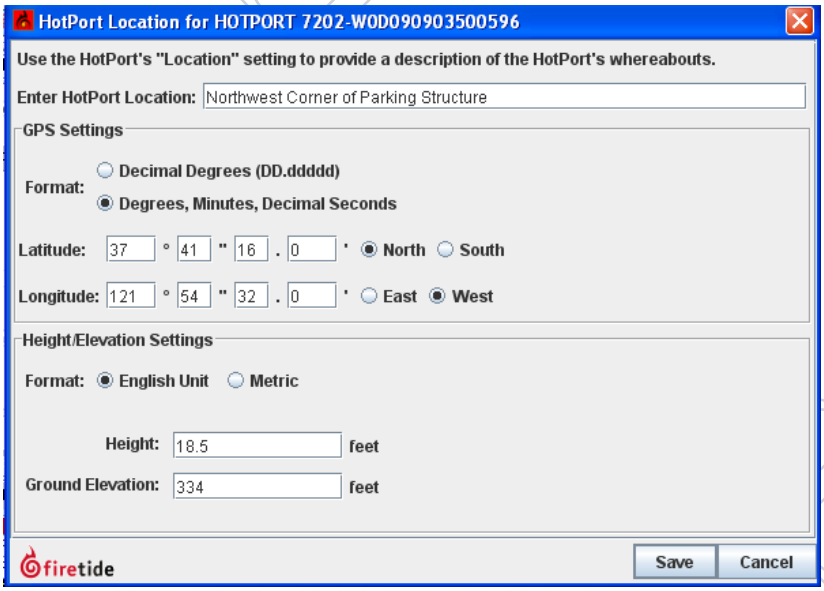
Radio Settings lets you over-ride mesh-wide radio settings, adjust transmit power, and other things. It is covered in more detail in Figure 1.19.

Node QoS allows you to define 802.1p and port-based traffic priority. This is described in more detail in Figure 1.20.

Configure Node Port has three sub-items in a flyout menu:

- **Port Configuration** lets you disable unused wired-Ethernet ports, for security. It also allows you to manually configure port speed and auto-sense.
- **Hybrid Trunk Configuration** is used as part of VLAN setup. Refer to the VLAN chapter for details.
- **VLAN ACL Configuration** is used as part of VLAN setup. Refer to the VLAN chapter for details.

Reboot HotPort reboots the node.



Backup and Restore Node Configuration allow you to make a backup file of a configured node, and then restore the node settings to the node.

NOTE: this is not a backup tool in the usual sense of the term. A backed-up node configuration CANNOT be applied to a different node. In other words, this command cannot be used to configure a node in order to replace a node that has failed in the field. A backed-up configuration file can only be applied to the same serial-number node from which it was extracted.

The file created by the Backup Node Configuration command is encrypted and is not human-readable.

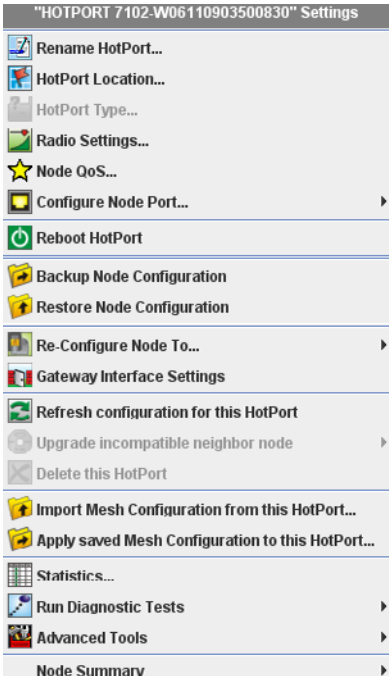


FIGURE 1.17 NODE-SPECIFIC

Node-specific commands can be accessed by right-clicking on a node.

FIGURE 1.18 LOCATION DIALOG WINDOW

Node-specific commands can be accessed by right-clicking on a node.

Re-Configure Node To... lets you re-define the operating mode of a node, to be either a normal node, a Gateway Server node, or a Gateway Server Controller node. Gateway Servers and Gateway Server Controllers are described in another chapter.

Gateway Interface Settings let you define the required parameters for nodes which are part of a Gateway Group. Gateway Groups are covered in another chapter.

Refresh Configuration for this HotPort node does just that.

Upgrade Incompatible Neighbor Node lets you upgrade the firmware on a down-rev node. It is grayed out here because it is not applicable; there are no down-rev nodes.

Delete this HotPort lets you remove the node from the software database.

Import/Apply Mesh Configuration... lets you create a file on your PC that contains all of the mesh-wide settings. (E.g., it "imports" from the mesh to the PC.) This is commonly used to back up mesh settings, and to then apply them to new nodes so that they can join the mesh, using the Apply... command.

NOTE: the mesh configuration files contain only basic mesh parameters. They do NOT contain all aspects of system configuration. In particular they contain no node-specific information, such as node names, local radio settings, etc.

The mesh configuration files are written in XML, and can be viewed in a browser; however, they are rather cryptic.

Statistics, Run **Diagnostic Tests**, and **Advanced Tools** are described in another chapter.

Node Summary shows a summary of node settings.

Individual Radio Settings

The two radios in each node can be individually configured. While a mesh will generally work with uniform mesh-wide settings, in most mesh deployments better performance can be obtained by optimizing radio settings.

The individual radio settings are:

- Receive Path Gain - This setting calibrates the radar-detection function of the US FCC-mandate DFS feature. Refer to the chapter on DFS for details.
- Select Transmit Power - Lets you to reduce transmit power in cases where the receive strength (RSSI) at the link far end is too high. In general, RSSI values stronger than -20 dBm can cause receiver overload, which increases the error rate and therefore the number of re-transmissions required. The exact level at which the receiver overloads depends on the total amount of background noise, as well as radio-to-radio variation.
- Transmit Data Rate - The maximum raw over-the-air data rate at which the radio will attempt to operate; e.g. for 802.11a, 54 Mbps. Radios will automatically attempt to run at the highest speed, but will fall back, then re-negotiate a higher speed later. This adds jitter to a network. Limiting the maximum data rate to a lower value reduces jitter. Low data rate applications can be set to a lower speed here, which reduces the RSSI requirement and permits longer links or smaller antennas.
- Override Channel Assignment - refer to the chapter on channel assignment for details.
- Fragmentation Threshold - Noisy RF environments may benefit from a smaller packet size. The fragmentation size should be reduced if retransmissions are common and other possible causes are eliminated. This option is not available in 802.11n mode (as shown).

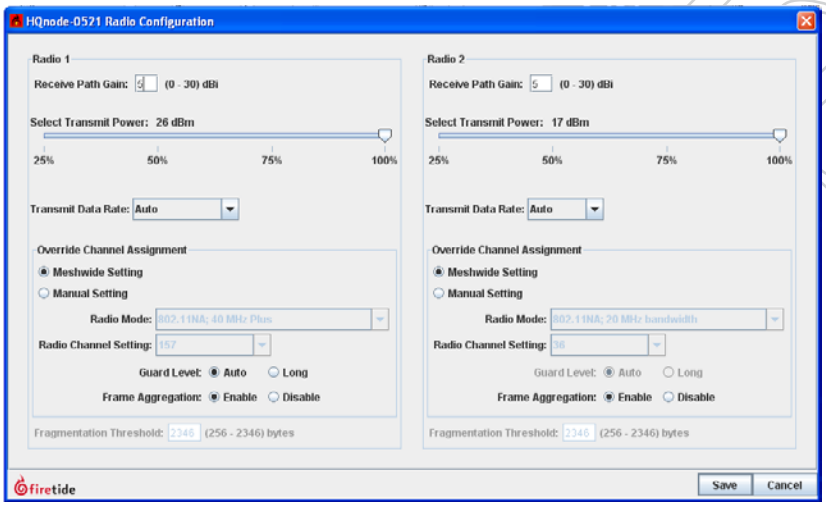


Figure 1.19 Node Radio Settings

The radios in each node can be configured individually.

Each radio's operating mode and channel can be changed from the mesh-wide defaults. This is commonly done in larger meshes to improve overall throughput.

Quality of Service

The Firetide mesh offers two Quality of Service (QoS) techniques.

- 802.1p - a standards-based method which lets you assign high, medium, or low priority to any of eight classes of traffic.
- Port-based QoS - in order to support equipment which does not implement 802.1p, priority can be assigned per port. Traffic entering the mesh on the specific port will be prioritized across the mesh based on the port's assigned priority.

Prioritization is applied to inbound traffic. If two pieces of equipment connected to the mesh need high priority assigned to traffic in both directions, both ports must be configured for high priority.

In video networks, it is common to set video traffic to medium or low priority, and other traffic to a higher priority, in order to ensure that the high volume of video traffic does not 'swamp' other traffic.

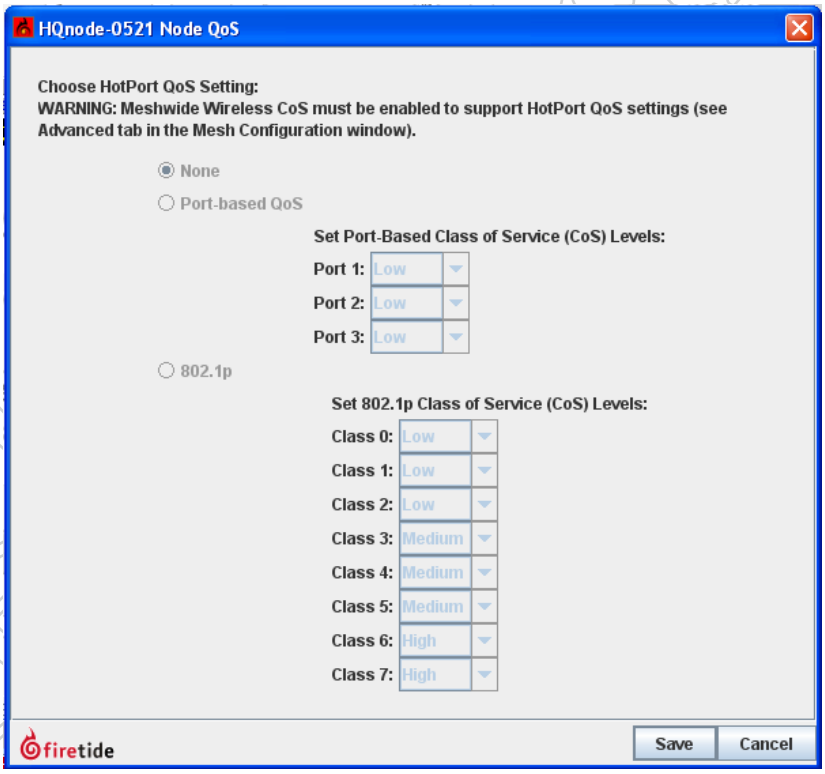


FIGURE 1.20 NODE QOS

Two types of QoS are offered. 802.1p QoS works with equipment that supports that protocol, but many devices do not. For devices that do not support 802.1p, you can set priority based on the port to which the device is connected. For example, you might place SCADA traffic, connected on port 1, to High Priority, and video traffic, connected on Port 2, to Medium Priority.

Client Preferences

Show All Links displays all of the active RF links in the mesh. For smaller meshes, this is the preferred setting, but for larger meshes, it can make the screen cluttered. In such cases, select the **Show Links Only**... or **Hide All Links** options.

Find HotPort lets you search for a node on the display. The found node will be highlighted.

Select New Background Image lets you replace the default image with a graphical representation of the area where the nodes are installed. Typically this is a floor plan or site map, represented as a bit-mapped file. You can also switch back to one of two default background images. You can turn the background image off altogether by unchecking the **Show Background Image** button.

Normally a node must be clicked on to select it. Enabling **Select HotPort automatically on mouse-over** does just that.

Show Information Bar opens a large section on the right side of the display. This new panel can be used to examine most settings and node settings.

Show Explorer Bar opens a pane on the left side of the screen. This provides a hierarchical view of all meshes, nodes, and other equipment.

Show Status Bar displays the small status bar at the very bottom of the display window.

Show Model Number displays the model number of each node under the node's icon.

Show HotPort IP Address reveals the hidden internal addresses the nodes use among themselves. These are not visible or accessible from outside the mesh, nor are they routable. They are used for certain internal tests only.

Show Selected HotPort Radio Info changes the display to show the Radio 1 and Radio 2 settings for each node when you click on the node. This is very useful in multi-channel mesh designs.

Show Mesh Configuration Conflicts checks the settings on each node to make sure they are in agreement.

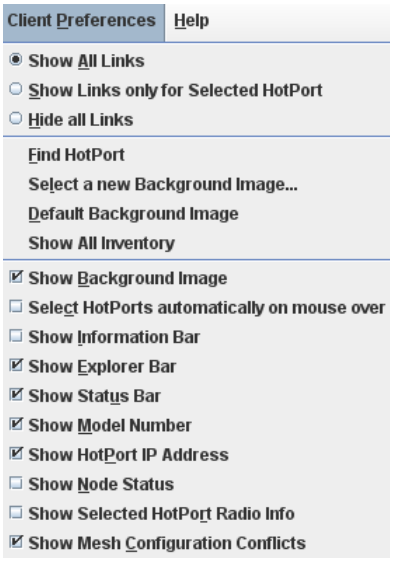


FIGURE 1.21 CLIENT PREFERENCES

The Client Preferences Menu lets you control the user interface.

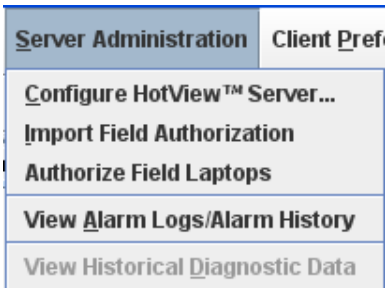


FIGURE 1.22 SERVER ADMINISTRATION MENU

These commands let you configure the server, and delegate management control.

It also lets you view alarms for all meshes under management.

Server Administration

Configure HotView Server lets you configure all aspects of server behavior. This is covered in more detail in “Server Configuration” on page 27.

Import Field Authorization and **Authorize Field Laptops** allow you to delegate licensed managed authority to another computer; typically a laptop.

View Alarm Logs/Alarm History lets you view all past alarms. Alarm configuration is defined in “Server Configuration - Alarm Management” on page 30.

3 Analyzing Performance

Aspects of Performance Analysis

The HotView Pro software system has several tools to assist in analyzing, troubleshooting, and optimizing system performance.

There are three basic aspects of performance analysis:

- RF signal quality
- Link throughput
- Reduction of link flap and other jitter sources

RF Signal Quality

The key element of RF signal quality is a good signal-to-noise ratio. Experience has shown that for 802.11a and 802.11g operating modes, a received signal strength indicator (RSSI) of -70 dBm is the absolute minimum strength required for reliable operation at full link speed. In RF-noisy environments, a stronger signal may be required. It is common practice to design links to achieve -50 dBm or better, to provide a reasonable fade margin.

For 802.11n, the RSSI must be -60 dBm or better. Links should be engineered to -40 dBm or better.

While it is unlikely to occur in the real world, extremely strong signals can over load the radio receivers. Avoid RSSI values in excess of -20 dBm.

RF signal quality is also affected by interference from other RF sources, and from incorrectly-configured meshes. These problems will show up as dropped packets and retries in the statistics panel.

Possible sources of interference include other devices, but also the other radio within the node. Dual-radio nodes should have antennas placed so that their radiation patterns do not overlap.

An incorrectly-set range parameter or multi-hop optimization can also cause collisions and dropped packets. Make sure multi-hop optimization is turned on for all meshes with more than two nodes.

Make sure the range setting is larger than the longest RF link in the mesh. If in doubt, set the range parameter larger than necessary to see if it solves the problem.

Both of these parameters are in the **Mesh Configuration** window, **Advanced** tab.

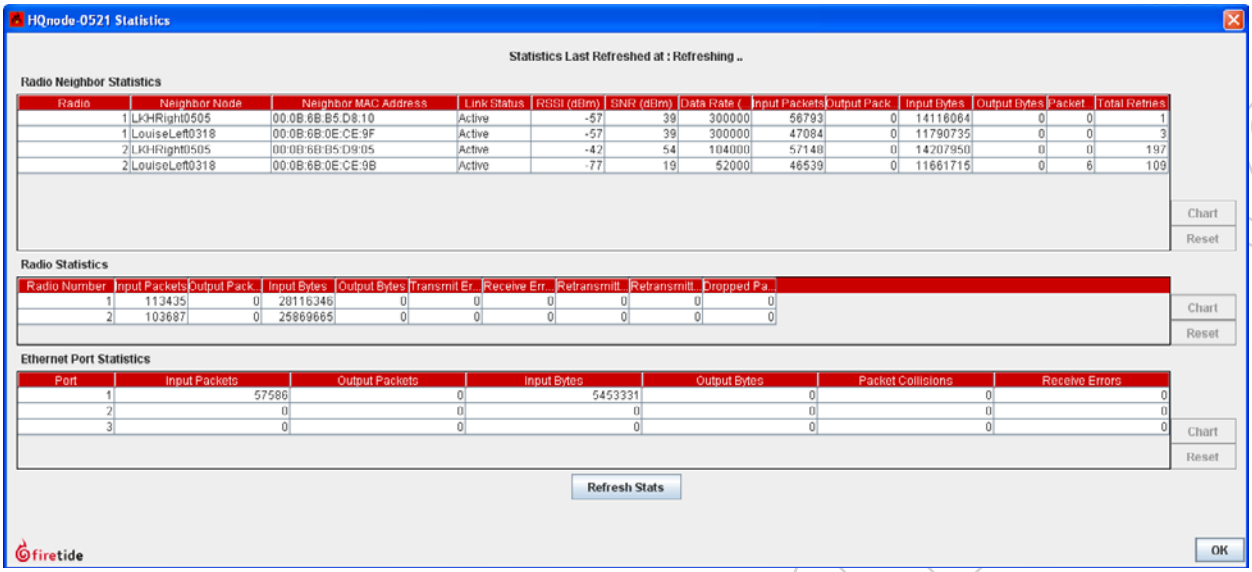
Understanding the Node Statistics Window

Each radio has a one-line entry for each neighbor with which it is communicating. Columns 1, 2, and 3 identify the link.

Column 4 will show whether a link has been eliminated, usually because it is marginal. Columns 5 and 6 show the RSSI and Signal-to-Noise ratio.

Figure 2.23 Node Statistics

The node statistics window shows key performance parameters for each radio link on a node.



Column 7, Data Rate, shows the current modulation rate of the link. Note that until there is traffic flowing over the link, this may remain at a low value. Use the Run Diagnostics command to generate traffic if the mesh is not busy.

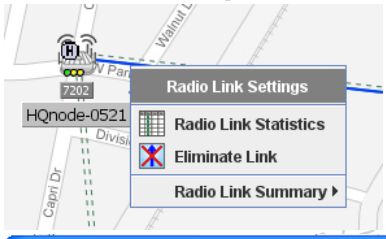
Columns 8-12 show traffic in (received) and out (transmitted) for each link.

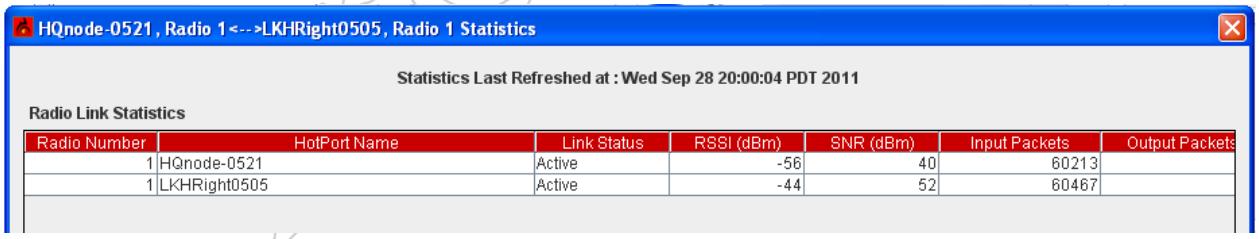
Columns 13 and 14 show dropped packets and total retries. It is normal to have a few such events, but if either parameter exceeds about one percent of total traffic, look for sources of interference.

Statistics for each link can be reset, and can be charted over time. Statistics refresh automatically, but can also be refreshed via the button.

Figure 2.24 Link Statistics

Individual link statistics can be viewed by first clicking on a link to select it, and then right-clicking. Select the Radio Link Statistics option.





Spectrum Analysis

The HotPort 7202 contains a spectrum analysis feature. This can be used to scan for interference from all other sources, and record this information for later analysis. It can be used for initial site survey work or to troubleshoot problems that appear later.

Spectrum analysis works by using one radio in the node to sequentially scan through the list of selected channels, recording the duration and power of any RF signals it finds. The other radio in the node is used to communicate the result back to HotView Pro, which stores the results and also displays a graph of them. Note that the radio doing the scanning is out of service and cannot carry mesh traffic. Plan accordingly when selecting a node and radio for analysis work. You may wish to temporarily add an extra node to an existing mesh.

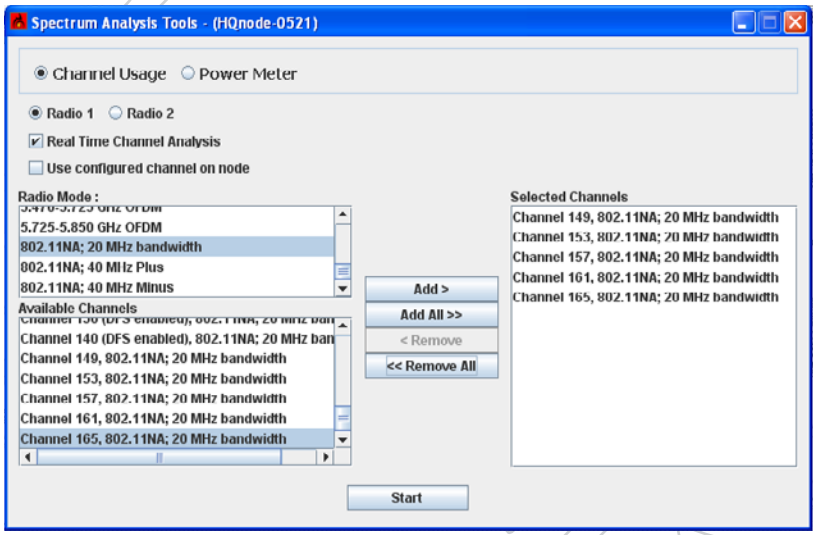


Figure 2.25 Spectrum Analysis Setup

You can select either Channel Usage, the percentage of time the channel is in use; or Power, the strength of the signal. The Power Meter mode will also report the MAC address of the transmitter; useful in determining whether the signal is from one's own mesh.

You also select the radio mode and the channels you wish to monitor. You can monitor up to ten channels.

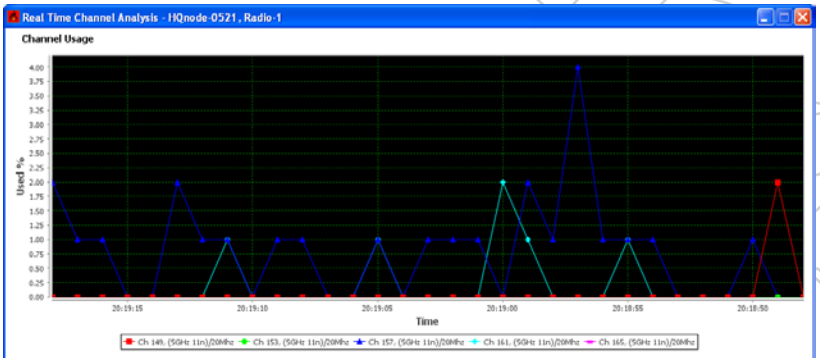


Figure 2.26 Spectrum Analysis Setup

This is the Channel Usage graph. The upper graph shows instantaneous usage; the lower graph shows a longer-period average.

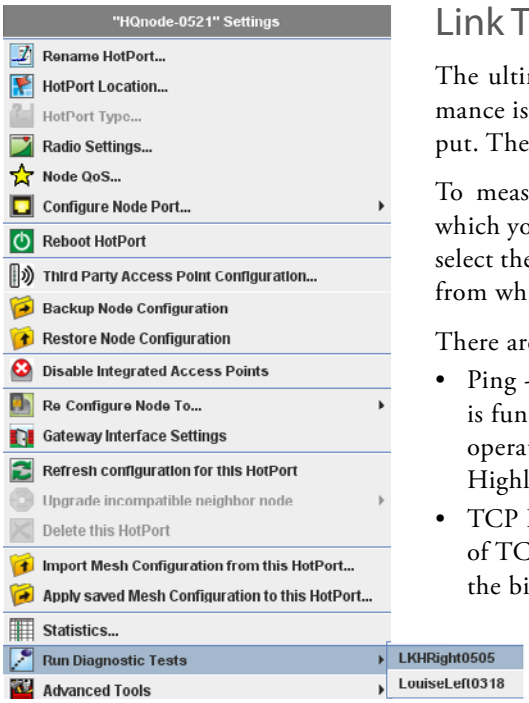


FIGURE 2.27 DIAGNOSTIC TOOLS

The Diagnostics menu is accessed by right-clicking on a node and selecting the Run Diagnostic Tools option. A flyout lets you select the second node of the test pair.

Link Throughput

The ultimate goal of any mesh is to move traffic. While good RF performance is necessary for this, you still need to verify actual effective throughput. The HotPort 7202 has a built-in performance tool to make this easy.

To measure performance, right-click on one of the two nodes between which you wish to measure performance. Select Run Diagnostics Tools, and select the second node from the flyout. You will be presented with a window from which to select the desired test.

There are five choices:

- Ping - this runs a simple ping between nodes to verify that the RF link is functioning. It does not generate enough traffic to affect overall mesh operation. The ideal result is a low, but consistent, ping response time. Highly inconsistent times indicated RF signal problems.
- TCP Iperf & Bi-Directional TCP Iperf. Both tests run a large amount of TCP traffic between the nodes, on one link. The difference is that the bi-directional test runs it in both directions simultaneously.
- UDP Iperf and Bi-Directional UDP. Both tests run a large amount of UDP traffic between the nodes, on one link. The difference is that the bi-directional test runs it in both directions simultaneously.

Note: the Iperf tests flood the chosen link with as much traffic as it can carry. This may disrupt other traffic on the mesh. Iperf attempts to send a large, fixed amount of traffic. It will time out if it is unable to complete the entire transfer in a fixed period of time, so you will occasionally see a "test failed" message. Re-run the test. If it fails consistently, it means there is substantial interference on the RF link.

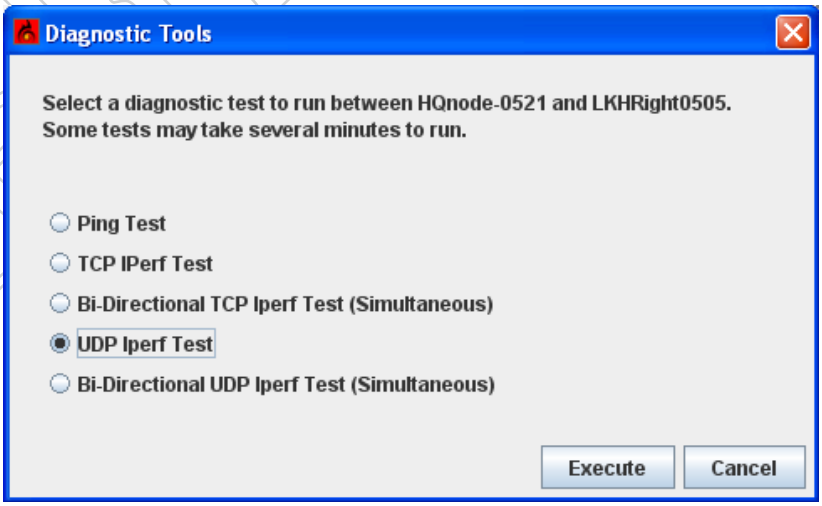


FIGURE 2.28 DIAGNOSTIC TOOL SELECTION

The Diagnostic Tools window lets you select the test to be run.

Also note that the CPU in the HotPort 7202 can only run iPerf traffic at about 115-120 Mbps; thus it cannot fully test a 40 MHz 802.11n link.

Performance Optimization

Once basic mesh performance has been verified, the mesh should be tuned. There are two parts to this; both involve reducing mesh overhead traffic and reducing mesh jitter.

Link Elimination

It is not uncommon to have nodes in the field form links among themselves that were unplanned; i.e., not needed as part of the mesh design. Because the nodes continuously update each other about the state of each link in the mesh; the more links there are the more overhead there will be.

Worse, unexpected links are usually of marginal quality; thus they are likely to drop out and recover as RF conditions change. This is a condition called 'link flap' and it too generates overheard traffic.

The easiest way to eliminate links is shown in Figure 2.29. There is also a Link Elimination command under the Mesh menu.

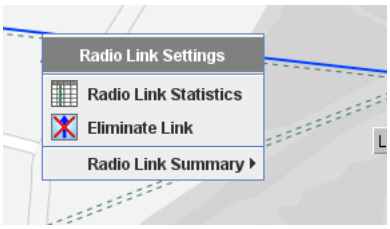


FIGURE 2.29 LINK ELIMINATION

Selecting an RF link by clicking on it will highlight the link in blue. Right-clicking brings up a pop-up which lets you eliminate the link

Fixing Maximum Data Rates

802.11 radios automatically negotiate the best speed possible under the existing RF conditions. If this is less than the maximum, the link will attempt to negotiate the speed upward, and then fall back again when necessary.

In most applications this is completely transparent and also irrelevant. However, in mesh applications it can introduce small amounts of jitter in mesh transit times, and it also creates more mesh overhead traffic, because the nodes share link speed information for routing purposes.

It is often useful to adjust the maximum possible speed at which an RF link can operate to a value less than the maximum. This has only a modest effect on performance but can reduce overheard and jitter. This is usually a beneficial trade-off in meshes which are carrying video or voice traffic. Figure 2.30 shows an example.

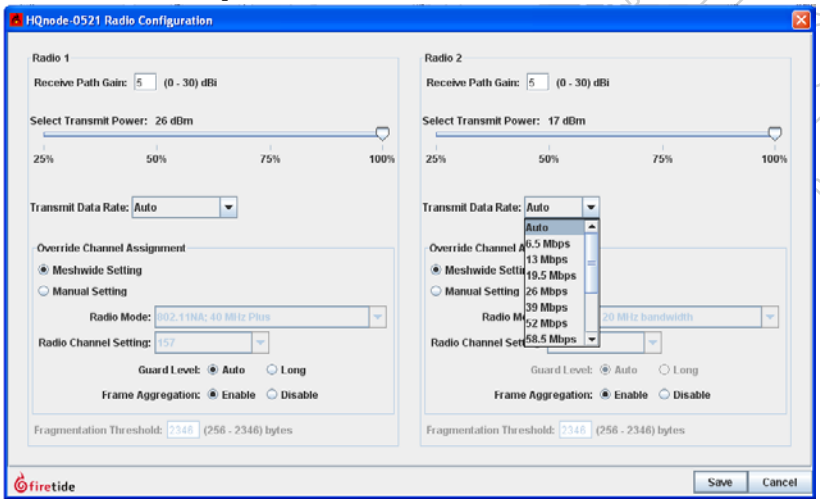


FIGURE 2.30 FIXING DATA RATES

Individual RF links can have their maximum data rate specified via the Radio Configuration option on each node; accessible by right-clicking the node.

Here, Radio 1 has been set to 36 Mbps, and Radio 2 shows the drop-down menu of available radio speeds.

The speed choices vary according to radio type operating mode

4 HotView Pro Server Configuration

This chapter explains how to configure the HotView Pro server application itself. The server is the always-on element of the overall system; thus it manages alarms, defines user accounts, and performs many other network-wide functions. The server can be configured whether it is running or not. To do so when it is not running, use the Server Configuration icon in the HotView Pro Launcher window, at the bottom of "Figure 1.3 Launcher Window" on page 7. Otherwise, click on the Server Administration menu.

As shown in Figure 3.31, the Server Configuration window has seven tabs along the left side, with a varying number of sub-tabs along the top. The Database Management and Licensing functions are covered in the software installation document. The other tabs are described herein.

Server Configuration - Network Management

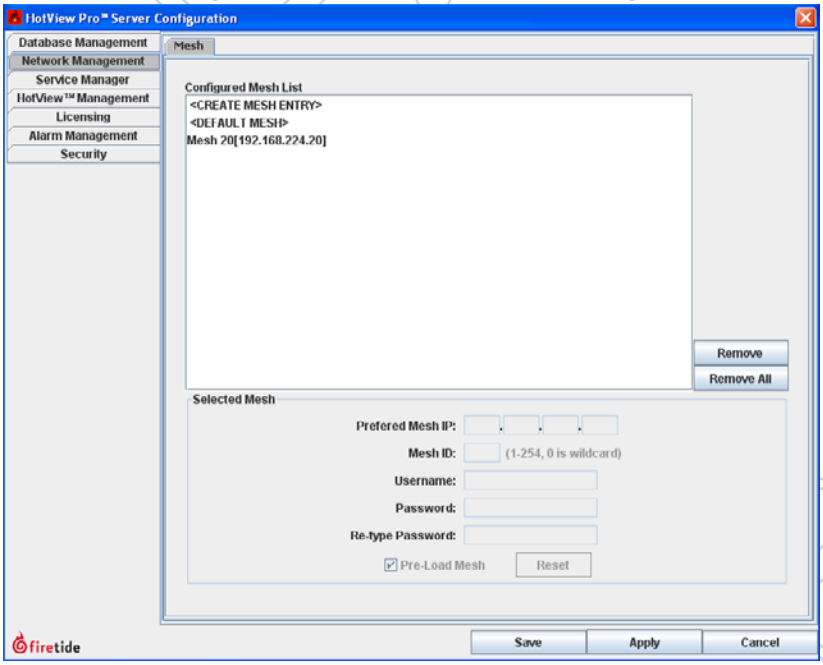


Figure 3.31 Server Configuration - Network Management

This tab shows the meshes, access points, and controllers that are under management by HotView Pro. In particular, it lets you tell the server application what the login credential is for each mesh.

It also allows you to remove from the server's database any mesh which you no longer wish to manage.

Note: the mesh username and password here do not represent the humans who use the system; instead it is the login credential specified in the Mesh Configuration window under the User Accounts tab. This is shown in Figure 3.32.

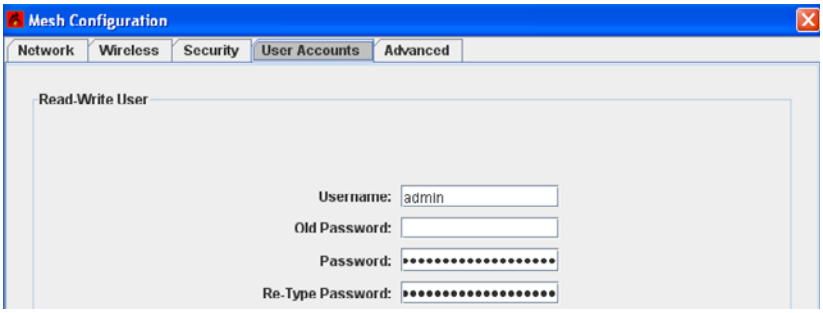


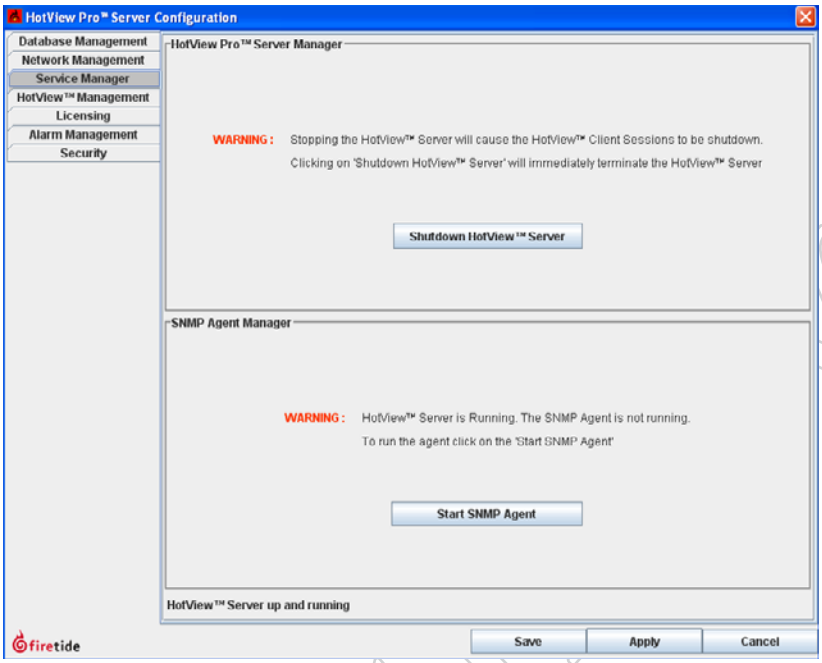
Figure 3.32 Mesh User Accounts

This tab defines the login information that the server uses to access the mesh.

Server Configuration - Service Manager

FIGURE 3.33 SERVICE MANAGER

The Service Manager tab are used to start and stop the server application and the SNMP agent application.



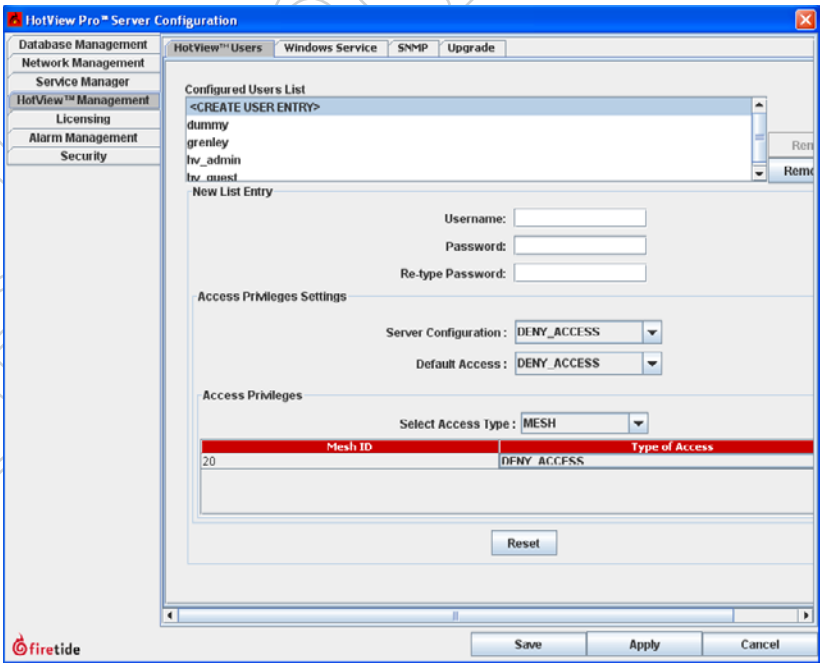
Server Configuration - User Management

FIGURE 3.34 HOTVIEW PRO MANAGEMENT - USERS TAB

This tab defines accounts for human users of the system.

Each user can be granted or denied server admin privileges.

Each user can also be granted read/write access to meshes, read-only access, or no access at all.



Server Configuration - Windows Service Manager

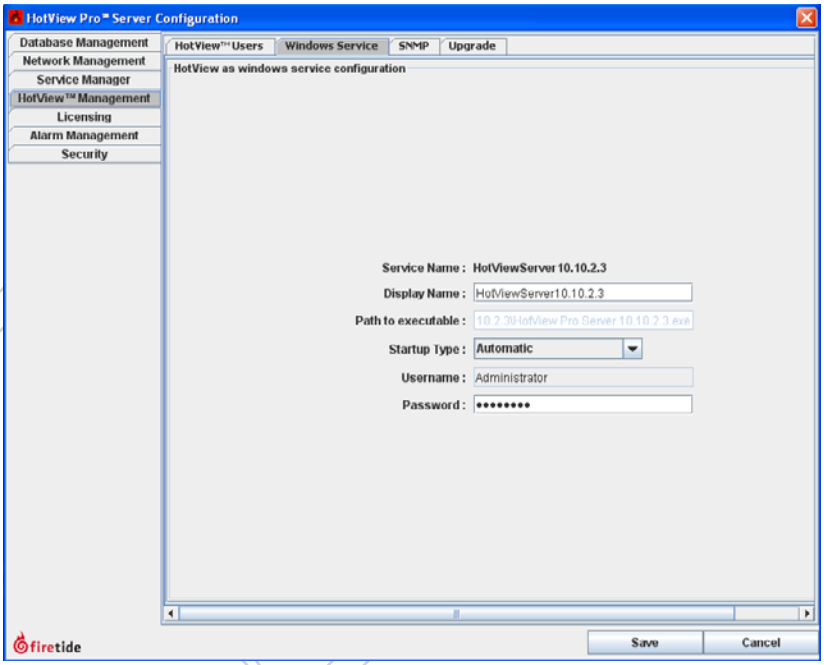


Figure 3.35 HotView Pro Management - Windows Service Tab

This tab lets you configure the server application as a Windows service, so that it starts (and re-starts) automatically.

Server Configuration - SNMP Setup

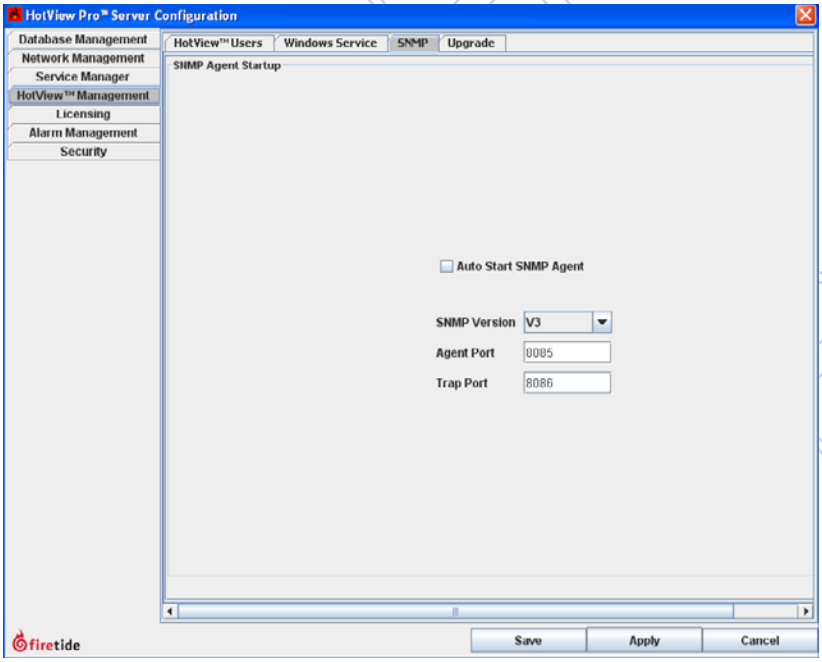


Figure 3.36 HotView Pro Management - SNMP Tab

This tab lets you configure the SNMP agent.

Server Configuration - Alarm Management

Figure 3.37 Alarm Management

The server can be configured to generate alarms. There are four aspects to alarm configuration and generation:

- Alarm Definition
- Alarm Severity Definition
- Alarm Action Configuration
- Alarm email (SMTP) Configuration

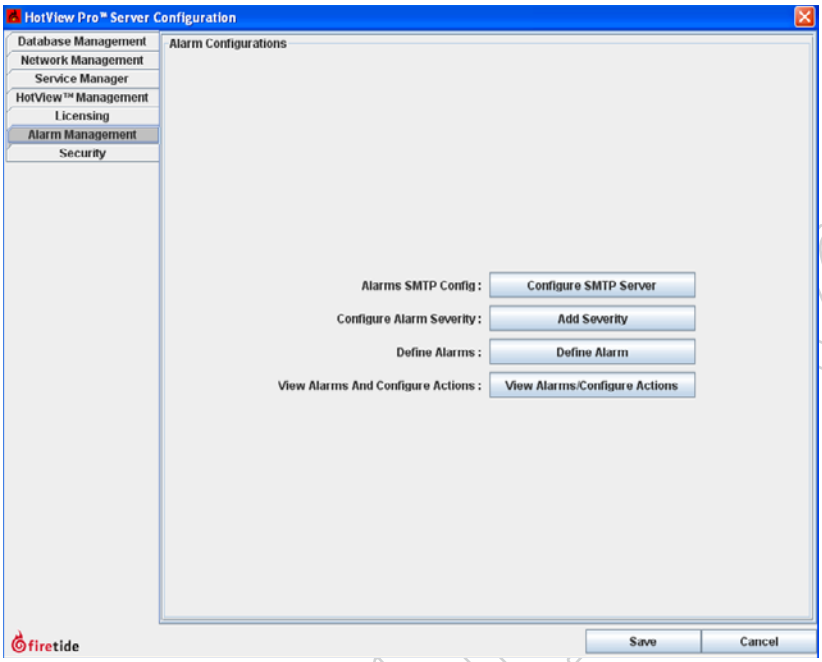
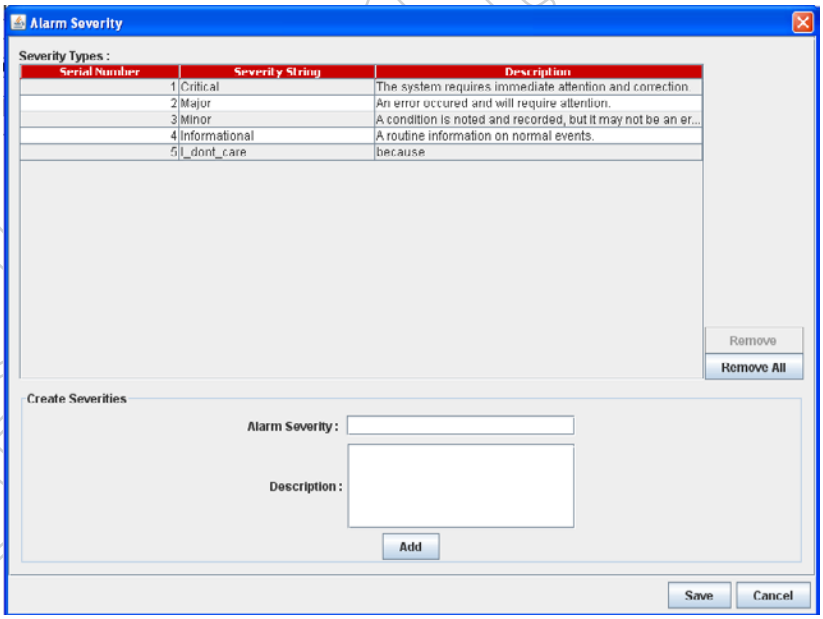


Figure 3.38 Alarm Configuration - Severity

There are four pre-defined levels of severity. Additional levels may be defined if needed.



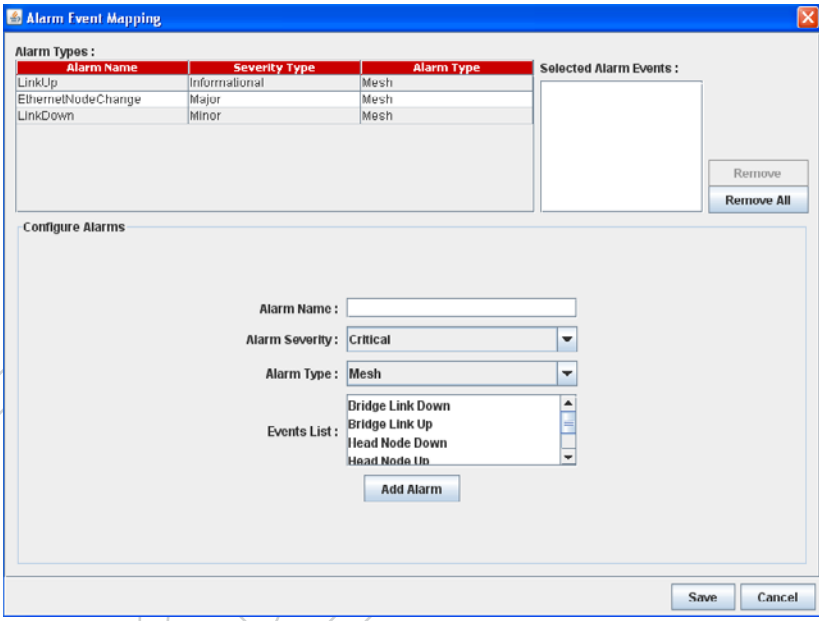


Figure 3.39 Alarm Events

This tab lets you select from a list of alarm events to create named alarms with associated severities.

Actions to be taken for each named alarm are defined in Figure 3.40.

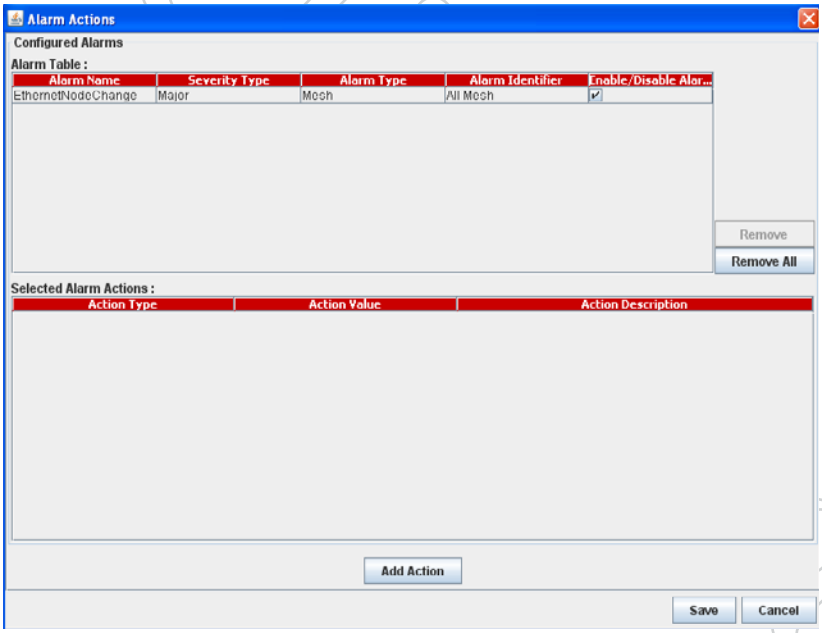


Figure 3.40 Alarm Actions

Named alarms can be assigned actions using this window. Actions include:

- Execute a System Command.

This causes the named system command program to be executed.

- Send an email.
- Do nothing (but write a log entry).
- Ignore.

If email is select, email parameters must be specified, as shown below:

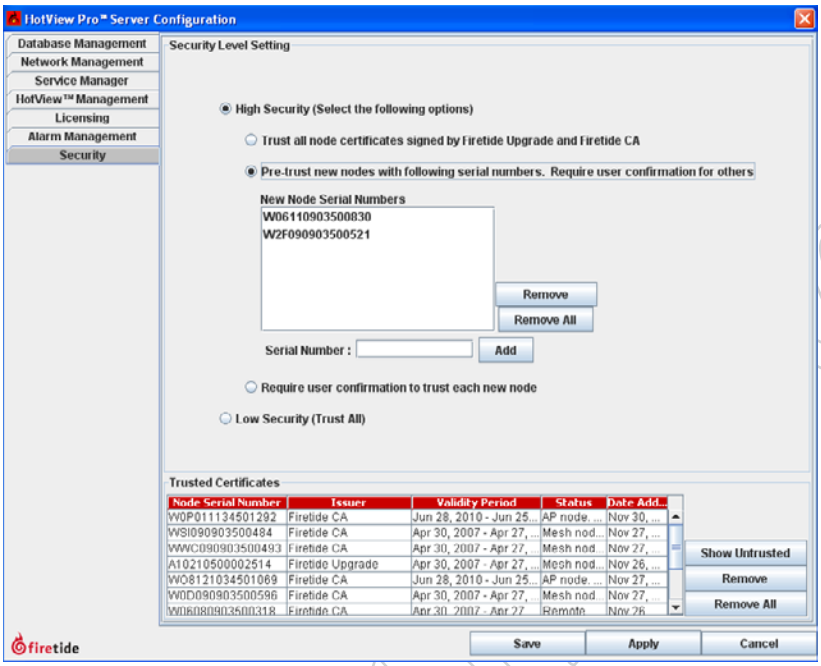
Server Configuration - Security

FIGURE 3.41 SECURITY

This tab lets you restrict the ability of nodes to join the mesh.

Normally, any node with the correct mesh settings can join the mesh. Enabling High Security requires that the node have a valid, digitally-signed certificate issued by Firetide.

It can further be restricted by requiring the server to obtain explicit human approval before allowing a node to join the mesh.



5 Upgrading Firmware

This chapter explains how to upgrade firmware in your nodes. The 'upgrade' tool is general-purpose; it can be used to upgrade firmware to a new release, roll back to an old release, or reload the same version. The upgrade tool is resilient and fault-tolerant. All firmware images are verified by checksum, and activation of the new image (reboot) does not occur unless a valid image is received. Activation can be delayed, so that firmware can be upgraded and 'ready to go' awaiting later activation.

When to Upgrade

From time to time, new firmware is released to address bugs, improve performance, or add features. Consult the release notes to help you decide whether the upgrade is applicable to your mesh. If you decide to upgrade, be sure to upgrade all nodes within a mesh. Firetide does not recommend operating a mesh with mixed firmware levels.

Some firmware upgrades require a new version of HotView Pro. If this is the case, upgrade the firmware first, then switch over to the new version of HotView Pro.

Upgrade Options

In general you will want to upgrade all of the nodes on a mesh at the same time, then activate. Use care when upgrading nodes and meshes. Firmware upgrades can consume considerable bandwidth. If you are planning an upgrade of a production mesh, upgrade only a few nodes at a time, and use the **Activate Later** command to schedule the activation/reboot for a convenient time. Note that the mesh will be offline for about two minutes when the new firmware is activated.

However, firmware upgrades can consume considerable bandwidth. There are several steps you can take to minimize the effect on the mesh, should this be necessary.

- You can upgrade only a few nodes at a time.
- You can use the **Activate Later** command to schedule the activation/reboot for a convenient time.
- You can reduce the block size used during upgrade.

Note that the mesh will be offline for about two minutes when the new firmware is activated.

How to Upgrade

To upgrade, begin by selecting the **Upgrade Firmware** command from the **Network** menu. A window opens, similar to the one in Figure 4.42. This shows the nodes available for upgrade. Check boxes let you select the nodes to be upgraded.

In most cases, an entire mesh can be upgraded at once. If you choose to do so, select the **Activate Later** icon. Activate after you have verified that all nodes have received valid images.

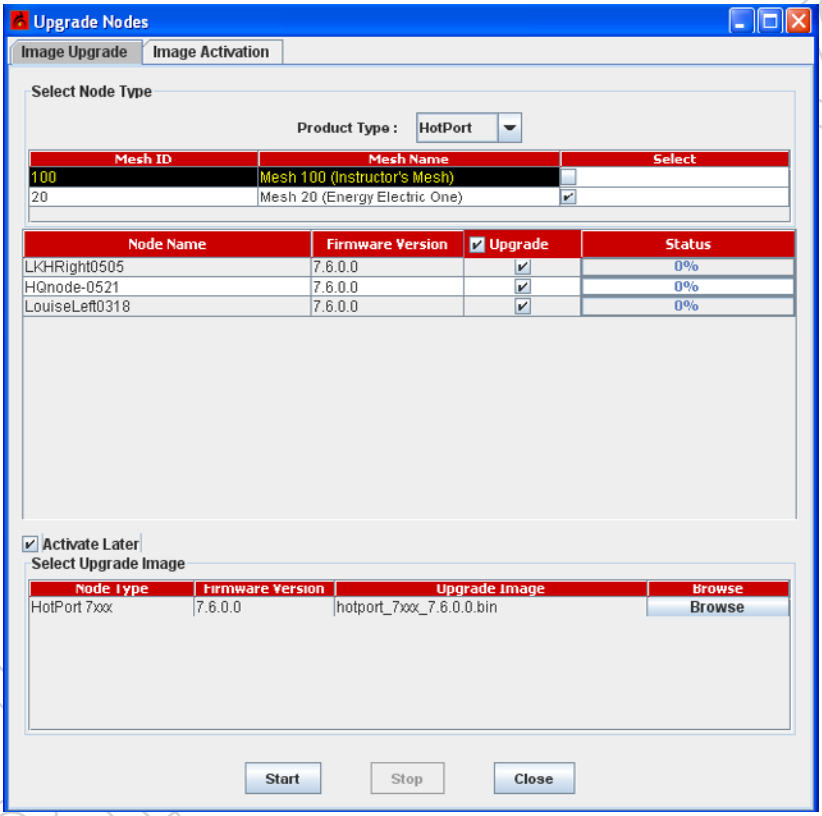


Figure 4.42 Firmware Upgrade

The upgrade window shows the meshes available for upgrade, and the nodes within each mesh.

It also allows you to select the firmware image you wish to apply to the nodes.

There is an Activate Later check-box and an image activation tab. This allows you to schedule the activation time.

Here, an image file has been selected. Image file names have a specific format; it includes the product type, numerical family number, and version number.

Suffixes can be either .bin or .bin2; the .bin2 option is digitally signed. Refer to the Security section for details on digitally-signed firmware versions.

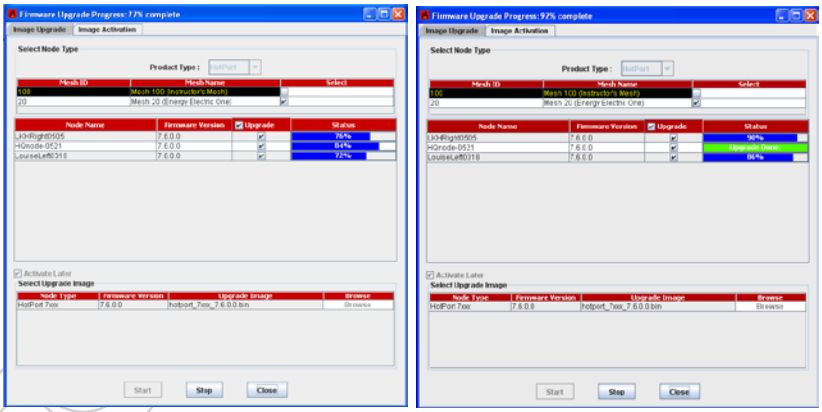


Figure 4.43 Upgrade in Progress

These images show the progression of the firmware upload.

Note that the 'upgrade complete' message does NOT mean that the new image has been activate, i.e. run, but only that it has been uploaded and fully checked for accuracy.

Also note that the **Activate Later** option has been selected.

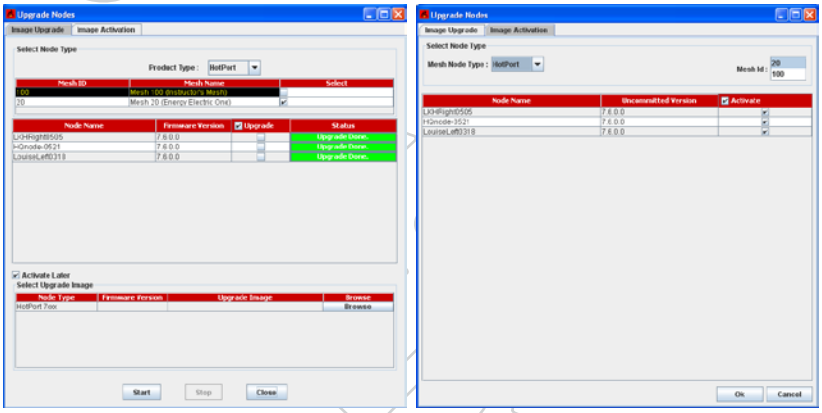


Figure 4.44 Completion & Activation

The **Image Activation** tab lets you activate the previously-uploaded image at a time of your choosing.

Note that this means the nodes will reboot, and be offline for approximately two minutes.

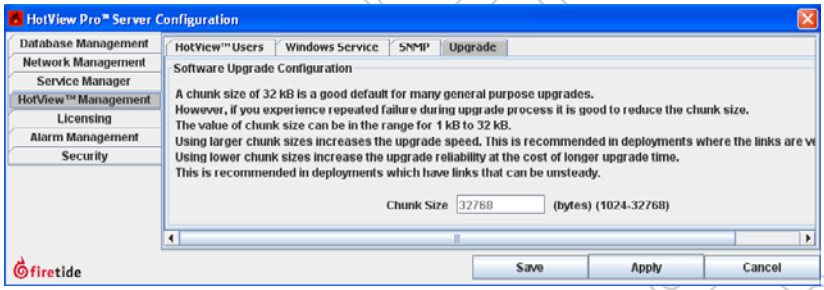


Figure 4.45 Upgrade Chunk Size

You can specify a smaller chunk size for the firmware upgrade process. This will increase the time it takes to perform an upgrade, but will also reduce the impact on production network traffic. It is also recommend if you must upgrade a mesh that is experiencing high levels of interference or intermittent connections.