5.1.9 Build Information

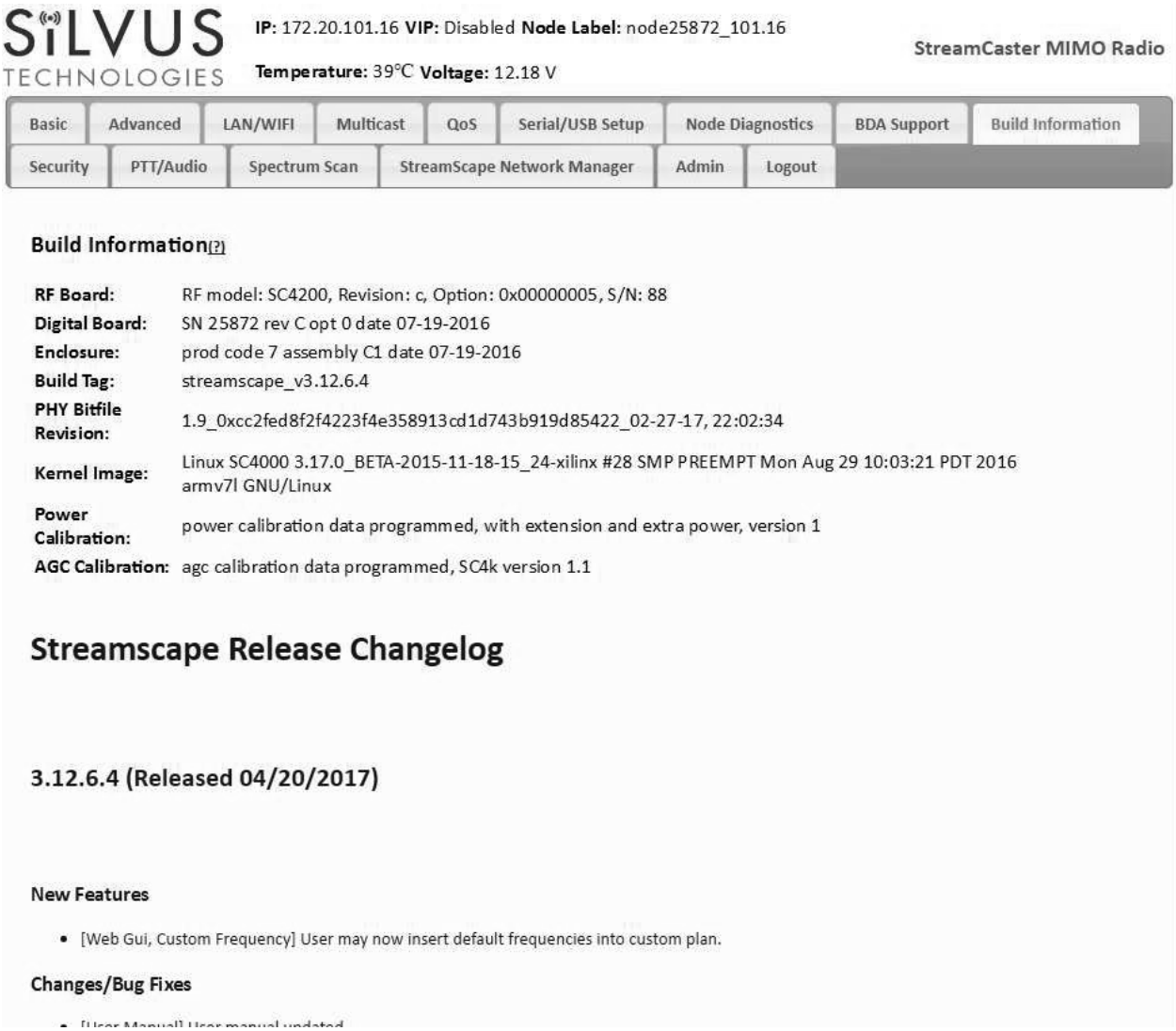


Figure 36 Build Information

The 'Build Information' page provides information about the hardware and firmware loaded onto the radio, as well as the changelog of the currently loaded and past firmware revisions.

5.1.10 Security

The Security section of StreamScape allows users to enable/disable encryption, upgrade radios, and load license files for enabling features such as AES encryption.

Encryption:

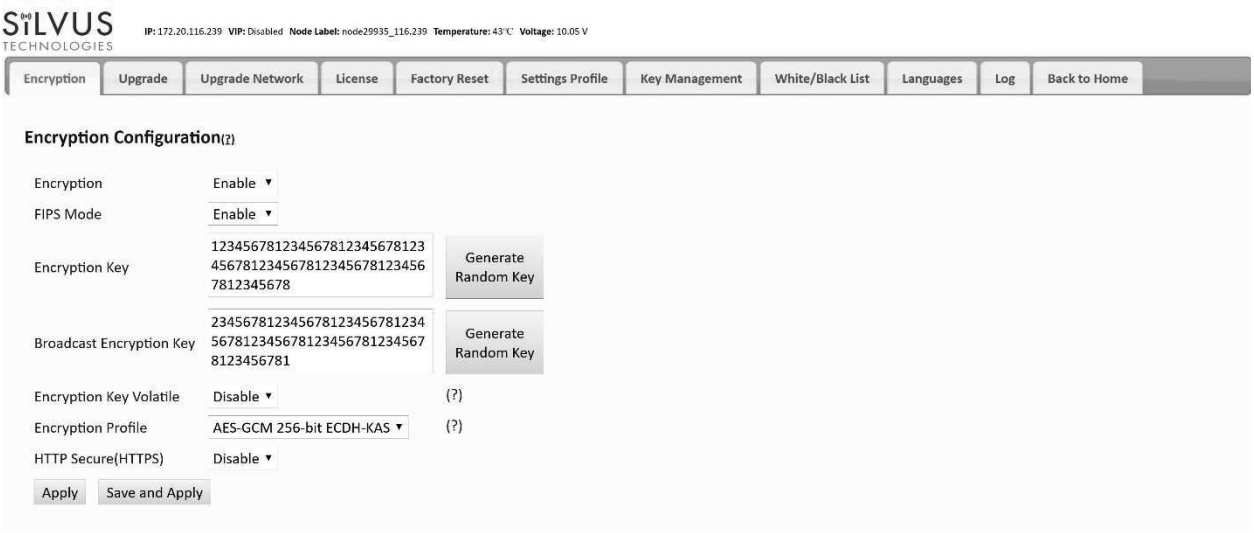


Figure 37 Security (Encryption)

- **Encryption**: Enable or disable encryption.

- **FIPS Mode**: Enabling FIPS mode is the first step to making the radio FIPS compliant (see Section 6.1 Enable FIPS Mode for details). Enabling/disabling will require a reboot and will erase all setting profiles, reset the encryption key, both SSH keys, the HTTPS certificate, and the login passwords to their factory default. Enabling will also turn on HTTPS and Login Authentication. After reboot, the operator must perform the following steps to complete the FIPS compliant process.

    - Update the web login password to something other than “HelloWorld”
    - Create new SSH keys and HTTPS certificate.
    - Update encryption key or click “Generate Encryption Key” and save.

- **Encryption Key**: Set an encryption key if encryption is enabled.

- **Encryption Profile**: Choose between various encryption profiles. Available options are:

    - **DES 56 bit** – DES encryption using 56 bit keys. This mode is backwards compatible with legacy SC3500/3800 radios.
    - **AES 128/256** – AES encryption using 128/256 bit keys. This mode is backwards compatible with legacy SC3500/3800 radios.
    - **AES-GCM 256 ECDH-KAS** – FIPS compliant AES encryption in GCM mode with authentication and ECDHE based re-keying. This is the recommended mode on the 4K series as it is the most secure and provides the highest throughput under varied conditions. It is currently undergoing FIPS certification for the 4K series.

- **HTTP Secure (HTTPS):** Enable or disable HTTPS access to StreamScape.

Upgrade:

Figure 38 Security (Upgrade)

The firmware can be upgraded by simply choosing the upgrade image from your desktop and uploading it to the radio. This field can be used to upgrade the radio root file system, linux kernel, or uboot.

Upgrade Network:

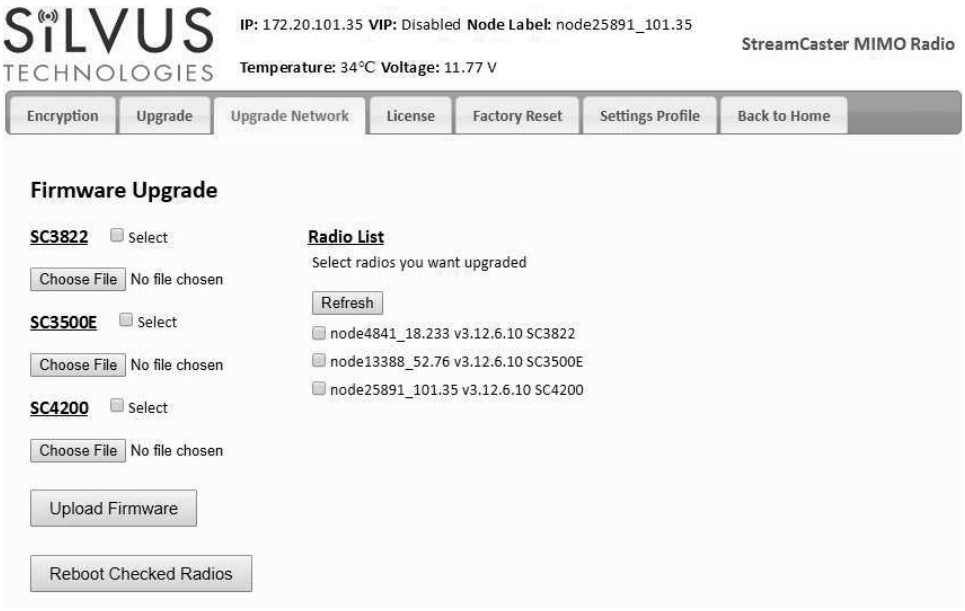


Figure 39 Security (Upgrade Network)

Starting with firmware version 3.12.6.8, multiple radios within the same network can be upgraded all at once. Users can simply choose the appropriate firmware file for the corresponding radio models to apply the upgrade to all the radios in the network. Currently, this feature is not available in HTTPS mode.

License:

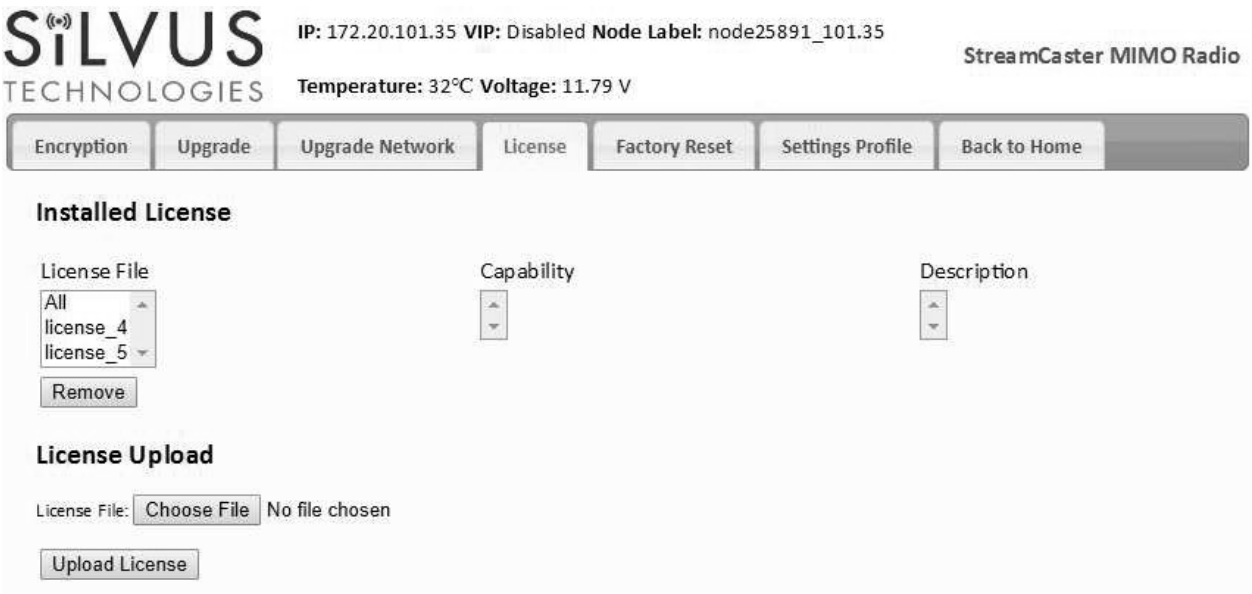


Figure 40 Security (License)

Features such as encryption levels and frequency ranges can be enabled by license keys obtained from Silvus. New license keys can be uploaded to the radio on this page.

Factory Reset:

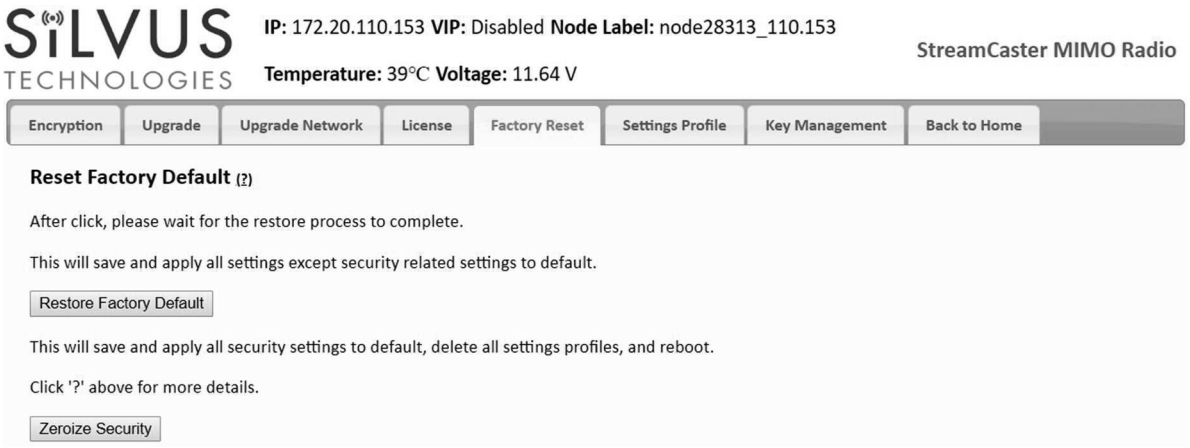


Figure 41 Security (Factory Reset)

- **Restore Factory Default:** Restores all settings to default except those related to security (such as login passwords, encryption keys, FIPS mode, etc.). This is useful if the user changed some advanced settings and now they don't know how to get to the defaults.

- **Zeroize Security:** This will set login passwords and all security keys to their defaults. This includes the Encryption Key, SSH Login Key, SSH Host Key, HTTPS Certificate, and Encryption Key Volatile. It will also erase all settings profiles. Also, if FIPS mode is off, it will turn off HTTPS and login mode. The current FIPS mode will not be changed.

Settings profile:

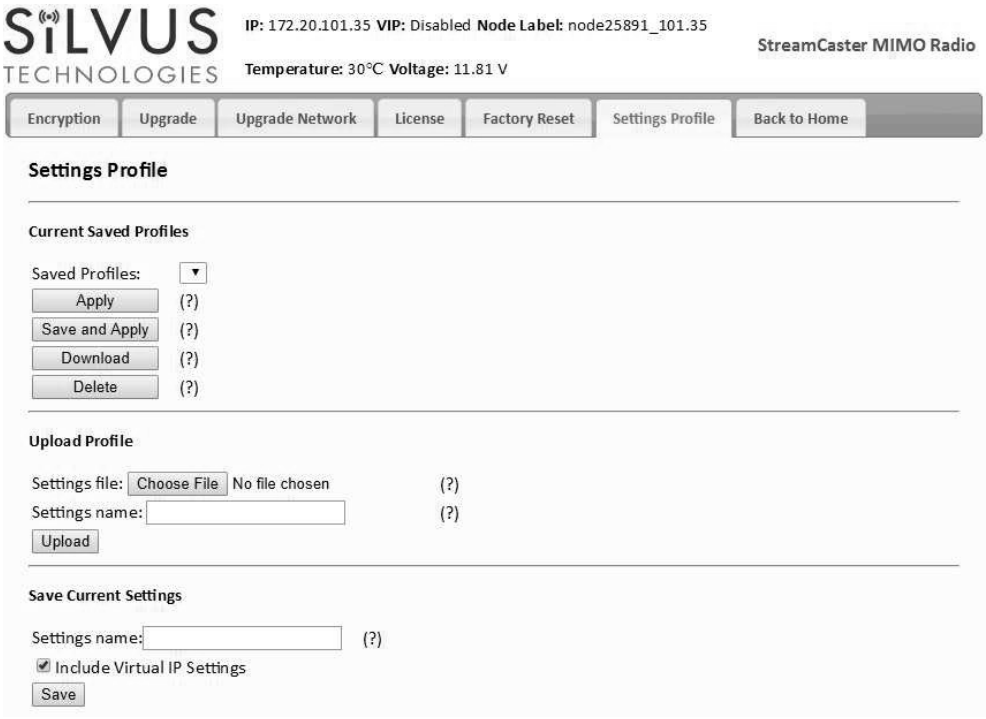


Figure 42 Security (Setting Profile)

- **Current Saved Profiles:** Select a saved profile and apply the settings to use the selected profile. The profile stored can be downloaded or deleted.
- **Upload Profile:** Select a downloaded profile from the computer and upload to the radio as a saved profile.
- **Save Current Settings:** Store the current settings on to the radio for future access. Note that the FIPS mode setting is not saved in the profile. You must manually enable/disable it after applying the profile.

Key Management:

Figure 43 (Key Management)

This page is used to manage the radio's SSH login keys, SSH host key, and HTTPS Certificate. All key pairs used are elliptic curves.

- **SSH Login Keys:** In order to SSH into the radio, you must first generate a key pair and upload the public key onto the radio. A common way this is done on a computer is through the command `*ssh-keygen -t ecdsa -b 521*`. You will need to do this for each machine that wants to SSH into the radio, or you can share a single key pair amongst machines.

- **SSH Host Key:** This key is used for authenticating the radio to all machines that want to connect to it via SSH. A common way this key is generated on a computer is *'openssl ecparam -name secp521r -genkey -noout -out yourfilename`*. You may either upload your own key or generate one on the radio. Once you upload/generate a new key, the previous one is gone. You can get the original key by Factory Reset -> Zeroize. (Note that the generated text from the above command will encode both a private and public key in the text).

- **HTTPS Certificate:** This certificate is used to establish a HTTPS connection. If you are using a factory default or radio generated certificate and haven't added an exception of this certificate to your browser, you will see a message like below from your browser. This is because the certificate is signed by the radio and not a trusted Certificate Authority. You can bypass this by clicking "ADVANCED" in chrome, (or adding an exception in Firefox). The simplest way to generate a new certificate is to click "Generate Certificate and Save" button. If you are on HTTPS when you do this, you must also refresh the page. If you want to generate your own certificate, you must first generate a key pair (secp256r1, secp384r1, or secp521r1). Then create a X.509 certificate and append your private key to it. Copy the certificate text to the "Add a HTTPS Certificate" section, then click "Add Certificate and Save."

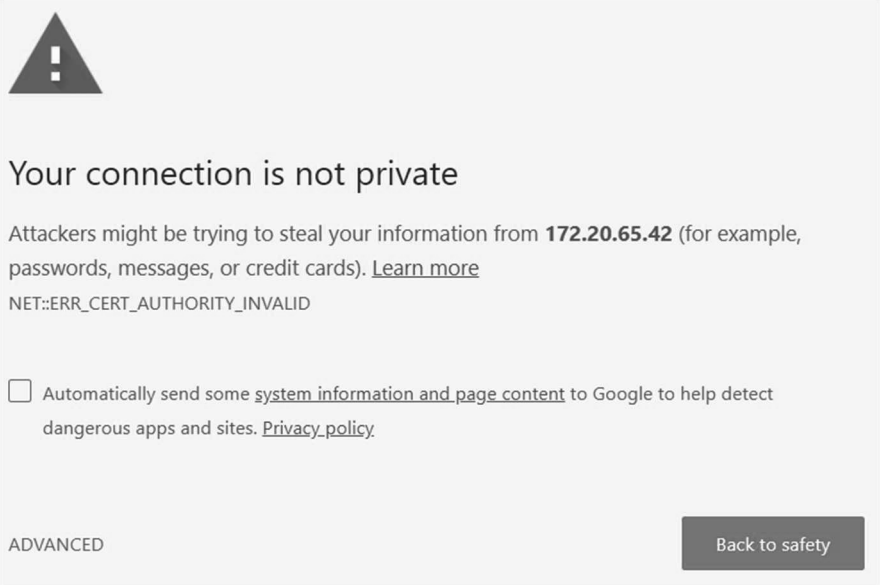


Figure 44 (Chrome Browser Warning)

5.1.11 PTT (SC4400/SC4200 Only)

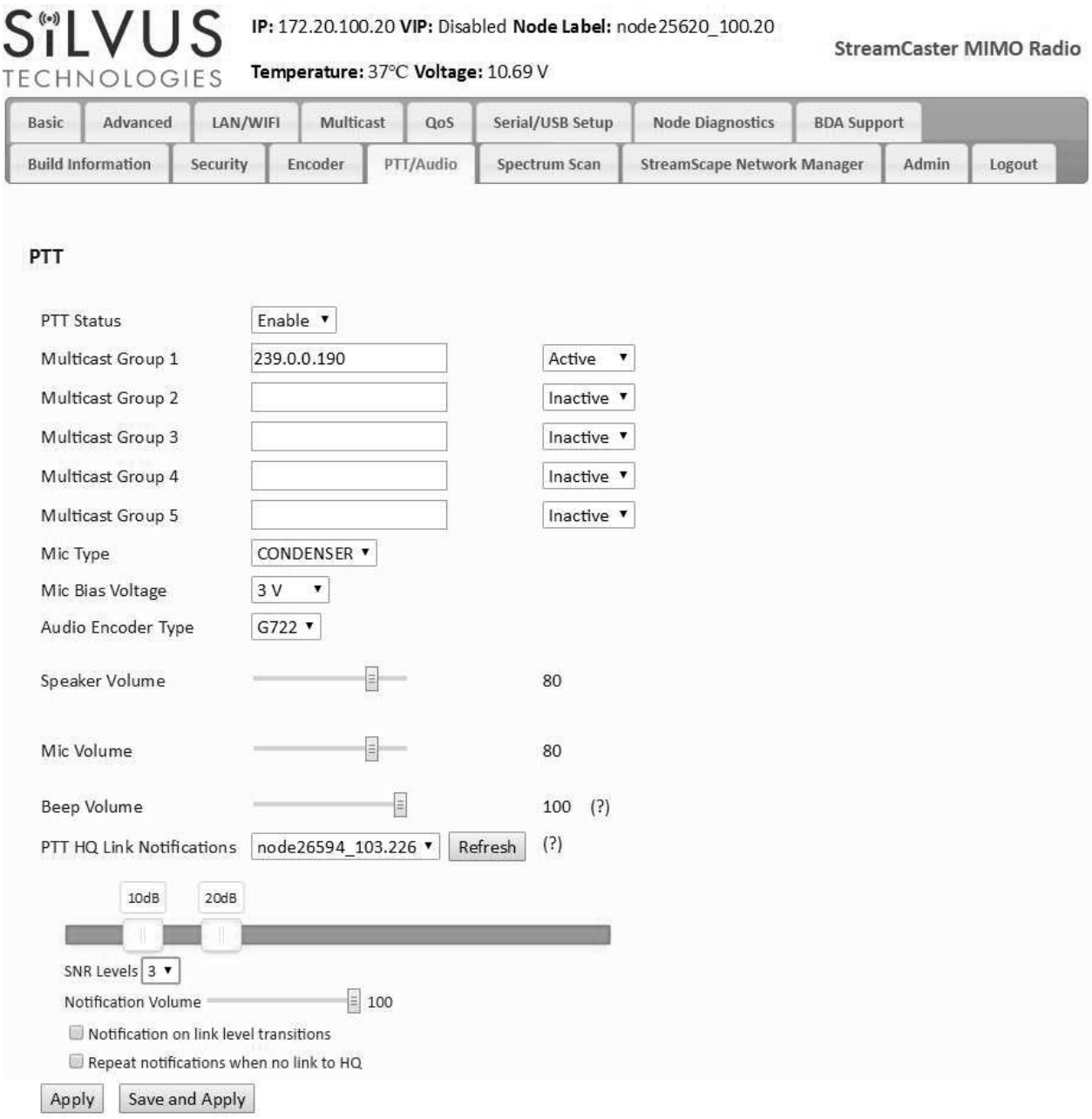


Figure 45 PTT (Push-to-Talk)

The PTT page can be used to configure talk groups (Multicast Groups) and speaker/mic settings for PTT enabled radios. Radios will only communicate with other radios that are subscribed to the same 'Multicast Group'. Radios can be active in multiple talk groups.

Multicast Group – Input the IP address of the multicast group. Radios will only communicate to radios within the same group. There are three different modes to select which dictate how a radio behaves within a group:

- **Active:** Radio may send and receive PTT audio on this group.
- **Inactive:** Group is disabled, no PTT audio will be sent or received.
- **Monitor:** Radio may listen to PTT audio from other users on this group, but may not talk.

Mic Type – Supported MIC types are Moving Coil or Condenser. The input amplification is adjusted based on the Mic Type chosen on this page

Mic Bias Voltage – Options are 90% (3V) or 65% (2.15V).

Audio Encoder Type – Default option is 'Variable Rate Code (OPUS)'. 'G.722 (high quality)' and 'G.711' are also supported for backwards compatibility

Speaker Volume – Moving slider adjusts the gain on the speaker

Mic Volume – Moving slider adjusts the gain on the microphone

Beep Volume + PTT Override – When the PTT button is pressed while another user is speaking, a warning beep will be played. This setting controls the volume of the Beep as a percent (%) of the speaker volume above. Pressing the PTT button three times (and holding on the third) within 1s will allow a user to override the channel and speak.

PTT HQ Link Notifications – When the PTT button is pressed twice within 1s, an audio notification will read out the SNR level to the user-specified HQ node. If the level transitions option is enabled, the notification will be played automatically when the SNR crosses the specified thresholds. The SNR thresholds can be set by first choosing the number of levels desired, and then moving the sliders accordingly.

5.1.12 Spectrum Scan

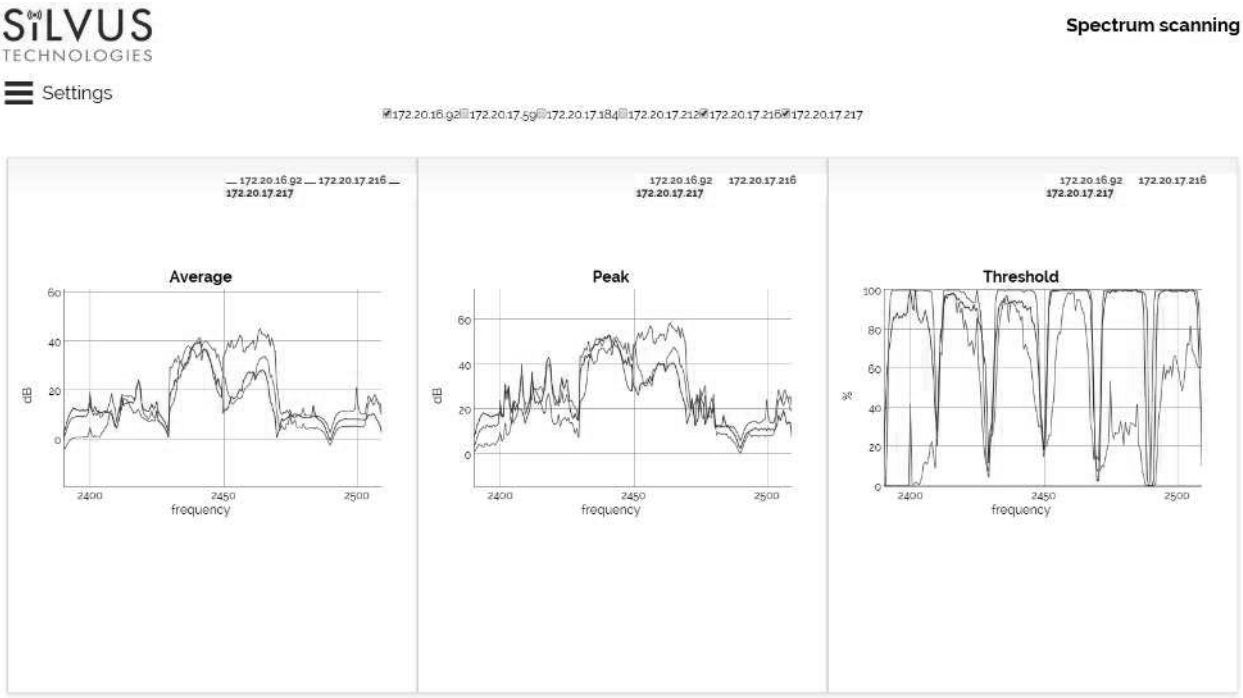


Figure 46 Spectrum Scan Results

The spectrum scan feature turns a Silvus network of radios into a distributed spectrum analyzer. When a scan is initiated, each selected radio in the network will go offline, perform a scan of the requested range, and report back. **Figure 46 Spectrum Scan** above shows the results from a scan of a network of 6 radios. The checkboxes at the top allow users to show or hide plots from specific radios. The three plots provided are:

Average – Displays the average power over the time duration specified in the settings.

Peak – Displays the peak power seen at any point during the scan for each frequency. This is the equivalent of the 'Max Hold' feature on common spectrum analyzers.

Threshold – Displays the duty cycle of interference stronger than the user specified 'Threshold' power. In the example above, the threshold was set to 5dB. The plot is showing the percentage of time that the measured power is more than 5dB above the radio's noise floor.

Settings:

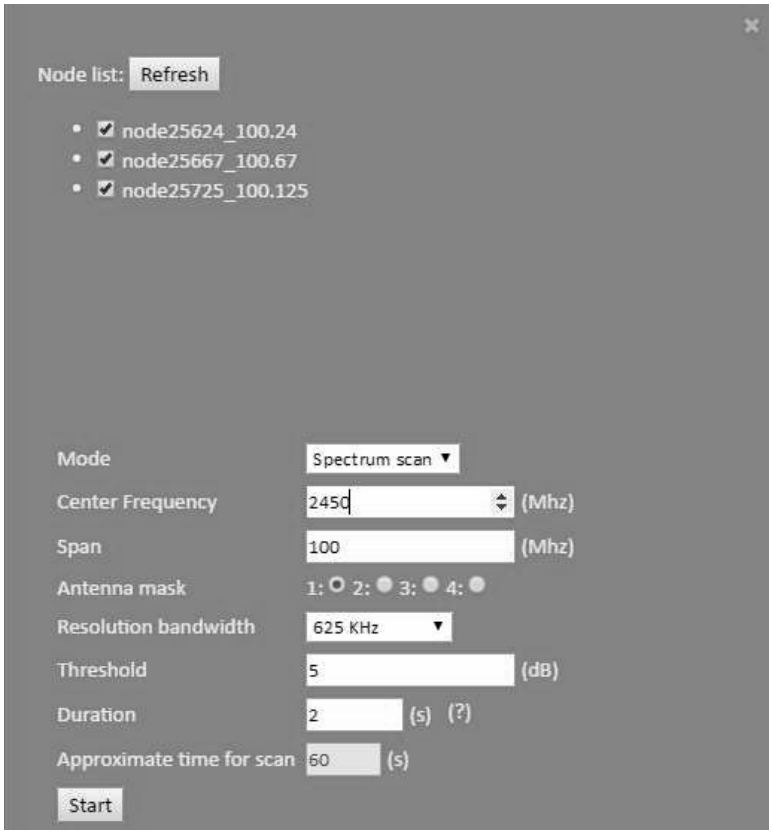


Figure 47 Spectrum Scan Settings

Clicking the settings button at the top left of the window will show the settings pane as shown in **Figure 47 Spectrum Scan Settings** The node list shows the list of nodes currently connected into the mesh network. Any nodes selected will be used as part of the spectrum scan. Nodes that are unchecked will resume normal operation. Note that an unchecked node will continue transmitting in the frequency channel it is operating in and its transmission will show up in the scan results of scanning radios.

Mode – Set to Spectrum Scan or Zero Span. Spectrum Scan mode provides plots of signal strength over frequency. Zero Span provides a plot of power over time in a 20MHz Bandwidth (see **Figure 49 Zero Span Results** below.

Spectrum Scan Mode:

Center Frequency – Specify the center frequency of the scan.

Span – Specify the span of the scan, centered on the center frequency. (e.g. Center freq of 2450MHz and span of 100MHz will scan 2400-2500MHz). A large span will take longer to complete.

Antenna Mask – Choose which antenna on the radio to use for scanning. If there are 2 antenna radios in the network antenna 1 or 2 must be chosen.

Resolution Bandwidth – Specify the RBW for the scan. A smaller RBW will provide a more detailed plot, but will take longer to complete the scan. 625KHz is a good balance between scan detail and time of scan.

Threshold – Specify the threshold for measurement of the duty cycle of interference.

Duration – Duration of each scan. A longer duration will provide better accuracy but will take longer to complete.

Approximate time for scan – Approximate time that the network will be down for the scan to complete.

Zero Span Mode:

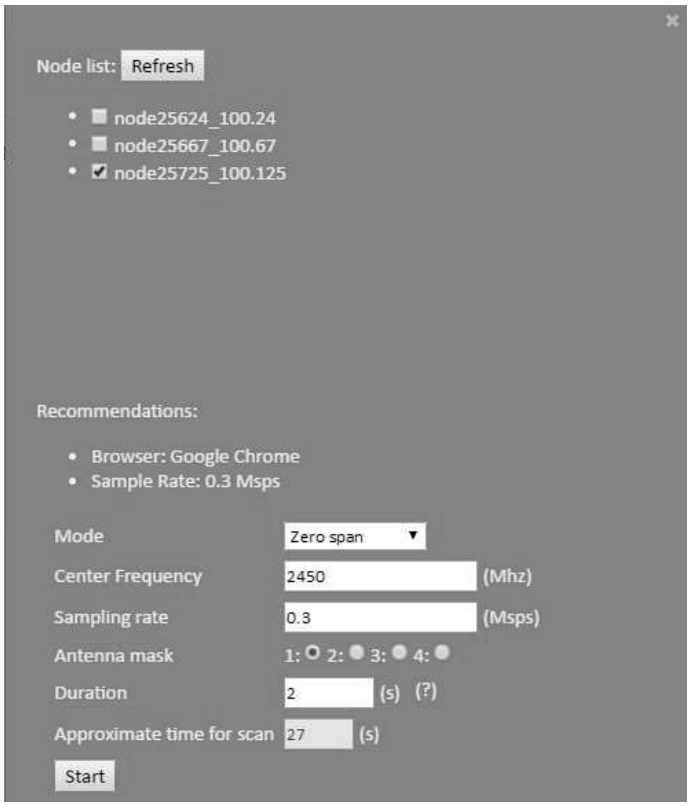


Figure 48 Zero Span Settings

In the Zero Span mode, the radio will provide a plot of the power measured in a 20MHz bandwidth across time. Zero Span can only be conducted on one radio in the network at a time. Other radios in the network will continue to operate and transmit so a zero span

scan should not be conducted within the same frequency that the mesh network is operating in.

Center Frequency – Specify the center frequency of the scan.

Sampling Rate – Set the sampling rate of the scan. (0.3Msps recommended)

Antenna Mask – Choose which antenna on the radio to use for scanning. If there are 2 antenna radios in the network antenna 1 or 2 must be chosen.

Duration – Duration of each scan. A longer duration will provide better accuracy but will take longer to complete.

Approximated time for scan – Approximate time that the network will be down for the scan to complete.

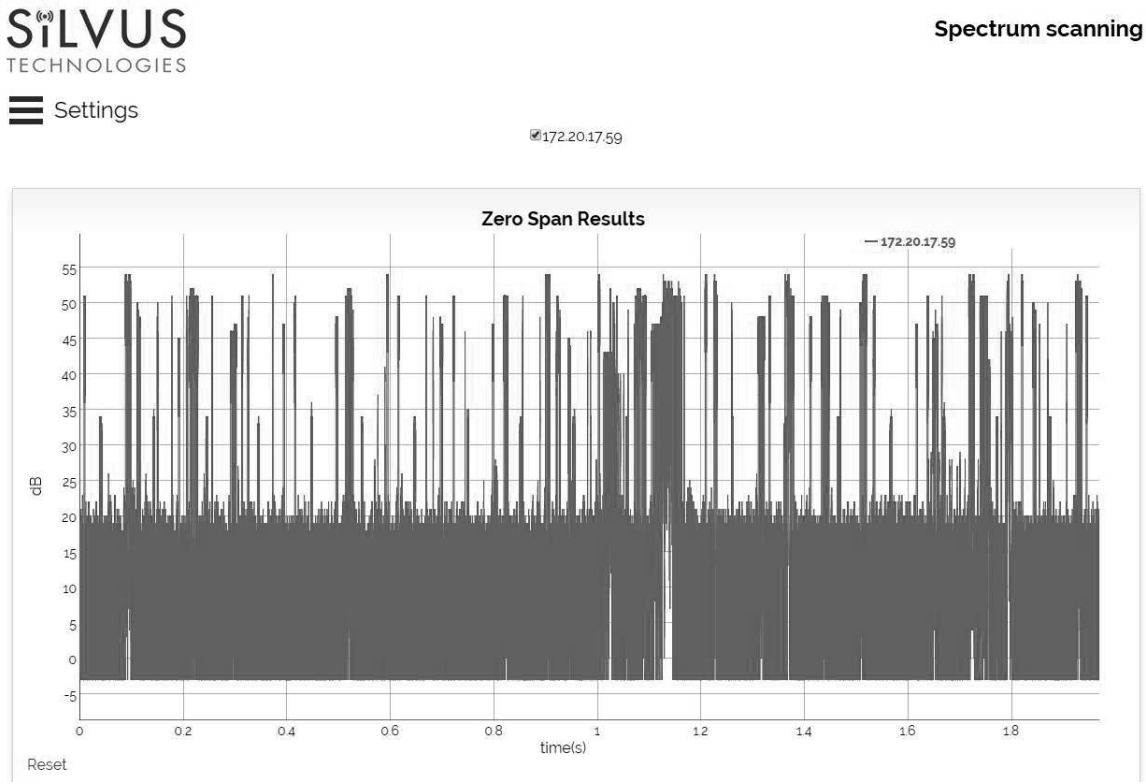


Figure 49 Zero Span Results

5.1.13 MPS (Multi-Position Switch)

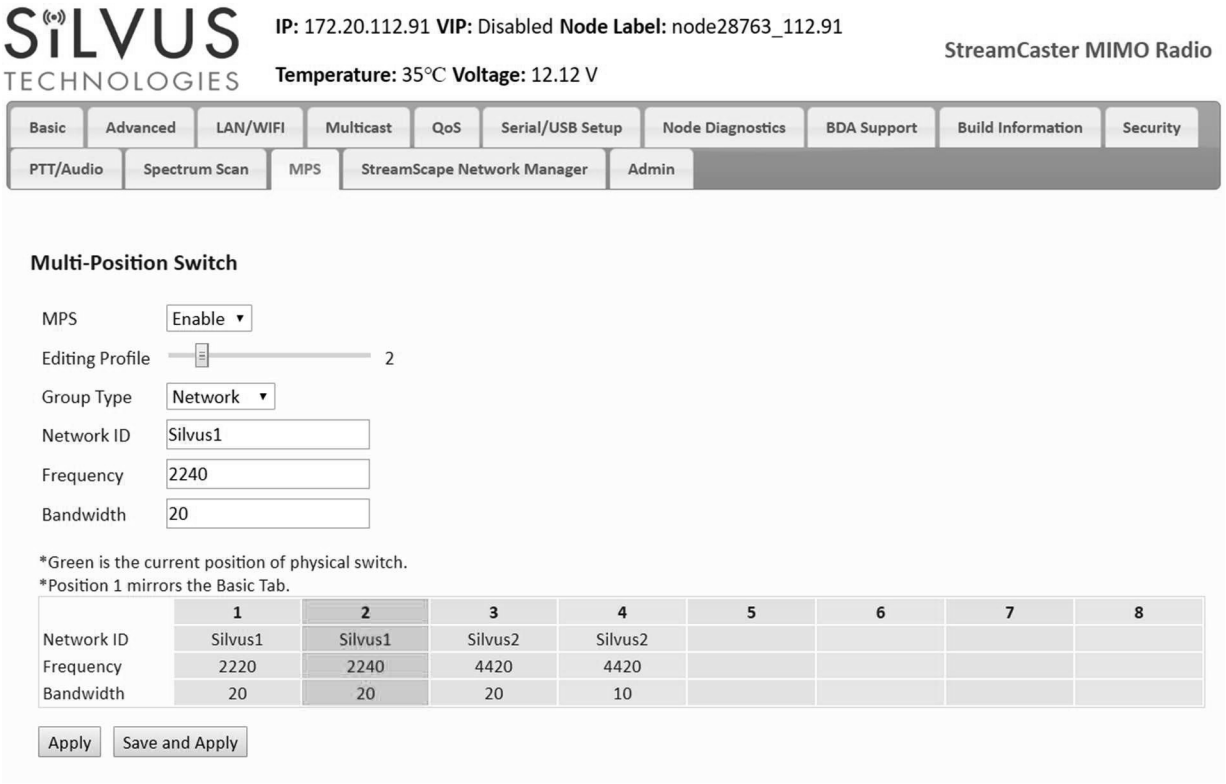


Figure 50 Multi-Position Switch

The Multi-Position Switch allows you to change various settings of the radio by using the new physical switch, no web GUI required (This is not available on all radios).

You must first configure the settings you want to correspond with each switch position. The "Editing Profile" slider represents which position is currently being edited. "Group Type" represents the collection of settings that will be applied. Only one "Group Type" is active at a given time. When the MPS switch is turned, the LED light on the radio will quickly flash green. This means the settings are being applied for this position. When the LED stops quickly flashing, the settings have been applied.

Position 1 is special. Any time settings are updated from the GUI without using the MPS page (i.e. Basic Tab, PTT/Audio Tab), position 1 will be updated with those results. The green highlight shows the current position of the physical switch.

If the radio boots up in position "Z," MPS will be disabled until the radio is rebooted in another position.

5.1.14 Admin Settings

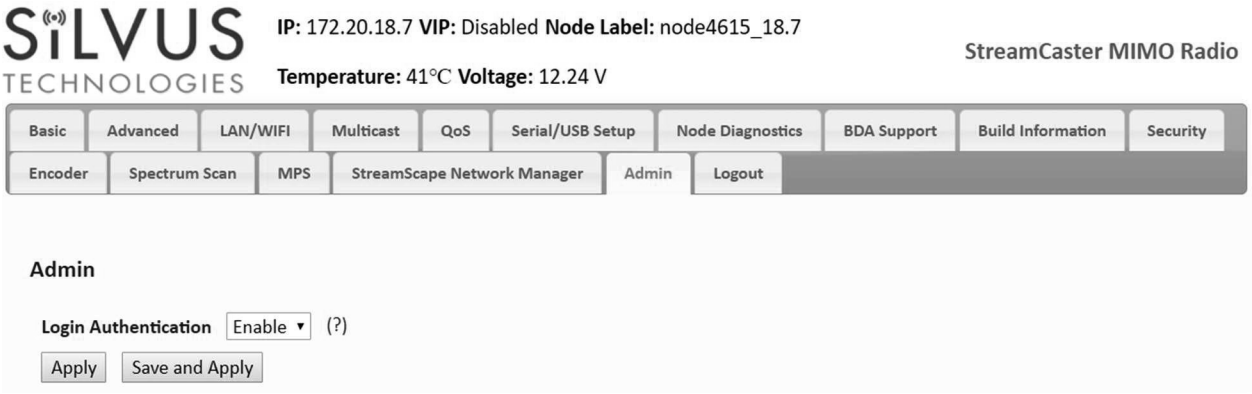


Figure 51 Admin Settings

The Admin Settings page provides the option of password protecting access to Streamscape. There are three usernames, Basic, Advanced, and Admin, each with increasing privileges on the GUI and backend API. For example, only Admin can access the Security tab. To enable, set the Login Authentication to Enable and provide a password. Once Login Authentication is enabled, access to Streamscape will require a username and password as shown below. To change the password, click "Change Password," then select the username whose password will change, type the Admin password, then type the new password.

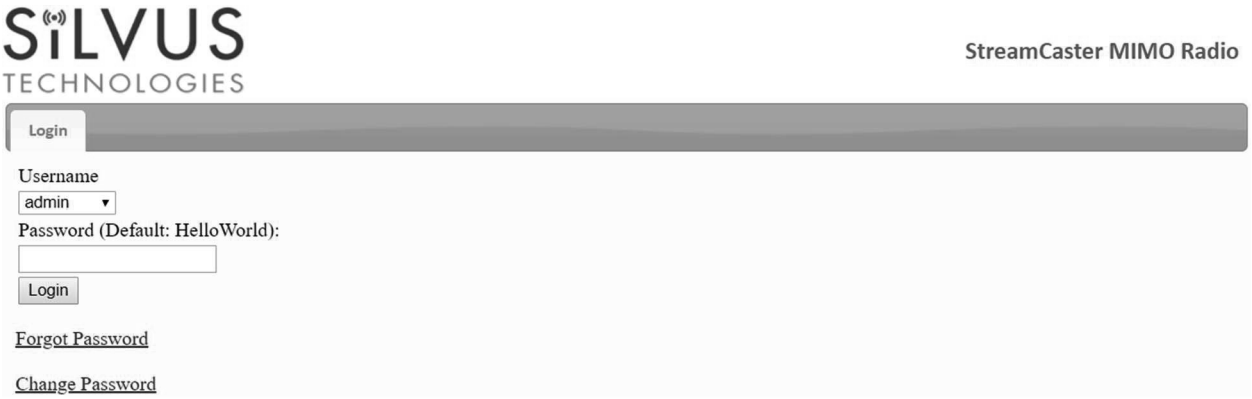


Figure 52 Login

Reset Password:

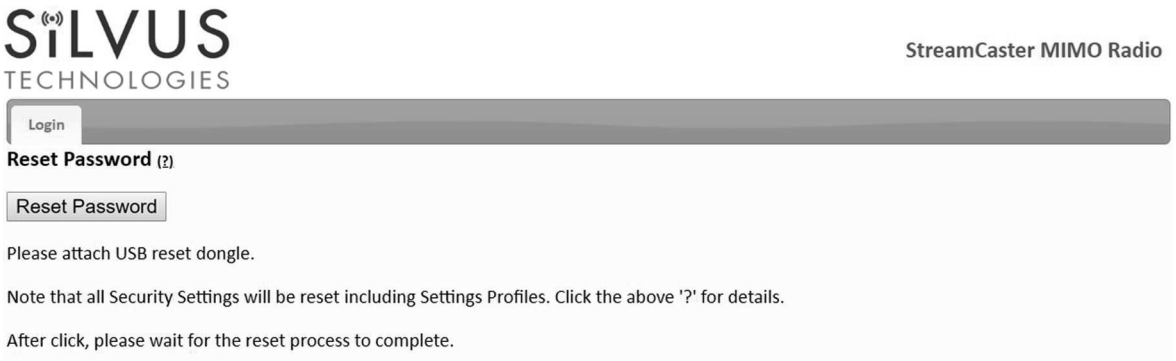


Figure 53 Reset Password

If a user forgets the password, click "Forgot Password." They can reset the password using a USB flash drive and a password reset key provided by Silvus. On the USB, the password reset key file must be called reset_pass.txt.signed. Note that since the SC3500 and SC3800 do not have USB ports, you will not be able to set a password for these radios.

This will set login passwords and all security keys to their defaults. This includes the Encryption Key, SSH Login Key, SSH Host Key, HTTPS Certificate, and Encryption Key Volatile. It will also erase all settings profiles. Also, if FIPS mode is off, it will turn off HTTPS and login mode. The current FIPS mode will not be changed.

5.2 StreamScape Network Manager

Silvus' StreamScape Network Management Utility was designed to monitor the status of a Silvus mesh network in real-time. The graphical interface network map, shown in **Figure 44**, allows users to quickly and effortlessly view the network topology and configure key parameters of the network. For ease of use, the Silvus StreamScape utility is designed to be accessible from a Firefox or Chrome web browser.

5.2.1 Network Topology

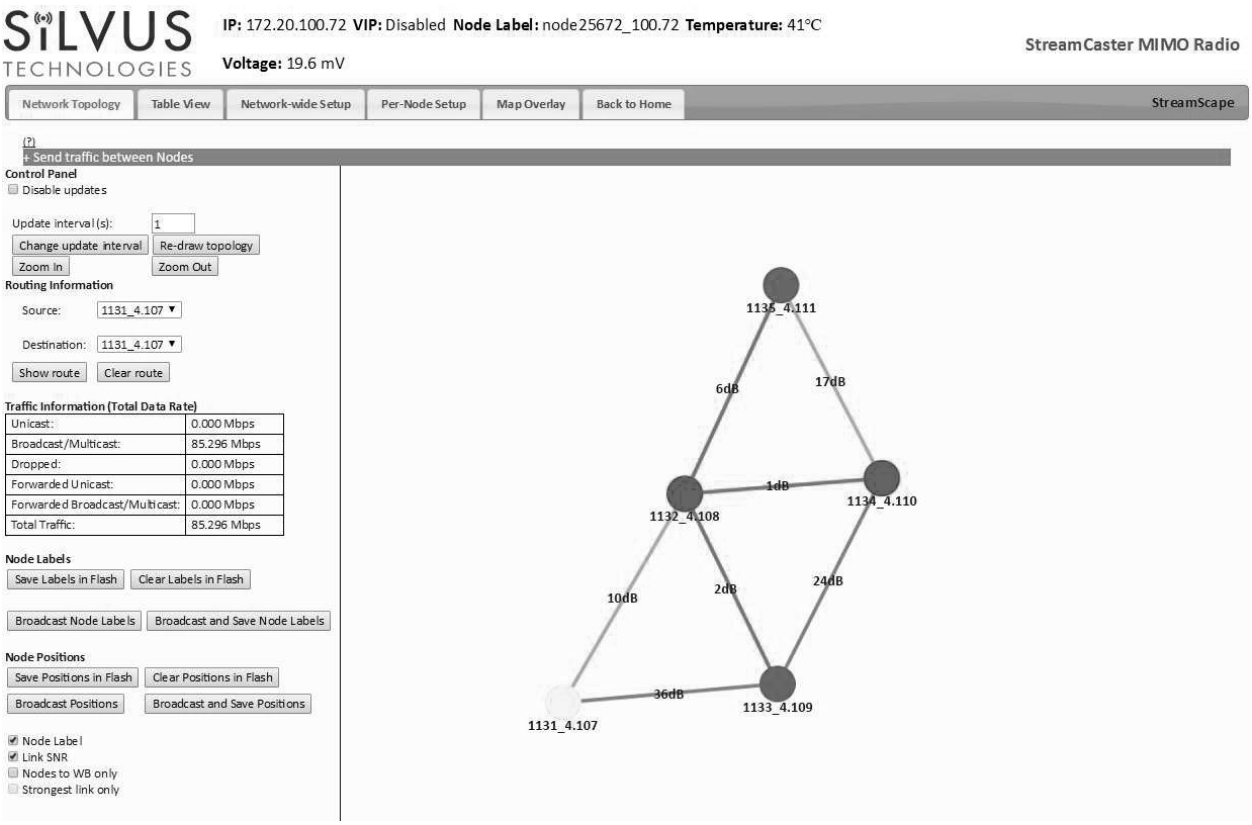


Figure 54 Silvus StreamScapeNetwork Manager

The network topology provides the user with real-time visual feedback of the network. Users will be able to determine several network characteristics at a glance with the following features:

- **Color Coded Link Health –** Color coding of each link in the network allows the user to quickly identify the weak links within a network. A link between two nodes will transition from green to yellow to red as the link weakens while also displaying the SNR of the link. This can be seen in **Figure 55**.

- **Route Health –** The Silvus StreamScape Utility will alert the user when too many packets are being routed through a single node. In such cases, a node will change from green to yellow to red as the packet queue increases (see '1132_4.108' and '1131_4.107'in **Figure 55**). This will allow the user to recognize the issue and rearrange the network accordingly. Table below also shows the values for each scenario.

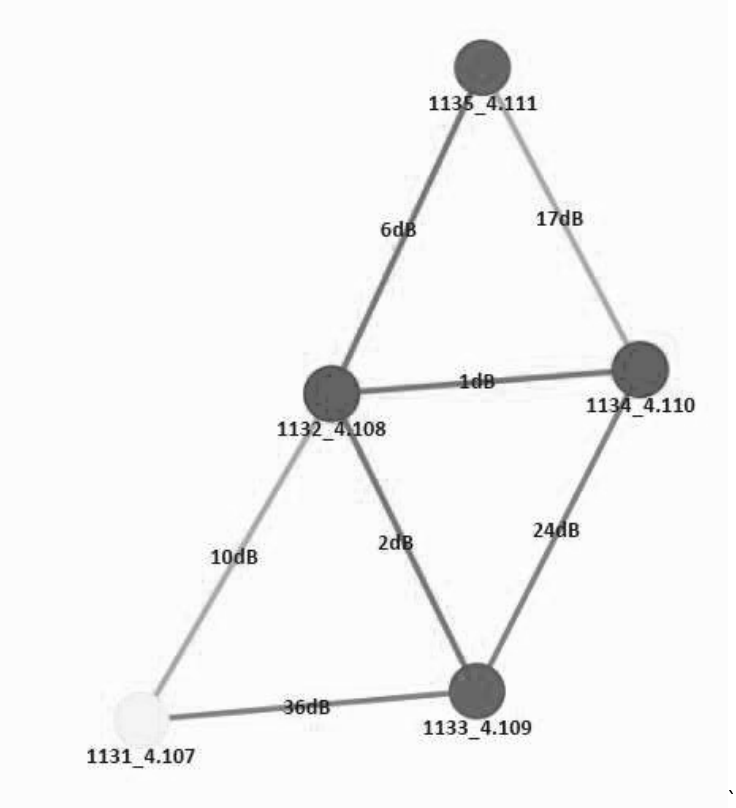


Figure 55 Example Network Topology

	Green	Orange	Red
Link	>20dB	10-20dB	<10dB
Node	<10 Packets in Queue	10-100 Packets in Queue	>100 Packets in Queue

Table 29 Color Coding for Links and Nodes

- **Routing Information –** The user can view the routing path between any 2 nodes within a network by simply specifying the source and destination node in the Control Panel on the left hand side. The path will turn bold as shown in **Figure 56** for the path from 'node4411' to 'node4569'.

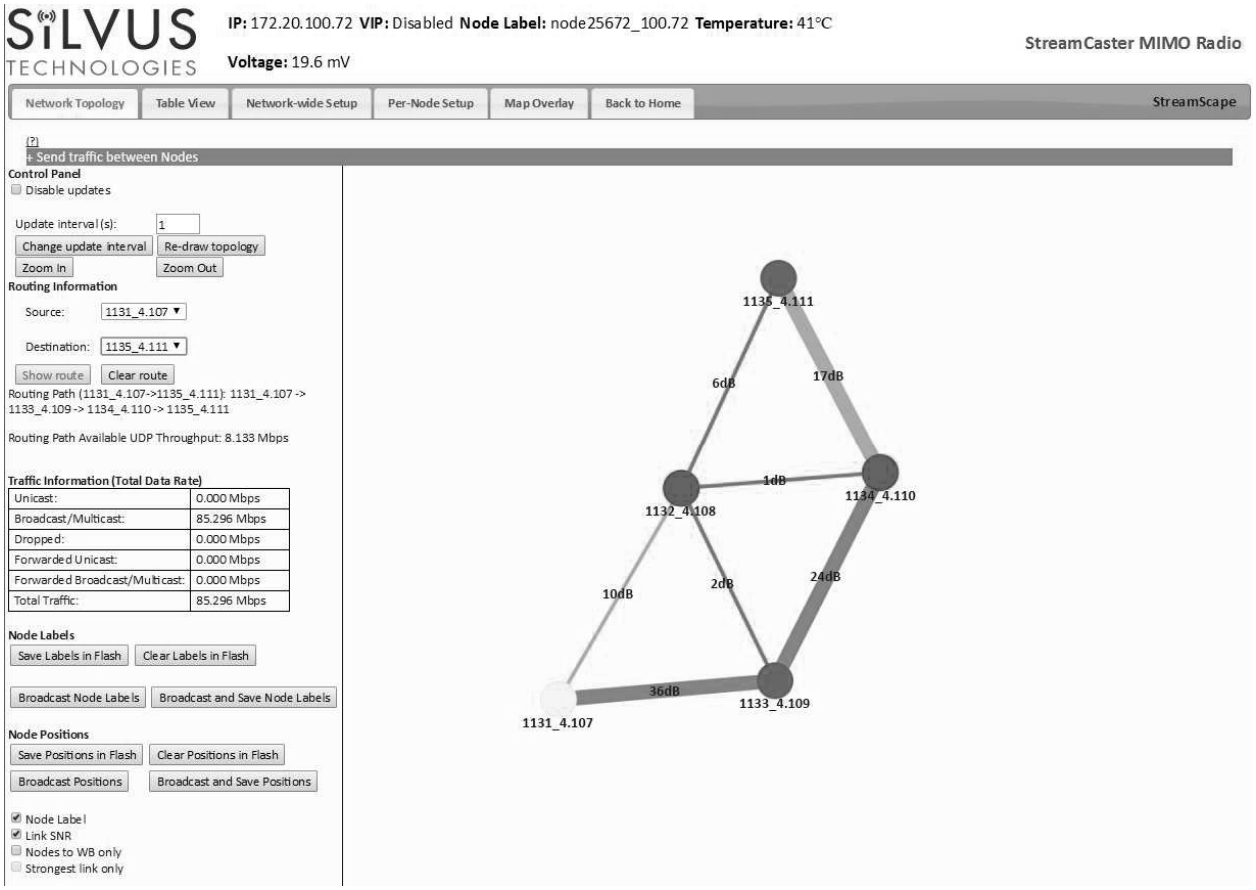


Figure 56 Routing Path

- **Custom Node Naming –** Naming each node in the network is as simple as double-clicking on the node name and typing in a new name as shown in **Figure 57**. Once this is done, the user need to hit enter to keep the node name. Otherwise it will change back to what it was. This feature enables quick identification of nodes in the field and is especially useful in mission critical situations with many mobile assets. The user can click on the 'Save Labels in Flash' button in the left pane to store the node names to the radio's flash memory. This will store the names on the radio even after the radio is powered off. The saved labels can also be cleared back to the defaults by clicking 'Clear Labels in Flash'. The node labels set in one radio can also be broadcasted to other radios in the network by clicking the 'Broadcast Node Labels' button.

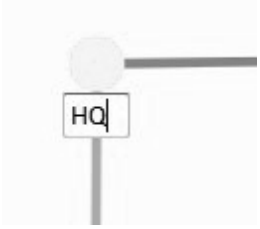
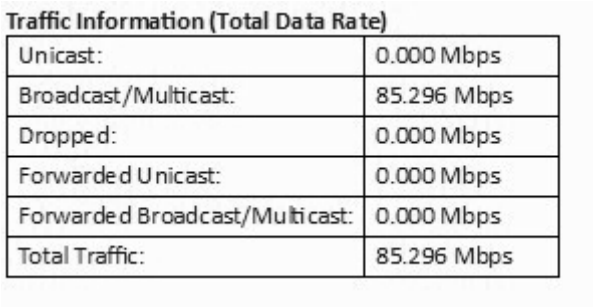


Figure 57 Custom Node Naming

- **Traffic Information –** The traffic information is shown in table form on the left side of the web GUI. It contains all the current network traffic information of the entire network.



Traffic Information (Total Data Rate)

Unicast:	0.000 Mbps
Broadcast/Multicast:	85.296 Mbps
Dropped:	0.000 Mbps
Forwarded Unicast:	0.000 Mbps
Forwarded Broadcast/Multicast:	0.000 Mbps
Total Traffic:	85.296 Mbps

Figure 58 Traffic Information

- **Individual Node Characteristics –** By simply rolling the mouse over any node in the network, users can view key operating characteristics of the node. **Figure 59** shows an example of this for 'node12593'. The characteristics shown are:

  - **Node ID**: The unique node ID assigned to each node at time of manufacture. This cannot be changed.

  - **IP**: IP address of the node.

  - **MAC:** MAC address of the node.

  - **Connections**: Number of direct connections to node. Each directly connected node is listed in the following format:

    <Node Name> <RX SNR> <TX MCS> <Pkts in TX Queue> <Num. of Spatial Streams>

<Air Time %><Data Rate (Mbps)><RSSI Ch1> <RSSI Ch2> <RSSI Ch3> <RSSI Ch4>

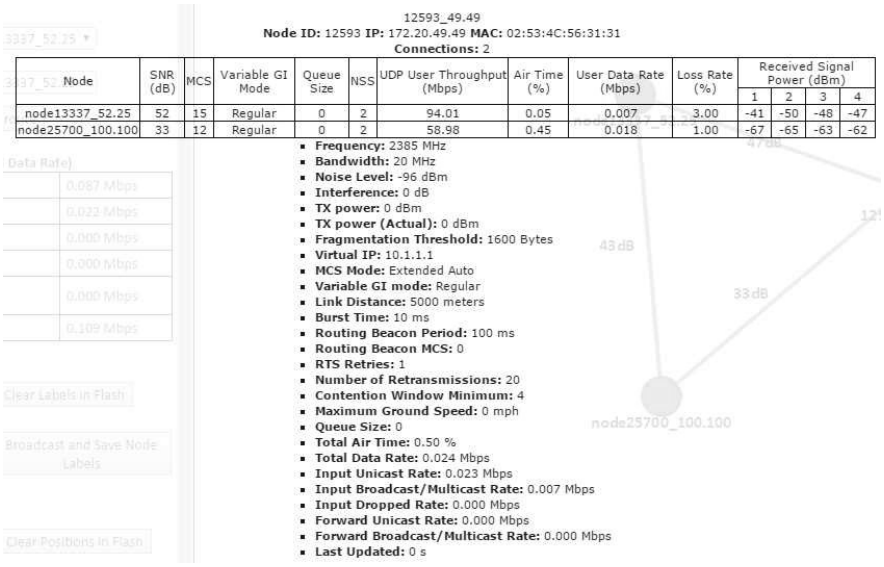
Notes:

- The 'Air Time' specifies the percentage of time the radio is transmitting.
- Data rate shown is actual user data rate in Mbps.
- MCS or NSS of N/A signifies that no data has been sent to that radio yet.

- **Frequency:** RF center frequency of the node.
- **Bandwidth:** RF bandwidth of the node.
- **Noise Level:** Received noise level of the node.
- **Interference:** Approximate in-band interference level.
- **TX Power:** Total target transmit power of node.
- **TX Power (Actual):** Actual transmit power of node. This value may differ from the target transmit due to temperature variation or inability to transmit a clean signal with the selected MCS at the target power.
- **Fragmentation Threshold:** Chosen fragmentation threshold.
- **Virtual IP:** Secondary IP address of node (0 if none set).
- **MCS Mode:** Transmit MCS of node.
- **Variable GI mode:** The variable GI mode setting for this node.

- **Link Distance:** Link distance setting of node.
- **Burst Time:** Burst time setting of node.
- **Routing Beacon Period:** Routing Beacon Period setting of node.
- **RTS Retries:** RTS Retry setting of radio.
- **Contention Window Minimum:** Low Priority Contention Window Minimum setting of node.
- **Maximum Ground Speed:** Maximum Ground Speed setting of node.
- **Queue Size:** Number of packets currently waiting to be transmitted.
- **Total Air Time:** Total percentage of air time being used by this radio.
- **Total Data Rate:** Total data rate in Mbps being transmitted from this radio.
- **Input Unicast Rate:** Total data rate pushed into the radio as Unicast
- **Input Broadcast/Multicast Rate:** Total data pushed into the radio as Multicast
- **Input Dropped Rate:** Total data rate dropped by the radio
- **Forwarded Unicast Rate:** Total data rate forwarded by the radio as Unicast
- **Forwarded Broadcast/Multicast Rate:** Total data rate forwarded by the radio as Multicast

- **Last Updated:** Duration that has passed in seconds since last update.



Node	SNR (dB)	MCS	Variable GI Mode	Queue Size	NSS	UDP User Throughput (Mbps)	Air Time (%)	User Data Rate (Mbps)	Loss Rate (%)	Received Signal Power (dBm)			
										1	2	3	4
node13337_52.25	52	15	Regular	0	2	94.01	0.05	0.007	3.00	-41	-50	-48	-47
node25700_100.100	33	12	Regular	0	2	58.98	0.45	0.018	1.00	-67	-65	-63	-62

Figure 59 Individual Node Characteristics

- **Link Characteristics –** By simply rolling the mouse over any link in the network, users can view key operating characteristics of that link. **Figure 60 Link Characteristics** shows an example of this for the link between 'node25700' and 'node12593'. The characteristics shown are:

  - **SNR**: The SNR of the link in each direction.

  - **MCS**: The MCS used to transfer data in each direction.

  - **UDP User Throughput:** The estimated UDP User Throughput available for each direction of the link. This is estimated based on the current MCS used for transmission.

  - **Queue Size:** Number of packets in TX Queue in each direction.

  - **NSS:** Number of Spatial Streams in each direction.

  - **Air Time:** Percentage of air time used in each direction

- **Data Rate:** Data rate in each direction

- **Data Loss Rate:** Percentage of data lost during transmission

- **Received Signal Powers:** Received signal power for each antenna in each direction.

Figure 60 Link Characteristics

- **Send Traffic Between Nodes –** Users can send test traffic across radios within a network using the built-in iPerf feature. This feature can be accessed by clicking the blue bar at the top of the topology view, titled “Send traffic between nodes”. This will open up a drop down menu where users can specify UDP/TCP data, source/destination, port, time to send, and datagram size.

  - **Source:** Radio that sends data (Client)

  - **Destination:** Radio that is listening (Server)

  - **Destination port:** Port number for the data transfer

  - **Time to Send:** Amount of time user wants to send data

  - **Bandwidth to Send:** Data rate to send, in Mbps

  - **Datagram Size:** Size of the datagram

  - **Effective Bandwidth:** The actual network load.

  - **Jitter:** The variation in delays in the received packet.

  - **Lost/Total Datagrams:** The amount of packets lost vs total packets sent

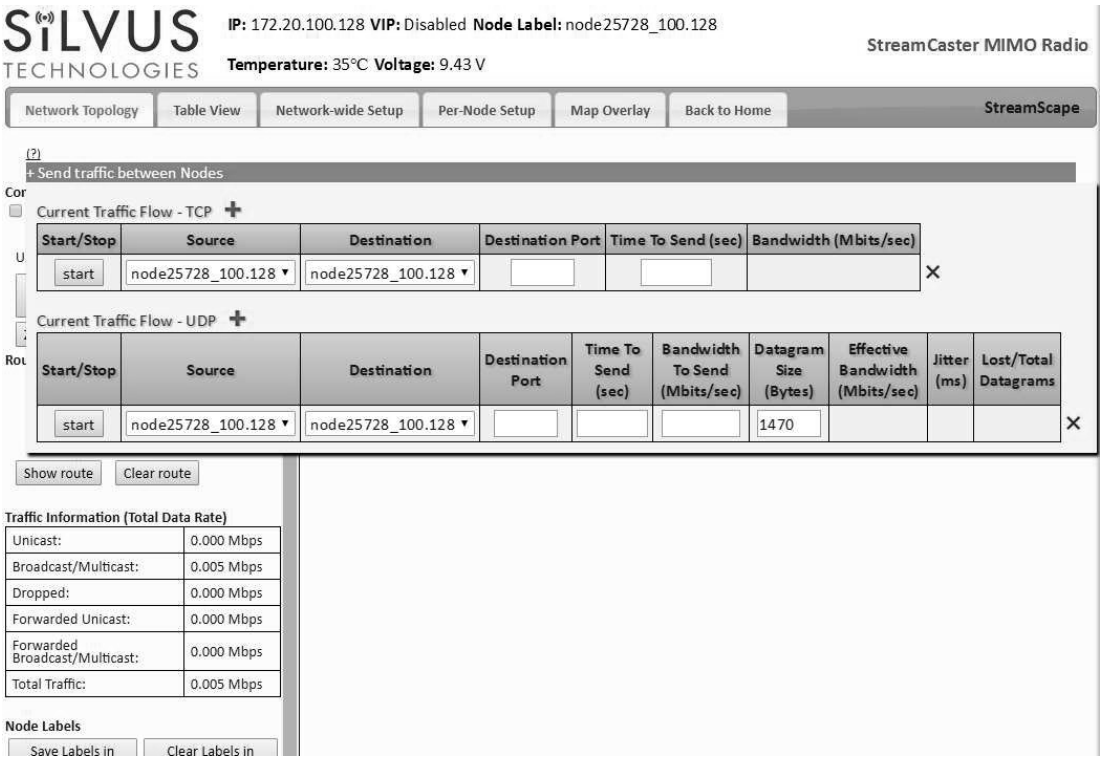
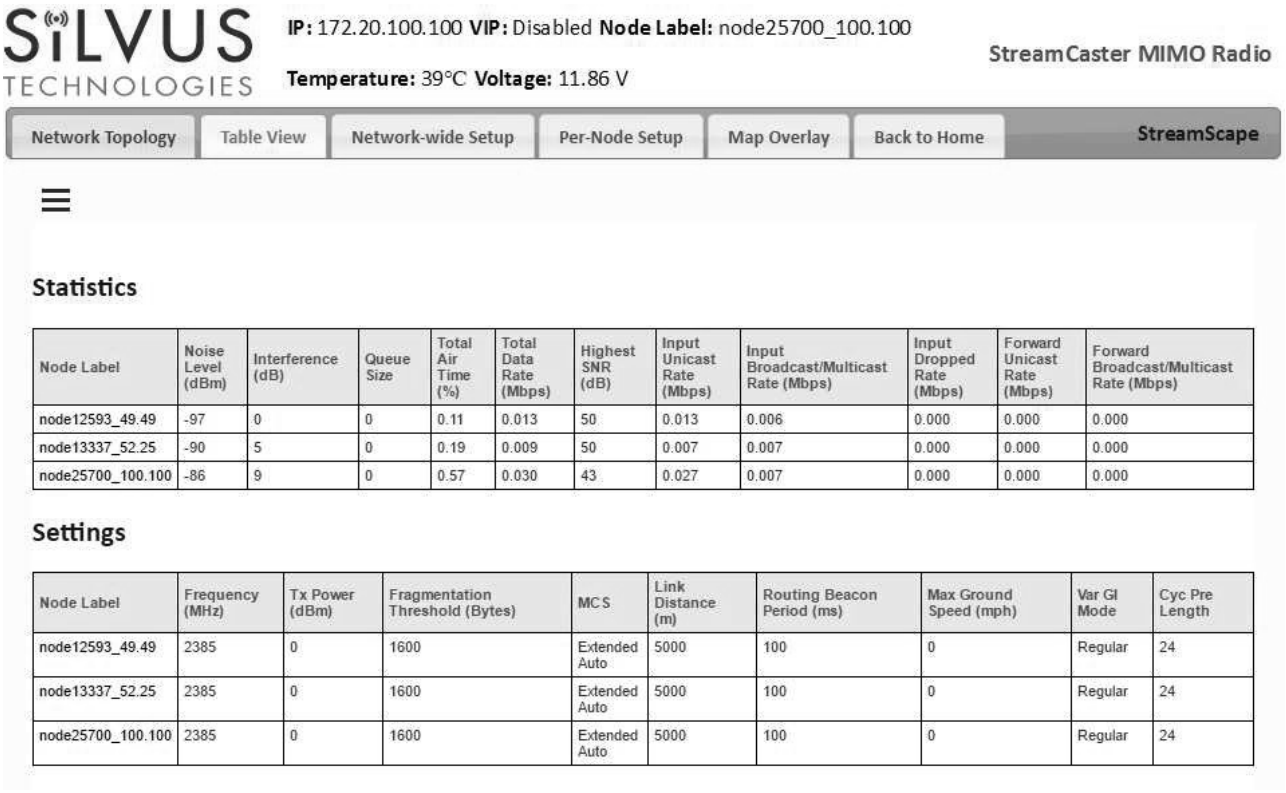


Figure 61 iPerf Function within GUI

5.2.2 Table View



Node Label	Noise Level (dBm)	Interference (dB)	Queue Size	Total Air Time (%)	Total Data Rate (Mbps)	Highest SNR (dB)	Input Unicast Rate (Mbps)	Input Broadcast/Multicast Rate (Mbps)	Input Dropped Rate (Mbps)	Forward Unicast Rate (Mbps)	Forward Broadcast/Multicast Rate (Mbps)
node12593_49.49	-97	0	0	0.11	0.013	50	0.013	0.006	0.000	0.000	0.000
node13337_52.25	-90	5	0	0.19	0.009	50	0.007	0.007	0.000	0.000	0.000
node25700_100.100	-86	9	0	0.57	0.030	43	0.027	0.007	0.000	0.000	0.000

Node Label	Frequency (MHz)	Tx Power (dBm)	Fragmentation Threshold (Bytes)	MCS	Link Distance (m)	Routing Beacon Period (ms)	Max Ground Speed (mph)	Var GI Mode	Cyc Pre Length
node12593_49.49	2385	0	1600	Extended Auto	5000	100	0	Regular	24
node13337_52.25	2385	0	1600	Extended Auto	5000	100	0	Regular	24
node25700_100.100	2385	0	1600	Extended Auto	5000	100	0	Regular	24

Figure 62 Table View

The table view tab shows all the statistics and setting profiles in table view. Users can select what is needed through the drop-down menu on the upper left side. The dropdown is shown in **Figure 63 Table View (Settings)**

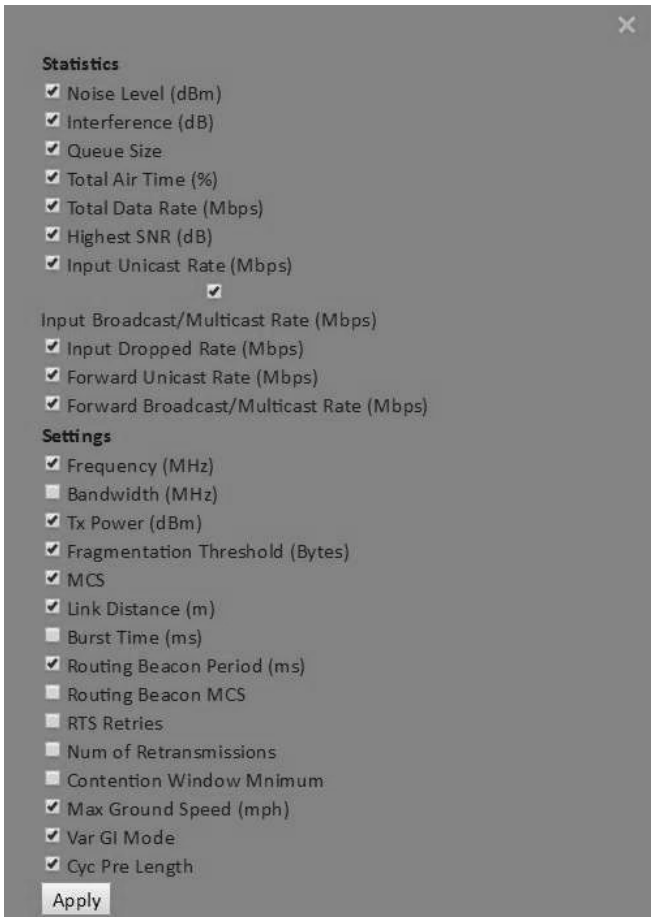


Figure 63 Table View (Settings)

5.2.3 Network-wide Setup

Using the network-wide setup users can configure key parameters of every node in the network with just one click. Users simply need to check off the parameters they wish to be updated across the network and click on *Apply* to apply but not write new values to flash or *Save and Apply* to apply and save values to flash. The *Broadcast Update Interval* field determines how often, in seconds, the new parameters will be broadcast to the entire network. A list of all nodes will appear on the right with a check box next to each node. This box will be checked off as each node receives the update.

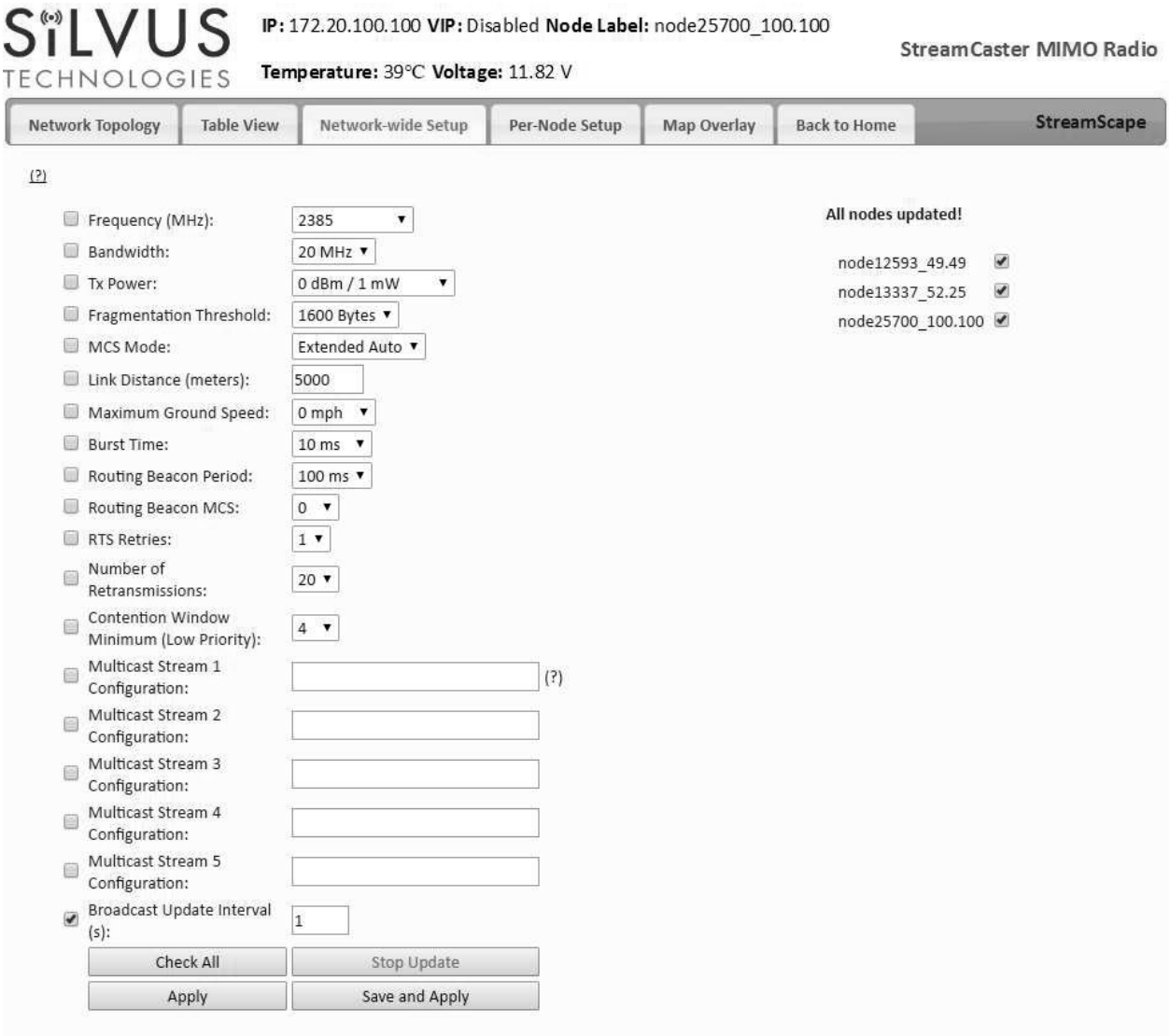


Figure 64 Network-wide Setup

5.2.4 Per-Node Setup

The per-node setup can be used to modify key parameters of individual nodes within the network. As shown in **Figure 65**, users will see a list of all nodes available within the network. The directly connected node is listed first with the rest ordered lexically. From here, users can click on an individual node and modify its parameters. Any parameters changed from this interface can either be applied or saved and applied.

In addition, this page can be used to upgrade a radio's firmware by simply choosing the upgrade image from your desktop and uploading it to the radio. This field can be used to upgrade the radio root file system, linux kernel, or uboot. The upgrade system accepts the root file system image for upgrade or a tar file containing up to 3 files (uboot, kernel, rootfs) for upgrade. A radio reboot will be required after update before the changes take effect.

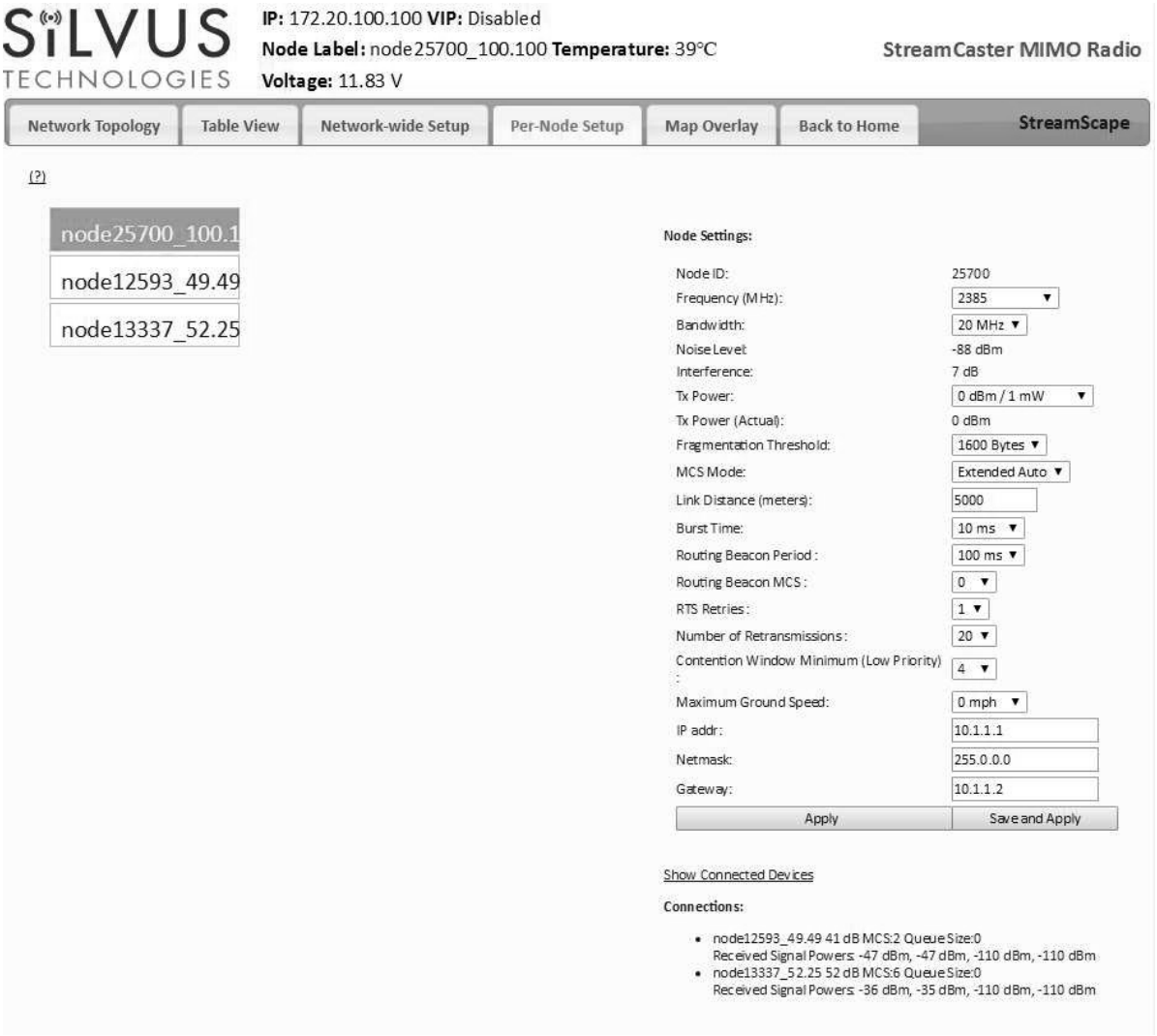


Figure 65 Per-Node Setup

5.2.5 Map Overlay

The Map Overlay page provides an easy to use method of tracking the location of nodes in real-time. Nodes with GPS modules attached will be placed on the map as shown in **Figure 66**.

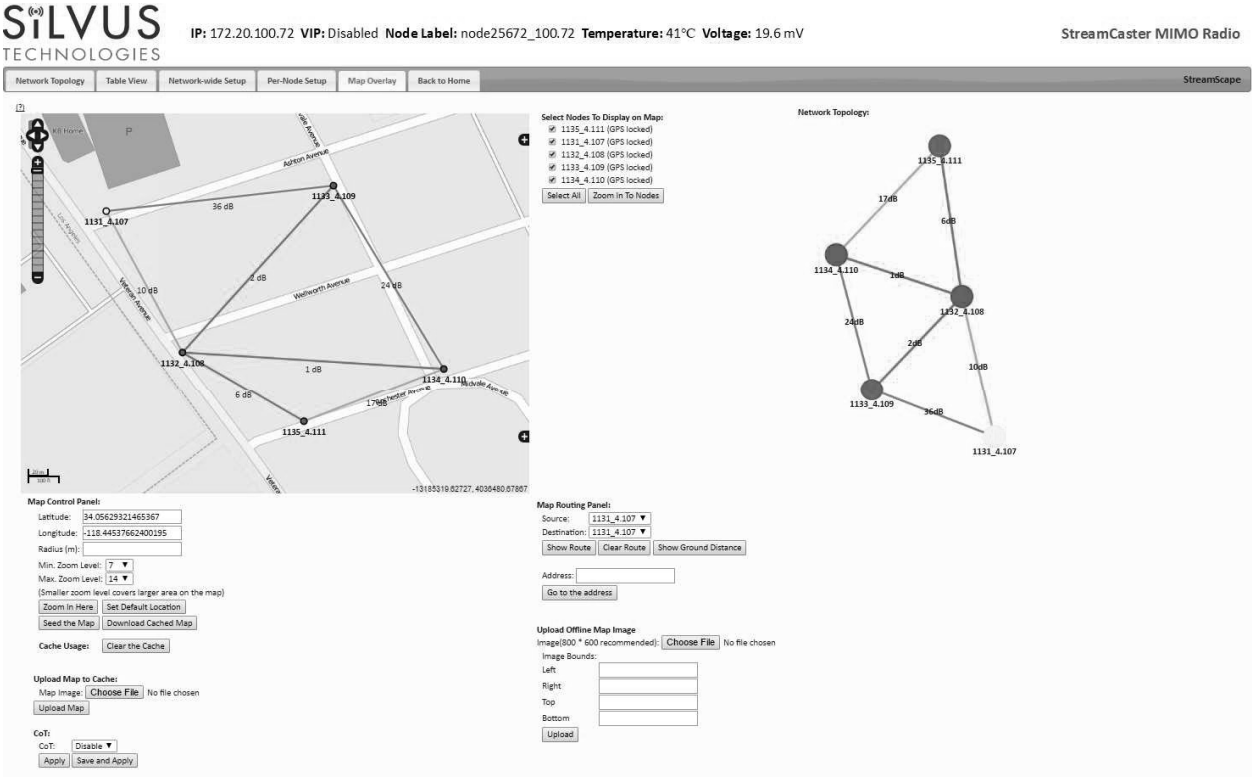


Figure 66 Map Overlay

For convenience, a small copy of the network topology is displayed on the right-hand side of the page. This allows users to clearly view the network characteristics in instances where nodes are physically close to one another and difficult to distinguish on the map overlay.

5.2.5.1 Map Options

There are 4 map options currently available in the Map Overlay view. The default map is OpenStreet Maps. OpenStreet Maps and OpenStreet Maps Silvus can be saved to the radio's internal memory for offline use. For instructions to Download OpenStreet Maps into the radio, see section 5.2.5.2. OpenStreet Maps Silvus is a version of OpensStreet maps which is hosted on Silvus' servers in case of an interruption in service with OpenStreet Maps. The Silvus maps currently only cover the United States.

In Addition to OpenStreet Maps, Google Maps and Google Satellite are also available. This can be changed by clicking the '+' symbol at the top right of the map:

Figure 67 Google Maps

Note that Google Maps and Google Satellite require an active internet connection on the viewing computer. These maps cannot be saved for offline use.

Offline Map Image:

In addition to the preset map options, the user can also upload a custom image or blueprint in place of the map.

Figure 68 Offline Map Image

To upload a custom image (800 x 600 pixels recommended), first choose the file from your desktop. You will then need to provide the image bounds. These bounds will be the latitude of the left and right bounds of the image and longitude of the top and bottom bounds of the image. Once entered, click upload and there will now be a 4th option when clicking the '+' at the top left of the map overlay.

5.2.5.2 Downloading Maps

An internet connection is required to obtain map data, however, users can cache map data on a node beforehand. For map caching follow these steps:

1. Attach the radio to a laptop and open the advanced tab.
2. Set the Virtual IP address, netmask and gateway to values appropriate for your local network. Your local network should be able to access the internet.
3. Attach the radio to your local network and open the Map Overlay tab.
4. Input the address of the location you wish to download
5. You now have two options for caching map data:
    a. Zoom/pan around the area you are interested in at the zoom level you will be using. This will automatically cache the map data at this zoom level.
    b. Fill in the radius field (in meters), set the Min/Max zoom levels and click on 'Seed the Map'. This is a beta feature and will attempt to cache the entire area for all appropriate zoom levels. Users should be careful in using this feature since it may take some time and will use up the radio's available memory. For reference, a radius of ~3000m will use approximately 5 percent of the total memory.

5.2.5.3 Manual GPS for Nodes without GPS Module

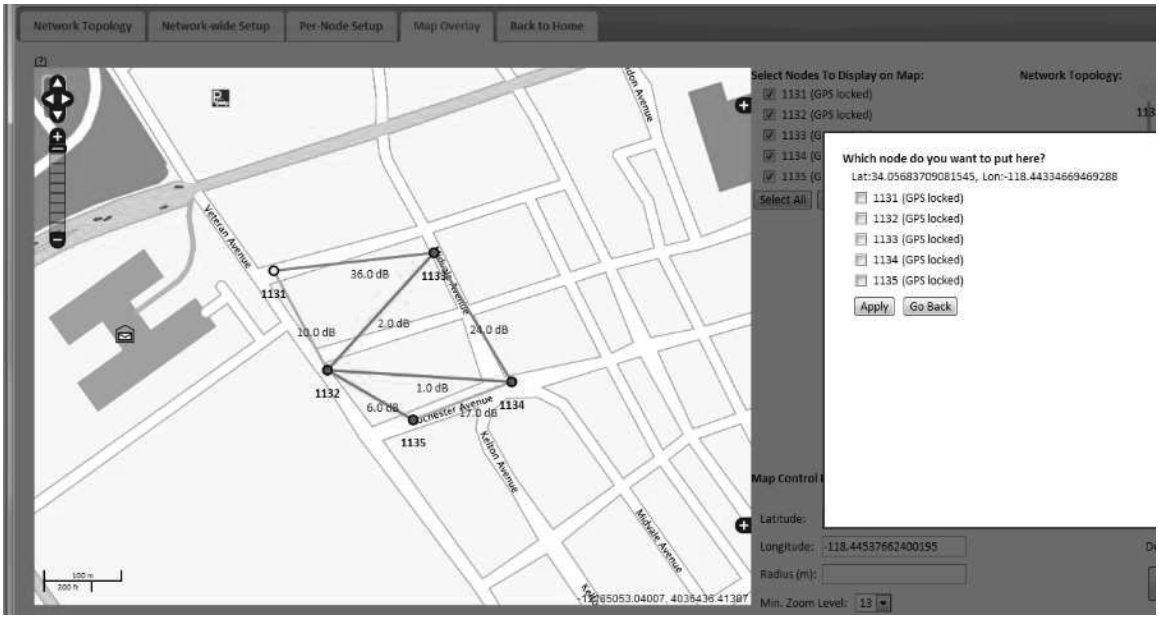


Figure 69 Placing Nodes on the Map

If there are nodes within the mesh that do not have a GPS module connected, or are located in an area with no GPS connectivity, the user can easily place the node on the map by right clicking on the desired location on the map and choosing which node to place there. These values will be ignored if GPS coordinates are available via a GPS module.

5.2.4.4 Cursor on Target

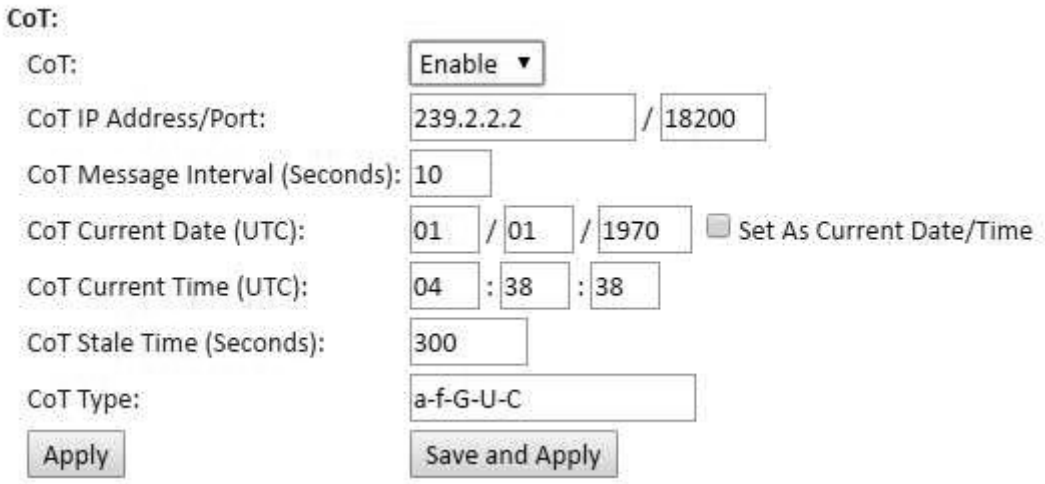


Figure 70 Cursor on Target Settings

Cursor on Target is an exchange standard that is used to share information about targets.

- **CoT:** Enable/disable cursor on target
- **CoT IP Address/Port:** IP address/port for the communication to establish
- **CoT Message Interval (Seconds):** How often to send CoT messages
- **CoT Current Date (UTC):** Time stamp of the date. If *Set AS Current Date/Time* is selected, it will be set as the current time displayed on your computer
- **CoT Current Time (UTC):** Time stamp of the time
- **CoT Stale Time (Seconds):** Data outside of this time window becomes invalid
- **CoT Type:** The event type of the target

6. FIPS Mode

6.1 Enable FIPS Mode

The following steps are required to make the radio FIPS compliant.

1. Enable FIPS mode under Security -> Encryption tab. This will require a reboot and will erase all setting profiles, reset the encryption key, both SSH keys, the HTTPS certificate, and the login passwords to their factory default. It will also turn on HTTPS and Login Authentication.

2. After the radio comes back online, you will need to login to continue. You must change the default password of "HelloWorld," for all three users. Do this by clicking "Change Password," and then follow the instructions in section 5.1.13 Admin Settings.

3. Next go to Security -> Key Management. You must change the SSH Login Key, SSH Host Key, and HTTPS Certificate from their defaults. See section 5.1.10 under Key Management for details.

4. Now you must create an encryption key that will be shared amongst all radios on a network. For initial setup, you must have a direct connection to each radio from your laptop (since a mesh cannot be formed without a shared encryption key). On the first radio, click Generate Random Key, then click Apply. For the rest of the radios, instead of clicking Generate Random Key, copy/paste the first generated key to the rest of the radios under the same section.

    - If you want to change the encryption key after initial setup, you must carefully sequence the order in which you change the keys if you don't have a direct connection to all radios. First change the radios at the very edge of the network. As soon as you do this, those radios will be disconnected from the network. Now change the new radios at the edge of the network. After you have changed the encryption key for all radios on the network, they will all reconnect again.

6.1.1 Potential User Errors

- Do not use the same encryption key you were using in non FIPS mode because these may have been broadcasted in plain text. Generate new ones once in FIPS mode.

6.2 List of Security Parameters

- **Passwords (Basic, Advanced, and Admin User):** Used to login to the radio as either Basic, Advanced, or Admin user.
- **Encryption Key (also called RF-Auth-Key):** This is a 256-bit sequence, represented as 64 hex numbers. It is used to establish an encrypted connection in a network.
- **SSH Host Key:** This key is used for authenticating the radio to all machines that want to connect to it via SSH.
- **SSH Login Key(s):** These are ecdsa private/public key pairs. They are used for authorizing SSH access to the radios. These key pairs are used instead of passwords since they are more secure.
- **TLS Host Key (also called HTTPS Certificate):** This certificate is used to establish a HTTPS connection. The underlying elliptic curve keys can be either secp256r1, secp384r1, or secp521r1.

7. Wired Backbone

Wired Backbone extends the StreamCaster mesh functionality over LAN (Ethernet) and WAN (Internet) links. This feature is transparent to end-users - they do not have to re-configure their devices in any manner to use this feature.

The StreamCaster routing protocol will automatically detect and route data on wired links to preserve air bandwidth.

7.1 LAN Backbone

The LAN backbone feature allows more than one radio to be connected to a LAN.

7.1.1 Implementation

One of these radios must be configured as a "gateway" radio. This radio then begins listening promiscuously on its ethernet interface to "register" all devices on the LAN as being connected to the gateway radio. At the same time, it auto-detects other non-gateway radios connected to the LAN and establishes "wired" links to them. StreamScape Web GUI will show LAN links with SNR of 150 dB to differentiate from wireless links.

The non-gateway radios do not register any devices, they merely act as relays. The gateway radio will forward traffic originating from the LAN, destined for a device attached to a wireless radio, to the non-gateway radio that is closest to the destination. Similarly, any traffic originating from a device attached to a remote wireless radio, destined to a device on the LAN will be forwarded by non-gateway radios to the gateway radio. The gateway radio will then send it to the device.

Currently we support data rates of up to 65 Mbps on the LAN without encryption. Since all LAN traffic goes via the gateway radio, this is the upper limit of all traffic that can enter or go out of the LAN from/to devices connected to wireless radios. Of course, this limit does not affect the throughput between two devices connected directly to the LAN backbone.

7.1.2 Use Case

Consider the following scenario. A business wants to do video monitoring of its grounds. High speed LAN hookups are available only in the HQ building. They want to use the StreamCaster radios on towers to provide complete coverage of the grounds. All video feeds are sent back and displayed at the HQ. To conserve air bandwidth and possible interference to other users, we want video data to go through the high-speed LAN backbone as much as possible. The below diagram shows the scenario.

Towers 1-3 are equipped with IP cameras attached to StreamCaster radios 1-3. Radios 4-6 are mounted on three sides of the HQ building with their Ethernet interfaces connected to the high-speed LAN. Tower 1 can only communicate wirelessly with radio 4, Tower 3 with radio 5 and Tower 2 with radio 6. Video from Tower 1 will flow wirelessly to radio 4, then via the LAN backbone to the HQ viewer which is also attached to the LAN backbone. Even though the radios 4-6 may communicate wirelessly, they will choose to do so via the LAN backbone.

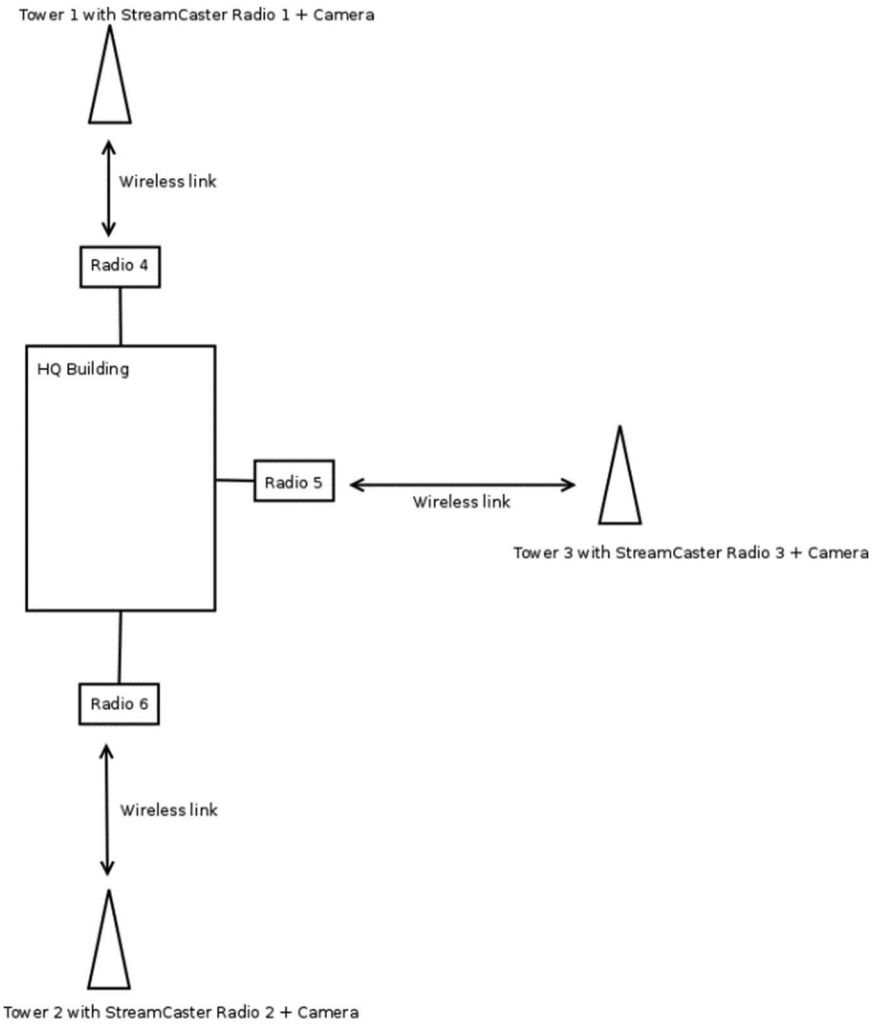


Figure 71 LAN Backbone Example

7.2 WAN Backbone with Roaming

The WAN backbone feature allows the wireless mesh network to extend over Internet links. Multiple geographically separate “sites” can be connected into one single layer 2 network as long as each site has

an uplink to the Internet. The roaming feature allows mobile devices connected to StreamCaster radios to roam from one site to another without any network re-configuration.

7.2.1 Implementation

Each site wishing to become part of the wireless mesh needs to connect one StreamCaster radio to its LAN. Such a radio has to be configured to connect to a remote VPN server using the N2N protocol. Radios from multiple sites will be connected at layer 2 via the N2N VPN server creating a single broadcast domain for such nodes. By broadcasting routing packets in this domain, the nodes will auto-detect each other and establish WAN links. Such links will appear on the StreamScape GUI with a link SNR of 120 dB to differentiate from LAN links (150 dB) and wireless links.

The N2N VPN server will try to establish peer-to-peer links between the radios if it can. Under some cases (e.g. symmetric NATs), this is not possible, in which case traffic between the peers is relayed by the N2N server.

The N2N server can be hosted at any server with a public IP on the Internet. As a proof-of-concept, a server has been set up on Amazon Web Services. Currently we support up to 10 Mbps unencrypted between any two sites.

7.2.2 Use Case

Consider a military scenario where a platoon of soldiers begins its mission at an HQ, then breaks up into two groups. Each group has at least one soldier with an uplink to the Internet (provided by a 4G card). The HQ also has an uplink to the Internet. Every soldier and the HQ have a StreamCaster radio attached to their devices.

The soldiers in the two groups want seamless and transparent communication between 1) other soldiers in the same group 2) soldiers in the other group 3) back to HQ. Some lone soldiers (e.g. Soldier A with a StreamCaster radio) may break up from each group and move about on their own. As they get close to group 1, 2 or the HQ, they should be able to immediately establish communication and talk to all other soldiers in the network.

The StreamCaster radios connected to the uplinks in Group 1-2 and the HQ will automatically connect and form WAN links.

Note that the WAN and LAN backbone are complementary features. E.g. at the HQ, multiple radios can be connected to a LAN backbone so that any approaching soldier or group has a direct line of sight wireless connection to the HQ.

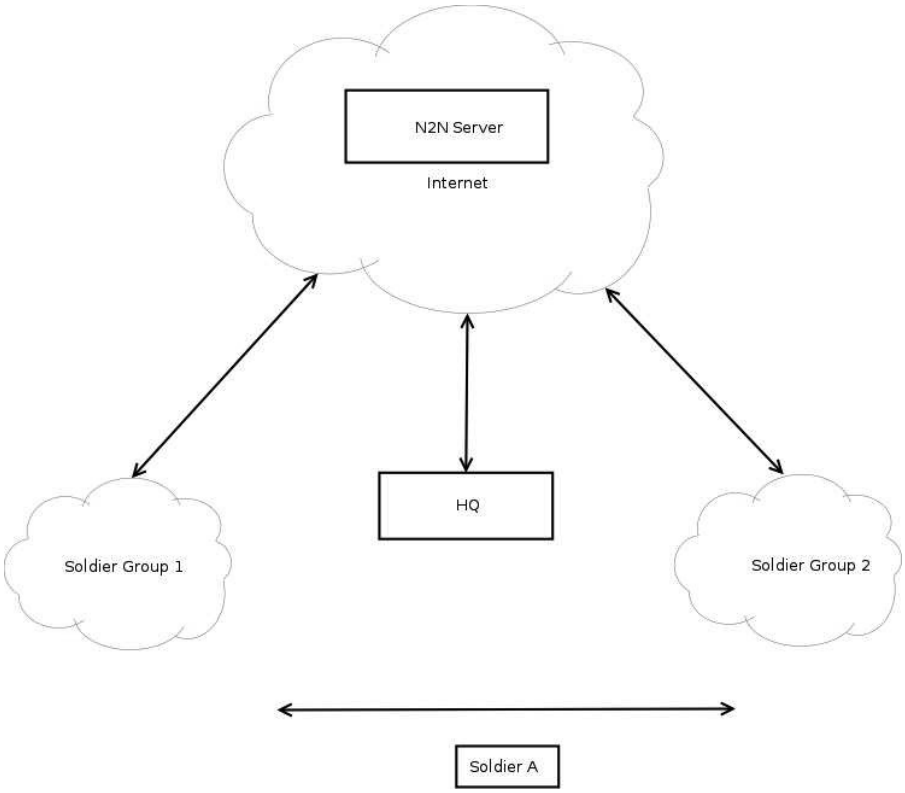


Figure 72 WAN Backbone Example

8. Custom Frequency Plan

8.1 Accessing and Installing CFP

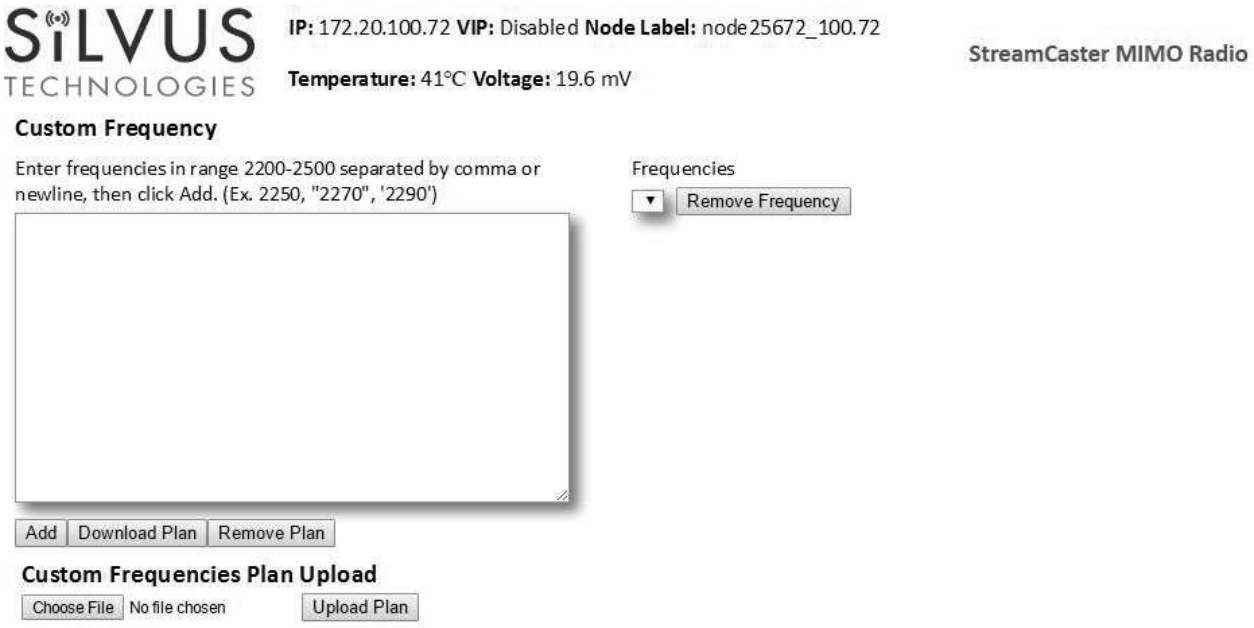


Figure 73 Custom Frequency Page

There are two ways to install the frequency plan. The first method is simpler. Users can simply click on *Create Custom Frequencies* next to the frequency selection window to get to the custom frequency page shown in **Figure 63**.

- **Add:** Add the frequencies in the text box to the list
- **Download Plan:** Download the frequency plan the radio is currently using
- **Remove Plan:** Removing the entire frequency plan. If this field is left empty, the radio will use the default frequency plan.
- **Download Plan:** Download the current frequency plan to a file that can be uploaded to other radios.
- **Remove Frequency:** Remove the currently selected frequency.
- **Custom Frequencies Plan Upload:** Upload the selected frequency plan.

The second method requires accessing the hidden Custom Frequency Plan page. Note radios on older firmware only support this method.

The hidden Custom Frequency Plan page can be accessed via http://<radio IP>/custom_freq.sh

The interface will allow an upload of a custom frequency plan file which should be in the following format:

```
{
    "type": "custom_frequency_plan",
    "name": "cfp_example",
    "description": "CFP Example",
    "frequencies": [
      "2412",
      "2417",
      "2422",
      "2427",
      "2432",
      "2437",
      "2442",
      "2447",
      "2452",
      "2457",
      "2462",
      "2467",
      "2472",
      "5745",
      "5765",
      "5785",
      "5805",
      "5825"
    ]
}
```

(Put the above format in a Text file. Name/description can be changed)

Custom Frequency Plan Text file example:
https://drive.google.com/file/d/0ByThlCSjgHe1TDMtZ2xDXzhEblE/view?usp=sharing

The numbers can be changed to the frequencies desired. The name of the text file does not matter in order to be utilized. After uploading the file, the web interface will be populated with the Custom Frequency Plan.

Note:
Once installed, the Custom Frequency Plan will be cross-checked with hardware capability and the licensed frequency range previously installed on the radio. The Custom Frequency Plan will only change what is displayed. It will not give new frequencies that are previously out of licensed range.

9. Streaming Response

Some users may be interested in streaming specific information from the radio e.g. RSSI, noise floor, temperature, etc. After enabling the response, they need using the above commands, the radio will transmit the desired information in the form of UDP packets to a specific IP address and port. The format of each report message will be in the type-length-value format as shown below:

TYPE LENGTH VALUE TYPE LENGTH VALUE …

- TYPE and LENGTH will be 16-bit unsigned integers in network-endian format.
- TYPE indicates the kind of information being transmitted. Pre-defined types are listed later in this document.
- LENGTH indicates the length of the VALUE field in bytes, including the terminating null byte.
- VALUE will be ASCII-encoded text terminated with a null byte ('\0').
- A single report will comprise of a set of type-length-value fields beginning with a “begin” report type. It will have a type which is specific to the type of report being generated, length of 1 byte and a value of an empty string (“”). Note the empty string is still null terminated.
- Each report will end with an end of report which has type 1 (type = end of report, length = 1, value = "").
- **T**he empty string listed above has a NULL character and has length 1. Any length number in the streaming report includes the NULL character
- A UDP packet may contain more than one report.
- The UDP packets have a maximum size of 1400 bytes.

9.1 RSSI and Noise Floor Reporting

The type/length/value for RSSI and noise floor reporting are listed in the following table:

Report Type	Data Type	Information
5009	Empty string ""	Begin of RSSI report
5010	Float	Revision number for RSSI report
5000	Integer	Raw signal power of first antenna, represented in half dBm steps.
5001	Integer	Raw signal power of second antenna represented in half dBm steps.
5002	Integer	Raw signal power of third antenna represented in half dBm steps.
5003	Integer	Raw signal power of fourth antenna represented in half dBm steps.
5004	Integer	Raw noise power represented in half dBm steps.
5005	32-bit integer	Sync signal power (from digital domain, see note below).
5006	32-bit integer	Sync noise power (from digital domain, see note below).
5007	16-bit integer	Node ID of the radio.
5008	32-bit integer	Report sequence number, increments for every report, resets after 9999.
1	Empty string ""	End of report.

Table 30 RSSI Reporting Format

Note:

The sync noise and power (types 5005, 5006) are special values obtained after packet processing in the digital domain. They cannot be directly compared to the raw signal and noise values. To obtain an SNR from these values the user needs to run the below formula on these values:

X = sync signal power;

Y = sync noise power;

Z = (Y-X)/51

SNR_mw = (X – 12 * Z)/(64 * Z)

SNR_db = 10 * log(SNR_mw)/log(10)

SNR_db is the SNR in dB and it is averaged across all antennae.

The SNR obtained above is more accurate when the real SNR goes below 10 dB. Above 10 dB, the SNR obtained from the raw signal and noise values are more accurate.

Below is an example of the RSSI report:

Report Type	Length	Information
5009	1	""
5010	4	"1.0"
5008	5	"2333"
5000	5	"-43"
5001	5	"-31"
5002	5	"-28"
5003	5	"-66"
5004	5	"-190"
5005	8	"8604568"
5006	8	"8861322"
5007	5	"1025"
1	1	""

Table 31 Sample RSSI Report

The corresponding raw UDP dump in hexadecimal format is attached below. For the purpose of easier reading, each byte is separated by a space, and each item is separated by a new line. The real streaming report is continuous without any spaces or newlines and is currently 109 bytes long.

13 ffffff91 0 1 0

13 ffffff92 0 4 31 2e 30 0

13 ffffff90 0 5 32 33 33 33 0

13 ffffff88 0 5 20 2d 34 33 0

13 ffffff89 0 5 20 2d 33 31 0

13 ffffff8a 0 5 20 2d 32 38 0

13 ffffff8b 0 5 20 2d 36 36 0

13 ffffff8c 0 5 2d 31 39 30 0

13 ffffff8d 0 a 20 20 38 36 30 34 35 36 38 0

13 ffffff8e 0 a 20 20 38 38 36 31 33 32 32 0

13 ffffff8f 0 5 31 30 32 35 0

0 1 0 1 0

9.2 Temperature Reporting

The type, length and value for temperature reporting are listed in the following table:

Report Type	Data Type	Data
8	Empty string ""	Begin of temperature report.
9	Float	Revision number for temperature report.
2	Integer	Current Temperature on the radio.
3	Integer	Maximum Temperature reached on the radio after last booting.
4	Integer	Overheat Count: number of times the radio temperature has exceeded temp_reporting_max_threshold.
1	Empty string ""	End of report

Table 32 Temperature Reporting Format

9.3 Voltage Reporting

The type, length and value for temperature reporting are listed in the following table:

Report Type	Data Type	Data
4001	START REPORT	Indicates start of voltage monitoring report
1	END REPORT	Indicates end of report
4003	REVISION_REPORT	Indicates revision of this report, currently always “1.1”
4004	CUR_VOLTAGE_REPORT	Current voltage value as a floating point string
4005	MIN_VOLTAGE_REPORT	Minimum voltage seen so far, as a floating point string
4006	MAX_VOLTAGE_REPORT	Maximum voltage seen so far, as a floating point string
4007	UNDERVOLTAGE_COUNT _REPORT	Number of times voltage dropped below min threshold, as an integer string
4008	OVERVOLTAGE_COUNT_ REPORT	Number of times vltage spiked above max threshold, as an integer string.

Table 33 Voltage Reporting Format

10. Setting up an Iperf Test

10.1 Required Equipment

- Two laptops with jperf installed. It is beyond the scope of this manual to cover the installation and operation of these tools. The laptops must be on the same subnet but not necessarily the same subnet as the radios (172.20.xx.yy). It is not required for the user to set a secondary IP address on the radio to perform this test. It is recommended the iperf or jperf tests are first conducted between the laptops using an Ethernet switch or cross-over Ethernet cable between them to verify the laptops and iperf/jperf tools.
- Two or more StreamCaster radios properly configured.

10.2 Running Iperf Test

- Connect a laptop to one StreamCaster radio using the Ethernet cable.
- Connect the other laptop to another StreamCaster radio.
- Power up the radios and verify the radios are booted and connected wirelessly.
- At the receiver side type the following in a terminal
    - iperf –s –u -i 1
- At the transmitter side type the following in a terminal
    - iperf –c receiver_laptop_ip_address –u –i 1 –b 1M –t 60

11. Precautions and Recommendations

11.1 Saving the Radio Configuration

It is very important that the radio does not lose power during any configuration changes in which the user requests a “save and apply” operation. Partial saving of the configuration to the radio due to power interruption may disable the radio requiring reprogramming at the factory. Also, please wait for a “done” feedback at the web interface before proceeding to any other configuration changes.

12. Troubleshooting

12.1 LED Issues

- If flashing red LED is present, radio is in safe boot mode. Click save and apply to resume normal operation.
- If LED is orange and node won't connect to another node, click "restore factory defaults" on both radios to ensure all settings are reverted to factory settings.

12.2 Intermittent Link

- In a long range scenario if SNR is good but link drops unexpectedly check link distance parameter and make sure that the link distance is set the same on all radios and sufficiently large enough.
- Check interference levels as strong interference can result in an intermittent link.

13. FCC Notice

13.1 FCC Identifier: N2S-SC3500

Silvus Model #: SC3500-243541

Equipment Class: Digital Transmission System

The following parameters must be used to be compliant to the appropriate FCC requirements:

Antenna: 3dB Omni (AOV3T245515575)

Bandwidth: 20MHz

Maximum Output Power across Frequency Range #1: 495.28mW from 2427MHz to 2447MHz

Maximum Output Power across Frequency Range #2: 493.62mW from 5745MHz to 5830MHz

13.2 FCC Identifier: N2S-SC3822

Silvus model #: SC3822-245580

Equipment Class: Digital Transmission System

The following parameters must be used to be compliant to the appropriate FCC requirements:

Antenna: 3dB Omni (AOV3T245515575)

Bandwidth: 20MHz

Maximum Output Power across Frequency Range #1: 268.64mW from 2420MHz to 2450MHz

Maximum Output Power across Frequency Range #2: 329.02mW from 5760MHz to 5810MHz

13.3 FCC Identifier: N2S-SC42-245

Silvus model #: SC4210-245-BB, SC4240-245-BB

Equipment Class: Digital Transmission System

The following parameters must be used to be compliant to the appropriate FCC requirements:

Antenna: 2.1dBi Omni Antennas (AOV2S230515)

Bandwidth: 10MHz

Maximum Output Power @ Frequency #1: 810.17mW @ 2430MHz

Maximum Output Power @ Frequency #2: 795.3mW @ 2440MHz

13.4 FCC Identifier: N2S-SC44-245

Silvus model #: SC4410-235-SBST, SC4480-235-SBST

Equipment Class: Digital Transmission System

The following parameters must be used to be compliant to the appropriate FCC requirements:

Antenna: 2.1dBi Omni Antennas (AOV2S230515)

Bandwidth: 10MHz

Maximum Output Power @ Frequency #1: 582.1mW @ 2430MHz

Maximum Output Power @ Frequency #2: 523.6mW @ 2440MHz

13.5 FCC Identifier: N2S-SC42-520

Silvus model #: SC4210E-520-BB, SC4240E-520-BB

Equipment Class: Digital Transmission System

The following parameters must be used to be compliant to the appropriate FCC requirements:

Antenna: 6dBi Omni Antennas (Peak Antennas CO520-6-LS)

Bandwidth: 20MHz

Maximum Output Power @ Frequency #1: 414.03mW @ 5220MHz

Maximum Output Power @ Frequency #2: 498.92mW @ 5240MHz

13.6 FCC Identifier: N2S-SC44-520

Silvus model #: SC4410E-520-SBST, SC4480E-520-SBST

Equipment Class: Digital Transmission System

The following parameters must be used to be compliant to the appropriate FCC requirements:

Antenna: 6dBi Omni Antennas (Peak Antennas CO520-6-LS)

Bandwidth: 20MHz

Maximum Output Power @ Frequency #1: 241.48mW @ 5220MHz

Maximum Output Power @ Frequency #2: 246.52mW @ 5240MHz

13.7 FCC Identifier: N2S-SC42E-245

Silvus model #: SC4210E-245-EBEquipment Class: Digital Transmission System

The following parameters must be used to be compliant to the appropriate FCC requirements:

Antennas: 2.1dBi Omni Antennas (Silvus AOV2D230515) & 4dBi Omni Antennas (Silvus AOV4S235)

Bandwidth: 10MHz

Maximum 10MHz Bandwidth Output Power @ Frequency #1: 789.84mW @ 2430MHz

Maximum 10MHz Bandwidth Output Power @ Frequency #2: 790.06mW @ 2440MHz

Bandwidth: 20MHz

Maximum 20MHz Bandwidth Output Power @ Frequency #1: 123.82mW @ 2440MHz

13.8 FCC Identifier: N2S-SC42E-235470

Silvus model #: SC4240E-235470-BB

Equipment Class: Digital Transmission System

The following parameters must be used to be compliant to the appropriate FCC requirements:

Antennas: 2.5dBi Omni Antennas (Silvus part# 1001-071)

Bandwidth: 10MHz

Maximum 10MHz Bandwidth Output Power @ Frequency #1: 891.25mW @ 4945MHz, 4950MHz, 4955MHz, 4960MHz, 4965MHz, 4970MHz

Maximum 10MHz Bandwidth Output Power @ Frequency #2: 955mW @ 4975MHz, 4980MHz, 4985MHz

13.9 FCC Identifier: N2S-SC44E-235470

Silvus model #: SC4480E-235470-SBST

Equipment Class: Digital Transmission System

The following parameters must be used to be compliant to the appropriate FCC requirements:

Antennas: 2.5dBi Omni Antennas (Silvus part# 1001-071)

Bandwidth: 10MHz

Maximum 10MHz Bandwidth Output Power @ Frequency #1: 912mW @ 4945MHz, 4950MHz, 4955MHz

Maximum 10MHz Bandwidth Output Power @ Frequency #2: 933.25mW @ 4960MHz, 4965MHz, 4970MHz

Maximum 10MHz Bandwidth Output Power @ Frequency #3: 912mW @ 4975MHz, 4980MHz, 4985MHz

13.10 Notes

This equipment has been tested and found to comply with the limits for a class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

* Reorient or relocate the receiving antenna.
* Increase the separation between the equipment and receiver.
* Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

* Consult the dealer or an experienced radio/TV technician for help.

In order to maintain compliance with FCC regulations, shielded cables must be used with this equipment. Operation with non-approved equipment or unshielded cables is likely to result in interference to radio and TV reception. The user is cautioned that changes and modifications made to the equipment without the approval of the manufacturer could void the user's authority to operate the equipment.
To satisfy RF exposure requirements, this device and its antennas must operate with a separation distance of at least 20 cm from all persons for the 2-antenna radios, and 24 cm for the 4-antenna radios, and must not be co-located or operating in conjunction with any other antenna or transmitter.

14. Notes Regarding CE Mark (-206 models only)

The following Silvus Technologies models are declared to conform to CE Mark requirements:

Silvus P/N: SC4240-206-EB, SC4480-206-SBST, SC4240E-206-EB, SC4480E-206-SBST

Relevant standards:

ETSI EN 302 064 V2.1.1 (2016-09), Wireless Video Links, Harmonized Standard

ETSI EN 301 489-1 V2.2.0 (2017-03), EMC, Common Technical Requirements

ETSI EN 301 489-28 V1.1.1 (2004-09), EMC, Specific conditions for wireless digital video links

EN 60950-1, Information Technology Equipment, Safety

Frequency range: 2025-2110 MHz

Maximum RF power: 500 mW per channel, up to a maximum EIRP of 1.6 watts for the SC4240-206-EB, SC4240E-206-EB and 3.2 watts for the SC4480-206-SBST, SC4480E-206-SBST

Antenna: 2.15dBi Omni Antennas (AOV2D230515)

Cable: Silvus cable assembly (SC22-PRICBL02-6)

External Bandpass Filter:

Microwave Filter Co. model 3813

(a filter of equivalent performance may also be used, contact Silvus Technologies customer support for more information)

AC Adapter (if used): EDAC Power Electronics EA10523C-120 (this adapter is approved for indoor use only) (this adapter was certified by the manufacturer to IEC 60950-1)

External DC supply: If the customer provides DC power from their own source, the supply should be fused for a 5-amp circuit.

Safe Working Distance:

Maintain safe working distance of minimum 20cm. For more details, refer to TUV report no. SD72128709-0617A-0617C, "Radio Frequency Exposure Verification of the Silvus Technologies Inc. StreamCaster SC420-206 and SC4480 Tactical MIMO Radio EN 62311 January 2008" (copy of report available upon request). The CE Mark Technical File is available upon request for inspection.

To satisfy RF exposure requirements, this device and its antennas must operate with a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter, except in accordance with RED RF Exposure requirements.

This equipment has been constructed so that the product complies with the requirement of with Article 10(2) as it can be operated in at least one Member State as examined and the product is compliant with Article 10(10) as it has no restrictions on putting into service in all EU member states.

See restrictions mentioned in ERC Recommendation 25-10, Table 7-C2, for guidance of restrictions applicable to specific countries.

Table 7-C2: additional information regarding the national conditions for the identified tuning ranges for video PMSE applications - Band C2

Frequency Band	Country	Implementation	Conditions/remarks
C2 2025-2110 MHz	AUT	L*I	Max. 10MHz Channels; max. 20dBW eirp; 2070-2090 MHz: Restricted to Broadcasters only. 2090-2110 MHz: Restricted to fire brigades and private users
	AZE	Y*	On a secondary basis
	BIH	L	PBS old MW link systems for PMSE. Military use in 2025-2110 MHz
	BUL	Y	ECC Report 219. Available for Cordless Cameras, Portable video links and Mobile video links
	CZE	Y*	The band may be used in the coordination with the Ministry of Defence of the Czech Republic. https://www.ctu.eu/sites/default/files/obsah/o-ctu/rsup-p_06_09-2014-07_en_.pdf, new version is avalaible only in czech https://www.ctu.cz/sites/default/files/obsah/ctu/vyzva-k-uplatneni-pripominek-k-navrhu-opatreni-obecne-povahy-casti-planu-vyuziti-radioveho-spektra-c.pv-p/6/xx.2017-yy-pro-kmitoctove-pasmo-1900-2200-mhz/obrazky/pv-p6-2017.pdf
	D	N	Deviations from the specifications in the Frequency Plan (FreqP) could be permitted for a limited time in accordance with §58 TKG. This is provided that the frequency usages indicated in the Frequency Ordinance (FreqV) and the Frequency Plan are not adversely affected (for more details see: https://www.bundesnetzagentur.de/cln_1412/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/SpezielleAnwendungen/Kurzzeitzuteilungen/kurzzeitzuteilungen-node.html)
	DNK	Y*	
	E	N	Band not available
	EST	L*	2075.25-2110 MHz SAP/SAB. See Regulation of Ministry of Communication and Economical Affairs 21.05.2013 No 35. Otherwise governmental use.
	F	L*I	Temporary licenses, e.i.r.p. max = 10 dBW. Use of 10 MHz bandwidth centered on 2055 MHz and 2095 MHz for ground-to-ground link and 10 MHz bandwidth centered on 2065 MHz and 2105 MHz for air-to-ground link. Coordination required between assigning authorities (la Défense and Space) regarding the use of the other available bands in order to avoid harmful interference. ARCEP Decision 2016-1130
	FIN	L*I	Cordless cameras, temporary use on a case- by-case basis. Standard EN 302064. Other use includes military use and space operation
	G	Y*I	Technology and application neutral but typically used for wireless cameras, typically licensed at 100 mW e.r.p.
	GEO	L*	
	GRC	L*I	Cordless Cameras. Portable/Mobile video links. 2087.5- 2108.5 MHz : not available (exclusive use by security services)
	HNG	N	Band not available (governmental use). However, the band may be used for short-term PMSE use if the user demand makes it necessary at certain occasions like main events. In this case the authority handles the requests on a case-by-case basis and if the frequency use can be authorised the users receive an individual license
	HOL	L*	2070-2110 MHz for ENG-OB only

Possible implementation status: Y = the whole band is available for PMSE L = Limited availability N = the band is not available for PMSE * - Individual licence may be required I – restrictions apply (e.g. geographical restrictions)

Table 34 Additional Restrictions on Band C2

EU DECLARATION OF CONFORMITY

Number: *STDOC1001*

Name and address of the Manufacturer

Silvus Technologies, Inc.,
10990 Wilshire Blvd., Suite #1500
Los Angeles, CA 90024 U.S.A

This declaration of conformity is issued under the sole responsibility of the manufacturer.

Object of the declaration

Product information	StreamCaster SC4240-206-EB, SC4480-206-SBST, SC4240E-206-EB, SC4480E-206-SBST
Additional information	SW version : v3.12.6.4 for SC4240-206-EB and SC4480-206-SBST HW version : C5 for SC4240-206-EB, B1 for SC4480-206-SBST SW version : v3.17.1.1 for SC4240E-206-EB and SC4480E-SBST HW version : C7 for SC4240E-206-EB and B1 for SC4480E-SBST

The object of the declaration described above is in conformity with the relevant Union harmonisation legislation:

- References to the relevant harmonised standards used or references to the technical specifications in relation to which conformity is declared

Radio Equipment Directive 2014/53/EU	RoHS Directive 2011/65/EU
EN 301 489-1 V2.1.1 *EN 301 489-28 V1.1.1* *EN 302 064 V2.1.1* *EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013* *EN62311:2008*	*EN 50581:2012*

The notified body Name: *TÜV SÜD American* Number:1929 **performed** • a conformity assessment of the technical construction file

and issued the certificate CB-19-0102

Additional information

N/A

Signed for and on behalf of: Silvus Technologies

Authorised Representative:

Name and Surname / Function:

Weijun Zhu, Vice President of Engineering

Date of issue: 8-12-2019

1/1

15. ISED Canada Notice

15.1 IC: 24980-SC42E245

Silvus model #: SC4210E-245-EB. Note that the SC4210E is a subset of the generic SC4200E, the "1" in the model # indicates it is a 1 watt maximum output power product or if lower the limits found by the ISED testing.

Equipment Class: Digital Transmission System

The following parameters must be used to be compliant to the appropriate ISED requirements:

Antennas: 2.1dBi Omni Antennas (Silvus AOV2D230515) & 4dBi Omni Antennas (Silvus AOV4S235)

Bandwidth: 10MHz

Maximum 10MHz Bandwidth Output Power @ Frequency #1: 789.84mW @ 2430MHz

Maximum 10MHz Bandwidth Output Power @ Frequency #2: 790.06mW @ 2440MHz

Bandwidth: 20MHz

Maximum 20MHz Bandwidth Output Power @ Frequency #1: 123.82mW @ 2440MHz

Modulation and Coding Schemes tested: MCS0 to MCS15

15.2 Software License

A Software License is used to ensure only parameters and limits that are allowed by the ISED certificate shown in section 15.1 can be selected. These parameters include Frequency, Output Power, Modulation and Bandwidth.

15.3 Firmware Encryption

The details of our Firmware Encryption are considered proprietary and are discussed in depth in the submitted document SC4210E-245 Circuit Description v1.2 section 1.5. Also described is the method to ensure only Silvus released firmware and Software License can be loaded on the product. This will ensure only the parameters and limits that are allowed by the Industry Canada certificate shown in section 15.1 can be selected.

15.4 IC Statement: English

This radio transmitter 24980-SC4210E245 has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

1. Omnidirectional antenna, Silvus P/N A0VD230515, maximum antenna gain 2.1 dBi, 50 ohm
2. Omnidirectional antenna, Silvus P/N A0V4S235, maximum antenna gain 4dBi, 50 ohm

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.
(2) This device must accept any interference, including interference that may cause undesired operation of the device.

15.5 IC Statement: French

Le présent émetteur radio 24980-SC4210E245 a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenna énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cetter liste, et dont le gain est supérieur au gain maximal indiqué, pour tout type figurant sur la liste, sont strictement interdits pour l'expolitation de l'émetteur.

1. Omnidirectional d'onde, Silvus P/N A0VD230515, le gain max 2.1 dBi, 50 ohm
2. Omnidirectional d'onde, Silvus P/N A0V4S235, le gain max 4 dBi, 50 ohm

L'émettur/récepteur exempt de licence conenu dans le présent appareil est conforme aux CNR Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

(1) L'appareil ne doit pas produire de brouillage;
(2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

15.6 Radiation Exposure Statement: English

Radiation Exposure Statement:

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 32 cm between the radiator and your body.

15.7 Radiation Exposure Statement: French

Déclaration d'exposition aux radiations

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non controlé. Cet équipement doit étre installé et utilize avec un minimum de 32 cm de distance entre la source de rayonnement et votre corps.