StreamCaster 4000 series MIMO Radio

User Manual

Document Number	10017C000
Version	4.0.3.11
Date	10/26/2022

Silvus Technologies, Inc.

10990 Wilshire Blvd, #1500

Los Angeles, CA 90024

Notice

Silvus Technologies reserves the right to make changes to its products or discontinue any of its products or offerings without notice.

Silvus Technologies warrants the performance of its products to the specifications applicable at the time of sale in accordance with Silvus Technologies' standard warranty.

Revision History

Version	Date	Changes
1.0	April 8, 2020	Original
4.0.0.0	April 17, 2020	Updated 7.2.1 N2N server capability
4.0.0.0	May 1, 2020	Added mounting hole information to mechanical drawings in section 4.3. Revised default setting for auto noise estimation Renamed Local Broadcast feature to MANET Multicast/Broadcast in section 5.1.2.3
4.0.0.0	May 7, 2020	Updated GI mode description in section 5.1.1.2 Removed section 12.1 LED troubleshooting and revised section 4.1 to include correct LED status description Corrected referenced figures throughout user manual
4.0.0.3	February 9, 2020	Updated to match production release version Removed Auto Noise Estimation (will always be enabled moving forward) Added color coding to pins on primary and aux cables for 4200E/4400E radios Added SL4200 to product line Revised USB2 to USB0 naming scheme Added more details to login authentication Added HMAC key and Wrapping key in Encryption Added MCS sensitivity tables for 1.25 & 2.5 MHz Revised SC4200E P/N to SC4200EP
4.0.0.10	March 26, 2021	Update section 5.1.2 Networking. Added DLEP, DHCP server, and infrastructure network sections. Typo on section 9.3 Updated SL4200 specifications Added note for primary cable color scheme valid after 6/1/19 Revised "beam forming" to "beamforming" Added note that MAN-IA disables Tx beamforming Updated FIPS compliance/certified Updated section 5.0 initial description Added IPv6 support details Revised typo in section 5.1.2.7 Added MPS zeroize details Removed End-to-End ARQ

		Added details in section 5.1.2.7 for scan on start, and failover mode
4.0.0.11	August 20, 2021	Revised description of DHCP in section 5.1.2.4 Revised description of infrastructure networks in section 5.1.2.7 Revised the narrow bandwidth sensitivity chart radio name table 19 and 20 Revised section 5.1.2.3 to note that WiFi dongle SC-WIFI-DNGL2-RGD-ODU supports WPA2-PSK-AES encryption Revised table 25 in section 9.1 to show that report type 5000, 5001, 5002, 5003, and 5004 should take full dBm steps, not half. Updated section 1.1 Health & Safety section
4.0.2.3	September 10, 2021	Added some clarification on the mapping section of network management section 5.2.2 Update SL4200 mechanical drawing in section 4.3.3 Add a section on MAN-IM in section 5.3.2
4.0.2.8	December 3, 2021	Added section 16. MIC Japan Notice Revised table 19-23 columns for sensitivity of type of radio Revised description of radio mesh type in Infrastructure Networks section 5.1.2.7 Revised typo on table 10 pin 11 Replace SL4200 pin out diagram. Add high power radio versions 10W and 20W Added explanation that zeroize will require a radio reboot to sections 5.5.3 and 5.6.2. Updated sensitivity figures on table 19
4.0.2.10	December 28, 2021	Update RSSI reporting format on table 25 Added MAN-IC section 5.3.4 Added mention of x-pol antenna config when beamforming disabled in section 5.1.1.2 Updated Encryption section 5.4.1 Updated Languages section 5.5.4 Updated Basic section 5.1.1.1 to include routing mode Added serial server to section 5.1.4 Added link to DLEP document in section 5.1.2.2
4.0.3.0	February 11, 2022	Updated section 5.2.2 Mapping. OpenStreetMap no longer supported. OpenStreetMap (US) still available. Updates to section 5.3.4 MAN-IC. Updated section 5.1.2.5 Multicast. Added description for Default Multicast Algorithm, Broadcast, and Flooding Multicast. Added note on multicast method for CoT in section 5.2.2. Added note on PTT multicast method in section 5.1.5.
4.0.3.6	April 8, 2022	Added description of VLAN Filter in section 5.1.2.1.

		Added description of LED bright control bar in section 5.5.2. Updated figure 77 and Login Authentication section 5.4.4. Added mention of port 1234 for PTT in section 5.1.5. Revised MCS throughput numbers to two decimal points in section 5.1.1.2 tables 19, 20, 21, 22, and 23. Added section 5.2.6 SNMP support Updated section 5.5.3 factory reset section to include quick zeroize parameter. Added caption for table 11 SL4200 supported USB modes Adjusted table spacing for pin out tables 2-19 Added Switchcraft P/N EN3C6FX to pin out tables 3, 7, 13, & 17 Updated section 4 spacing Adjusted table spacing for MCS tables 20-24
4.0.3.7	April 14, 2022	Removed the mention that WIFI is not available on SL4200. SL4200 does support WIFI. Added description for Broadcast FIPS mode, view key, and generate random key in section 5.4.1
4.0.3.11	October 26, 2022	Added section 13.10 FCC ID N2S-SL42-245

Copyright © 2016, Silvus Technologies

Contents

1. General Safety Information 9
1.1 Health & Safety 9
2. Introduction 12
3. StreamCaster Network 12
4. StreamCaster Hardware Overview 13
4.1 Hardware Interfaces 13
SC4400E 13
SC4200EP 14
SL4200 15
SC4400: 16
SC4200: 17
4.2 Connector Pinouts 18
4.2.1 SC4400E Pinouts 18
4.2.2 SC4200EP Pinouts 22
4.2.3 SL4200 Pinouts 26
4.2.4 SC4400 Pinouts 28
4.2.5 SC4200 Pinouts 32
4.3 Mechanical and Operating Specifications 36
4.3.1 SC4400E Enclosure Mechanical Drawing 41
4.3.2 SC4200EP Enclosure Mechanical Drawing 42
4.3.3 SL4200 Enclosure Mechanical Drawing 43
4.3.4 SC4400 Enclosure Mechanical Drawing 44
4.3.5 SC4200 Enclosure Mechanical Drawing 45
4.4 SC4400E Specifications 46
4.5 SC4200EP Specifications 47
4.6 SL4200 Specifications 49
4.7 SC4400 Specifications 50
4.8 SC4200 Specifications 51
5. Web Interface 53
5.0 Getting Started 53
5.1 Local Radio Configuration 54

5.1.1 RF 54
5.1.2 Networking 62
5.1.3 Bidirectional Amplifier (not available on SL4200) 77
5.1.4 Serial/USB Setup 78
5.1.5 PTT (push-to-talk) (not available on SL4200) 80
5.2 StreamScape Network Configuration 82
5.2.1 Network Topology 82
5.2.2 Mapping 91
5.2.3 Table View 99
5.2.4 Network-wide Setup 100
5.2.5 Per-Node Setup 101
5.2.6 SNMP (Simple Network Management Protocol) 102
5.3 Spectrum Dominance 108
5.3.1 Spectrum Analyzer 109
5.3.2 MAN-IM (MANET Interference Monitoring) 113
5.3.3 MAN-IA (MANET Interference Avoidance) (License enabled) 115
5.3.4 MAN-IC (MANET Interference Cancellation) (License enabled) 117
5.4 Security 119
5.4.1 Encryption 119
5.4.2 SSH/HTTPS Certificates 121
5.4.3 White/Black List 123
5.4.4 GUI/Login Authentication 124
5.5 Tools and Diagnostics 127
5.5.1 Firmware and Licenses 127
5.5.2 Faults and Indicators 131
5.5.3 Factory Reset 133
5.5.4 Languages 134
5.5.5 Log 136
5.6 Configuration Profiles 138
5.6.1 Settings profile 138
5.6.2 MPS (Multi-Position Switch) (not available on SL4200) 139
6. FIPS Mode 140
6.1 Enable FIPS Mode 140
6.1.1 Potential User Errors 140

6.2 List of Security Parameters 141
7. Wired Backbone 142
7.1 LAN Backbone 142
7.1.1 Implementation 142
7.1.2 Use Case 142
7.2 WAN Backbone with Roaming 144
7.2.1 Implementation 144
7.2.2 Use Case 144
8. Custom Frequency Plan 146
8.1 Accessing and Installing CFP 146
9. Streaming Response 149
9.1 RSSI and Noise Floor Reporting 150
9.2 Temperature Reporting 153
9.3 Voltage Reporting 154
10. Setting up an Iperf Test 155
10.1 Required Equipment 155
10.2 Running Iperf Test 155
11. Precautions and Recommendations 156
11.1 Saving the Radio Configuration 156
12. Troubleshooting 157
12.1 Intermittent Link 157
13. FCC Notice 158
13.1 FCC Identifier: N2S-SC3500 158
13.2 FCC Identifier: N2S-SC3822 158
13.3 FCC Identifier: N2S-SC42-245 159
13.4 FCC Identifier: N2S-SC44-245 159
13.5 FCC Identifier: N2S-SC42-520 159
13.6 FCC Identifier: N2S-SC44-520 160
13.7 FCC Identifier: N2S-SC42E-245 160
13.8 FCC Identifier: N2S-SC42E-235470 161
13.9 FCC Identifier: N2S-SC44E-235470 161
13.10 Notes…. 162
14. Notes Regarding CE Mark (-206 models only) 163

15. ISED Canada Notice 167
15.1 IC: 24980-SC42E245 167
15.2 Software License 167
15.3 Firmware Encryption 167
15.4 IC Statement: English 168
15.5 IC Statement: French 168
15.6 Radiation Exposure Statement: English 169
15.7 Radiation Exposure Statement: French 169
16. MIC Japan Notice 170
16.1 ID: 211-210701 170
16.2 ID: 011-210045 170
16.3 Software License 172
16.4 Firmware Encryption 172

List of Figures

Figure 1 Product Symbols with Definition 11
Figure 2 StreamCaster 4400E Ruggedized Enclosure 13
Figure 3 StreamCaster 4200EP Ruggedized Enclosure 14
Figure 4 StreamCaster SL4200 Ruggedized Enclosure 15
Figure 5 StreamCaster 4400 Ruggedized Enclosure 16
Figure 6 StreamCaster 4200 Ruggedized Enclosure 17
Figure 7 SC4400E Primary Power/Serial/Ethernet Pinout Diagram (Radio Side) 18
Figure 8 Switchcraft connector on Primary/Power cable 19
Figure 9 SC4400E AUX Pinout Diagram (Radio Side) 20
Figure 10 SC4400E PTT Pinout Diagram (Cable Side) 21
Figure 11 SC4200EP Primary Power/Serial/Ethernet Pinout Diagram (Radio Side) 22
Figure 12 Switchcraft connector on Primary/Power cable 23
Figure 13 SC4200EP AUX Pinout Diagram (Radio Side) 24
Figure 14 SC4200EP PTT Pinout Diagram (Cable Side) 25
Figure 15 SL4200 20 pin POGO connector 26
Figure 16 SC4400 Power (Optional)/Serial/Ethernet Pinout Diagram (Cable Side) 29
Figure 17 SC4400 AUX Pinout Diagram (Cable Side) 30
Figure 18 SC4400 PTT Pinout Diagram (Cable Side) 31
Figure 19 SC4200 Primary Power/Serial/Ethernet Pinout Diagram (Cable Side) 33
Figure 20 SC4200 AUX Pinout Diagram (Cable Side) 34
Figure 21 SC4200 PTT Pinout Diagram (Cable Side) 35
Figure 22 SC4400E Mechanical Drawing (top) and Mounting Pattern (bottom) 41
Figure 23 SC4200EP Mechanical Drawing (top) and Mounting Pattern (bottom) 42
Figure 24 SL4200 Mechanical Drawing 43
Figure 25 SC4400 Mechanical Drawing (top) and Mounting Pattern (bottom) 44
Figure 26 SC4200 Mechanical Drawing (top) and Mounting Pattern (bottom) 45
Figure 27 Initial boot up warning 53
Figure 28 Basic Configuration Page 54
Figure 29 Advanced Configuration Page 56
Figure 30 LAN Settings Page 62
Figure 31 DLEP 65
Figure 32 WIFI AP Configuration Page 66
Figure 33 WIFI Client configuration page 67

Figure 34 DHCP Server 69
Figure 35 Multicast Configuration Page 71
Figure 36 Quality of Service (QoS) Configuration Page 74
Figure 37 Infrastructure Networks 76
Figure 38 Bidirectional Amplifier (BDA) Configuration Page 77
Figure 39 Serial/USB Setup Page 78
Figure 40 Push-to-Talk (PTT) & Audio Page 80
Figure 41 Silvus StreamScape Network Topology Page 82
Figure 42 Example Network Topology 83
Figure 43 Individual Node Characteristics 85
Figure 44 Link Characteristics 86
Figure 45 Traffic Information 87
Figure 46 Graph Views 87
Figure 47 Routing Path 88
Figure 48 Custom Node Naming 89
Figure 49 iPerf Function within GUI 90
Figure 50 Mapping Page 91
Figure 51 Google Maps 92
Figure 52 Map Control Panel (Lat/Long coordinates) 93
Figure 53 Map Control Panel (Cache Settings) 94
Figure 54 Cursor on Target Settings 95
Figure 55 Map Control Panel (Nodes to Display on Map) 96
Figure 56 Map Control Panel (map routing panel) 96
Figure 57 Map Control Panel (address) 97
Figure 58 Offline Map Image 97
Figure 59 Manually Placing Nodes on the Map 98
Figure 60 Table View 99
Figure 61 Network-wide Setup 100
Figure 62 Per-Node Setup 101
Figure 63 Silvus OID tree loaded into the iReasoning MIB Browser 102
Figure 64 SNMP 104
Figure 65 Spectrum Dominance 108
Figure 66 Spectrum Scan Settings 109
Figure 67 Spectrum Scan Results 111

Figure 68 Zero Span Settings 111
Figure 69 Zero Span Results 112
Figure 70 MAN-IM 113
Figure 71 MAN-IA 115
Figure 72: MAN-IC Configuration Page 117
Figure 73: MAN-IC Nodes Displayed as Triangles in Network Topology 117
Figure 74: Node Statistics Pop-Up w/ MAN-IC Enabled 118
Figure 75 Security (Encryption) 119
Figure 76 Security (SSH/HTTPS Certificates) 121
Figure 77 (Chrome Browser Warning) 122
Figure 78 Security (White/Black List) 123
Figure 79 Admin page 124
Figure 80 Login 126
Figure 81 Reset Password 126
Figure 82 Build Information 127
Figure 83 Tools and Diagnostics (Firmware Upgrade) 128
Figure 84 Tools and Diagnostics (Network-Wide Upgrade) 129
Figure 85 Radio Login Authentication during Network-Wide Upgrade 129
Figure 86 Tools and Diagnostics (Licenses) 130
Figure 87 Faults and Indicators Page 131
Figure 88 Tools and Diagnostics (Factory Reset) 133
Figure 89 Tools and Diagnostics (Languages) 134
Figure 90 example Source PO file for custom languages 135
Figure 91 Security (Log) 136
Figure 92 Example of security log 137
Figure 93 Configuration Profiles (Setting Profile) 138
Figure 94 Multi-Position Switch 139
Figure 95 LAN Backbone Example 143
Figure 96 WAN Backbone Example 145
Figure 97 Custom Frequency Page 146

List of Tables

Table 1 Safe Working Distances 10
Table 2 SC4400E Primary Power/Ethernet/Serial Connector Pinout 18
Table 3 SC4400E Serial and GPS Pinout 19
Table 4 SC4400E USB/GPIO Connector Pinout 20
Table 5 SC4400E PTT Connector Pinout 21
Table 6 SC4200EP Primary Power/Ethernet/Serial Connector Pinout 22
Table 7 SC4200EP Serial and GPS Pinout 23
Table 8 SC4200EP AUX USB/GPIO Connector Pinout 24
Table 9 SC4200EP PTT Connector Pinout 25
Table 10 SL4200 POGO Connector Pinout 26
Table 11 SL4200 supported USB modes 27
Table 12 SC4400 Primary Power/Ethernet/Serial Connector Pinout 28
Table 13 SC4400 Serial and GPS Pinout 28
Table 14 SC4400 AUX USB/GPIO Connector Pinout 30
Table 15 SC4400 PTT Connector Pinout 31
Table 16 SC4200 Primary Power/Ethernet/Serial Connector Pinout 32
Table 17 SC4200 Serial and GPS Pinout 32
Table 18 SC4200 AUX USB/GPIO Connector Pinout 34
Table 19 SC4200 PTT Connector Pinout 35
Table 20 MCS vs. Sensitivity Chart (1.25MHz Bandwidth)* 59
Table 21 MCS vs. Sensitivity Chart (2.5MHz Bandwidth)* 59
Table 22 MCS vs. Sensitivity Chart (5MHz Bandwidth)* 60
Table 23 MCS vs. Sensitivity Chart (10MHz Bandwidth)* 60
Table 24 MCS vs. Sensitivity Chart (20MHz Bandwidth)* 61
Table 25 Color Coding for Links and Nodes 83
Table 26 Silvus SNMP OIDs 107
Table 27 RSSI Reporting Format 150
Table 28 Sample RSSI Report 151
Table 29 Temperature Reporting Format 153
Table 30 Voltage Reporting Format 154
Table 31 Additional Restrictions on Band C2 164

1. General Safety Information

The information that follows, together with local site regulations, should be studied by personnel concerned with the operation or maintenance of the equipment, to ensure awareness of potential hazards.

Switch off supplies before removing covers or disconnecting any RF cables, and before inspecting damaged cables or antennas.

Avoid standing in front of high gain antennas (such as a dish) and never look into the open end of a waveguide or cable where strong RF power may be present.

Users are strongly recommended to return any equipment that requires RF servicing to Silvus Technologies.

CAUTION: This system contains MOS devices. Electro-Static Discharge (ESD) precautions should be employed to prevent accidental damage.

1.1 Health & Safety

Exposure to Non-Ionizing (RF) Radiation/Safe Working Distances

The safe working distance from a transmitting antenna may be calculated from the relationship:

$$D = \sqrt{\frac{P_T \cdot G_R}{4\pi \cdot 10 \cdot w}}$$

In which D = safe working distance (meters)

PT = total transmit power (watts)

GR = antenna gain ratio $=10^{\left(\frac{G}{10}\right)}$ where G is the antenna gain in dBi.

w = maximum allowed RF power density (mW/cm^2)

The maximum allowed RF power density value is determined by reference to regulatory safety guidelines for exposure of the human body to non-ionizing radiation. It is important to note that the guidelines adopted differ throughout the world and are from time-to-time re-issued with revised guidelines. For use in the United States, one can find the FCC guideline at the following link as of this writing:

"https://transition.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet65/oet65.pdf". Specifically, page 67 of this link contains the table of RF power density limits for different frequency bands.

Below is a table of some example safe distances calculated based on the FCC guidelines using the limits for occupational/controlled exposure. For countries other than the US, please use the limits in the local guideline to adjust the calculation.

Frequency	Antenna			Transmitter Power					FCC limits
	Type	**Gain (dBi)**	**Gain Ratio (GR)**	**1W**	**2W**	**4W**	**10W**	**30W**	
2400 MHz	Omni	3	2	0.06	0.08	0.11	0.18	0.31	5 mW/cm^2
1370 MHz	Sector	20	100	0.42	0.59	0.84	1.32	2.29	4.567 mW/cm^2
4700 MHz	Parabolic Dish	35	3162	2.24	3.17	4.5	7.1	12.3	5 mW/cm^2
				Minimum Safe Distance (meters)					

Table 1 Safe Working Distances

Important Note: It must be remembered that any transmitting equipment radiating power at frequencies of 100kHz and higher, has the potential to produce thermal and a-thermal effects upon the human body.

To be safe:

a) Operators should not stand or walk in front of any high gain antenna such as dish antennas, nor should they allow anyone else to do so.

b) Operators should not operate any RF transmitter or power amplifier with any of its covers removed, nor should they allow anyone else to do so.

General Safety Notes

- A flashing/steady Red LED status indication is a normal condition and is not meant to convey a fault condition.
- The Power Disconnect Device for the product is the connector for the external AC/DC Adapter or other DC power source.
- Although the Low Voltage DC powered units are approved for Outdoor use (Dust/Temporary Immersion), the optional AC power option with AC/DC power supply is only certified for indoor use.
- The unit housing serves as a heatsink and must be mounted on a non-combustible surface.
- The units are not User Serviceable. Contact the manufacturer for further instructions on servicing or repair.
- All symbols, markings and warning statements marked on the equipment are shown below for reference.

Product Symbols

This table describes the symbols marked on the device.

Symbol		Description
	Caution Read User Manual	Please follow all instructions in this User Manual including all warnings, cautions, and precautions before using the Organelle. Unit is not user serviceable. Contact the manufacturer if defective or damaged.
	RoHS Compliant	The product is compliant with the RoHS 2 Directive 2011/65/EU (RoHS 2). (Note: This Symbol may not be marked on device)
	CE	Product complies with the European Union Low Voltage Directive (LVD), RoHS 2 and EMC Directives.
	HOT SURFACE SYMBOL	Please avoid bodily contact with the product housing and do not mount the product on a combustible surface.
	Disposal	Per the European WEEE Directive, please dispose the product in accordance with local regulations

Figure 1 Product Symbols with Definition

- Product cleaning should only be done with a soft cloth and mild detergent, do not use any solvents that might remove case markings or labels.
- The unit, at the end of its useful life is to be disposed in accordance with local regulations or may be returned to the manufacturer.
- If the equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment and/or equipment performance may be impaired.

2. Introduction

The StreamCaster family of MIMO radios was designed with operator ease of use in mind. Each radio is capable of operating in a multitude of configurations that are accessed via simple web pages within the radio. Settings such as transmit power, frequency, channel bandwidth, link adaptation and range control can be accessed by simply using a web browser to log into any radio within the network. This user manual contains all essential information for the user to configure the StreamCaster radio as well as how to run an iperf network test.

3. StreamCaster Network

Each StreamCaster MIMO radio has a fixed static IP address in the 172.20.xx.yy network. The radio operates as a network switch; the user equipment does not need to be on the same subnet as the radio during operation. It is possible to setup a secondary IP address on the radio if the user finds this feature convenient. Setting up a secondary IP address is useful if the user wishes to access the radio's web interface in their network.

4. StreamCaster Hardware Overview

4.1 Hardware Interfaces

SC4400E

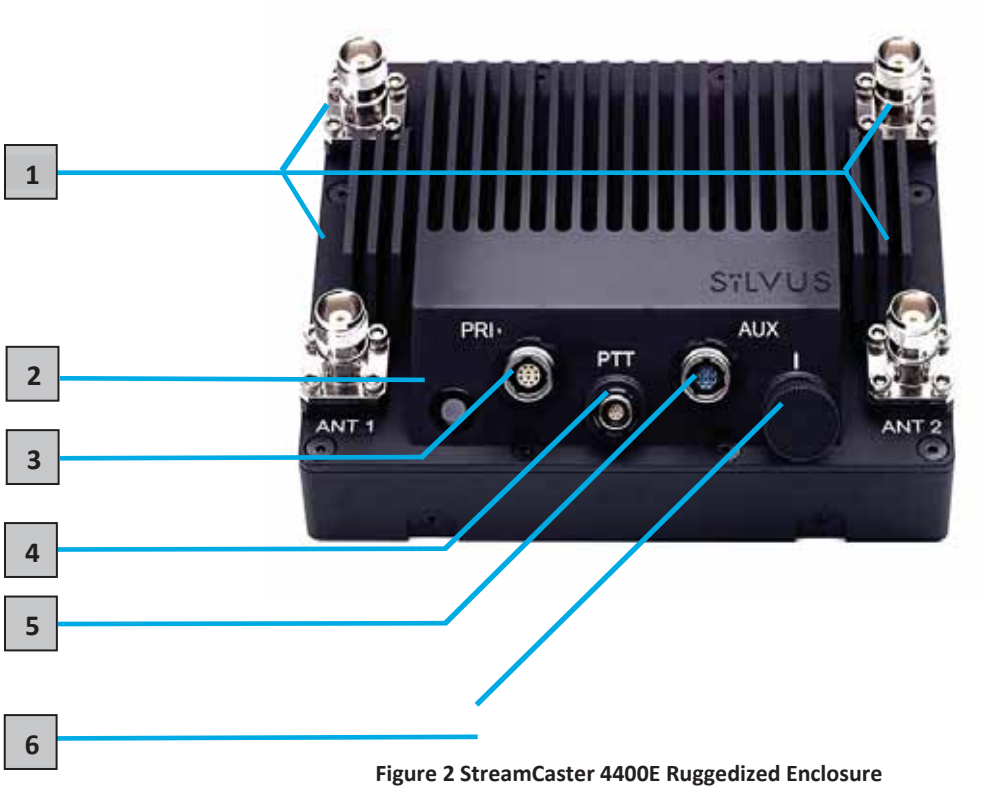


Figure 2 StreamCaster 4400E Ruggedized Enclosure

1 RF Channels 1-4 Connectors [TNC Female]

2 Bi-Color Status LED

- Red – Radio is in the process of booting up
- Flashing Green – Radio is fully booted but not wirelessly connected to any other radio
- Green – Radio is wirelessly connected to at least one other radio
- Flashing Red – Spectrum Scan in Progress
- Flashing Red – Radio has recovered from a bad state.
- Rapid Flashing Green – When the multi position switch is rotate to a new position, LED will rapidly flash green while new settings are being applied. LED will resume normal indication after settings have been applied.

3 Power (9-20V), Ethernet, and Serial Port Connector [ODU GK0YAR-P10UC00-000L]

4 Push-to-Talk (PTT) Connector [ODU GKCWAM-P07UB00-000L]

5 AUX Connector [ODU GK0YCR-P10UC00-000L]

6 Power Switch [15-Position Rotating]

SC4200EP

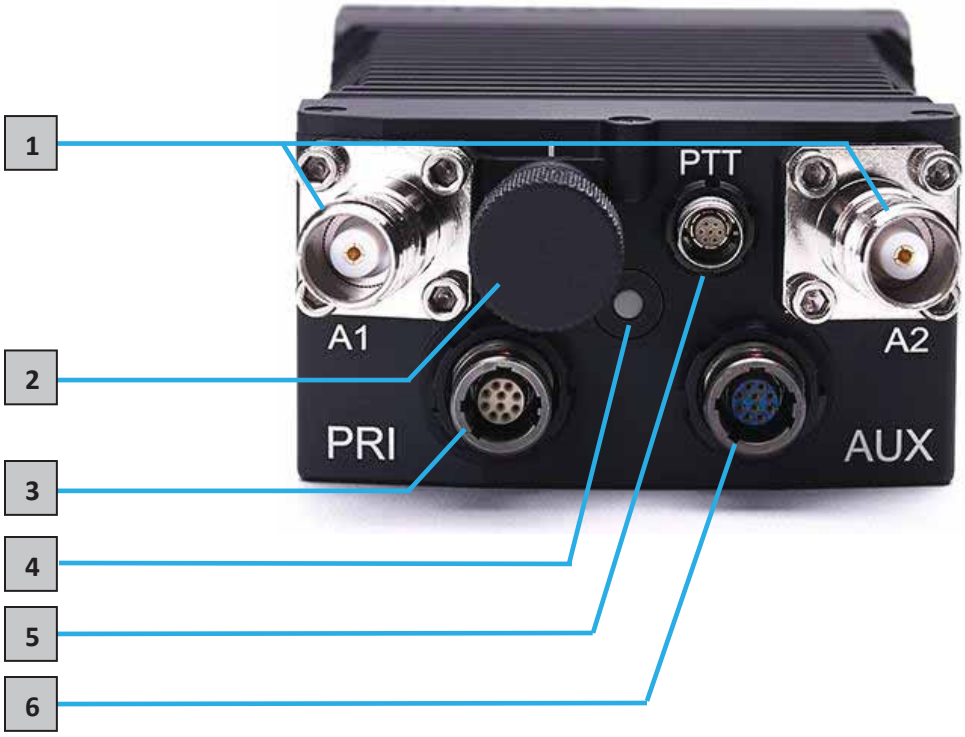


Figure 3 StreamCaster 4200EP Ruggedized Enclosure

1 RF Channels 1-2 Connectors [TNC Female]

2 Power Switch [15-Position Rotating]

3 Power (EB Version Only, 9-20V), Ethernet, and Serial Port Connector [ODU GK0YAR-P10UC00-000L]

4 Bi-Color Status LED

- Red – Radio is in the process of booting up
- Flashing Green – Radio is fully booted but not wirelessly connected to any other radio
- Green – Radio is wirelessly connected to at least one other radio
- Flashing Red – Spectrum Scan in Progress
- Flashing Red – Radio has recovered from a bad state.
- Rapid Flashing Red for 1 second – The battery is less than or equal to 20%. LED will blink red rapidly for 1 second then go back to normal. This will repeat every 5 seconds.
- Rapid Flashing Green – When the multi position switch is rotate to a new position, LED will rapidly flash green while new settings are being applied. LED will resume normal indication after settings have been applied.

5 Push-to-Talk (PTT) Connector [ODU GKCWAM-P07UB00-000L]

6 AUX Connector [ODU GK0YCR-P10UC00-000L]

SL4200

Figure 4 StreamCaster SL4200 Ruggedized Enclosure

1 RF Channels 1-2 Connectors [TNC Female]

2 Power Switch [2-Position Rotating]

3 Bi-Color Status LED

- Red – Radio is in the process of booting up
- Flashing Green – Radio is fully booted but not wirelessly connected to any other radio
- Green – Radio is wirelessly connected to at least one other radio
- Flashing Red – Spectrum Scan in Progress
- Flashing Red – Radio has recovered from a bad state and has reverted to factory default settings.
- Rapid Flashing Red for 1 second – The battery is less than or equal to 20%. LED will blink red rapidly for 1 second then go back to normal. This will repeat every 5 seconds.

4 20-pin pogo style connector

- 8-32VDC input / USB-C PD (9VDC)
- 2x USB 2.0 (Host / OTG)
- Serial RS-232
- +5VDC output

SC4400:

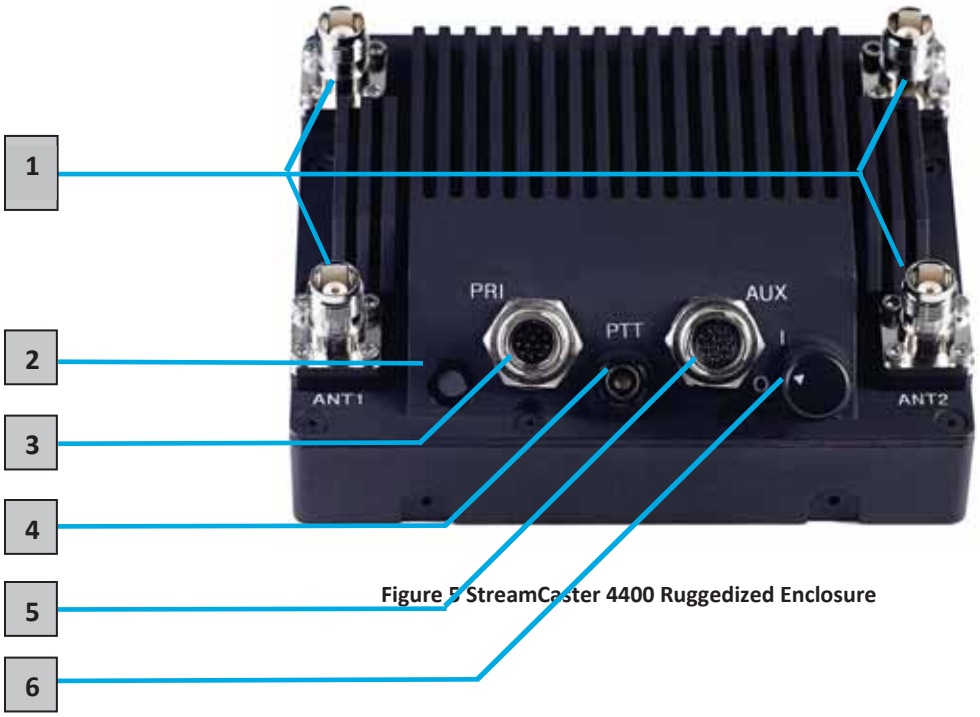


Figure 5 StreamCaster 4400 Ruggedized Enclosure

1 RF Channels 1-4 Connectors [TNC Female]

2 Bi-Color Status LED

- Red – Radio is in the process of booting up
- Flashing Green – Radio is fully booted but not wirelessly connected to any other radio
- Green – Radio is wirelessly connected to at least one other radio
- Flashing Red – Spectrum Scan in Progress
- Flashing Red – Radio has recovered from a bad state.

3 Power (9-20V), Ethernet, and Serial Port Connector [Hirose LF10WBRB-12PD]

4 Push-to-Talk (PTT) Connector [ODU GKCWAM-P07UB00-000L]

5 AUX Connector [Hirose LF10WBRB-12SD]

6 Power Switch [2-Position Rotating]

SC4200:

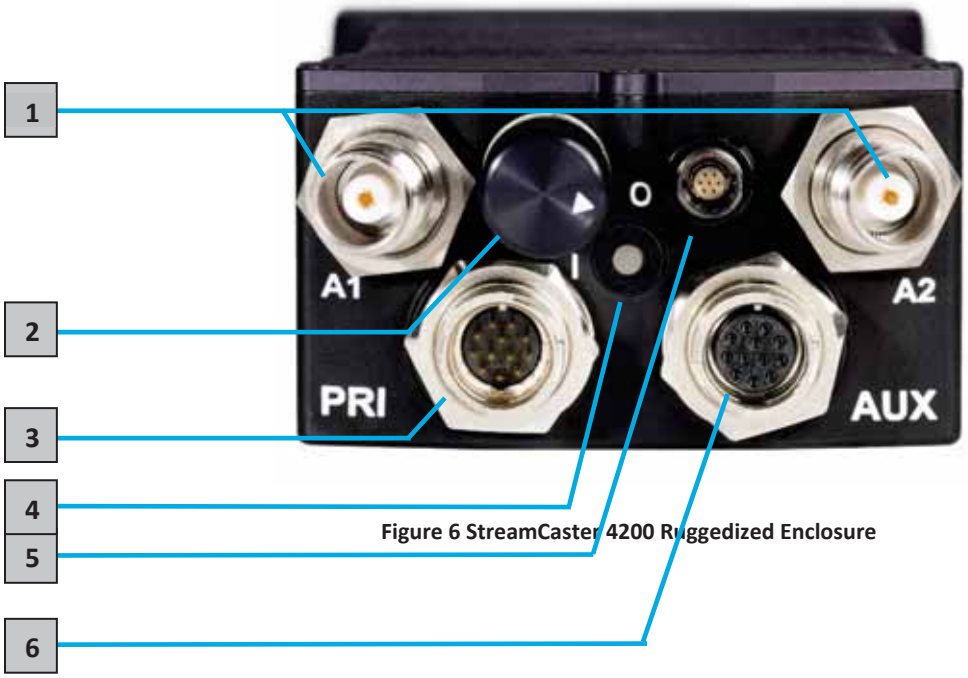


Figure 6 StreamCaster 4200 Ruggedized Enclosure

1 RF Channels 1-2 Connectors [TNC Female]

2 Power Switch [2-Position Rotating]

3 Power (EB Version Only, 9-20V), Ethernet, and Serial Port Connector [Hirose LF10WBRB-12PD]

4 Bi-Color Status LED

- Red – Radio is in the process of booting up
- Flashing Green – Radio is fully booted but not wirelessly connected to any other radio
- Green – Radio is wirelessly connected to at least one other radio
- Flashing Red – Spectrum Scan in Progress
- Flashing Red – Radio has recovered from a bad state.

5 Push-to-Talk (PTT) Connector [ODU GKCWAM-P07UB00-000L]

6 AUX Connector [Hirose LF10WBRB-12SD]

4.2 Connector Pinouts

4.2.1 SC4400E Pinouts

SC4400E Primary Power/Ethernet/Serial Connector Pinout			
Enclosure PWR/COMM (GK0YAR-P10UC00-000L)	**Signal**	**Switchcraft Pinout (EN3C2F16X)**	**Color of wires coming from ODU connector**
1	5V OUT (For External GPS Puck)	NC	Pink
2	GND IN	2	Yellow/Blue
3	VCC IN	1	Green/Violet
4	ETH0_MX2N (RX-)	NC	Black
5	ETH0_MX2P (RX+)	NC	Brown
6	ETH0_MX1P (TX+)	NC	Red
7	RS232_RXD	NC	Gray
8	RS232_TXD	NC	White
9	GND	NC	Light Green
10	ETH0_MX1N (TX-)	NC	Orange

Table 2 SC4400E Primary Power/Ethernet/Serial Connector Pinout

*color scheme is valid for cables built after 6/1/19

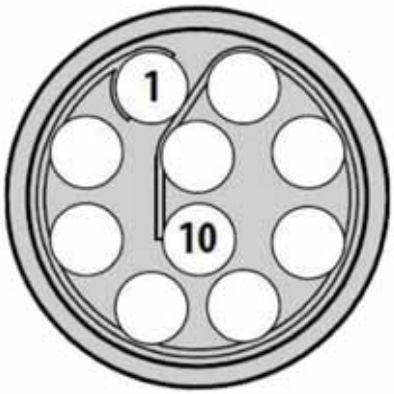


Figure 7 SC4400E Primary Power/Serial/Ethernet Pinout Diagram (Radio Side)

SC4400E RS-232 Pinout		
RS-232 (DB9)	**Signal**	**Switchcraft Pinout (EN3C6FX)**
3	TxD	2
2	RxD	1
NC	NC	4
NC	5V OUT	6
NC	NC	5
5	Ground	3

Table 3 SC4400E Serial and GPS Pinout

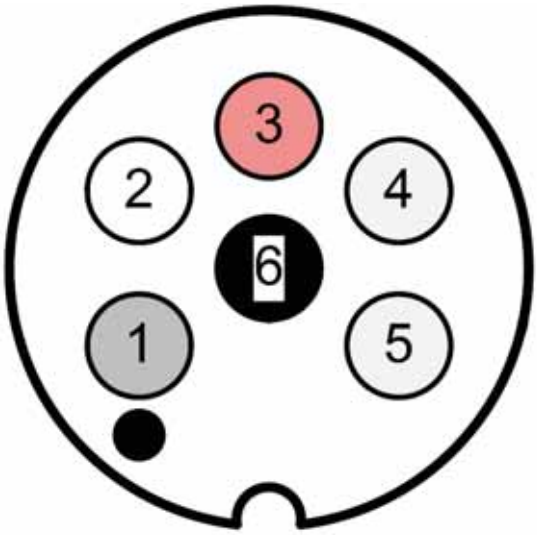


Figure 8 Switchcraft connector on Primary/Power cable

SC4400E AUX Connector Pinout		
Enclosure AUX (GK0YCR-P10UC00-000L)	**Signal**	**Color of wires coming from ODU connector**
1	USB GND	Yellow/Blue
2	USB1_D-	Red
3	USB1_VBUS	Green
4	USB0_VBUS	Violet
5	GPIO1 (BDA control)	Pink
6	USB0_D+	Black
7	USB0_D-	Brown
8	GND	Light Green
9	USB1_ID	Gray
10	USB1_D+	Orange

Table 4 SC4400E USB/GPIO Connector Pinout

*color scheme is valid for cables built after 6/1/19

**(USB1 is USB 2.0 OTG, USB0 is USB 2.0 Host Mode Only)

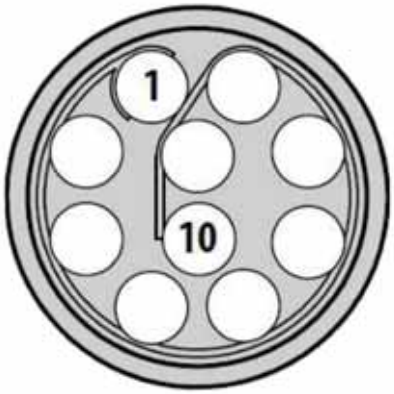


Figure 9 SC4400E AUX Pinout Diagram (Radio Side)

SC4400E PTT Connector	
Enclosure PTT Connector (ODU GKCWAM-P07UB00-000L)	**Signal**
1	5V_OUT (Up to 400mA)
2	COR/DUAL_PTT
3	AUDIO_GND
4	PTT
5	SPEAKER_OUT
6	MIC_IN
7	RESERVED (Do Not Connect)

Table 5 SC4400E PTT Connector Pinout

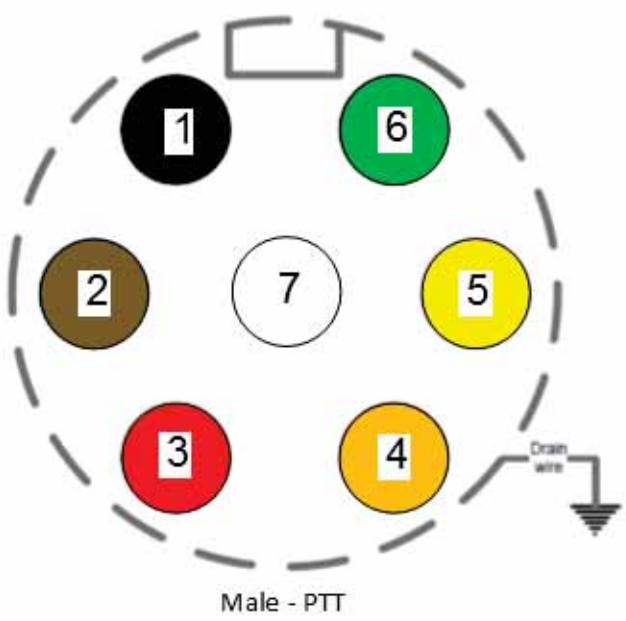


Figure 10 SC4400E PTT Pinout Diagram (Cable Side)

4.2.2 SC4200EP Pinouts

SC4200EP Primary Power/Ethernet/Serial Connector Pinout			
Enclosure PWR/COMM (GK0YAR-P10UC00-000L)	**Signal**	**Switchcraft Pinout (EN3C2F16X)**	**Color of wires coming from ODU connector**
1	5V OUT (For External GPS Puck)	NC	Pink
2	GND IN	2	Yellow/Blue
3	VCC IN	1	Green/Violet
4	ETH0_MX2N (RX-)	NC	Black
5	ETH0_MX2P (RX+)	NC	Brown
6	ETH0_MX1P (TX+)	NC	Red
7	RS232_RXD	NC	Gray
8	RS232_TXD	NC	White
9	GND	NC	Light Green
10	ETH0_MX1N (TX-)	NC	Orange

Table 6 SC4200EP Primary Power/Ethernet/Serial Connector Pinout

*color scheme is valid for cables built after 6/1/19

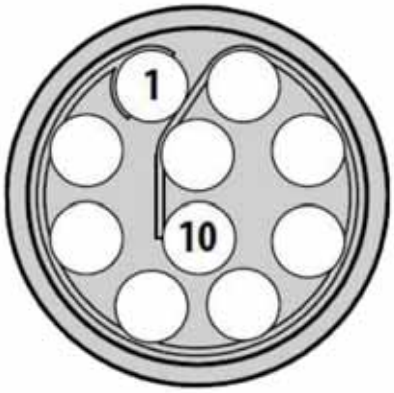


Figure 11 SC4200EP Primary Power/Serial/Ethernet Pinout Diagram (Radio Side)

SC4200EP RS-232 Pinout		
RS-232 (DB9)	**Signal**	**Switchcraft Pinout (EN3C6FX)**
3	TxD	2
2	RxD	1
NC	NC	4
NC	5V OUT	6
NC	NC	5
5	Ground	3

Table 7 SC4200EP Serial and GPS Pinout

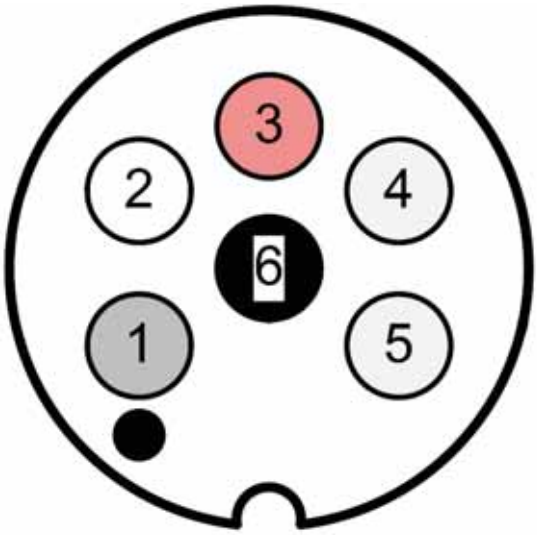


Figure 12 Switchcraft connector on Primary/Power cable

SC4200EP AUX Connector Pinout		
Enclosure AUX (GK0YCR-P10UC00-000L)	**Signal**	**Color of wires coming from ODU connector**
1	USB GND	Yellow/Blue
2	USB1_D-	Red
3	USB1_VBUS	Green
4	USB0_VBUS	Violet
5	GPIO1 (BDA control)	Pink
6	USB0_D+	Black
7	USB0_D-	Brown
8	GND	Light Green
9	USB1_ID	Gray
10	USB1_D+	Orange

Table 8 SC4200EP AUX USB/GPIO Connector Pinout (USB1 is USB 2.0 OTG, USB0 is USB 2.0 Host Mode Only)

*color scheme is valid for cables built after 6/1/19

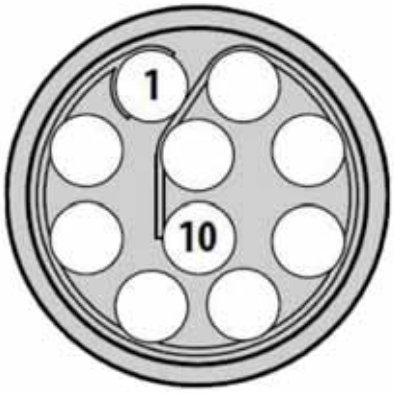


Figure 13 SC4200EP AUX Pinout Diagram (Radio Side)

SC4200EP PTT Connector	
Enclosure PTT Connector (ODU GKCWAM-P07UB00-000L)	**Signal**
1	5V_OUT (Up to 400mA)
2	COR/DUAL_PTT
3	AUDIO_GND
4	PTT
5	SPEAKER_OUT
6	MIC_IN
7	RESERVED (Do Not Connect)

Table 9 SC4200EP PTT Connector Pinout

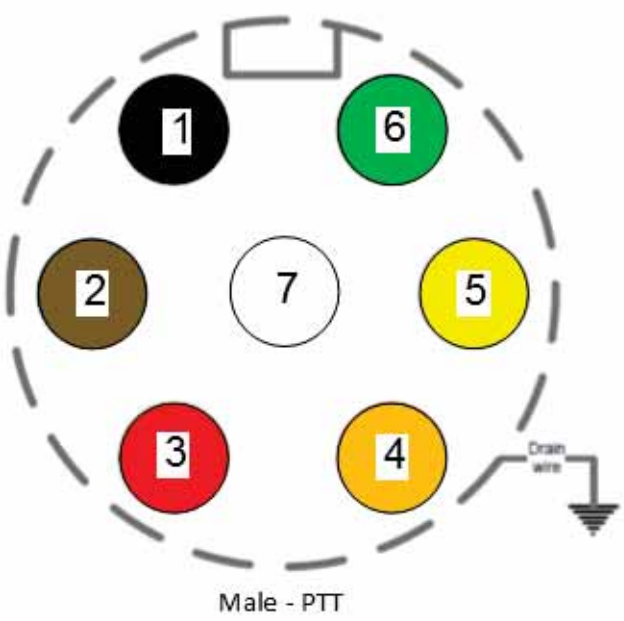


Figure 14 SC4200EP PTT Pinout Diagram (Cable Side)

4.2.3 SL4200 Pinouts

SL4200 POGO Connector Pinout	
Pin	**Signal**
1	Vbat 8-32 VDC input *
2	RS232 TXD
3	RS232 RXD
4	GPIO1
5	CC2 (PD mode-config)
6	CC1 (CC) (PD mode-config)
7	USB PD VBUSS (+9 VDC) *
8	USB0 Vbus (USB 0 always in host mode)
9	USB0 D+
10	USB0 D-
11	USB0_GND
12	N/C
13	N/C
14	GND *
15	USB1_GND
16	USB1 D+
17	USB1 D-
18	USB1 ID (Gnd for Host Mode; Float for Client mode)
19	N/C
20	VCC_5V0 OUT * (500 ma max (GPS Puck); connect to USB1 Vbus in host mode (e.g, USB-A pin 1))

Table 10 SL4200 POGO Connector Pinout

*Note: Pins 1,7,14,20 rated for 3A, 36V

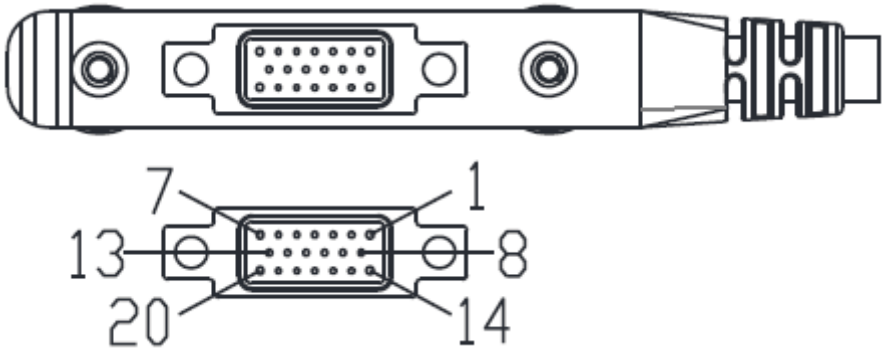


Figure 15 SL4200 20 pin POGO connector

Supported USB 1 Modes	Wiring instruction
USB-PD and USB 2.0 from the same source	USB1_ID floating and USB1 in client mode. Connect VCC_5V to USB1_VBUS on the pogo plug side or in the cable
USB 1 as client but not using USB-PD or PD comes from a different source	USB1_ID floating and USB1 in client mode, standard USB 2.0 wiring
USB 1 as host but not using USB-PD or PD comes from a different source	USB1_ID grounded and USB1 in host mode, standard USB 2.0 wiring

Table 11 SL4200 supported USB modes

4.2.4 SC4400 Pinouts

SC4400 Power/Ethernet/Serial Connector Pinout		
Enclosure PWR/COMM (LF10WBRB-12PD)	**Signal**	**Switchcraft Pinout (EN3C2F16X)**
1	5V OUT (For External GPS Puck)	NC
2	GND IN	2
3	GND IN	2
4	VCC IN	1
5	VCC IN	1
6	100-Base T ETH0 M2N (RX-)	NC
7	100-Base T ETH0 M2P (RX+)	NC
8	100-Base T ETH0 M1P (TX+)	NC
9	RS232_RXD	NC
10	RS232_TXD	NC
11	RS232_GND	NC
12	100-Base T ETH0 M1N (TX-)	NC

Table 12 SC4400 Primary Power/Ethernet/Serial Connector Pinout

SC4400 RS-232 and PS/2 (GPS) Pinout			
RS-232	**PS/2 (GPS)**	**Signal**	**Switchcraft Pinout (EN3C6FX)**
3	4	TxD	2
2	5	RxD	1
NC	NC	NC	4
NC	2	5V OUT	6
NC	NC	NC	5
5	1	Ground	3

Table 13 SC4400 Serial and GPS Pinout

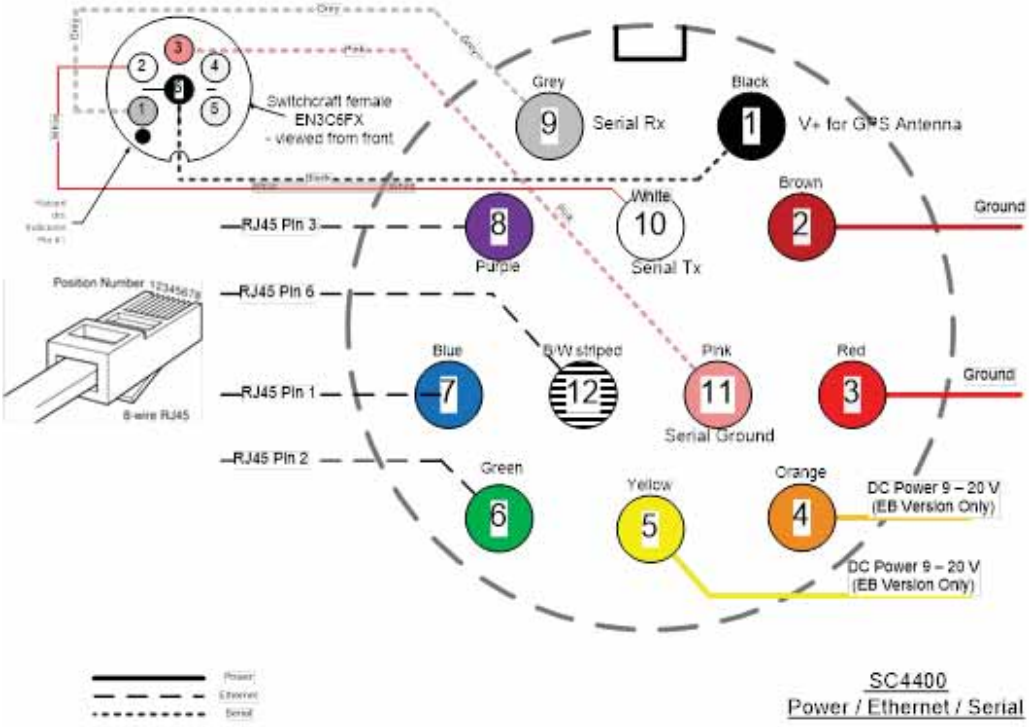


Figure 16 SC4400 Power (Optional)/Serial/Ethernet Pinout Diagram (Cable Side)

SC4400 AUX Connector Pinout	
Enclosure AUX (LF10WBRB-12SD)	**Signal**
1	USB1_GND
2	USB1_D-
3	USB1_VBUS
4	USB0_VBUS
5	GPIO1 (PA Enable 3.3V)
6	USB0_D+
7	USB0_D-
8	RESERVED (Do Not Connect)
9	GND
10	USB1_Sense
11	USB1_D+
12	USB0_GND

Table 14 SC4400 AUX USB/GPIO Connector Pinout (USB1 is USB 2.0 OTG, USB0 is USB 2.0 Host Mode Only)

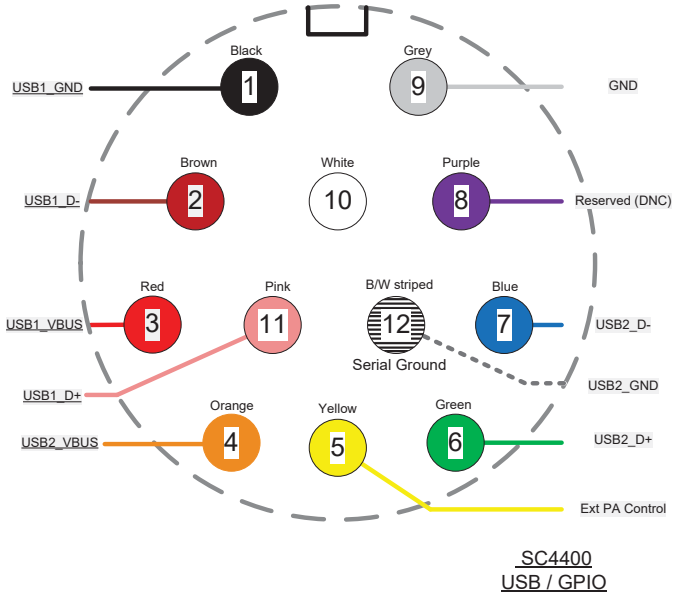


Figure 17 SC4400 AUX Pinout Diagram (Cable Side)

SC4400 PTT Connector	
Enclosure PTT Connector (ODU GKCWAM-P07UB00-000L)	**Signal**
1	RESERVED (Do Not Connect)
2	RESERVED (Do Not Connect)
3	AUDIO_GND
4	PTT
5	SPEAKER_OUT
6	MIC_IN
7	RESERVED (Do Not Connect)

Table 15 SC4400 PTT Connector Pinout

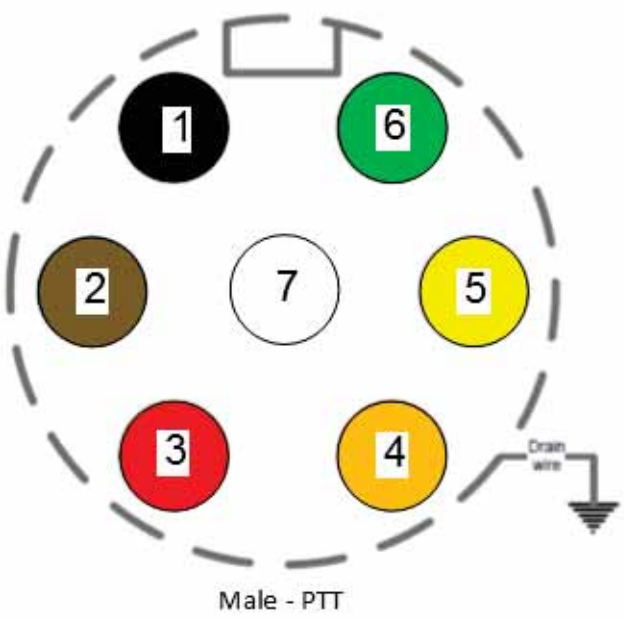


Figure 18 SC4400 PTT Pinout Diagram (Cable Side)

4.2.5 SC4200 Pinouts

SC4200 Power/Ethernet/Serial Connector Pinout		
Enclosure PWR/COMM (LF10WBRB-12PD)	**Signal**	**Switchcraft Pinout (EN3C2F16X)**
1	5V OUT (For External GPS Puck)	NC
2	GND IN (External Power Option Only)	2
3	GND IN (External Power Option Only)	2
4	VCC IN (External Power Option Only)	1
5	VCC IN (External Power Option Only)	1
6	100-Base T ETH0 M2N (RX-)	NC
7	100-Base T ETH0 M2P (RX+)	NC
8	100-Base T ETH0 M1P (TX+)	NC
9	RS232_RXD	NC
10	RS232_TXD	NC
11	RS232_GND	NC
12	100-Base T ETH0 M1N (TX-)	NC

Table 16 SC4200 Primary Power/Ethernet/Serial Connector Pinout

SC4200 RS-232 and PS/2 (GPS) Pinout			
RS-232	**PS/2 (GPS)**	**Signal**	**Switchcraft Pinout (EN3C6FX)**
3	4	TxD	2
2	5	RxD	1
NC	NC	NC	4
NC	2	5V OUT	6
NC	NC	NC	5
5	1	Ground	3

Table 17 SC4200 Serial and GPS Pinout

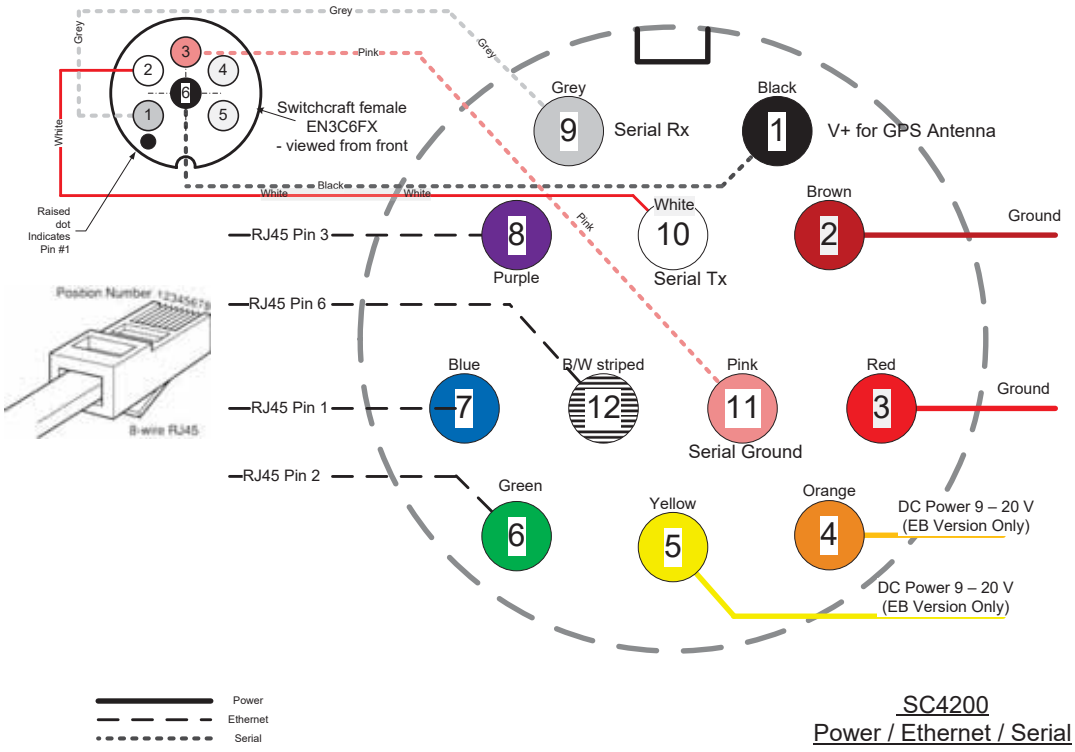


Figure 19 SC4200 Primary Power/Serial/Ethernet Pinout Diagram (Cable Side)

SC4200 AUX Connector Pinout	
Enclosure AUX (LF10WBRB-12SD)	**Signal**
1	USB1_GND
2	USB1_D-
3	USB1_VBUS
4	USB0_VBUS
5	GPIO1 (PA Enable 3.3V)
6	USB0_D+
7	USB0_D-
8	RESERVED (Do Not Connect)
9	GND
10	USB1_Sense
11	USB1_D+
12	USB0_GND

Table 18 SC4200 AUX USB/GPIO Connector Pinout (USB1 is USB 2.0 OTG, USB0 is USB 2.0 Host Mode Only)

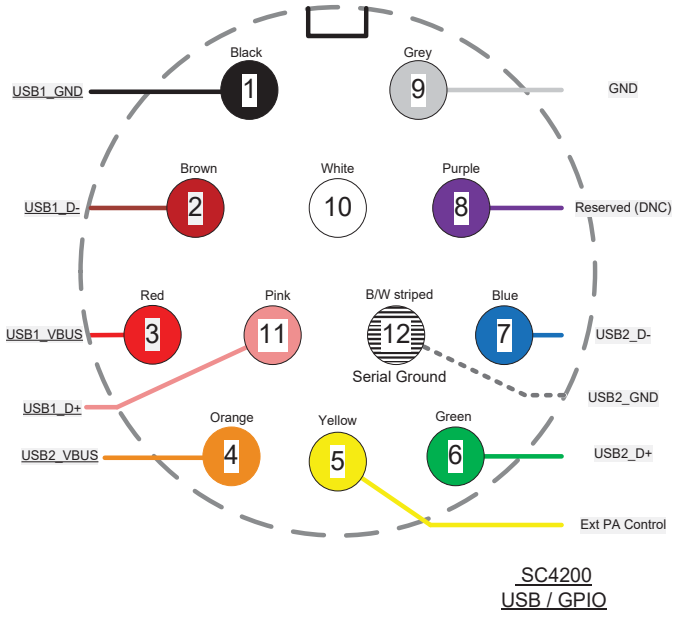


Figure 20 SC4200 AUX Pinout Diagram (Cable Side)

SC4200 PTT Connector	
Enclosure PTT Connector (ODU GKCWAM-P07UB00-000L)	**Signal**
1	RESERVED (Do Not Connect)
2	RESERVED (Do Not Connect)
3	AUDIO_GND
4	PTT
5	SPEAKER_OUT
6	MIC_IN
7	RESERVED (Do Not Connect)

Table 19 SC4200 PTT Connector Pinout

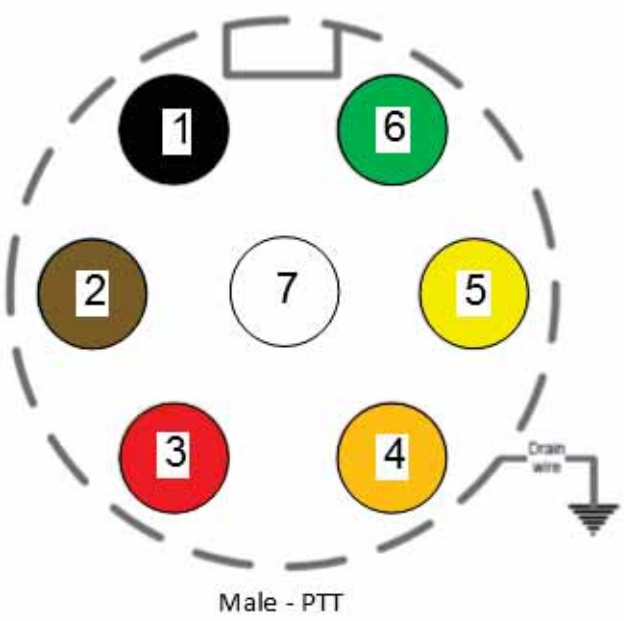


Figure 21 SC4200 PTT Pinout Diagram (Cable Side)

4.3 Mechanical and Operating Specifications

SC4400E:

Mechanical

- **Ambient Temp.** -40° to +65° C
- **IP Rating** IP-68 (Dust / Submersible in Water to 20m)**
- **Dimensions** 5.25” x 4.5” x 1.8” (Excluding Connectors)
- **Weight** 2.5 lbs. (40 oz./1.13 kg.)
- **Color** Black Anodized
- **Mounting** 4-Hole Mounting Pattern

Power

- **Voltage/Current** 9 – 20 VDC (± 5%), 5A
- **Power Consumption** 8 W – 100 W @ 20 W TX Power
  8 W – 43 W @ 8 W TX Power
  8 W – 24 W @ 1 W TX Power
- **Optional External Power Supply (for indoor only)** 12VDC, 5A

Interfaces

- **RF** 4 x TNC(f)
  [N(f) Optional]
- **Primary** Ruggedized Push/Pull Connector
  [1 x Ethernet, 1 x RS232, DC Input]
- **Auxiliary** Ruggedized Push/Pull Connector
  [1 x USB 2.0 Host, 1 x USB 2.0 OTG]
- **PTT (Push-to-Talk)** Ruggedized Break away Connector (Front Panel)
- **Status Indicator** Tri-Color LED
- **Control Interface** Multi-Position Switch

  13 presets plus zeroize crypto

  Web-Based StreamScape™ Network Manager

Mechanical – OEM

- **Dimensions** 4.29” x 3.3” x 0.82”
- **Weight** 9.1 oz (w/ Outer Shields)
- **RF Connectors** SMP (m)

(**) Must have all connectors mated with IP68+ cables/antennas

SC4200EP:

Mechanical

- **Ambient Temp.** -40° to +65° C
- **IP Rating** IP-68 (Dust / Submersible in Water up to 20m)**
- **Dimensions** 4.00” x 2.63” x 1.51” (Excluding Connectors)
- **Weight** 0.94 lbs. (15 oz./0.43 kg.)
- **Color** Black Anodized
- **Mounting** 4-Hole Mounting Pattern (Through-Hole)

Power

- **Voltage/Current** 9 – 20 VDC (± 5%), 5A
- **Power Consumption** 4.8 W – 48 W @ 10W TX Power
  4.8 W – 24 W @ 4W TX Power
  4.8 W – 16 W @ 1W TX Power
- **Battery Life** Up to 12 Hours (6.8Ah MBITR Battery)
- **Power Options** Twist-Lock Battery or Front Panel
- **Optional External Power Supply (for indoor only)** 12VDC, 5A

Interfaces

- **RF** TNC(f) (2 Each)
- **Primary** Ruggedized Push/Pull Connector (Front Panel)
  1 x Ethernet, 1x RS232, DC Input (Optional)
- **Auxiliary** Ruggedized Push/Pull Connector (Front Panel)
  1 x USB 2.0 Host, 1 x USB 2.0 OTG
- **PTT (Push-to-Talk)** Ruggedized Breakaway Connector (Front Panel)
- **Status Indicator** Tri-Color LED
- **Management Interface** Multi-Position Switch
  13 presets plus zeroize crypto
  Web-Based StreamScape™ Network Manager

Mechanical – OEM

- **Dimensions** 3.61” x 2.15” x 0.71”
- **Weight** 4.1 oz (w/ Outer Shields)
- **RF Connectors** SMP (m)

(**) Must have all connectors mated with IP68+ cables/antennas

SL4200:

Mechanical

- **Ambient Temp.** -40° to +65° C
- **IP Rating** IP-67 (Dust / Submersible in Water up to 1m)**
- **Dimensions** 119 x 74 x 18 mm (Excluding Connectors)
- **Weight** 295 grams
- **Color** Black Anodized Aluminum

Power

- **Voltage/Current** 8-32VDC input / USB-C PD (9VDC)
- **Power Consumption** 4.8 W – 17 W @ 1 W TX Power

Interfaces

- **RF** TNC(f) (2 Each)
- **Power/Data** 20-pin "POGO" style connector
  8-32VDC input / USB-C PD (9VDC)
  2x USB 2.0 (Host / OTG)
  Serial RS-232
  +5VDC output
- **Status Indicator** Tri-Color LED
- **Management Interface** On/Off Switch
  Web-Based StreamScape™ Network Manager

Mechanical – OEM

- **Dimensions** 0.45" x 2.15" (ears: 2.74")x 3.83"
- **Weight** 105 g (Module)
  45 g (PCBA only)
- **RF Connectors** SMA

(**) Must have all connectors mated with IP67+ cables/antennas

SC4400:

Mechanical

- **Ambient Temp.** -40° to +65° C
- **IP Rating** IP-67 (Dust / Immersion in Water up to 1m)**
- **Dimensions** 5.25” x 4.5” x 1.8” (Excluding Connectors)
- **Weight** 2.5 lbs. (40 oz./1.13 kg.)
- **Color** Black Anodized
- **Mounting** 4-Hole Mounting Pattern

Power

- **Voltage/Current** 9 – 20 VDC (± 5%), 5A
- **Power Consumption** 8 W – 43 W @ 8 W TX Power
  8 W – 24 W @ 1 W TX Power
- **Optional External Power Supply (for indoor only)** 12VDC, 5A

Interfaces

- **RF** 4 x TNC(f)
  [N(f) Optional]
- **Primary** Ruggedized Circular Connector
  [1 x Ethernet, 1 x RS232, DC Input]
- **Auxiliary** Ruggedized Circular Connector
  [1 x USB 2.0 Host, 1 x USB 2.0 OTG]
- **PTT (Push-to-Talk)** Ruggedized Break away Connector (Front Panel)
- **Status Indicator** Tri-Color LED
- **Management Interface** Web-Based StreamScape™ Network Manager

Mechanical – OEM

- **Dimensions** 4.29” x 3.3” x 0.82”
- **Weight** 9.1 oz (w/ Outer Shields)
- **RF Connectors** SMP (m)

(**) Must have all connectors mated with IP67+ cables/antennas

SC4200:

Mechanical

- **Ambient Temp.** -40° to +65° C
- **IP Rating** IP-67 (Dust / Immersion in Water up to 1m)**
- **Dimensions** 4.00” x 2.63” x 1.51” (Excluding Connectors)
- **Weight** 0.94 lbs. (15 oz./0.43 kg.)
- **Color** Black Anodized
- **Mounting** 4-Hole Mounting Pattern (Through-Hole)

Power

- **Voltage/Current** 9 – 20 VDC (± 5%), 5A
- **Power Consumption** 4.8 W – 24 W @ 4W TX Power
  4.8 W – 16 W @ 1W TX Power
- **Battery Life** Up to 12 Hours (6.8Ah MBITR Battery)
- **Power Options** Twist-Lock Battery or Front Panel
- **Optional External Power Supply (for indoor only)** 12VDC, 5A

Interfaces

- **RF** TNC(f) (2 Each)
- **Primary** Ruggedized Circular Connector (Front Panel)
  1 x Ethernet, 1x RS232, DC Input (Optional)
- **Auxiliary** Ruggedized Circular Connector (Front Panel)
  1 x USB 2.0 Host, 1 x USB 2.0 OTG
- **PTT (Push-to-Talk)** Ruggedized Break away Connector (Front Panel)
- **Status Indicator** Tri-Color LED
- **Management Interface** Web-Based StreamScape™ Network Manager

Mechanical – OEM

- **Dimensions** 3.61” x 2.15” x 0.71”
- **Weight** 4.1 oz (w/ Outer Shields)
- **RF Connectors** SMP (m)

(**) Must have all connectors mated with IP67+ cables/antennas

4.3.1 SC4400E Enclosure Mechanical Drawing

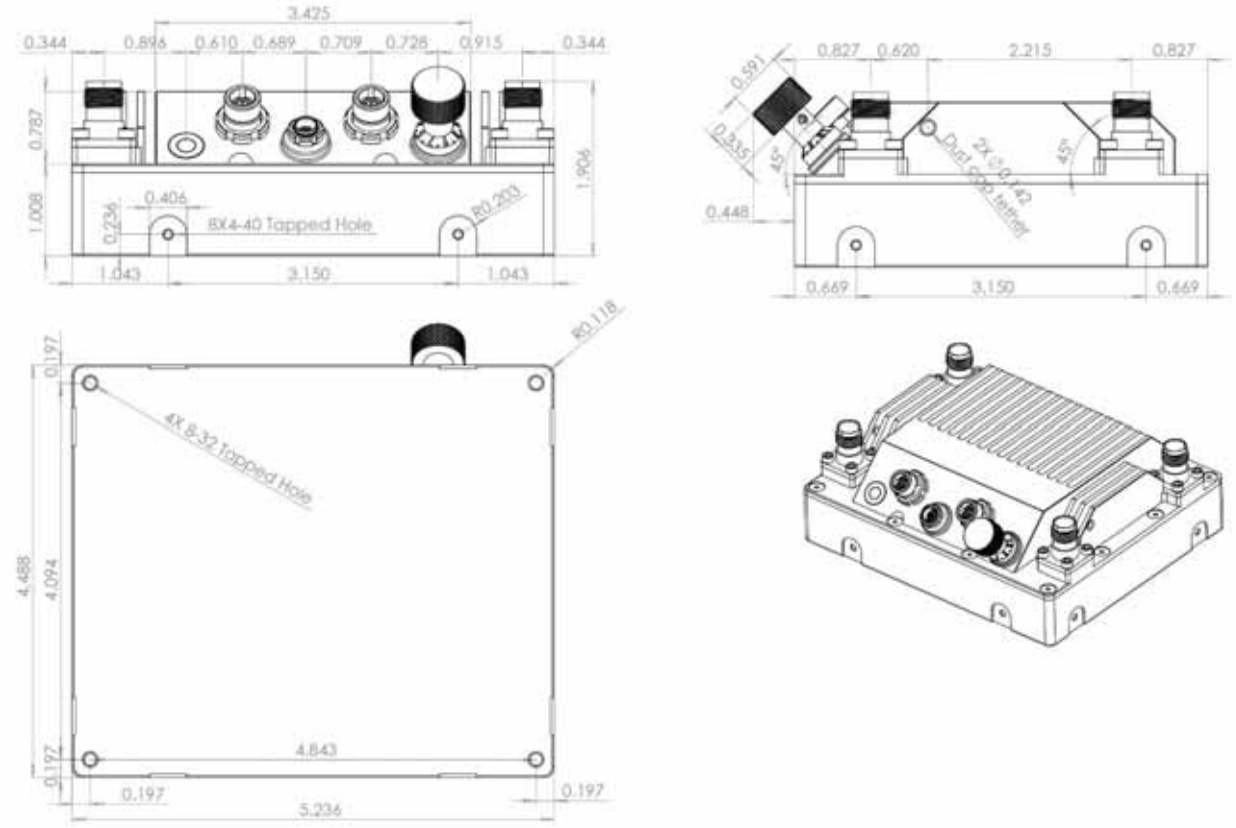


Figure 22 SC4400E Mechanical Drawing (top) and Mounting Pattern (bottom)

*Tapped mounting holes are available on bottom (8-32) and on the sides (4-40) of radio as indicated in

4.3.2 SC4200EP Enclosure Mechanical Drawing

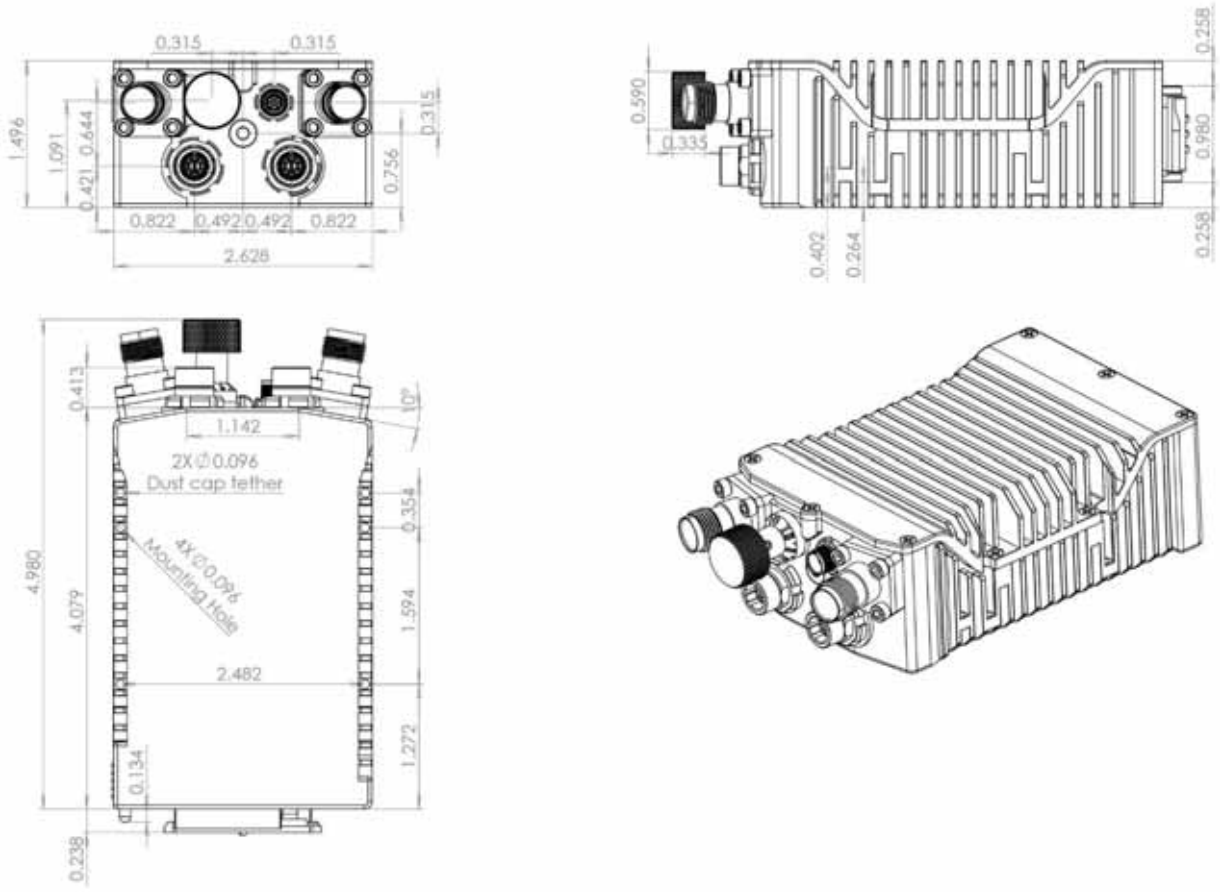


Figure 23 SC4200EP Mechanical Drawing (top) and Mounting Pattern (bottom)

*mounting holes utilize https://www.mcmaster.com/96006a234 or equivalent. Hex head (5/64” drive), 2-56 thread, head diameter 9/64”; stainless steel; 3/8” length or longer

4.3.3 SL4200 Enclosure Mechanical Drawing

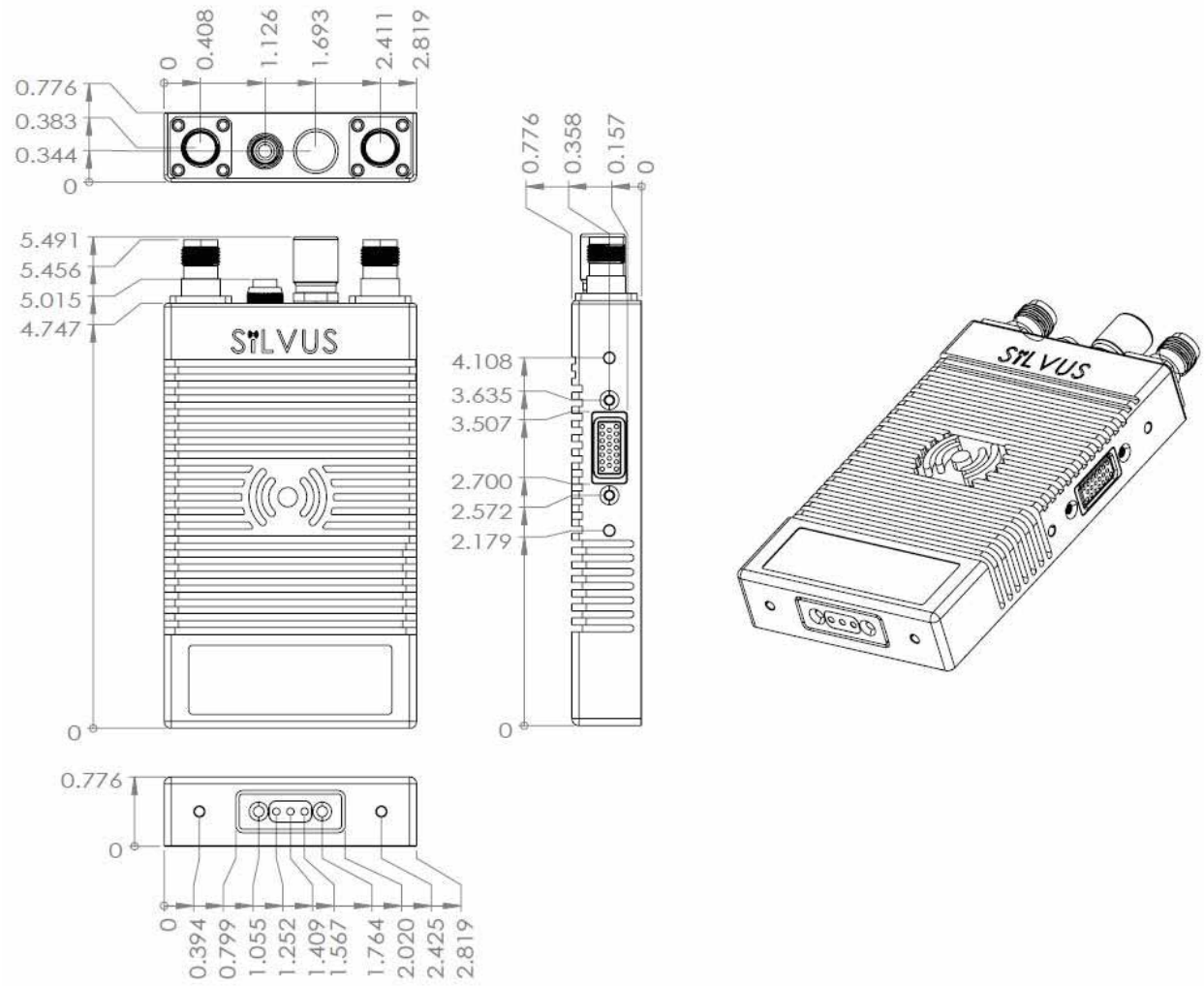
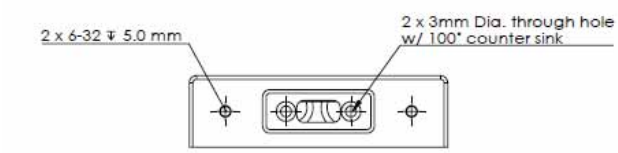


Figure 24 SL4200 Mechanical Drawing

***** Tapped mounting holes are available on bottom 6-32 screw, 0.196inch (5.0mm) depth.



4.3.4 SC4400 Enclosure Mechanical Drawing

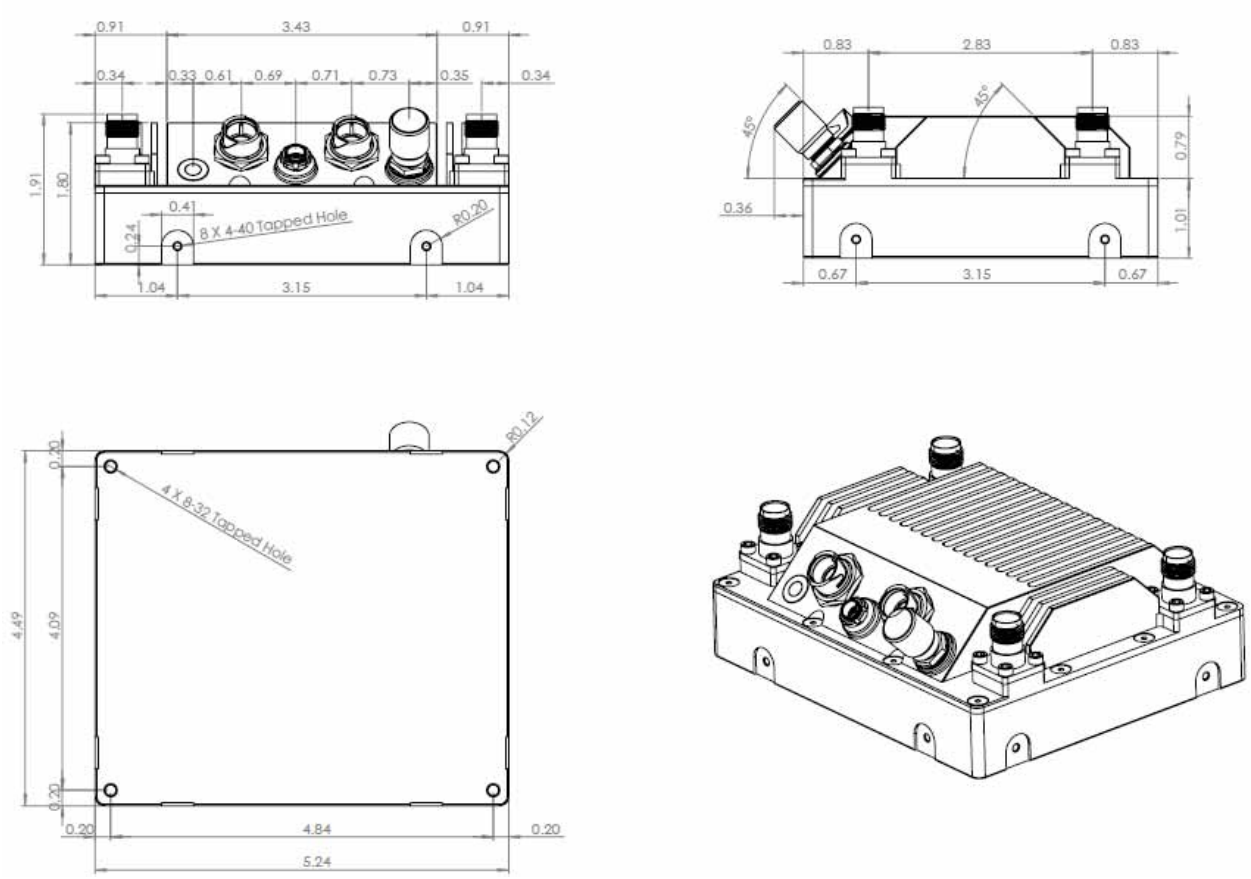


Figure 25 SC4400 Mechanical Drawing (top) and Mounting Pattern (bottom)

*Tapped mounting holes are available on bottom (8-32) and on the sides (4-40) of radio as indicated in **Figure 25 SC4400 Mechanical Drawing (top) and Mounting Pattern (bottom)**.

4.3.5 SC4200 Enclosure Mechanical Drawing

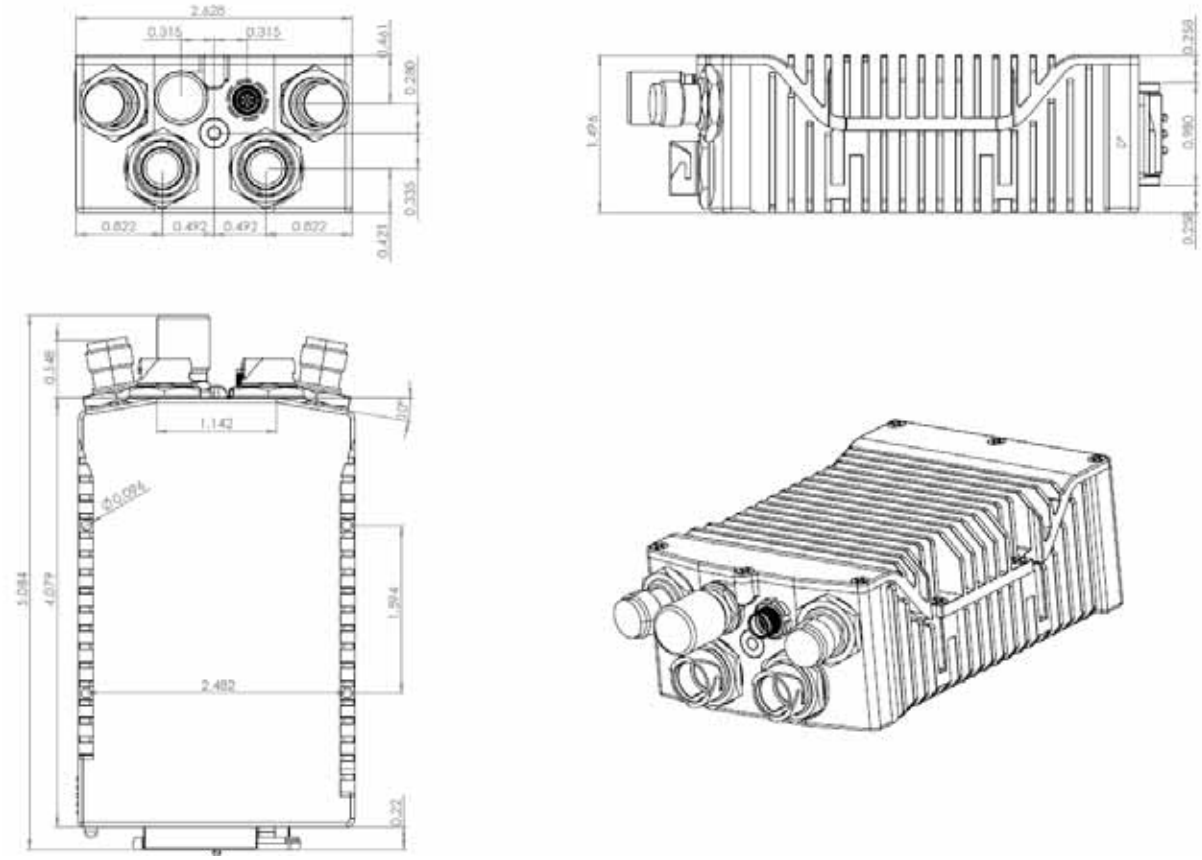


Figure 26 SC4200 Mechanical Drawing (top) and Mounting Pattern (bottom)

*mounting holes utilize https://www.mcmaster.com/96006a234 or equivalent. Hex head (5/64” drive), 2-56 thread, head diameter 9/64”; stainless steel; 3/8” length or longer

4.4 SC4400E Specifications

General

- **Waveform** — Mobile Networked MIMO (MN-MIMO™)
- **Modulation** — BPSK, QPSK, 16-QAM, 64-QAM
- **Channel Bandwidth** — 5, 10 & 20 MHz (1.25*, 2.5*)
- **Encryption** — DES Standard, AES/GCM 128/256 Optional (FIPS 140-2 Level 2 certified), Suite B
- **Tuning Step Size** — 1kHz
- **Data Rates** — Up to 100 Mbps (Adaptive)
- **Error Correction** — 1/2, 2/3, 3/4, 5/6
- **Antenna Processing** — Spatial Multiplexing, Space-Time Coding, TX Eigen Beamforming, RX Eigen Beamforming
- **No. of Spatial Streams** — 1-2
- **No. of Antennas** — 4

Performance

- **Latency** — 7ms Average (20MHz BW)
- **Sensitivity** — -102 dBm @ 5MHz BW
- **Frequency Bands** — Bands from 400MHz to 6GHz Available Dual Band Optional
- **Onboard Storage** — 64 GB*

Frequency Band Options

Band (Freq. Code)	Frequency Range	Band (Freq. Code)	Frequency Range
UHF (042)	400-450	**Low C Band (455)**	4400-4700
ISM 900 (091)	902-928	**Federal C-1 (467)**	4400-4940
L Band (137)	1350-1390	**High C Band (485)**	4700-5000
Upper L (181)	1780-1850	**5.2GHz ISM (520)**	5150-5250
Broadcast B (206)	2025-2110	**5.8GHz ISM (580)**	5725-5875
Federal S (225)	2200-2300		
S Band (235)	2200-2500		
2.4GHz ISM (245)	2400-2500		

(All bands listed in MHz)

Note: If band of interest is not listed, please contact a sales representative

Footnote: (*) in development

4.5 SC4200EP Specifications

General

- **Waveform** — Mobile Networked MIMO (MN-MIMO™)
- **Modulation** — BPSK, QPSK, 16-QAM, 64-QAM
- **Channel Bandwidth** — 5, 10 & 20 MHz (1.25*, 2.5*)
- **Encryption** — DES Standard, AES/GCM 128/256 Optional (FIPS 140-2 Level 2 certified), Suite B
- **Tuning Step Size** — 1kHz
- **Data Rates** — Up to 100 Mbps (Adaptive)
- **Error Correction** — 1/2, 2/3, 3/4, 5/6
- **Antenna Processing** — Spatial Multiplexing, Space-Time Coding, TX Eigen Beamforming, RX Eigen Beamforming
- **No. of Spatial Streams** — 1-2
- **No. of Antennas** — 2

Performance

- **Latency** — 7ms Average
- **Sensitivity** — -99 dBm @ 5MHz BW
- **Frequency Bands** — Bands from 400MHz to 6GHz Available Dual Band Optional
- **Onboard Storage** — 64 GB*

Frequency Band Options

Band (Freq. Code)	Frequency Range	Band (Freq. Code)	Frequency Range
UHF (042)	400-450	**Low C Band (455)**	4400-4700
ISM 900 (091)	902-928	**Federal C-1 (467)**	4400-4940
L Band (137)	1350-1390	**High C Band (485)**	4700-5000
Upper L (181)	1780-1850	**5.2GHz ISM (520)**	5150-5250
Broadcast B (206)	2025-2110	**5.8GHz ISM (580)**	5725-5875
Federal S (225)	2200-2300		
S Band (235)	2200-2500		
2.4GHz ISM (245)	2400-2500		

(All bands listed in MHz)

Note: If band of interest is not listed, please contact a sales representative

Footnote: (*) in development

SC4400E/SC4200EP PTT

Supported Mic Type	Moving Coil or Condenser (Software Configurable)
• **Max Avg. Speaker Output Power**	2.65W with 4 Ohm Speaker Impedance
• **MIC Bias**	2.15V or 3V (Software Configurable); Applied via a 2K Ohm Resistor
• **Recommended Speaker Impedance (Handset)**	4 Ohm to 16 Ohm
• **Recommended Speaker Impedance (Headset)**	75 Ohm to 300 Ohm
• **Recommended MIC impedance**	<= 1K Ohm
• **Peak Speaker Output Voltage**	5.5V
• **Absolute MIC Input Voltage**	3.3V

4.6 SL4200 Specifications

General

- **Waveform** — Mobile Networked MIMO (MN-MIMO™)
- **Modulation** — BPSK, QPSK, 16-QAM, 64-QAM
- **Channel Bandwidth** — 1.25, 2.5 or 5 MHz
- **Encryption** — DES Standard, AES/GCM 128/256 Optional (FIPS 140-2)
- **Tuning Step Size** — 1kHz
- **Data Rates** — Up to 20 Mbps (Adaptive)
- **Error Correction** — 1/2, 2/3, 3/4, 5/6
- **Antenna Processing** — Spatial Multiplexing, Space-Time Coding, TX Eigen Beamforming, RX Eigen Beamforming
- **No. of Spatial Streams** — 1-2
- **No. of Antennas** — 2

Performance

- **Latency** — 28ms Average (5MHz BW)
- **Sensitivity** — -104 dBm @ 1.25MHz BW
- **Frequency Bands** — 2.2 - 2.5 GHz
  4.4-4.94 GHz
  (additional bands in development)

4.7 SC4400 Specifications

General

- **Waveform** — Mobile Networked MIMO (MN-MIMO™)
- **Modulation** — BPSK, QPSK, 16-QAM, 64-QAM
- **Channel Bandwidth** — 5, 10 & 20 MHz (1.25*, 2.5*)
- **Encryption** — DES Standard, AES/GCM 128/256 Optional (FIPS 140-2 Level 2 certified), Suite B
- **Tuning Step Size** — 1kHz
- **Data Rates** — Up to 100 Mbps (Adaptive)
- **Error Correction** — 1/2, 2/3, 3/4, 5/6
- **Antenna Processing** — Spatial Multiplexing, Space-Time Coding, TX Eigen Beamforming, RX Eigen Beamforming
- **No. of Spatial Streams** — 1-2
- **No. of Antennas** — 4

Performance

- **Latency** — 7ms Average (20MHz BW)
- **Sensitivity** — -102 dBm @ 5MHz BW
- **Frequency Bands** — Bands from 400MHz to 6GHz Available Dual Band Optional
- **Onboard Storage** — 64 GB*

Frequency Band Options

Band (Freq. Code)	Frequency Range	Band (Freq. Code)	Frequency Range
UHF (042)	400-450	**Low C Band (455)**	4400-4700
ISM 900 (091)	902-928	**Federal C-1 (467)**	4400-4940
L Band (137)	1350-1390	**Federal C-2 (469)***	4400-4990
Upper L (181)	1780-1850	**High C Band (485)**	4700-5000
Broadcast B (206)	2025-2110	**5.2GHz ISM (520)**	5150-5250
Federal S (225)	2200-2300	**5.8GHz ISM (580)**	5725-5875
S Band (235)	2200-2500		
2.4GHz ISM (245)	2400-2500		

(All bands listed in MHz)

Note: If band of interest is not listed, please contact a sales representative

Footnote: (*) in development

4.8 SC4200 Specifications

General

- **Waveform** — Mobile Networked MIMO (MN-MIMO™)
- **Modulation** — BPSK, QPSK, 16-QAM, 64-QAM
- **Channel Bandwidth** — 5, 10 & 20 MHz (1.25*, 2.5*)
- **Encryption** — DES Standard, AES/GCM 128/256 Optional (FIPS 140-2 Level 2 certified), Suite B
- **Tuning Step Size** — 1KHz
- **Data Rates** — Up to 100 Mbps (Adaptive)
- **Error Correction** — 1/2, 2/3, 3/4, 5/6
- **Antenna Processing** — Spatial Multiplexing, Space-Time Coding, TX Eigen Beamforming, RX Eigen Beamforming
- **No. of Spatial Streams** — 1-2
- **No. of Antennas** — 2

Performance

- **Latency** — 7ms Average
- **Sensitivity** — -99 dBm @ 5MHz BW
- **Frequency Bands** — Bands from 400MHz to 6GHz Available Dual Band Optional
- **Onboard Storage** — 64 GB*

Frequency Band Options

Band (Freq. Code)	Frequency Range	Band (Freq. Code)	Frequency Range
UHF (042)	400-450	**Low C Band (455)**	4400-4700
ISM 900 (091)	902-928	**Federal C-1 (467)**	4400-4940
L Band (137)	1350-1390	**Federal C-2 (469)***	4400-4990
Upper L (181)	1780-1850	**High C Band (485)**	4700-5000
Broadcast B (206)	2025-2110	**5.2GHz ISM (520)**	5150-5250
Federal S (225)	2200-2300	**5.8GHz ISM (580)**	5725-5875
S Band (235)	2200-2500		
2.4GHz ISM (245)	2400-2500		

(All bands listed in MHz)

Note: If band of interest is not listed, please contact a sales representative

Footnote: (*) in development

SC4400/SC4200 PTT

Supported Mic Type

Moving Coil or Condenser (Software Configurable)

- **Max Avg. Speaker Output Power** — 2.65W with 4 Ohm Speaker Impedance
- **MIC Bias** — 2.15V or 3V (Software Configurable); Applied via a 2K Ohm Resistor
- **Recommended Speaker Impedance (Handset)** — 4 Ohm to 16 Ohm
- **Recommended Speaker Impedance (Headset)** — 75 Ohm to 300 Ohm
- **Recommended MIC impedance** — <= 1K Ohm
- **Peak Speaker Output Voltage** — 5.5V
- **Absolute MIC Input Voltage** — 3.3V

5. Web Interface

5.0 Getting Started

Connect a laptop to the StreamCaster radio using the supplied Ethernet cable and turn on the radio. Users can type “ping <IP address>” in order to determine whether the radio is fully booted. A web configuration will then be available by typing the radio IP address in a web browser. Please ensure that your laptop is on the same subnet as the radio (172.20.xx.xx by default). Users will initially see the link distance warning, then be directed to the Local Radio Configuration page. (See **Figure 27 Initial boot up warning**) You will be able to navigate to various configuration pages from the drop-down menu on the left-hand side. On the right, you can open additional details about the radio by selecting the four squares icon on the top right of the screen. After selecting, you will see details such as local radio IP, VIP, Node Label, temperature, voltage, and an option to use night mode or not. Night mode will have a dark background and below screen shots are an example of the GUI in night mode. Throughout the user interface, if there is a red bar below the parameter you will be able to click on it for either additional notes about the parameter or see additional options.

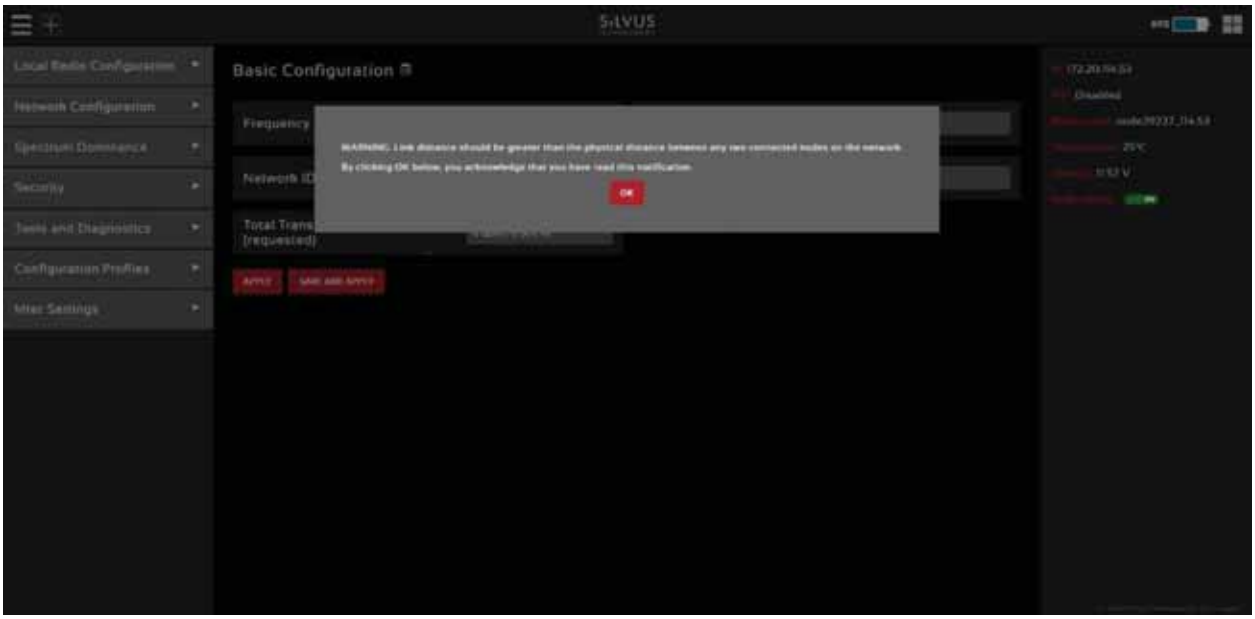


Figure 27 Initial boot up warning

Upon first boot up and login to the GUI, you will see a warning message. This message is meant to emphasize the importance of having the correct link distance setting.

5.1 Local Radio Configuration

The first group of configurations on the left side of the GUI is the Local Radio Configurations. This group of parameters can help adjust your network to perform better in various environments, conditions, and applications. You will be able to adjust the radio's RF characteristics, networking parameters, BDA configurations, serial/USB configurations, and PTT settings.

5.1.1 RF

The RF section of the Local Radio Configurations will let you adjust some Basic configurations as well as some Advanced parameters. These configurations will optimize the link performance in different types of deployments. To get radios to link and form a mesh network the center frequency, bandwidth, network ID, and Link Distance parameters in the Basic configuration page need to all match. To optimize the network's performance, you can make some adjustments to the MAC settings under the Advanced section.

5.1.1.1 Basic

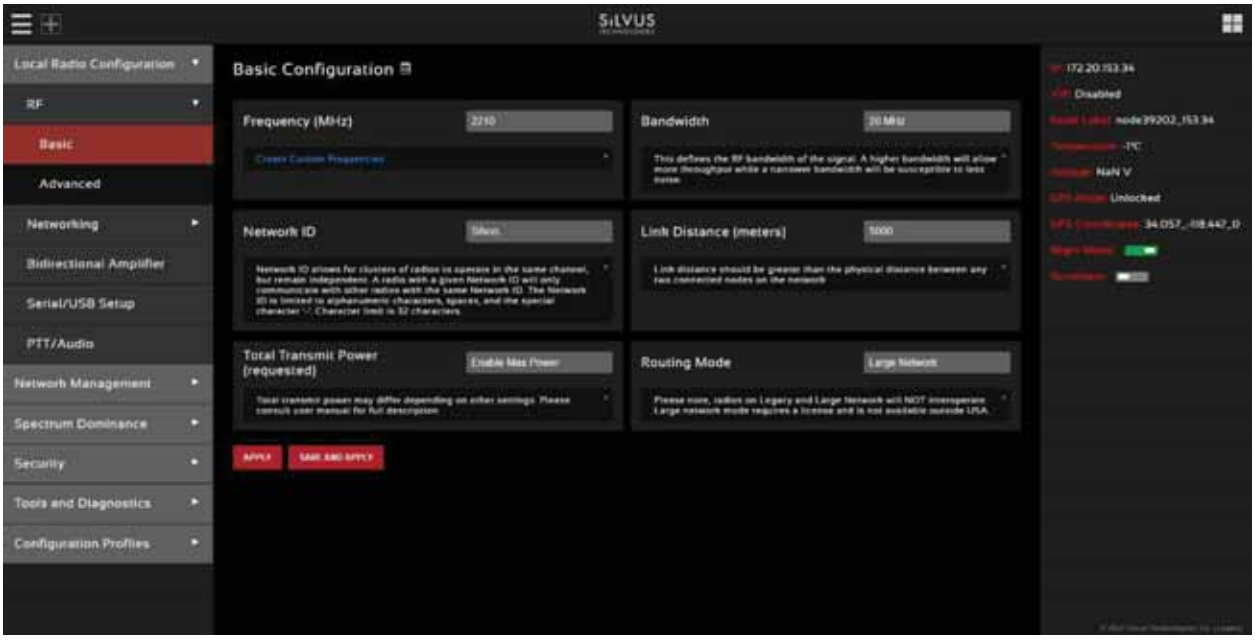


Figure 28 Basic Configuration Page

This page is used to set basic configurations. A brief description of each parameter is given below.

- **Frequency**: This defines the frequency of the signal. There is a drop-down menu for frequency selection. The frequency choices will vary depending on the StreamCaster model(s) you are using. In the additional information section of the frequency section (click on the red bar directly below), you can select a link that will take you to create custom frequencies. Please

see Section 8 Custom Frequency Plan for “Create Custom Frequencies” access and installation instructions.

- **Bandwidth**: This defines the RF bandwidth of the signal. A higher bandwidth will allow more throughput while a narrower bandwidth will be susceptible to less noise.
- **Network ID**: Network ID allows for clusters of radios to operate in the same channel but remain independent. A radio with a given Network ID will only communicate with other radios with the same Network ID. The Network ID is limited to alphanumeric characters, spaces, and the special character '-'. Character limit is 32 characters.
- **Link Distance**: Set to an approximate maximum distance between any two nodes in meters, e.g., 5000 for 5km (default). It is important to set the link distance to allow enough time for packets to propagate over the air. Failing to set the link distance to an approximate maximum distance can result in over the air collisions and a degradation of performance. It is recommended to set the link distance 10-15% greater than the actual maximum distance. Please note that this value should be set the same on all radios in the network.
- **Total Transmit Power**: This defines the total power of the signal (power is divided equally between the radio antenna ports). There is also an option to ‘Enable Max Power’ which will allow the radio to push to the highest TX power it can support. This will be slightly different on each radio.
- **Routing Mode**: Please note radios on Legacy and Large Network will NOT interoperate. Large network routing was designed to allow networks with a higher node count. However, there are marginal benefits even if operating smaller networks.
- **Apply**: Apply the new values. Values will change back to the default setting after reboot.
- **Save and Apply**: Apply the new values and set the new values as the default.

5.1.1.2 Advanced

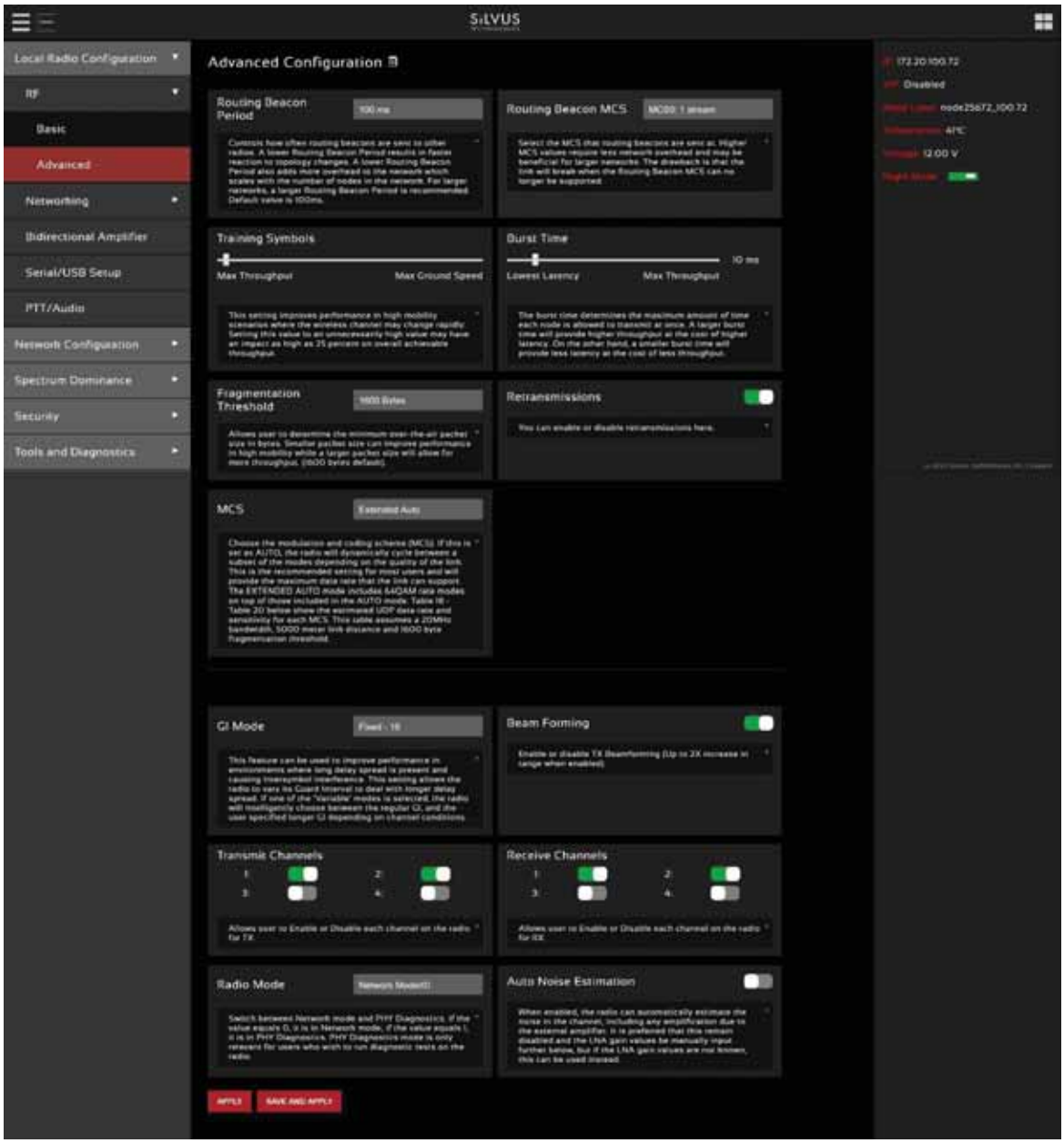


Figure 29 Advanced Configuration Page

This page is used to set the advanced settings. A brief description of each parameter is given below.

MAC Settings:

- **Routing Beacon Period**: Controls how often routing beacons are sent to other radios. A lower Routing Beacon Period results in faster reaction to topology changes. A lower Routing Beacon Period also adds more overhead to the network which scales with the number of nodes in the

network. For larger networks, a larger Routing Beacon Period is recommended. Default value is 100ms.

- **Routing Beacon MCS**: Select the MCS that routing beacons are sent at. Higher MCS values require less network overhead and may be beneficial for larger networks. The drawback is that the link will break when the Routing Beacon MCS can no longer be supported.
- **Training Symbols**: This setting improves performance in high mobility scenarios where the wireless channel may change rapidly. Setting this value to an unnecessarily high value may have an impact as high as 25 percent on overall achievable throughput.
- **Burst Time**: The burst time determines the maximum amount of time each node is allowed to transmit at once. A larger burst time will provide higher throughput at the cost of higher latency. On the other hand, a smaller burst time will provide less latency at the cost of less throughput.
- **Fragmentation Threshold**: Allows user to determine the minimum over-the-air packet size in bytes. Smaller packet size can improve performance in high mobility while a larger packet size will allow for more throughput. (1600 bytes default).
- **Retransmissions:** You can enable or disable retransmissions here.
- **MCS**: Choose the modulation and coding scheme (MCS). If this is set as AUTO, the radio will dynamically cycle between a subset of the modes depending on the quality of the link. This is the recommended setting for most users and will provide the maximum data rate that the link can support. The EXTENDED AUTO mode includes 64QAM rate modes on top of those included in the AUTO mode. **Table 22** below show the estimated UDP data rate and sensitivity for each MCS. This table assumes a 5000 meter link distance, 10ms burst time, and 1600 byte fragmentation threshold.
- **GI Mode:** This feature can be used to improve performance in environments where long delay spread is present and causing intersymbol interference*. This setting allows the radio to vary its Guard Interval** to allow for longer delay spread. When set to 'Extended Auto – GI', the radio will choose between the regular GI, and the user specified longer GI (Cyclic Prefix Length in the next setting) depending on channel conditions. Delay spread is often seen in environments where there are high rise buildings with metal, glass, cement, or other material with a high potential for reflections. Using a low GI mode will allow more time used sending data and therefore give you more throughput, however a higher GI mode will give you less chance of seeing loss due to delay spread. Below are some criteria for when you might want to increase the amount of guard interval:
    - Reported loss rate is high
    - Interference is not the cause of high loss rate
    - Environment radios are deployed in has the potential for RF reflections

  You will know that you have reach a more appropriate GI mode if the loss rate decreases after adjusting.

*(https://en.wikipedia.org/wiki/Intersymbol_interference)
**(https://en.wikipedia.org/wiki/Guard_interval)

- **Beamforming (SC4200/SC4400/SL4200):** Enable or disable TX Beamforming (Up to 2X increase in range when enabled) If beamforming is disabled while using cross polarized antennas, antennas should be arranged such that one polarity is on the odd ports and the other polarity on the even ports.
- **Transmit Channels:** Allows user to Enable or Disable each channel on the radio for TX.
- **Receive Channels:** Allows user to Enable or Disable each channel on the radio for RX.
- **Radio Mode**: Switch between Network mode and PHY Diagnostics. If the value equals 0, it is in Network mode; if the value equals 1, it is in PHY Diagnostics. PHY Diagnostics mode is only relevant for users who wish to run diagnostic tests on the radio.
- **Apply**: Applies the new values but does not save them to flash.
- **Save and Apply**: Save the new values to flash and apply.

Modulation Modes and Receiver Sensitivity

- Note that listed sensitivity values were measured using a controlled and cabled setup. Actual results may vary by +/- 2dB. Table assumes link distance of 5000m. 10ms, 20ms, and 40ms burst time for 20, 10, and 5MHz bandwidth respectively. 1600 byte Fragmentation Threshold.
- * Modes supported under the AUTO MCS option.
- * Modes supported under the EXTENDED AUTO MCS option in addition to AUTO MCS modes.
- *Modes currently not supported

NSS	MCS	Coding Rate	PHY Throughput (Mbps)	UDP User Throughput (Mbps)	SC4400/3500/3800 Sensitivity	SC4200/3822 SL4200 Sensitivity
1	0	BPSK 1/2	0.41	0.27	-108	-105
1	1	QPSK 1/2	0.81	0.55	-106	-103
1	2	QPSK 3/4	1.22	0.82	-103	-100
1	3	16-QAM 1/2	1.63	1.10	-101	-98
1	4	16-QAM 3/4	2.44	1.65	-98	-95
1	5	64 QAM 2/3	3.25	2.20	-93	-90
1	6	64 QAM 3/4	3.66	2.47	-91	-88
1	7	64 QAM 5/6	4.06	2.75	-86	-83
2	8	BPSK 1/2	0.81	0.55	-106	-103
2	9	QPSK 1/2	1.63	1.10	-103	-100
2	10	QPSK 3/4	2.44	1.65	-100	-97
2	11	16-QAM 1/2	3.25	2.20	-97	-94
2	12	16-QAM 3/4	4.88	3.30	-94	-91
2	13	64 QAM 2/3	6.50	4.35	-90	-87
2	14	64 QAM 3/4	7.31	4.75	-88	-85
2	15	64 QAM 5/6	8.13	5.10	-83	-80

Table 20 MCS vs. Sensitivity Chart (1.25MHz Bandwidth)*

NSS	MCS	Coding Rate	PHY Throughput (Mbps)	UDP User Throughput (Mbps)	SC4400/3500/3800 Sensitivity	SC4200/3822 SL4200 Sensitivity
1	0	BPSK 1/2	0.81	0.55	-104.5	-101.5
1	1	QPSK 1/2	1.63	1.10	-102.5	-99.5
1	2	QPSK 3/4	2.44	1.65	-99.5	-96.5
1	3	16-QAM 1/2	3.25	2.20	-97.5	-94.5
1	4	16-QAM 3/4	4.88	3.30	-94.5	-91.5
1	5	64 QAM 2/3	6.50	4.40	-89.5	-86.5
1	6	64 QAM 3/4	7.31	4.95	-87.5	-84.5
1	7	64 QAM 5/6	8.13	5.5	-82.5	-79.5
2	8	BPSK 1/2	1.63	1.10	-102.5	-99.5
2	9	QPSK 1/2	3.25	2.20	-99.5	-96.5
2	10	QPSK 3/4	4.88	3.30	-96.5	-93.5
2	11	16-QAM 1/2	6.50	4.40	-94.5	-91.5
2	12	16-QAM 3/4	9.75	6.60	-90.5	-87.5
2	13	64 QAM 2/3	13.00	8.70	-86.5	-83.5
2	14	64 QAM 3/4	14.63	9.50	-84.5	-81.5
2	15	64 QAM 5/6	16.25	10.20	-79.5	-76.5

Table 21 MCS vs. Sensitivity Chart (2.5MHz Bandwidth)*

NSS	MCS	Coding Rate	PHY Throughput (Mbps)	UDP User Throughput (Mbps)	SC4400/3500/3800 Sensitivity	SC4200/3822 SL4200 Sensitivity
1	0	BPSK 1/2	1.63	1.03	-102	-99
1	1	QPSK 1/2	3.25	2.06	-100	-97
1	2	QPSK 3/4	4.88	3.09	-97	-94
1	3	16-QAM 1/2	6.50	4.12	-95	-92
1	4	16-QAM 3/4	9.75	6.18	-92	-89
1	5	64 QAM 2/3	13.00	8.25	-87	-84
1	6	64 QAM 3/4	14.63	9.28	-85	-82
1	7	64 QAM 5/6	16.25	10.30	-80	-77
2	8	BPSK 1/2	3.25	2.06	-100	-97
2	9	QPSK 1/2	6.50	4.12	-97	-94
2	10	QPSK 3/4	9.75	6.18	-94	-91
2	11	16-QAM 1/2	13.00	8.25	-91	-89
2	12	16-QAM 3/4	19.50	12.38	-88	-85
2	13	64 QAM 2/3	26.00	16.21	-84	-81
2	14	64 QAM 3/4	29.25	17.62	-82	-79
2	15	64 QAM 5/6	32.50	18.94	-77	-74

Table 22 MCS vs. Sensitivity Chart (5MHz Bandwidth)*

NSS	MCS	Coding Rate	PHY Throughput (Mbps)	UDP User Throughput (Mbps)	SC4400/3500/3800 Sensitivity	SC4200/3822 SL4200 Sensitivity
1	0	BPSK 1/2	3.25	2.48	-99	-96
1	1	QPSK 1/2	6.50	4.96	-97	-94
1	2	QPSK 3/4	9.75	7.40	-94	-91
1	3	16-QAM 1/2	13.00	9.90	-92	-89
1	4	16-QAM 3/4	19.50	14.80	-89	-86
1	5	64 QAM 2/3	26.00	19.90	-84	-82
1	6	64 QAM 3/4	29.25	22.40	-82	-80
1	7	64 QAM 5/6	32.5	24.0	-77	-78
2	8	BPSK 1/2	6.50	4.96	-97	-94
2	9	QPSK 1/2	13.00	9.90	-94	-91
2	10	QPSK 3/4	19.50	14.80	-91	-88
2	11	16-QAM 1/2	26.00	19.90	-89	-86
2	12	16-QAM 3/4	39.00	29.90	-85	-82
2	13	64 QAM 2/3	52.00	39.70	-81	-79
2	14	64 QAM 3/4	58.50	43.50	-79	-77
2	15	64 QAM 5/6	65.00	48.10	-74	-75

Table 23 MCS vs. Sensitivity Chart (10MHz Bandwidth)*

NSS	MCS	Coding Rate	PHY Throughput (Mbps)	UDP User Throughput (Mbps)	SC4400/3500/3800 Sensitivity	SC4200/3822 SL4200 Sensitivity
1	0	BPSK 1/2	6.5	4.92	-96	-93
1	1	QPSK 1/2	13.00	9.82	-94	-91
1	2	QPSK 3/4	19.50	14.73	-91	-88
1	3	16-QAM 1/2	26.00	19.65	-89	-86
1	4	16-QAM 3/4	39.00	29.47	-86	-83
1	5	64 QAM 2/3	52.00	39.29	-82	-79
1	6	64 QAM 3/4	58.50	44.20	-80	-77
1	7	64 QAM 5/6	65.00	47.45	-78	-75
2	8	BPSK 1/2	13.00	9.82	-94	-91
2	9	QPSK 1/2	26.00	19.65	-91	-88
2	10	QPSK 3/4	39.00	29.47	-88	-85
2	11	16-QAM 1/2	52.00	39.29	-86	-83
2	12	16-QAM 3/4	78.00	57.04	-82	-79
2	13	64 QAM 2/3	104.00	75.00	-79	-76
2	14	64 QAM 3/4	117.00	85.00	-77	-74
2	15	64 QAM 5/6	130.00	94.00	-75	-72

Table 24 MCS vs. Sensitivity Chart (20MHz Bandwidth)*

Sensitivity numbers reflect "typical" values. Actual sensitivity will vary by band.

5.1.2 Networking

The Networking section will allow you to configure the various networking parameters involved with the mesh network. This includes various LAN settings, WIFI settings, Multicast parameters, as well as QoS (quality of service) settings.

5.1.2.1 LAN Settings

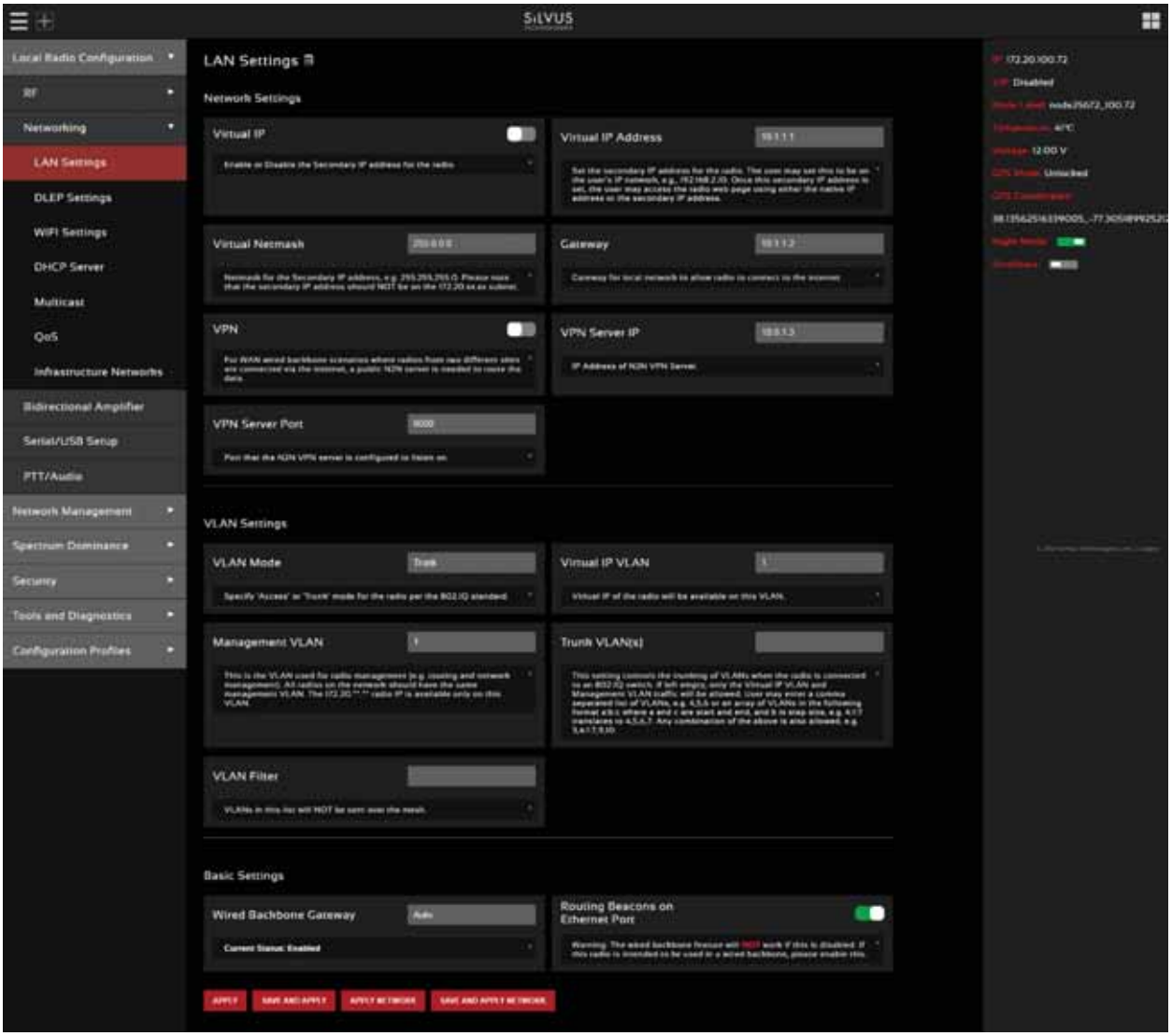


Figure 30 LAN Settings Page

LAN Settings:

- **Virtual IP**: Enable or Disable the Secondary IP address for the radio.
- **Virtual IP Address**: Set the secondary IP address for the radio. The user may set this to be on the user's IP network, e.g., 192.168.2.10. Once this secondary IP address is set, the user may access the radio web page using either the native IP address or the secondary IP address.
- **Virtual Netmask**: Netmask for the Secondary IP address, e.g. 255.255.255.0. Please note that the secondary IP address should NOT be on the 172.20.xx.xx subnet.
- **Gateway:** Gateway for local network to allow radio to connect to the internet
- **VPN:** For WAN wired backbone scenarios where radios from two different sites are connected via the internet, a public N2N server is needed to route the data. Here is an example of how to setup an N2N server on a server hosted by Amazon AWS running Ubuntu 12.04:

  Compile:

  git clone https://github.com/lukablurr/n2n_v2_fork ### downloads the code

  cd n2n_v2_fork

  export N2N_OPTION_AES=no

  make clean

  make

  Execute:

  ./supernode -l 9000 -v

  Server will be running on port 9000.

- **VPN Server IP**: IP Address of N2N VPN Server
- **VPN Server Port**: Port that the N2N VPN server is configured to listen on.
- **Block DHCP packets on Mesh**: This is a feature that will drop all DHCP packets from all interfaces on the radio (wireless, ethernet, wifi, usb-ethernet). This includes DHCP request, DHCP response, DHCP release packets. Enable to prevent potential IP conflicts caused by multiple DHCP servers.

VLAN Settings:

VLANs allow users to segregate the Ethernet layer by assigning one or more VLAN IDs to the ports of a VLAN switch. Ethernet packets are only allowed to travel between ports that belong to the same VLAN. To allow concatenating multiple VLAN switches and/or a single physical interface residing on multiple VLANs, a VLAN ID can be inserted to the Ethernet packet header to indicate which VLAN the

packet belongs to. This is called VLAN Tagging. A packet that contains a VLAN ID is called a tagged packet. A port on a VLAN switch typically operates in either access mode or trunk mode.

- **VLAN Mode:** Specify 'Access' or 'Trunk' mode for the radio per the 802.1Q standard.

- **Default (Native/PVID) VLAN:** This is the VLAN associated with untagged packets entering the radio. Tagged packets on this VLAN arriving at the radio will leave the radio untagged. The virtual IP of the radio is available on this VLAN. This is for Access mode only.

- **Virtual IP VLAN:** Virtual IP of the radio will be available on this VLAN. On this VLAN arriving at the radio will leave the radio untagged. The virtual IP of the radio is available on this VLAN.

- **Management VLAN:** This is the VLAN used for radio management (e.g. routing and network management). All radios on the network should have the same management VLAN. The 172.20.xx.yy IP of the radio is available only on this VLAN.

- **Trunk VLAN(s):** This setting enables the trunking of VLANs when the radio is connected to an 802.1Q switch. If left empty, only the native and management VLAN traffic will be allowed. User may enter a comma separated list of VLANS, e.g. 4,5,6 or an arry of VLANs in the format of a:b:c where a and c are start and end, and b is step size, e.g. 4:1:7 translates to 4,5,6,7. Any combination of the above is allowed.

- **VLAN Filter:** VLANs in this list will not be sent over the mesh. Prevent certain VLAN ids from going on the network (VLAN RF Filter).

Basic Settings:

- **Wired Backbone Gateway**: This setting pertains to wired backbone functionality (See Section 7: Wired Backbone). For normal operation, set Wired Backbone Gateway to 'Auto'. If multiple radios will be connected to a wired backbone, all radios on the backbone should be set to 'Auto'.

- **Routing Beacons on Ethernet Port**: For radios to be able to communicate and transfer data over a wired link, routing information needs to be sent over the wireline. These packets are broadcast packets that are sent even if there is only one radio on the network. If wired backbone is not being utilized, the user can disable these routing beacons to prevent loading their local network with these routing packets.

5.1.2.2 DLEP

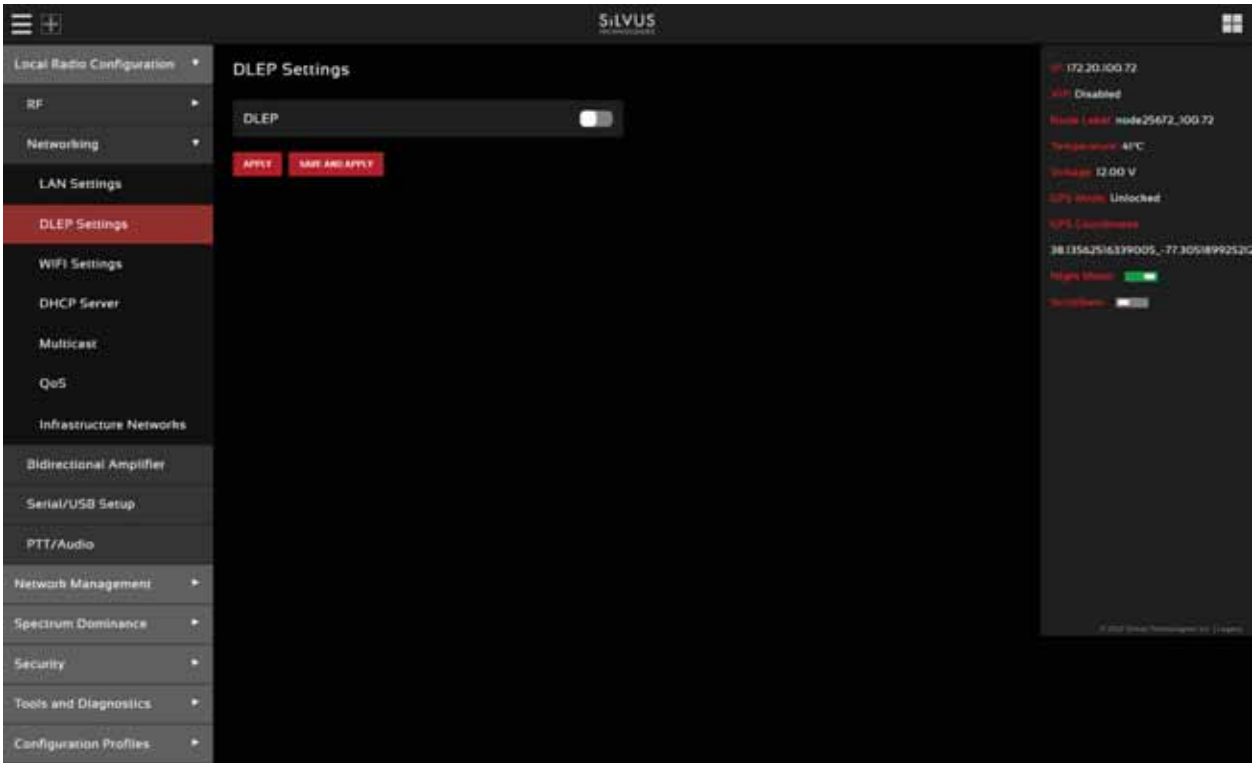


Figure 31 DLEP

DLEP Settings:

The Silvus radio supports Dynamic Link Exchange Protocol (DLEP). This is a feature where the Silvus radio would be able to pass feedback to a router to help optimize route selection. To enable DLEP you would need a DLEP capable router to connect to the radio ethernet connection. After that, come to this page and toggle the DLEP selection to the enable position will enable DLEP on the radio.

This feature has been tested with Cisco C5915 IOS Version 15.9(3)M1 by using OSPFv3 and EIGRP routing protocols.

Please see below link to DLEP document.

https://drive.google.com/file/d/1Aa34tGmx-GwKXj0VsAgkNrBEWFfkMJHL/view?usp=sharing

5.1.2.3 WIFI Settings

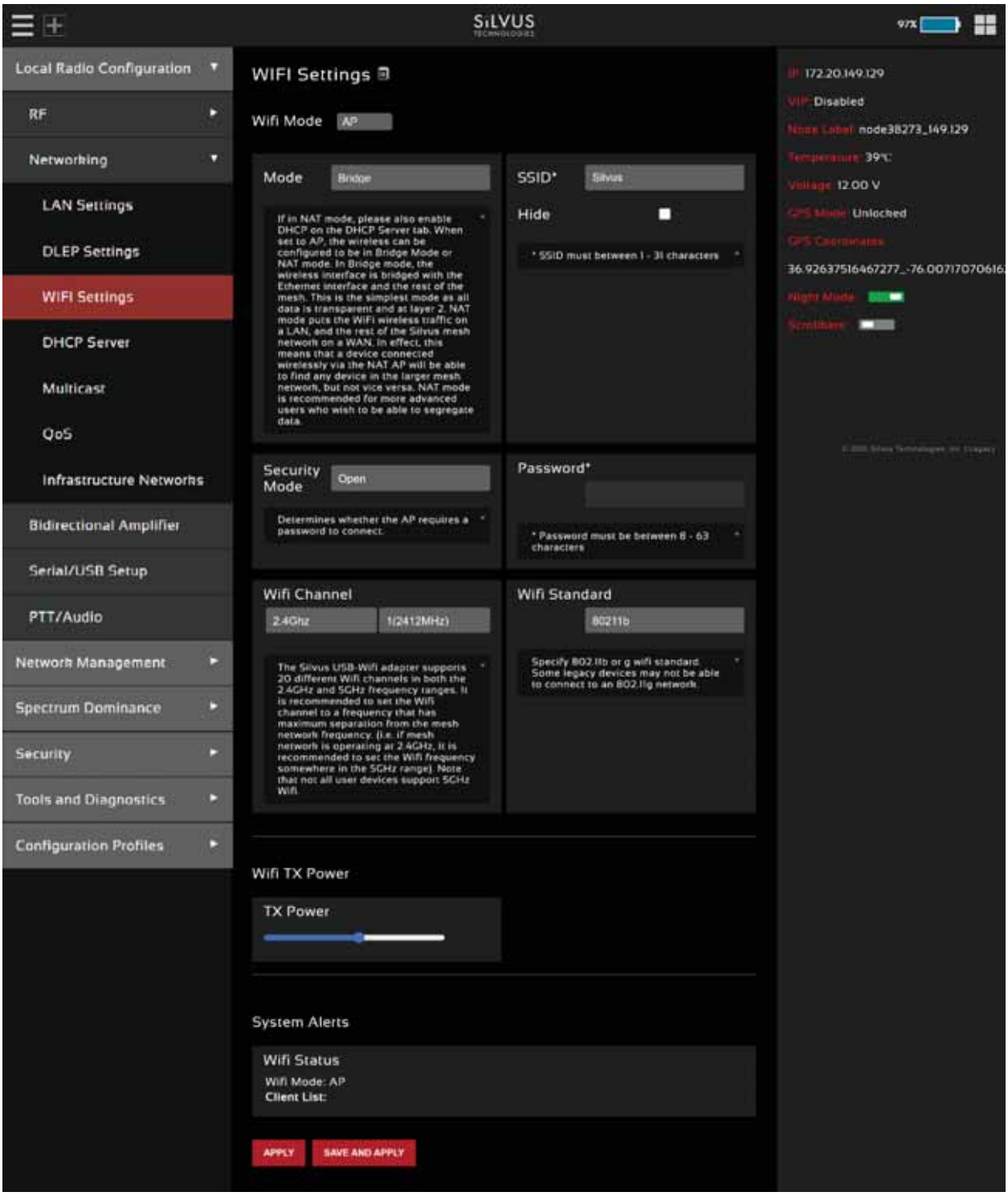


Figure 32 WIFI AP Configuration Page

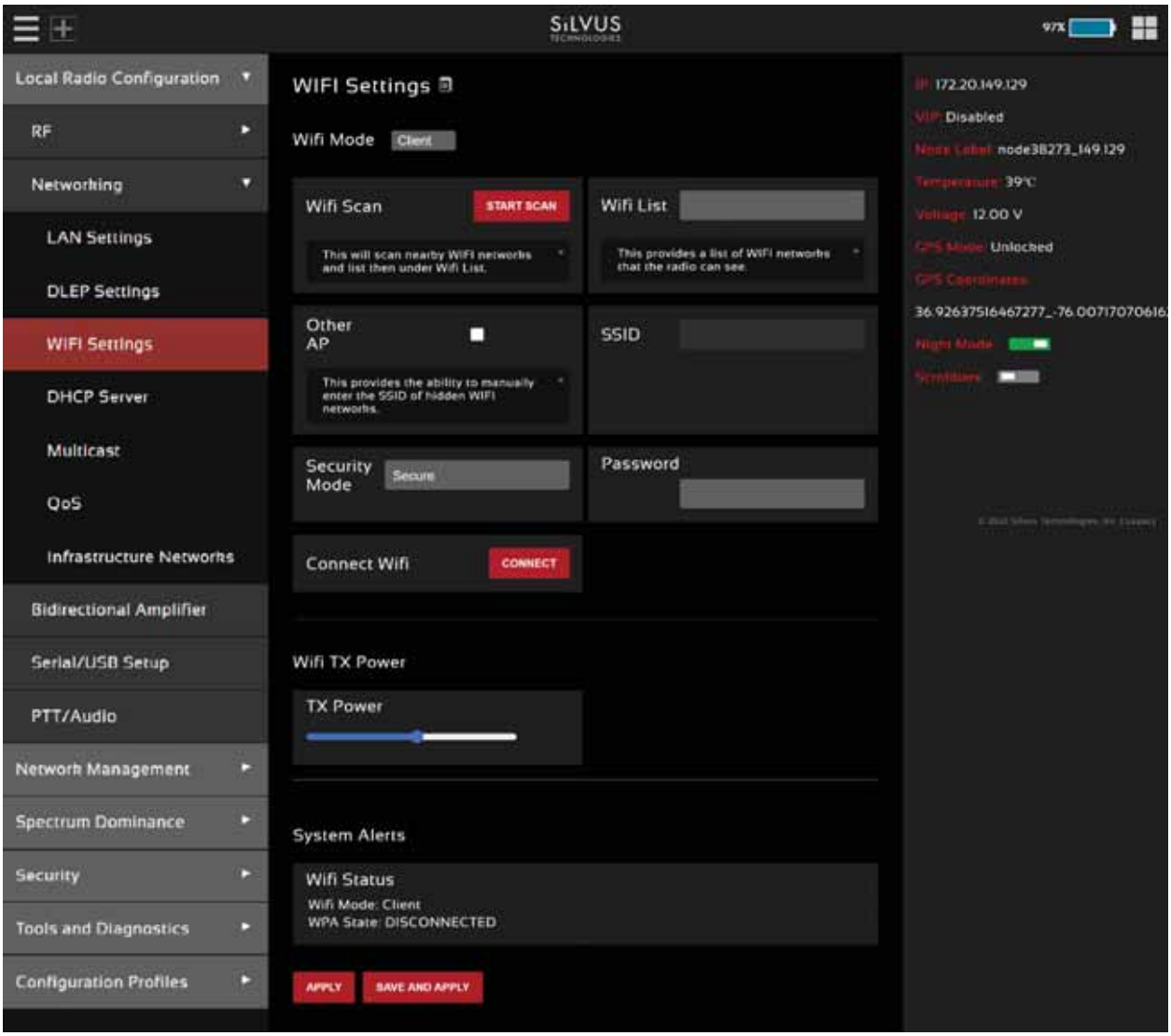


Figure 33 WIFI Client configuration page

WiFi Settings:

Note: Use of this feature requires a Silvus USB-WiFi adapter. The WiFi settings will only display if the WiFi dongle is attached to the radio's USB port before it is powered on. WiFi supports WPA2-PSK AES encryption on the wifi dongle part number SC-WIFI-DNGL2-RGD-ODU.

- **Wifi Mode**: Choose between AP, Client or Disabled. AP mode turns the WiFi dongle into a wireless AP. This mode is useful for connecting phones, tablets, laptops, etc. to the radio in order to pull up the web interface and access other devices in the mesh network. Client mode allows the radio to connect to another wireless AP. This mode is useful for connecting to wireless cameras and other devices which generate their own 'hotspot'. Once set to client mode, a list of detected wireless networks will be displayed with an option to connect.

- **Mode**: When set to AP, the wireless can be configured to be in Bridge Mode or NAT mode. In Bridge mode, the wireless interface is bridged with the Ethernet interface and the rest of the mesh. This is the simplest mode as all data is transparent and at layer 2. NAT mode puts the WiFi wireless traffic on a LAN, and the rest of the Silvus mesh network on a WAN. In effect, this means that a device connected wirelessly via the NAT AP will be able to find any device in the larger mesh network, but not vice versa. NAT mode is recommended for more advanced users who wish to be able to segregate data.

- **SSID**: Define the SSID for the wireless network. Must be between 1-31 characters. User also has the option to prevent the AP from broadcasting it's SSID by checking the 'Hide' box.

- **Security Mode**: Determines whether the AP requires a password to connect.

- **Password**: If 'Security Mode' is set to 'Secure', a password between 8 and 63 characters must be set.

- **Wifi Channel**: The Silvus USB-Wifi adapter supports 20 different Wifi channels in both the 2.4GHz and 5GHz frequency ranges. It is recommended to set the Wifi channel to a frequency that has maximum separation from the mesh network frequency. (i.e. if mesh network is operating at 2.4GHz, it is recommended to set the Wifi frequency somewhere in the 5GHz range). Note that not all user devices support 5GHz Wifi.

- **Wifi Standard**: Specify 802.11b or g wifi standard. Some legacy devices may not be able to connect to an 802.11g network.

- **Wifi TX Power**: This slider can be used to control the Wifi TX power from 0dBm (1mW) up to 17dBm (50mW).

- **Wifi Status**: Provides status information of the wifi adapter. A list of connected clients will also be shown here.

- **Wifi Scan**: will scan nearby WIFI networks and list then under Wifi List.

- **Wifi List**: provides a list of WIFI networks that the radio can see.

- **Other AP**: provides the ability to manually enter the SSID of hidden WIFI networks.

- **Apply**: Applies the new values but does not save them to flash.

- **Save and Apply**: Save the new values to flash and apply.

5.1.2.4 DHCP Server

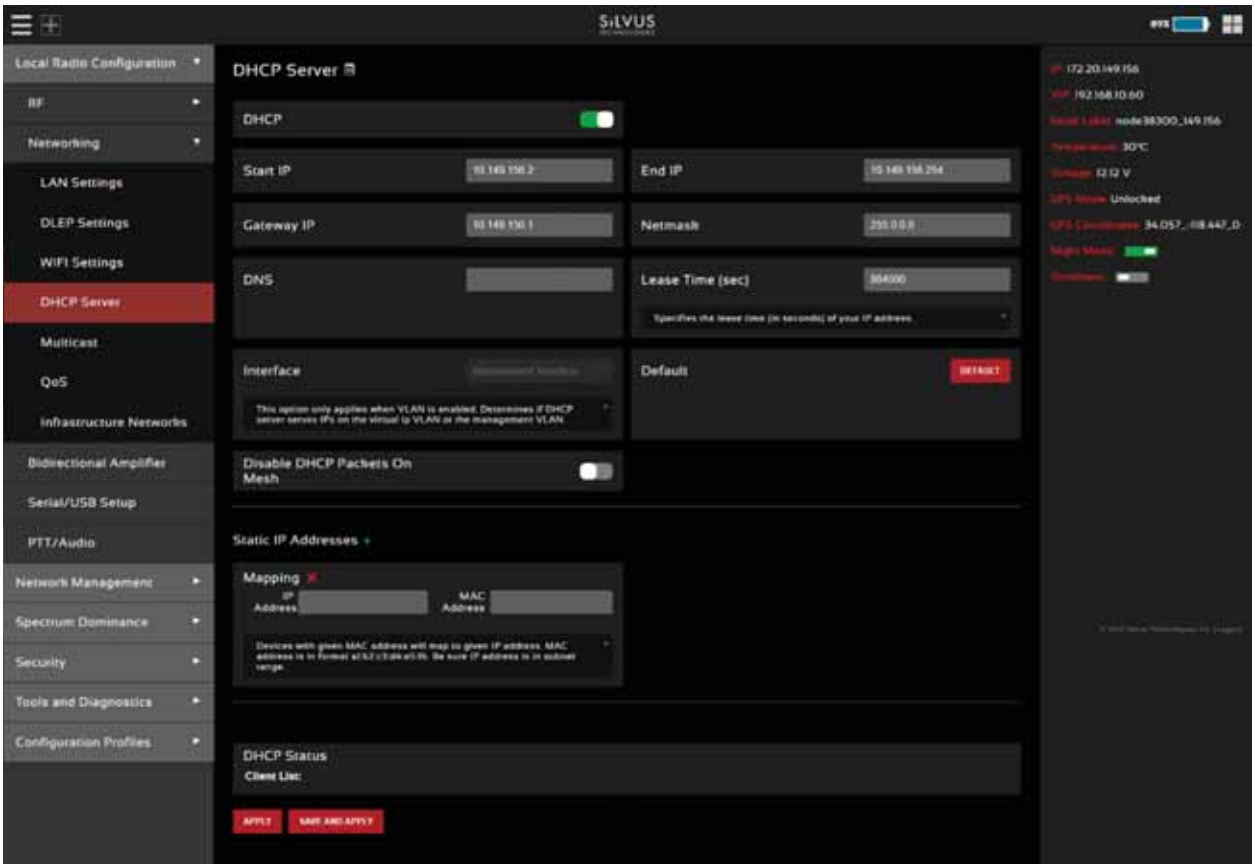


Figure 34 DHCP Server

DHCP Server Settings:

The Silvus radios have a built in DHCP server in them. Once you enable the DHCP server, the radio will automatically assign IP addresses to the devices that are connected to the mesh network. Below are the various parameters of the DHCP server.

- **DHCP**: When enabled, the DHCP server on the radio will assign IP addresses to devices connected to the Silvus network. Users should be careful to make sure that in the event there are multiple radios configured with DHCP to ensure that each DHCP server is serving a unique IP address range to prevent IP conflicts. When DHCP is enabled, the DHCP parameters must be set.

- **Start IP**: This will be the IP address that the DHCP starts to assign devices that are connected to the network

- **End IP**: This will be the last IP address that the DHCP will assign in sequential order from the start IP.

- **Netmask**: Netmask for the group of devices that the DHCP server will assign IP addresses for, e.g. 255.255.255.0.

- **Gateway:** Gateway for local network to allow radio or devices to connect to the internet
- **DNS:** The DNS is the domain name system and is an IP address that helps translate website URL addresses to IP addresses. You can specify the specific DNS you would like to use for your subnet of devices. A common one to use is Google's public DNS 8.8.8.8.
- **Lease Time:** Specifies the lease time (in seconds) of your IP address.
- **Interface:** This option only applies when VLAN is enabled. Determines if DHCP server serves Ips on the virtual ip VLAN or the management VLAN.
- **Default:** a button that will automatically configure some suggested parameters for the DHCP.
- **Disable DHCP Packets on Mesh:** This will disable all DHCP server packets on the network. This is a feature to prevent conflicting IP addresses that are being assigned to multiple devices by multiple DHCP servers.
- **Static IP addresses:** Devices with given MAC address will map to given IP address. MAC address is in format a1:b2:c3:d4:e5:f6. Be sure IP address is in subnet range.
- **DHCP Status client list:** This section will list all devices that the DHCP is assigning IP address to.

5.1.2.5 Multicast

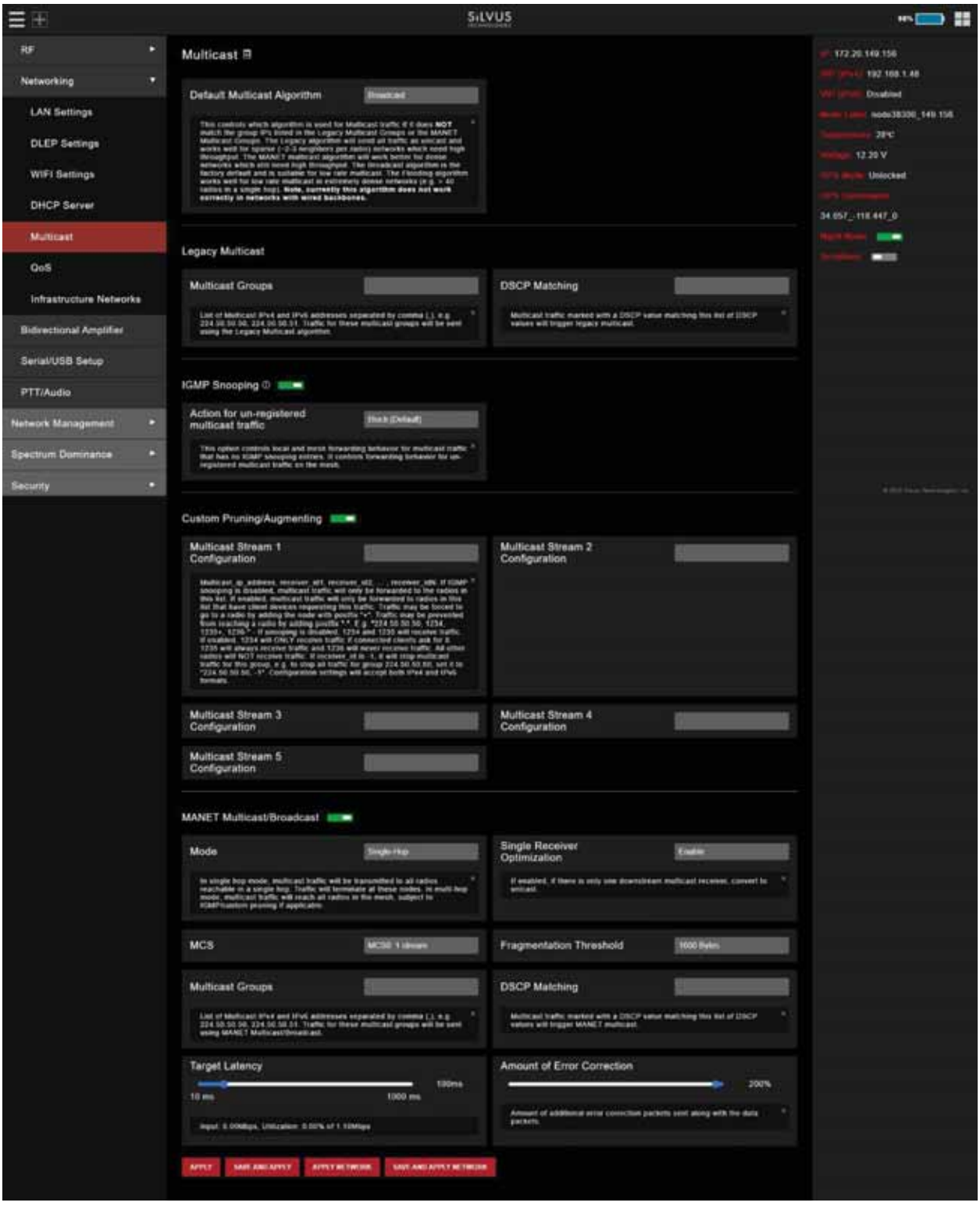


Figure 35 Multicast Configuration Page

- **Default Multicast Algorithm**: This controls which method of multicast transmission is used if it does NOT match the group IPs listed in the Legacy Multicast Groups or the MANET Multicast Groups. The Legacy algorithm will send all traffic as unicast and works well for sparse (~2-3 neighbors per radio) networks which need high throughput. Each link will send its own copy of the data payload to the receiving node, and optimize the transmission based on individual link conditions. The MANET multicast algorithm will work better for dense networks which still need high throughput. This multicast method will send the multicast data payload to each node at the same time and use the same MCS. For high receiving node counts, this could save significant airtime. The Broadcast algorithm is the factory default and is suitable for low-rate multicast. Each radio sends every multicast or broadcast packet 3 times if there are downstream radios. Broadcast uses routing tree to send packets. If node is not on the route the packet is thrown out. MCS used for this transmission will be the same as the routing beacon MCS. The Flooding algorithm works well for low-rate multicast in extremely dense networks (e.g., >40 radios in a single hop). All broadcast/multicast packets will be combined, compressed, and broadcasted out. Due to the way it is implemented, there is a possibility of out of order and duplicates. Note, currently this algorithm does not work correctly in networks with wired backbones.

- **Legacy Multicast** (Multicast groups): List of Multicast IPv4 and IPv6 addresses separated by comma (,), e.g., 224.50.50.50, 224.50.50.51. Traffic for these multicast groups will be sent using the Legacy Multicast algorithm.

- **Legacy Multicast** (DSCP Matching): Multicast traffic marked with a DSCP value matching this list of DSCP values will trigger legacy multicast.

- **IGMP Snooping**: Enable or Disable IGMP Snooping for Multicast traffic

- **Action for un-registered multicast traffic**: This option controls default behavior for local and mesh multicast traffic that has no IGMP snooping entries. If set to 'Block', all unregistered multicast traffic will be block. If set to 'Send to All', all unregistered multicast traffic will be sent to all radios.

- **Custom Pruning/Augmenting**: Enable or Disable the Multicast group. The format for the field is Multicast_ip_address, receiver_id1, … receiver_idn If IGMP snooping is disabled, multicast traffic will only be forwarded to the radios in this list. If enabled, multicast traffic will only be forwarded to radios in this list that have client devices requesting this traffic. Traffic may be forced to go to a radio by adding the node with postfix "+". Traffic may be prevented from reaching a radio by adding postfix "-". (e.g. 224.50.50.50 1234, 1235-, 1236+) If receiver_id is -1, it will stop multicast traffic for this group.

Multicast Pruning Examples:

Data for multicast group 224.50.50.51 will be received only by radios with node-ids 1131 and 1261:

224.50.50.51, 1131, 1261

Data for multicast group 224.50.50.51 will be discarded at the transmitter and not put on the air:

224.50.50.51, -1

- **MANET Multicast/Broadcast**: Enable or Disable the MANET Multicast/Broadcast feature.

- **MANET Multicast/Broadcast** (Mode): The broadcast mode can be either single-hop or multi-hop. In single-hop mode, multicast traffic will be transmitted to all radios reachable in a single hop. Traffic will terminate at these nodes. In multi-hop mode, multicast traffic will reach all radios in the mesh, subject to IGMP/custom pruning if applicable.

- **MANET Multicast/Broadcast** (single Receiver Optimization): If enabled and there is only one downstream multicast receiver this multicast stream will convert to unicast.

- **MANET Multicast/Broadcast** (MCS): MCS that will be designated to all receive nodes for this multicast method. Typically a lower MCS is selected to allow lower SNR links to also obtain this transmission. Auto in this parameter will support MCS0, MCS1, MCS2, and MCS3 only.

- **MANET Multicast/Broadcast** (fragmentation threshold): This parameter will be designated to all receive nodes for this multicast method

- **MANET Multicast/Broadcast** (Multicast Groups): List of multicast IPv4 addresses separated by comma (,), e.g. 224.50.50.50, 224.50.50.51. Traffic for these multicast groups will be sent using this Broadcast feature.

- **MANET Multicast/Broadcast** (DSCP Matching): Multicast traffic marked with a DSCP value matching this list of DSCP values will trigger MANET multicast.

- **MANET Multicast/Broadcast** (Target latency): will make the node wait for the time set in parameter and collect all data and construct forward error correction packets to send out. Higher latencies are better since the low density parity check code can generate more robust codes resulting in better error correction on the receiver.

- **MANET Multicast/Broadcast** (Amount of Error Correction): This is the amount of additional error correction packets sent along with the data packets. A 100% amount of error correction equates to sending the data packets twice.

IPv6

The radios can support IPv6 for the following items:

- unique local ipv6 address
- QoS
- IGMP snooping
- custom Pruning/Augmenting
- MANET multicasting

5.1.2.6 Quality of Service (QoS)

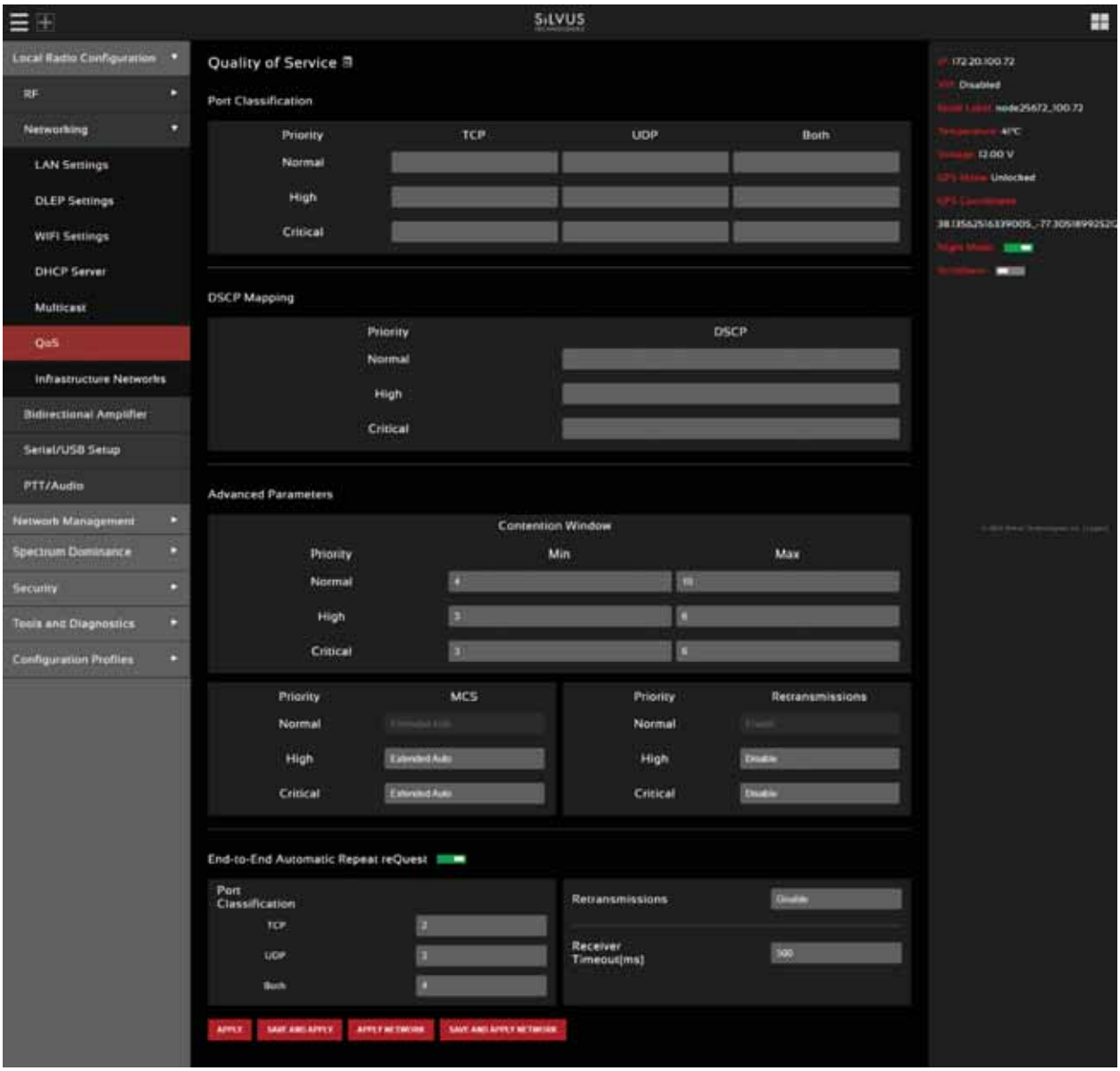


Figure 36 Quality of Service (QoS) Configuration Page

Quality of Service Port Classification:

The Quality of Service configuration page allows the user to make a distinction between three priority levels for managing traffic. These levels are normal, high, and critical.

Critical priority traffic will always jump to the front of the queue and bypass any awaiting high and normal priority traffic. High priority traffic will pass through the network when bandwidth can support critical and high priority, but not normal priority.

To specify priority traffic, the user needs to simply input the port number that the traffic will be arriving on. Multiple ports of the same priority can be separated by a comma (i.e. 5001, 6001, 6002). Alternatively, the user can specify a range of ports using a dash (i.e. 5001-5006). Any combination of commas and dashes will work as well (i.e. 5001, 6001-6007, 8000). Any field can be cleared by removing the text and clicking 'Apply' or 'Save and Apply'. If unspecified, traffic is treated as Low Priority.

Another method of assigning priority levels is to use DSCP mapping. By designating DSCP header bits to data packets, you can distinguish priority levels of that data payload.

Quality of Service Contention Window Control:

The Quality of Service Contention Window Control tunes the aggressiveness of CSMA backoffs when collisions occur. The MAC takes random backoffs in the range [0, 2^cw_min]. Every time there is a collision/noise it will increase this cw_min by 1, until it is capped by cw_max.

E.g. 4,10 translates to random backoffs in the range [0,16] in the beginning for a packet. If the first try results in a collision, it will pick another backoff in the range [0,32], then [0,64], until [0,1024]. After successful transmission, backoff is reset to [0,16]. The default is 4,10 for low priority, and 3,6 for high priority. For larger networks, it is recommended to increase the Low Priority minimum to reduce the chance of collisions occurring.

MCS and Retransmissions can also be customized to specific priority levels.

5.1.2.7 Infrastructure Networks

This section controls two features in the Silvus radios. The Scan on Start feature and the failover mode. The Scan on Start feature will enable Edge configured radios to check for Infrastructure configured radios that are set with same center frequencies and bandwidths upon bootup. Based on the best SNR that can be obtained from infrastructure radios at boot up, the Edge radio will boot up connecting to that Infrastructure network with the best signal.

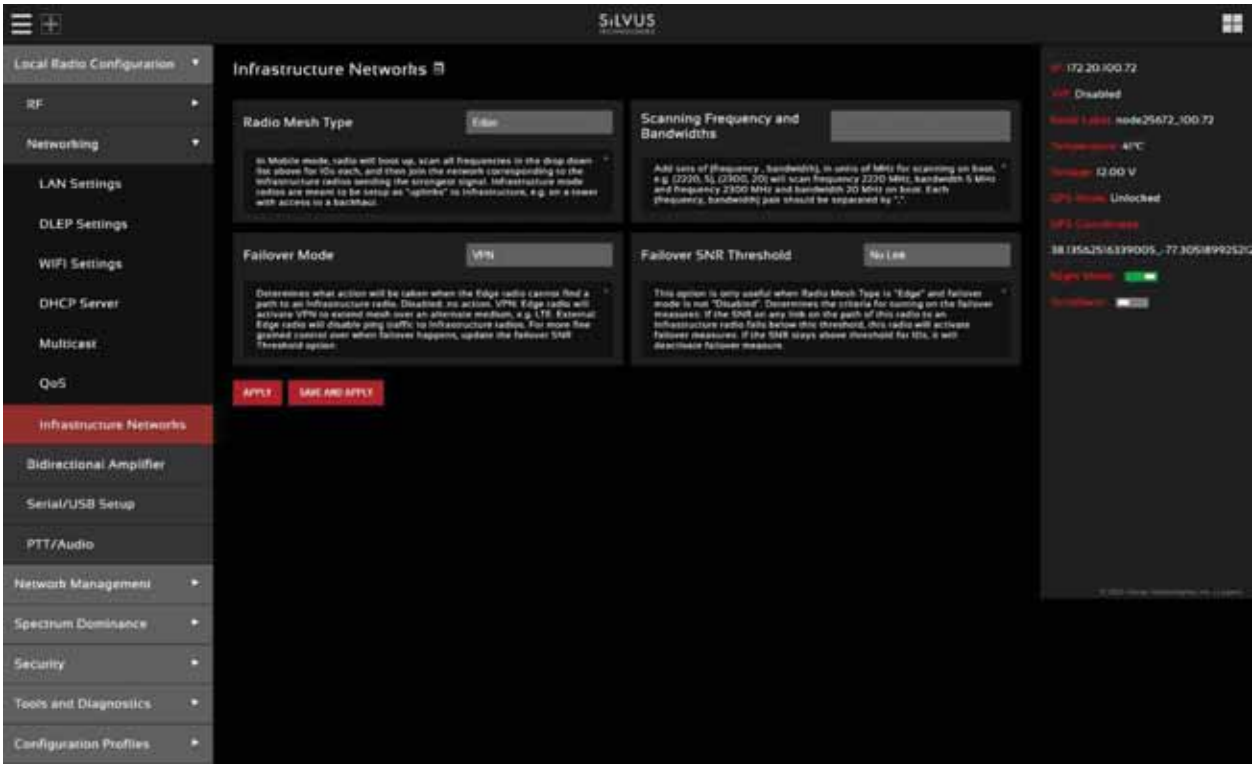


Figure 37 Infrastructure Networks

- **Radio Mesh Type**: Mesh is the normal operating mode. The other options are related to large-scale city-wide network type deployments where you have several fixed sites that have backhaul to each other. In Edge mode, radio will boot up, scan all frequencies listed in the "scanning frequency and bandwidths" parameter on this page for 10s each, and then join the network corresponding to the infrastructure radios sending the strongest signal. Infrastructure mode radios are meant to be setup as "uplinks" to infrastructure, e.g. on a tower with access to a backhaul.

- **Scanning Frequency and Bandwidths**: This field will populate after radio mesh type is set to Edge. Edge radios on the ground will connect to the tower radio that has the strongest signal. When the Edge radio is booting up, it either scan the frequencies from the supported frequencies (default) or from the Scanning Frequency and Bandwidths field (if specified). Input each frequency and bandwidth to scan in the (frequency, bandwidth) format. The radio will scan each frequency for 5.5 seconds, then it will pick the frequency with the best SNR, and switch to that frequency. You'll see the edge radio join the network of the infrastructure mode.

- **Failover mode**: Determines what action will be taken when the Edge radio cannot find a path to an Infrastructure radio. Disabled: no action. VPN: Edge radio will activate VPN to extend mesh over an alternate medium, e.g. LTE. External: Edge radio will disable ping traffic to Infrastructure radios. For more fine grained control over when failover happens, update the failover SNR Threshold option.

- **Failover SNR Threshold**: This option is only useful when Radio Mesh Type is "Edge" and failover mode is not "Disabled". Determines the criteria for turning on the failover measures: If the SNR on any link on the path of this radio to an Infrastructure radio falls below this threshold, this radio will activate failover measures. If the SNR stays above threshold for 10s, it will deactivate failover measure.

5.1.3 Bidirectional Amplifier (not available on SL4200)

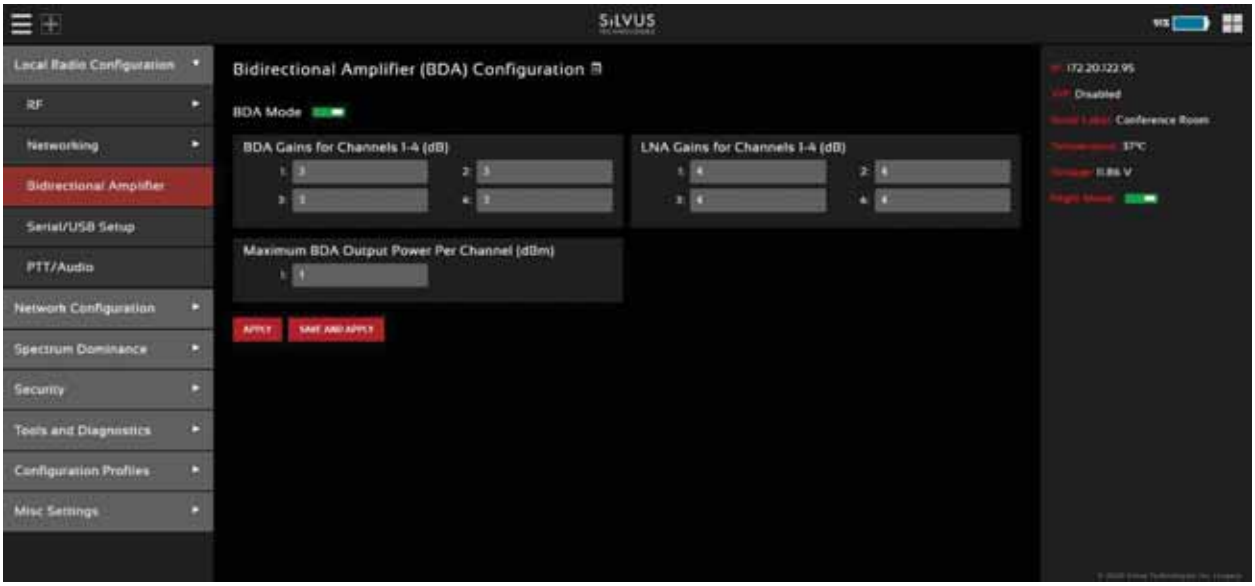


Figure 38 Bidirectional Amplifier (BDA) Configuration Page

The BDA Support page is used to configure the radio to work with an external bi-directional amplifier. These settings should be configured before connecting the amplifier to the radio.

- **BDA Mode**: You can enable or disable the BDA mode here.

Basic Settings:

- **BDA Gains for Channels 1-4**: Enter the gain (dB) for the power amplifier connected to each channel of the radio. This is sometimes labeled as Tx gains.

- **LNA Gains for Channels 1-4**: Enter the gain (dB) for the LNA connected to each channel of the radio. This is sometimes labeled as Rx gains.

- **Maximum BDA Output Power Per Channel (dBm)**: Enter the maximum output power for each PA. If the dBm is not listed, you should be able to calculate this from the Watt rating of the amp.

- **Apply**: Apply the new values but does not save them to flash.

- **Save and Apply**: Save the new values to flash and apply.

5.1.4 Serial/USB Setup

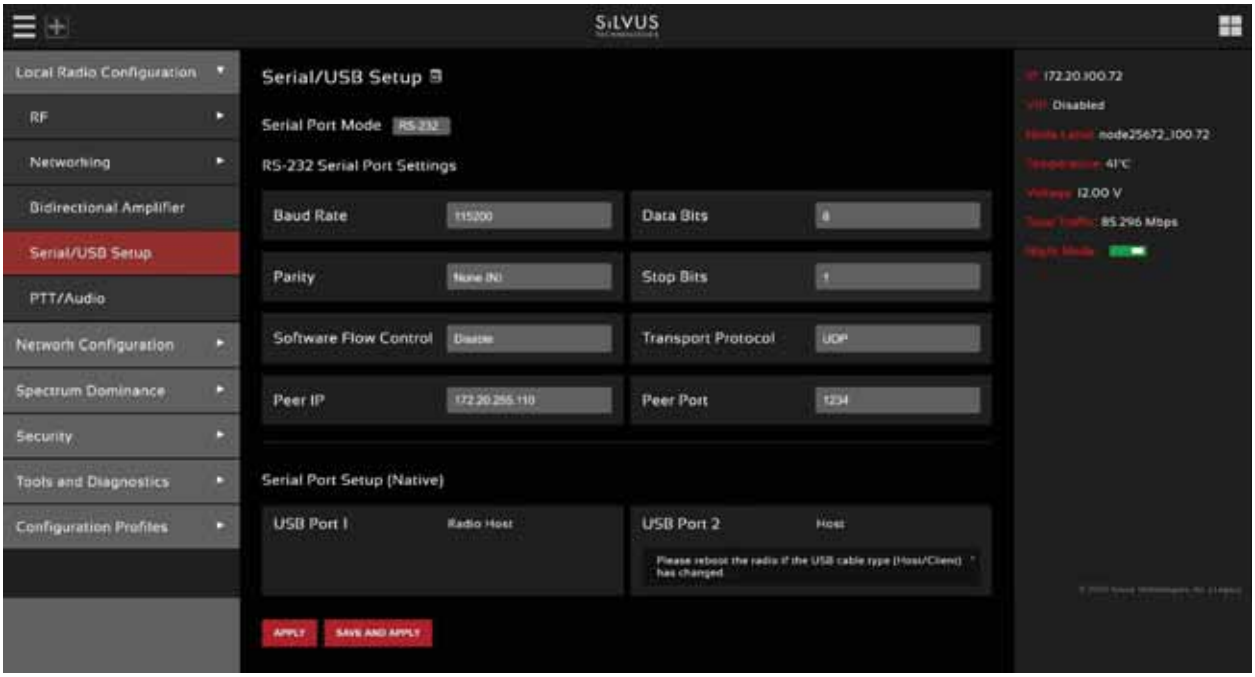


Figure 39 Serial/USB Setup Page

Serial Port Setup:

Each StreamCaster is equipped with one user configurable serial port. A special power cable and null modem cable are required for access to the radio's serial port. A brief description of each parameter is given below.

- **Serial Port Mode**: The user can select one of four available modes for the serial port: *GPS, RS232, Debug,* and *Disabled*.

    - ***GPS***: In GPS mode, an external serial GPS module can be connected to and powered from the serial port of the radio. A gpsd service daemon running on the node will make the GPS information available to any user on the network from TCP/IP port 2947. For more information on gpsd please see: http://catb.org/gpsd/

      In addition, GPS information can be pushed to the radio via the Ethernet or pulled by the radio from a remote device. If using a remote device to obtain GPS, set the GPS mode to

remote, the GPS Server IP to the IP address of the remote device, and the Port. The radio will try to connect via TCP to server on local subnet. It will expect data in GPSd format. If GPS information is pushed to the radio via Ethernet, the radio will listen on specified port and expect GPS data as NMEA Formatted UDP packets.

- ***RS-232***: The RS-232 mode provides a wireless serial connection between any two serial devices connected to StreamCaster radios on the network. In this mode, the user must configure the RS-232 protocol parameters shown in **Figure 39 Serial/USB Setup Page** above. The transport protocol for the serial data can be set as either TCP or UDP. For data that is sensitive to latency such as command and control data, UDP is recommended. For data that cannot tolerate any data loss, such as telemetry data, TCP is recommended.
  - The Peer IP should be the IP address of the radio on the other end of the RS-232 communication.
  - The Peer IP can be the native or virtual IP address but must be consistent at both ends.
  - Baud rate must match the baud rate of data being sent from the device.
  - Note – An additional 'null modem' cable may be needed at either end, depending upon whether connected device is acting as a terminal or as a control (DTE or DCE)
- ***Debug***: The debug mode is used to gain terminal access to the StreamCaster radio and is available for debug or interface purposes (API commands). The user's terminal client should be set to a baud rate of 115200 for console access to the radio.
- ***Disabled****:* This mode completely disables the serial terminal of the radio.
- ***Serial Server:*** This will have the same parameter inputs as the RS-232, but will not have a peer IP or transport protocol. This is because you are not trying to connect to just one peer IP. The transport protocol is automatically configured for TCP. On the client side of this connection, ethernet will be used and so the serial port is not configured. It is recommended to configure the serial port as GPS or disabled.

- **Apply**: Apply the new values but does not save them to flash.
- **Save and Apply**: Save the new values to flash and apply.

USB Status (3822/4200/4400):

The USB port on the 3822/4200/4400 can auto-detect whether the connected device is a USB host or client device. The USB cable should not be unplugged while the radio is running.

5.1.5 PTT (push-to-talk) (not available on SL4200)

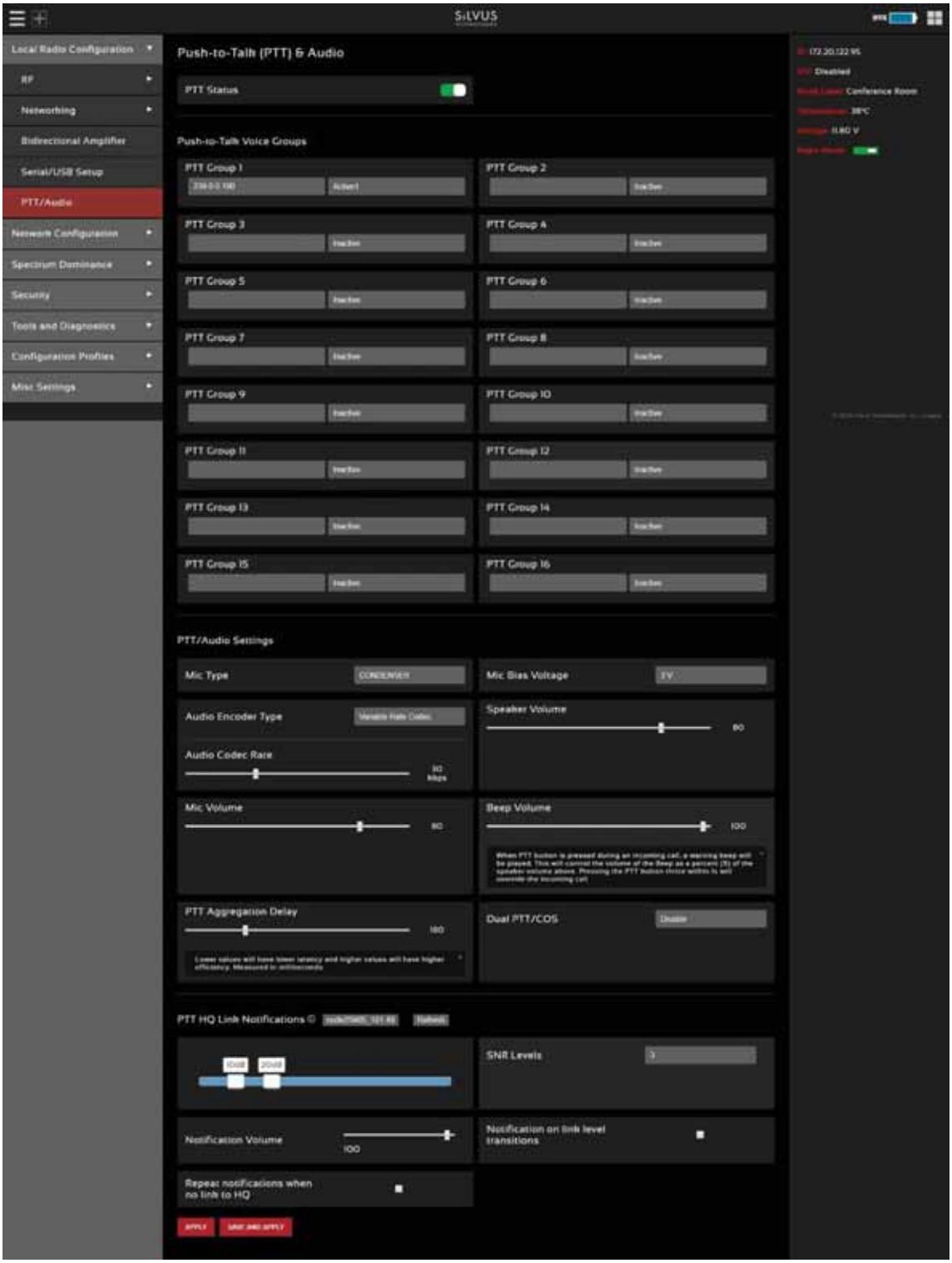


Figure 40 Push-to-Talk (PTT) & Audio Page

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. PTT will always send its multicast traffic using MANET Multicast method. PTT traffic will use port 1234.

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 Aggregation Delay – Lower values will have lower latency and higher values will have higher efficiency. Measured in milliseconds.

Dual PTT/COS – This allows Dual PTT functionality for some mic handsets to talk on two talk groups at the same time. COS is to allow ROIP functionality.

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.

5.2 StreamScape Network Configuration

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 41 Silvus StreamScape Network Topology Page**, allows users to quickly and effortlessly view the network topology and observe 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

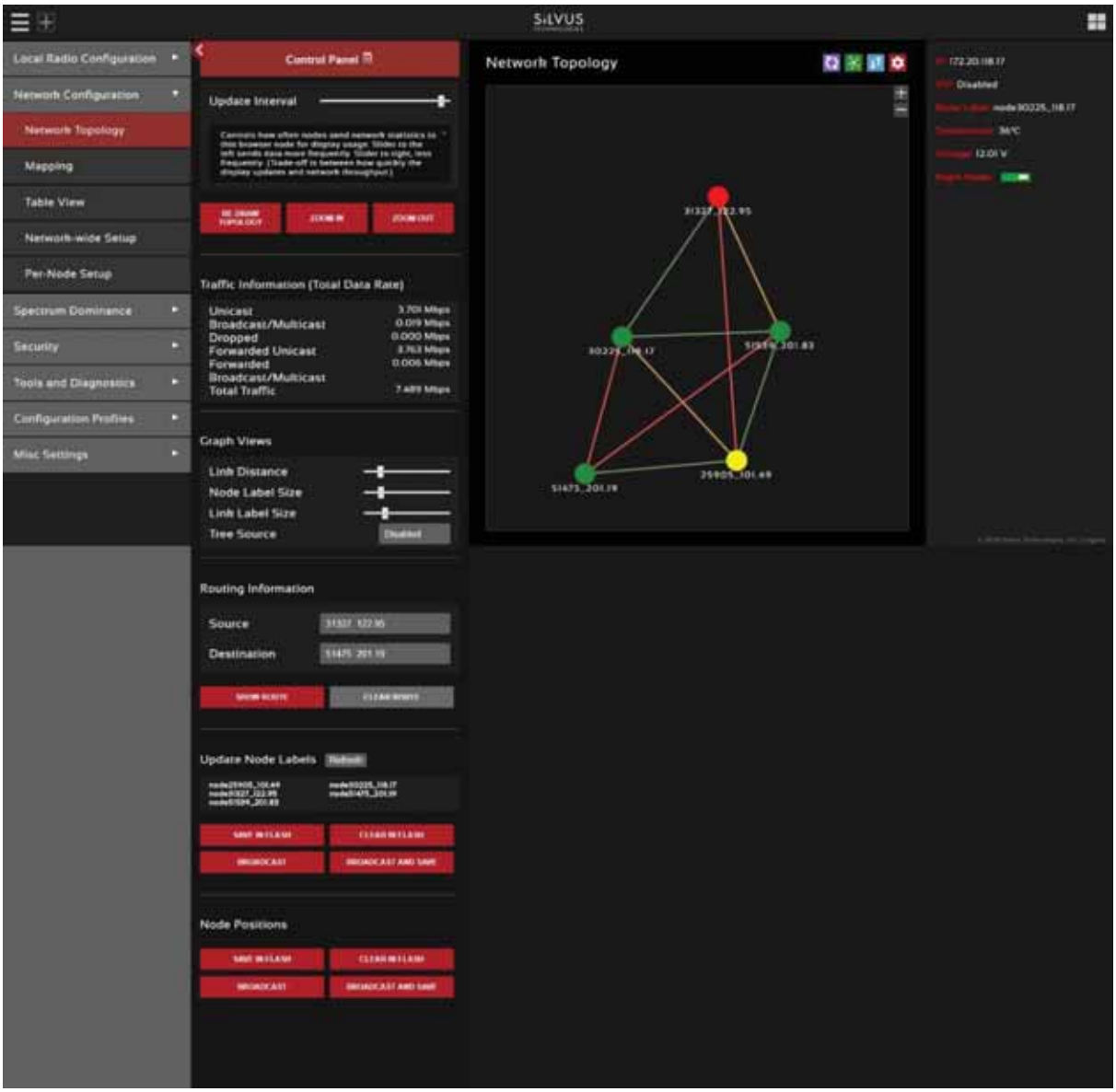


Figure 41 Silvus StreamScape Network Topology Page

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 42 Example Network Topology**.

- **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 '31327_122.95' and '25905_101.49' in **Figure 42 Example Network Topology**). This will allow the user to recognize the issue and configure the network accordingly. Table below also shows the values for each scenario.

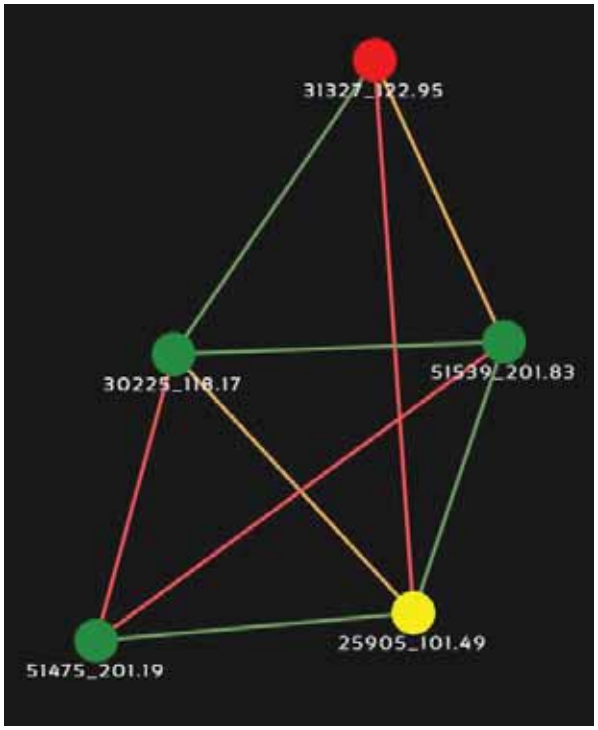


Figure 42 Example Network Topology

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

Table 25 Color Coding for Links and Nodes

- **Individual Node Characteristics –** By double clicking on any node in the network, users can view key operating characteristics of the node. **Figure 43 Individual Node Characteristics** shows an example of this for 'node25905'. 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> <Variable GI Mode><Pkts in TX Queue> <Num. of Spatial Streams><UDP User Throughput (Mbps)>

      <Air Time %><Data Rate (Mbps)><Loss Rate %><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.

- **Routing Beacon MCS:** This is the MCS setting that the routing beacons will use.
- **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.

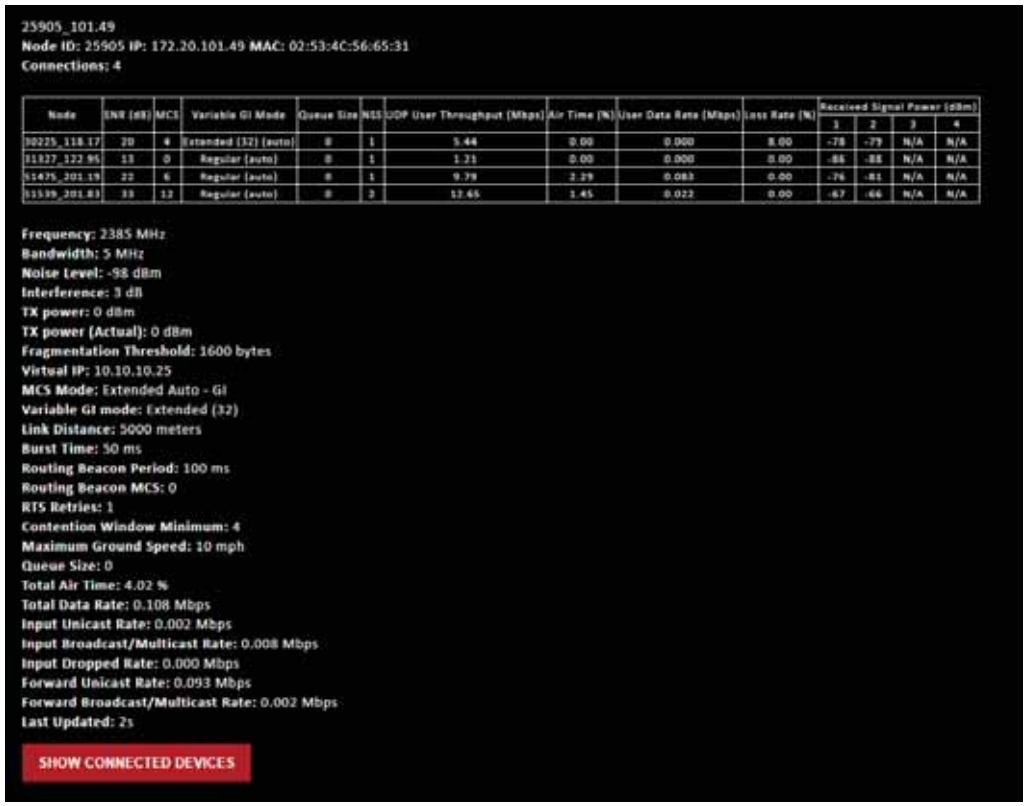


Figure 43 Individual Node Characteristics

- **Link Characteristics –** By double clicking the mouse on any link in the network, users can view key operating characteristics of that link. **Figure 44 Link Characteristics** shows an example of this for the link between 'node30225' and 'node51539'. The characteristics shown are:
    - **SNR**: The SNR of the link in each direction.
    - **MCS**: The MCS used to transfer data in each direction.
    - **Variable GI Mode:** The variable GI mode used for the transmitting node.
    - **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.

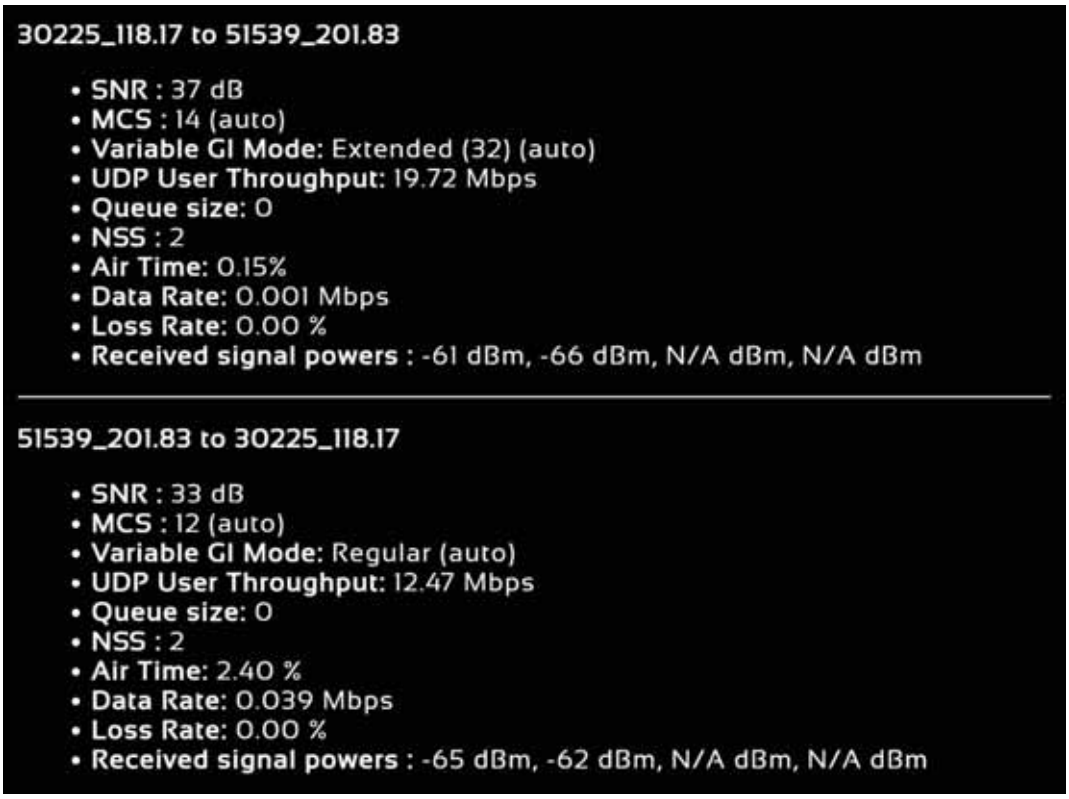


Figure 44 Link Characteristics

5.2.1.1 Control Panel

To open the control panel left-click on the red settings icon ( ) at the top right of the graphic, and the control panel will populate on the left-hand side.

- **Update Interval –** Controls how often nodes send network statistics to this browser node for display usage. Move the slider to the left sends data more frequently. Move the slider to right, less frequently. (Trade-off is between how quickly the display updates and network throughput required to send the updates.)
- **Traffic Information –** The traffic information is shown in table form in the control panel as well. It contains all the current network traffic information of the entire network.

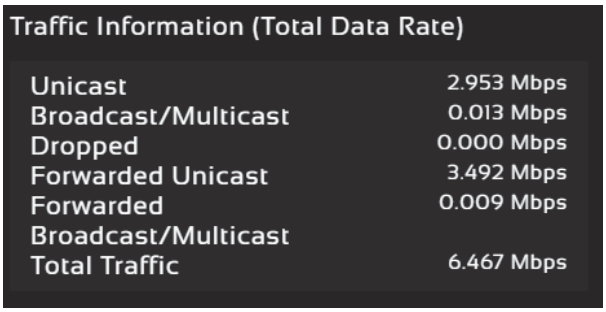


Figure 45 Traffic Information

- **Graph Views –** The graph views section allows you to edit the graph to the preference of the network administrator. You can extend the distance between nodes by dragging the link distance bar to the right. Sliding the node label size or link label size to the right will use a larger font for the labels of the node or link respectively. Tree source is suggested for dense networks when the structure of the network is not immediately apparent from the regular view (tree source disabled). By selecting a specific node to be the tree source, the network topology will show you how each radio is routed to that node. Tree source views will only display the link colors and not the SNR.

Figure 46 Graph Views

- **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. The path will turn bold

as shown in **Figure 47 Routing Path** for the path from 'node31327' to 'node51475'. In the control panel section it will also list the routing path used between these two nodes, and the routing path available link capacity in UDP.

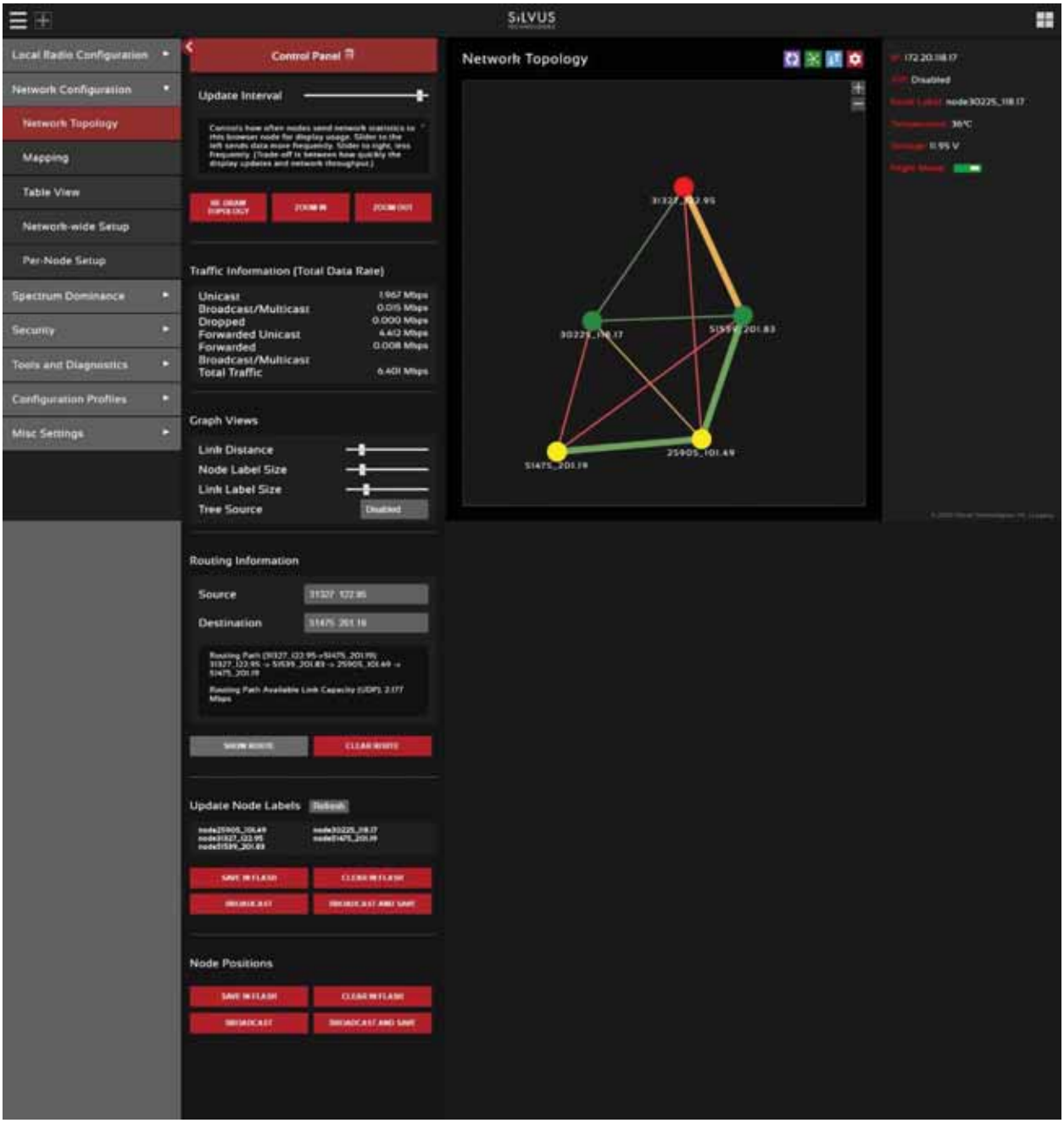


Figure 47 Routing Path

- **Update Node Labels –** Naming each node in the network is as simple as double-clicking on the node name and typing in a new name in the update node label section of the control panel as shown in **Figure 48 Custom Node Naming**. Once this is done, the user will 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 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.

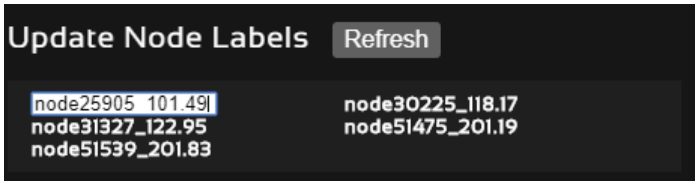


Figure 48 Custom Node Naming

- **Node Position –** You can customize the node positions in the network topology page by click and dragging the node dot. If you would like to save the custom node positions, you can save these positions to the flash memory on the radio. You can also broadcast and save these node positioning to all other radios on the network.

5.2.1.2 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 arrow icon ( ) on the top right of the graphic. If you hover over the icon the title "Send traffic between nodes" will appear. This will pull out the menu where users can specify UDP/TCP data, source/destination, port, time to send, and datagram size as seen below in **Figure 49 iPerf Function within GUI**.

- **Source:** Radio that sends data (Client)
- **Destination:** Radio that is listening (Server)
- **Destination port:** Port number for the data transfer
- **Time to Send (TTS):** Amount of time user wants to send data
- **Bandwidth (BW) 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

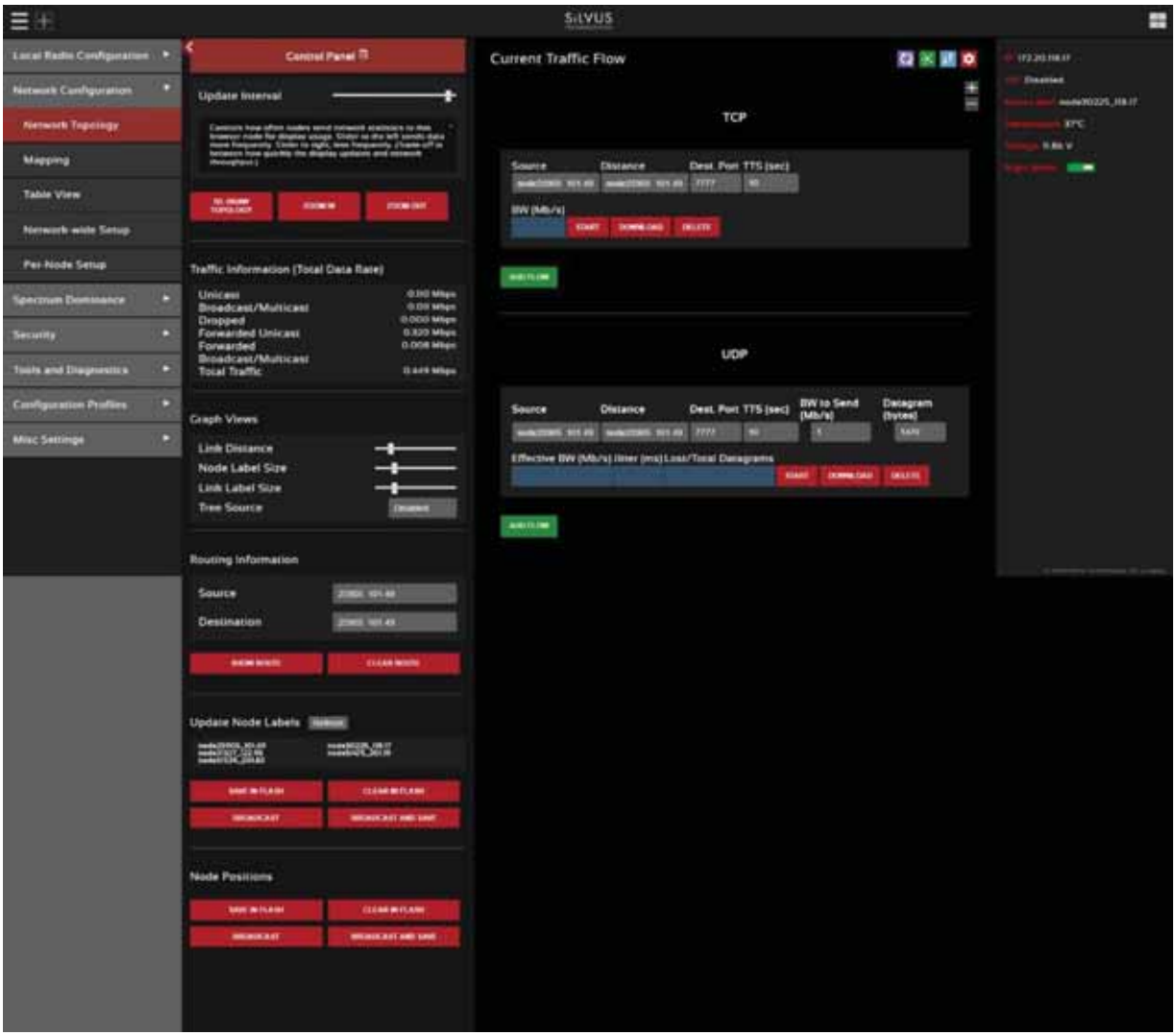


Figure 49 iPerf Function within GUI

You can add multiple iPerf sessions to run at the same time by click on the green “ADD FLOW” button. You can start and stop each session individually and download the results of the iPerf test by clicking on the download button after the iPerf test is complete.

5.2.2 Mapping

The Mapping page provides an easy-to-use method of tracking the location of nodes in real time. Nodes with GPS modules attached will be tracked on the map as shown in **Figure 50 Mapping Page**.

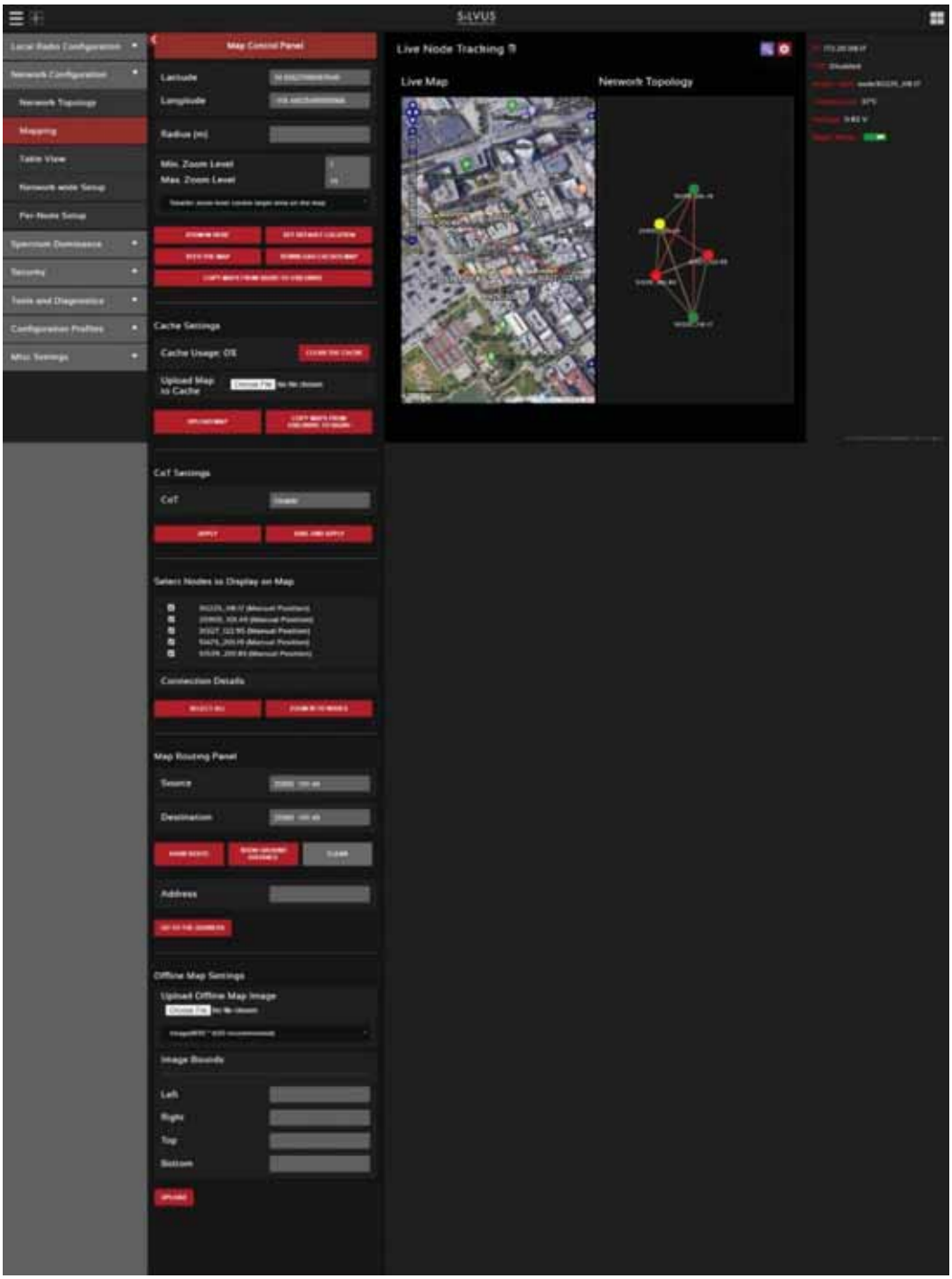


Figure 50 Mapping Page

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.

5.2.2.1 Map Options

There are 3 map options currently available in the Map Overlay view. The default map is OpenStreet Maps. 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 Downloading Maps. OpenStreet Maps Silvus is a version of OpenStreet maps which is hosted on Silvus' servers in case of an interruption in service with OpenStreet Maps. The Silvus maps is currently only guaranteed to cover the United States. However it should have some international maps as well.

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 51 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.

5.2.2.2 Map Control Panel

To open the Map Control Panel, please select the red settings icon ( ) on the top right of the page. This will populate the map control panel on the left side of the map overlay.

Lat/Long coordinates:

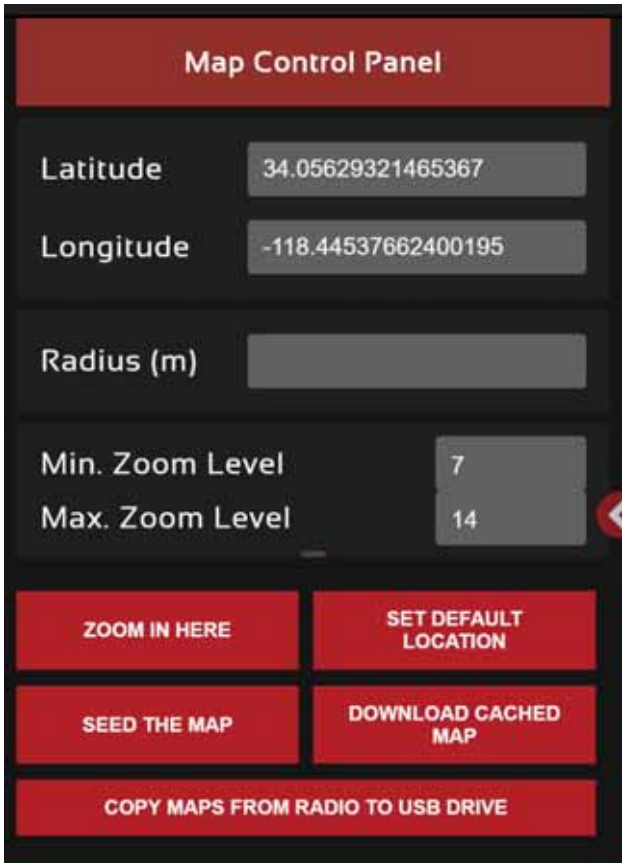


Figure 52 Map Control Panel (Lat/Long coordinates)

The first section of the Map Control Panel will allow you to input a lat/long coordinate. After entering the lat/long coordinates you can have the map overlay zoom to these coordinates.

The 'Zoom in Here' function does not consider the radius parameter. It will simply zoom to that location. The 'Radius' is used when you want to cache (Seed) the map. The radio will download the map area based on the coordinates and radius as well as the zoom levels specified.

The zoom level corresponds to the different zoom levels available on the map (from 0-14). This is used to determine what zoom levels of the map you want to 'Seed' Zoom in Here.

Set Default Location – This is referring to setting the default location of a radio when that radio doesn't have GPS lock. You can do this by right clicking on the map in the location that you want to place the radio, and that will pop-up a menu where you can choose which radio to set there. That radio will default to that location when no GPS data is present. If the radio gets a GPS lock, it will use the real GPS data instead.

Seed the Map – This is when you download or cache the map. This function allows you to store map imagery into the radio for offline use. You can only cache the 'OpenStreet Maps' option. To download map imagery, you should set the lat/long of the center point, input a desired radius, specify desired zoom

levels, then click 'Seed the Map'. This will then download the map imagery within those parameters. Note that the radio needs to have access to the internet for this function to work.

Download Cached Map – allows you to download all map imagery stored in the radio into a file that can then be uploaded to another radio.

Copy Maps from Radio to USB Drive – This will copy all of the stored maps in the radio to a file on a USB drive which can then be plugged into another radio and uploaded. This is so you don't need to repeat the caching steps each time.

Cache Settings:

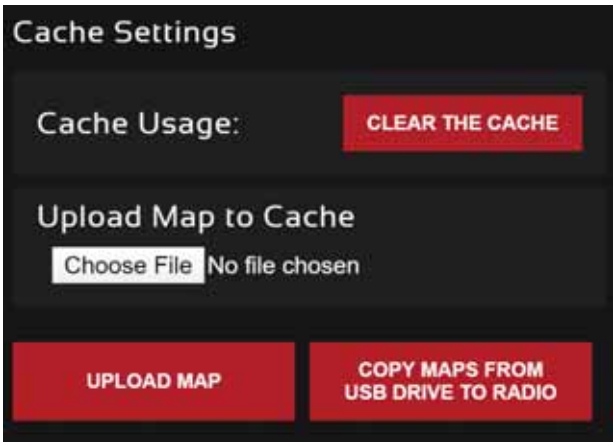


Figure 53 Map Control Panel (Cache Settings)

This section of the Map Control Panel allows you to clear any cached map data, and upload maps saved previously.

Cursor on Target:

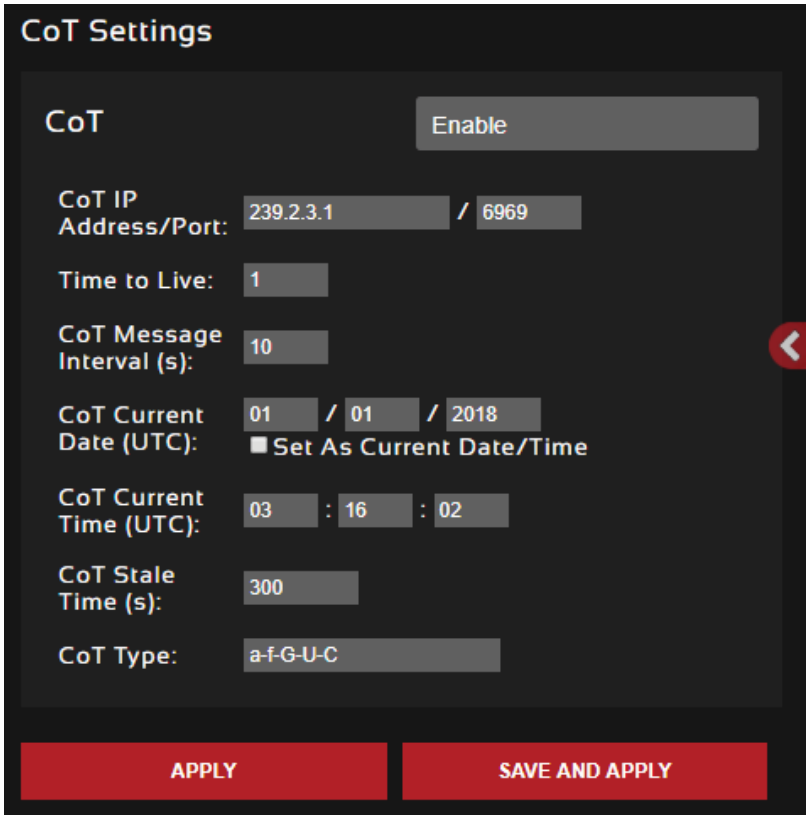


Figure 54 Cursor on Target Settings

Cursor on Target is an exchange standard that is used to share information about targets. This is a messaging format often used in blue force tracking applications such as ATAK. CoT is a multicast type of traffic that will follow the multicast method configured on the default setting under Multicast tab.

- **CoT:** Enable/disable cursor on target
- **CoT IP Address/Port:** IP address/port for the communication to establish
- **Time to Live:** Each time the data packets pass through a router, it will decrement this number. Once it reaches 0, the data packets will no longer continue.
- **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

Select Nodes to Display on Map:

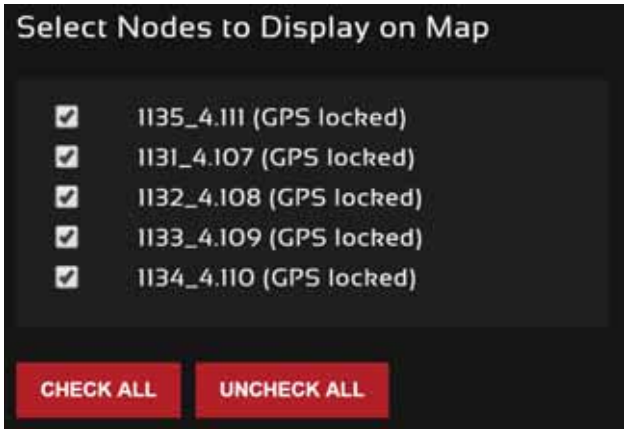


Figure 55 Map Control Panel (Nodes to Display on Map)

In the next section of the map control panel, you select or deselect nodes to be displayed on the map. This could be beneficial if you were trying to track locations of specific radios and wanted to zoom into their location.

Map Routing Panel:

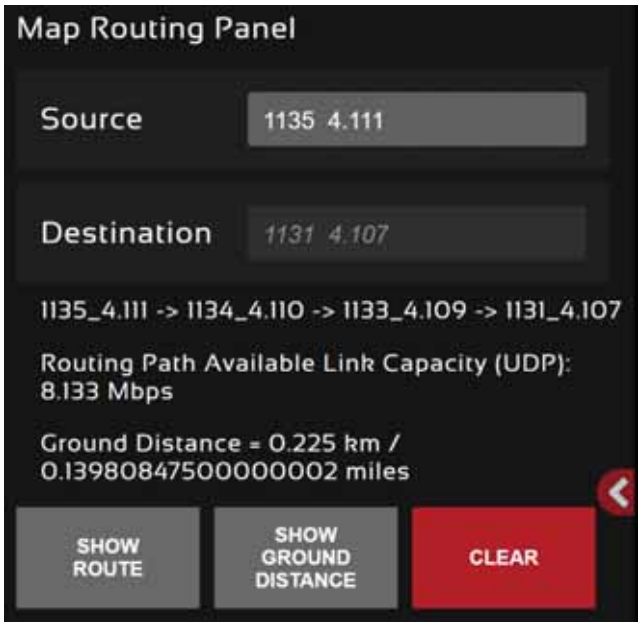


Figure 56 Map Control Panel (map routing panel)

The Map Routing Panel shows you the route path from one radio to another on the map. It also lists the link capacity between the two radios, and the ground distance.

Address:

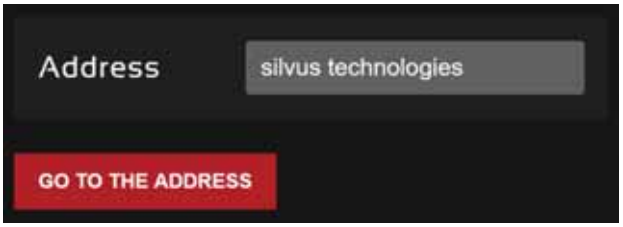


Figure 57 Map Control Panel (address)

The address function can help you zoom the map to a specific address without knowing the lat/long coordinates. This can be a useful tool and can also search for locations by just the name of it.

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.

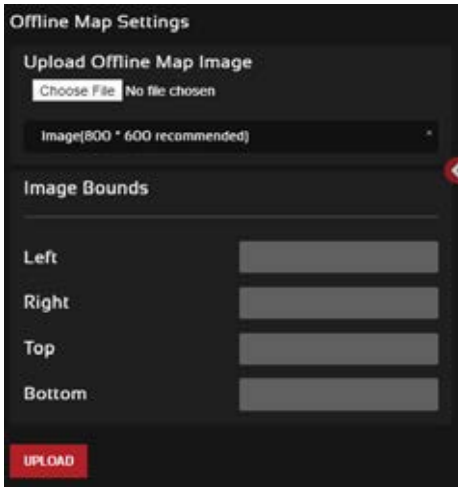


Figure 58 Offline Map Image

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.

5.2.2.3 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 Networking/LAN settings.

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.

5.2.2.4 Manual GPS for Nodes without GPS Module

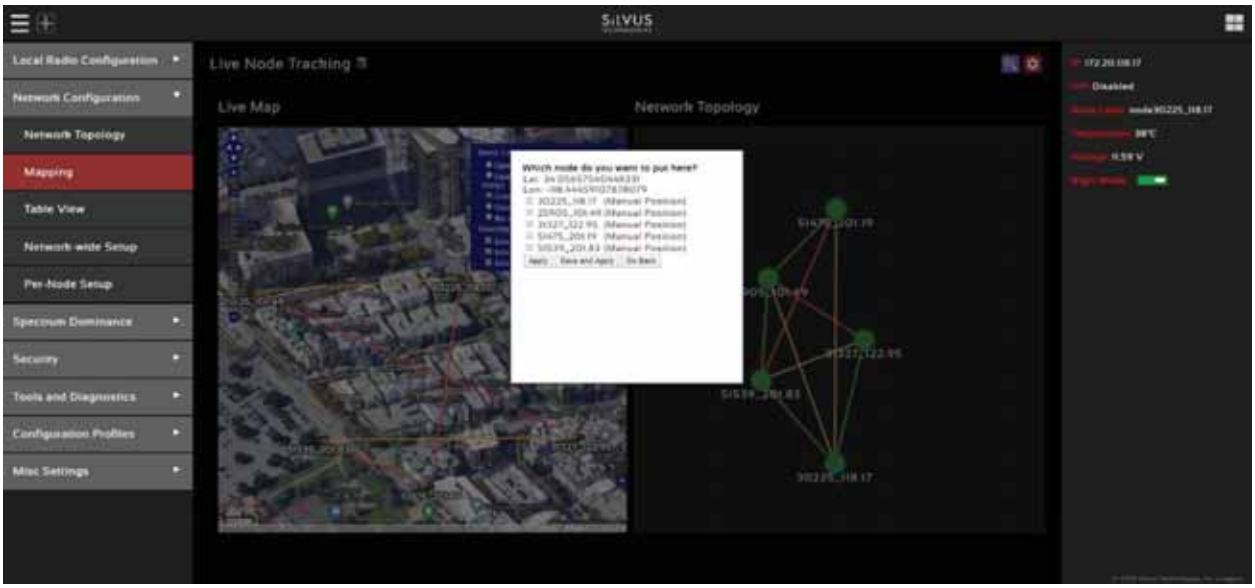


Figure 59 Manually Placing Nodes on the Map

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.

5.2.3 Table View

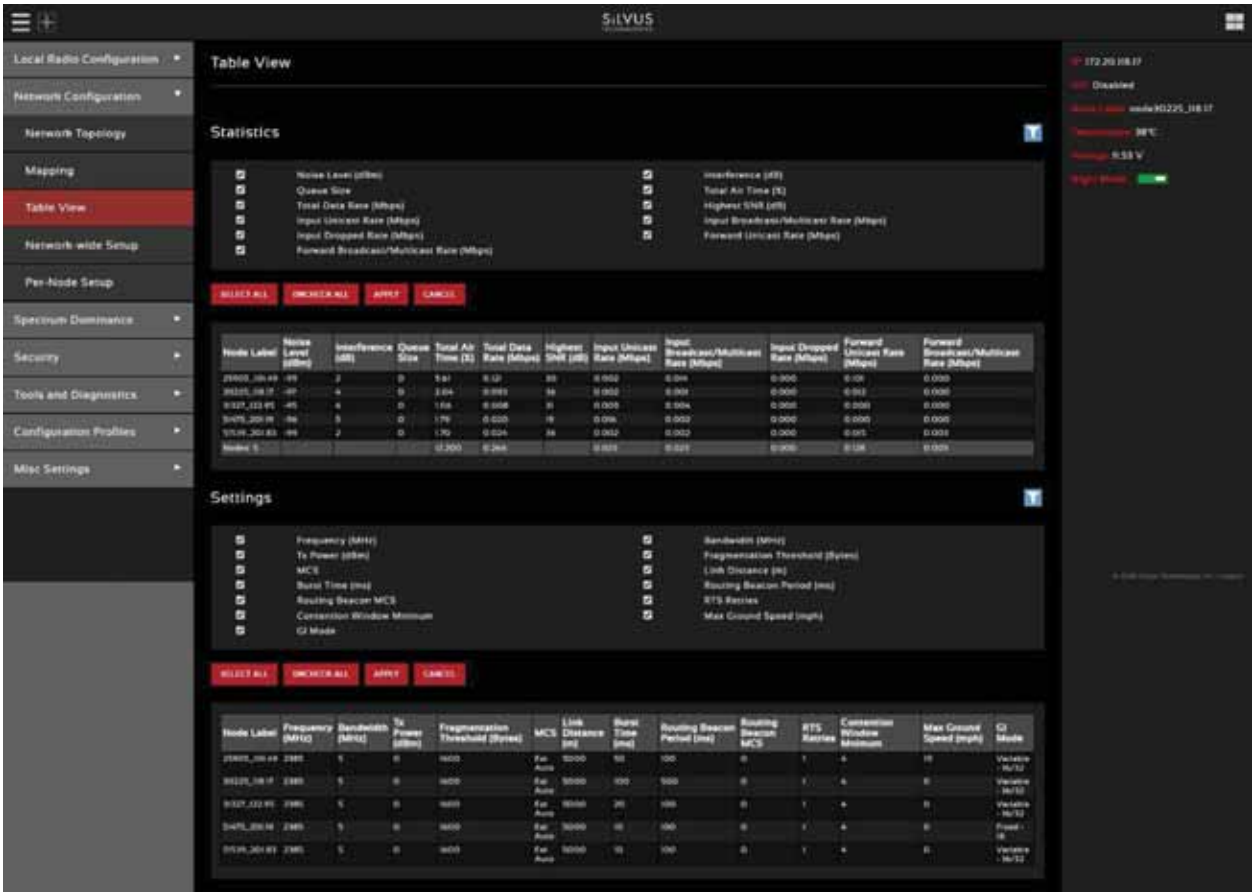


Figure 60 Table View

The table view tab shows all the statistics and setting profiles in table view. Users can select what is being displayed in the table view by clicking the blue filter icon ( ) to the top right of each table. You can deselect or select various parameters in this filter selection to display in the table view.

5.2.4 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.

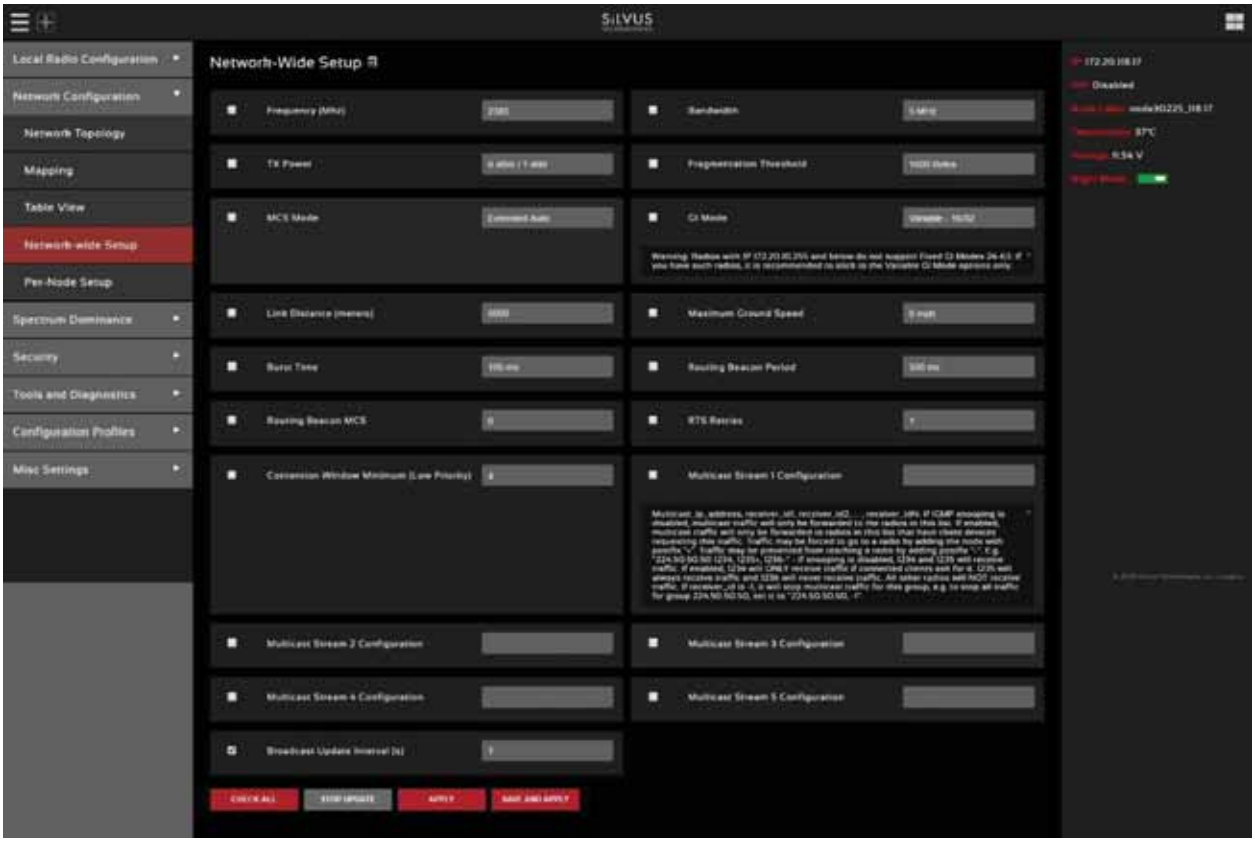


Figure 61 Network-wide Setup

5.2.5 Per-Node Setup

The per-node setup can be used to modify key parameters of individual nodes within the network. As shown in **Figure 62 Per-Node Setup**, 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.

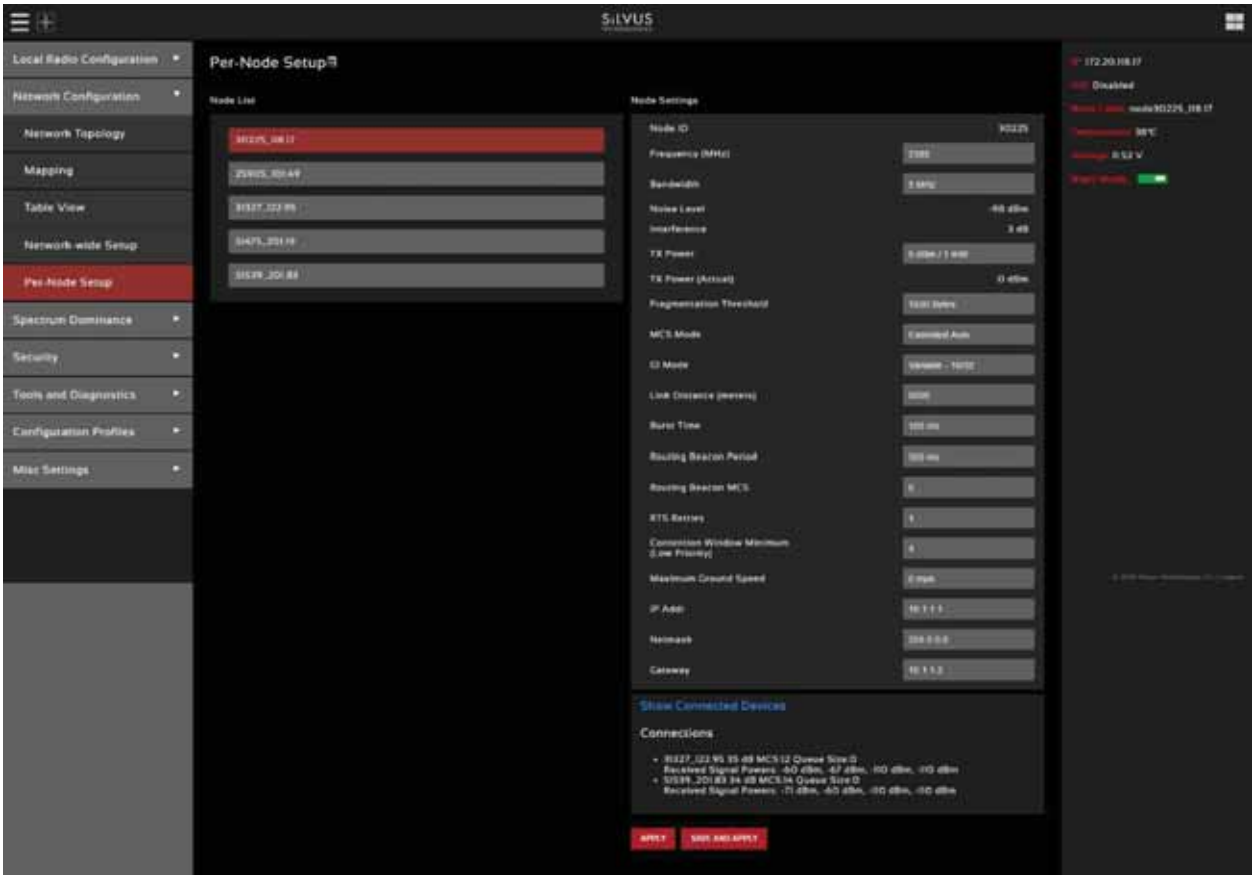


Figure 62 Per-Node Setup

5.2.6 SNMP (Simple Network Management Protocol)

The Silvus Streamscape SNMP service provides support for

- MIB-II (RFC 1213, Management Information Base for Network Management of TCP/IP-based internets). MIB-II provides access to standard properties of the system, interfaces, IPs, access, and others.
- DisMan (RFC 2981, Distributed Management) to enable event management and push notifications.
- Customizations to support specific properties of the Streamscape radios, described in SILVUS-MIB.txt. The Silvus OIDs are located in the .enterprise.silvus subtree (1.3.6.1.4.1.56320)

The SILVUS-MIB.txt can be downloaded from the radio with a standard http browser/downloader. The file is located in /SILVUS-MIB.txt.

(e.g wget http://${RADIO}/SILVUS-MIB.txt -O ~/.snmp/mibs/SILVUS-MIB.txt).

For snmp monitors and tools, load the MIB file in the corresponding folder and/or load the MIB module before accessing the radio.

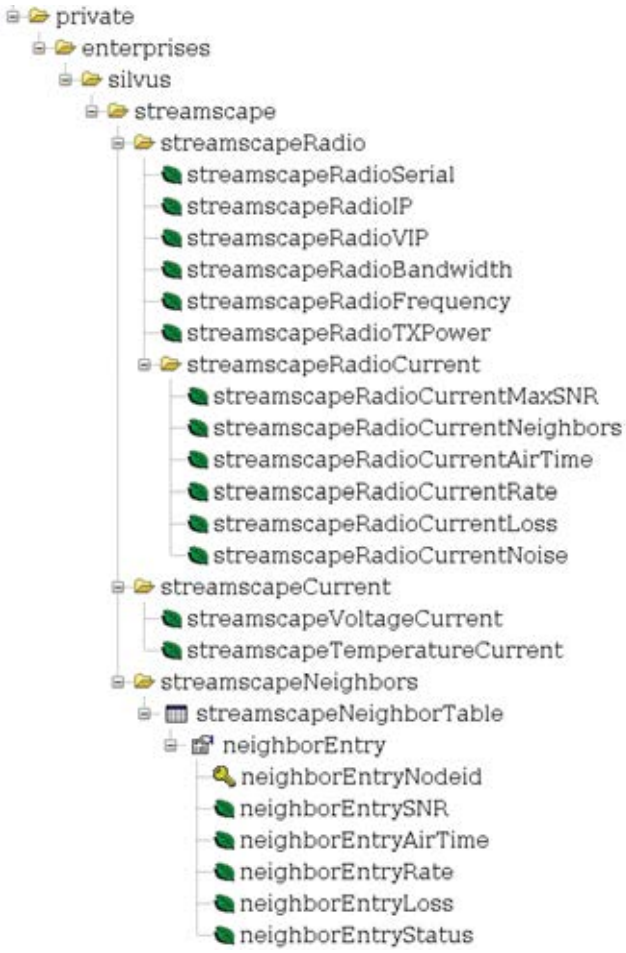


Figure 63 Silvus OID tree loaded into the iReasoning MIB Browser

Access:

The Streamscape snmp service (snmpd) starts automatically during the startup of the radio (unless disabled in the Web GUI). The snmp service is available on udp port 161.

The Streamscape snmp service supports snmp version 2 (v2c) and version 3 (v3).

To access the service use the following default credentials:

- for SNMP version 3: set user “silvus”, no password, no auth no priv
- for SNMP version 2: set community to “silvus”

Examples:

```
$ snmpwalk -m ALL -v3 -u silvus 172.20.11.3 silvus
SILVUS-MIB::streamscapeRadioSerial.0 = INTEGER: 2819
SILVUS-MIB::streamscapeRadioIP.0 = IpAddress: 172.20.11.3
SILVUS-MIB::streamscapeRadioVIP.0 = IpAddress: 192.168.50.113
SILVUS-MIB::streamscapeRadioBandwidth.0 = INTEGER: 20
SILVUS-MIB::streamscapeRadioFrequency.0 = INTEGER: 2280
SILVUS-MIB::streamscapeRadioTXPower.0 = INTEGER: 1
SILVUS-MIB::streamscapeRadioCurrentMaxSNR.0 = INTEGER: 50
SILVUS-MIB::streamscapeRadioCurrentNeighbors.0 = INTEGER: 2
SILVUS-MIB::streamscapeRadioCurrentAirTime.0 = INTEGER: 80
SILVUS-MIB::streamscapeRadioCurrentRate.0 = INTEGER: 79291648
SILVUS-MIB::streamscapeRadioCurrentLoss.0 = INTEGER: 2
SILVUS-MIB::streamscapeRadioCurrentNoise.0 = INTEGER: -100
SILVUS-MIB::streamscapeVoltageCurrent.0 = INTEGER: 11565
SILVUS-MIB::streamscapeTemperatureCurrent.0 = INTEGER: 46
SILVUS-MIB::neighborEntryNodeid.19499 = INTEGER: 19499
SILVUS-MIB::neighborEntryNodeid.30225 = INTEGER: 30225
SILVUS-MIB::neighborEntrySNR.19499 = INTEGER: 48
SILVUS-MIB::neighborEntrySNR.30225 = INTEGER: 52
SILVUS-MIB::neighborEntryAirTime.19499 = INTEGER: 62
SILVUS-MIB::neighborEntryAirTime.30225 = INTEGER: 0
SILVUS-MIB::neighborEntryRate.19499 = INTEGER: 64985984
SILVUS-MIB::neighborEntryRate.30225 = INTEGER: 0
SILVUS-MIB::neighborEntryLoss.19499 = INTEGER: 0
SILVUS-MIB::neighborEntryLoss.30225 = INTEGER: 0
SILVUS-MIB::neighborEntryStatus.19499 = INTEGER: up(1)
SILVUS-MIB::neighborEntryStatus.30225 = INTEGER: up(1)

$snmptable -m ALL -v 2c -c silvus 172.20.11.3 streamscapeneighbortable
SNMP table: SILVUS-MIB::streamscapeNeighborTable

nbNodeid      neighborEntrySNR neighborEntryAirTime neigEntryRate    nbEntryLoss    nbEntryStatus
19499               49                  74          73357696               3               up
30225               54                   0                 0               0               up
```

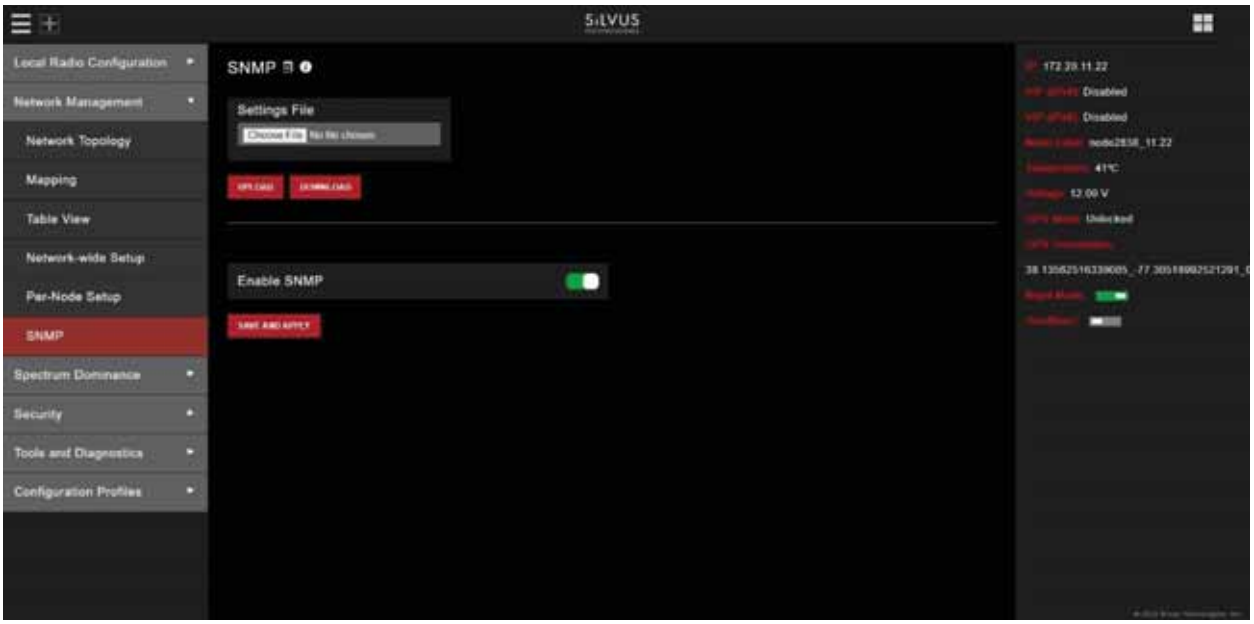


Figure 64 SNMP

Features available on this page include the below:

- SNMP service can be enabled/disabled on this page.
- Upload an extended SNMP configuration file
- Download the currently active extended SNMP configuration file.

Note: check http://[node]/snmpHandler.py?action=log to see the snmpd.log for configuration warnings or errors

Extended configuration for access control and traps

The Streamscape SNMP service can be further configured by uploading a configuration file.
Configurations are needed for
- Adding new users and access groups
- Setting up user credentials and passwords (for SNMP v3)
- Setting up traps, trap sinks and notifications

The format of the configuration file follows the net-snmp configuration file (see http://www.net-snmp.org/docs/man/snmpd.conf.html)

Examples:

Traps for SNMP v3:

```
createUser myuser MD5 mypassword DES myotherpassword
authtrapenable 1
trapsess -v 3 -l authPriv -u myuser  192.168.1.2

monitor -r 5 -e machineTooBusy "Machine Busy" HOST-RESOURCES-MIB::hrProcessorLoad > 60
monitor -r 5 -e temperatureHigh "Temp High" SILVUS-MIB::streamscapeTemperatureCurrent > 40

notificationEvent  neighborDownTrap linkDown SILVUS-MIB::neighborEntryNodeid
monitor -r 5 -e neighborDownTrap "Link Down" SILVUS-MIB::neighborEntryStatus > 1

notificationEvent  neighborUpTrap linkUp SILVUS-MIB::neighborEntryNodeid
monitor -r 5 -e neighborUpTrap "Link Up" SILVUS-MIB::neighborEntryStatus == 1
```

That example
- Adds a user “myuser” with MD5 and DES passwords
- Sets up the traps to be sent to the sink 192.168.1.2
- Sets up alarms for high system utilization, high temperature, and link up/down events

To receive SNMP v3 traps, it is necessary to set the correct user, with the correct passwords and engine ID on the trap receiver. For example in snmptrapd set

```
createUser -e 0x80001F888076AC0A51137A495A myuser MD5 mypassword DES myotherpassword
```

Each radio has its own engine ID. The engine ID can be obtained with

```
snmpwalk -m ALL -r 1 -t 1 -v 3 -u silvus [RADIO_IP]:161 1.3.6.1.6.3.10.2.1.1.0
```

Example for SNMP v2 traps to checks for low voltage, low SNR and high processor load - and sends it to a chosen sink:

```
monitor -r 5 lowVoltage SILVUS-MIB::streamscapeVoltageCurrent < 11
monitor -r 5 lowSNR SILVUS-MIB::neighborEntrySNR < 40
monitor -r 5 machineTooBusy HOST-RESOURCES-MIB::hrProcessorLoad > 50
trap2sink 172.20.2.2 silvus
```

For more details on monitoring/push see below link:
http://net-snmp.sourceforge.net/wiki/index.php/TUT:DisMan_Monitoring

Complete list of Silvus SNMP OIDs:

OID	Description and command to obtain the value
1.3.6.1.4.1.56320 enterprise.silvus	Registered enterprise OID for Silvus
1.3.6.1.4.1.56320.1 enterprise.silvus.streamscape	Subtree for StreamScape radios
1.3.6.1.4.1.56320.1.1 .streamscape.streamscapeRadio	Subtree for static radio properties
1.3.6.1.4.1.56320.1.1.1 .streamscapeRadio.streamscapeRadioSerial	Serial number of the radio
1.3.6.1.4.1.56320.1.1.2 .streamscapeRadio.streamscapeRadioIP	Primary IP address (of br0)
1.3.6.1.4.1.56320.1.1.3 .streamscapeRadio.streamscapeRadioVIP	virtual IP of the radio (if set)
1.3.6.1.4.1.56320.1.1.4 .streamscapeRadio.streamscapeRadioBandwidth	Bandwidth of the Radio (in MHz)
1.3.6.1.4.1.56320.1.1.5 .streamscapeRadio.streamscapeRadioFrequency	Radio frequency (in MHz)
1.3.6.1.4.1.56320.1.1.6 .streamscapeRadio.streamscapeRadioTXPower	Tx power in mW
1.3.6.1.4.1.56320.1.2 .streamscape.streamscapeRadioCurrent	Subtree for current radio properties
1.3.6.1.4.1.56320.1.2.1 .streamscapeRadioCurrent.streamscapeRadioCurrentMaxSNR	Current Maximum SNR to a wireless neighbor; a value of -150 indicates that the node is not connected wirelessly
1.3.6.1.4.1.56320.1.2.2 .streamscapeRadioCurrent.streamscapeRadioCurrentNeighbors	Current Number of Active Neighbors of the Node (wired and wireless)
1.3.6.1.4.1.56320.1.2.3 .streamscapeRadioCurrent.streamscapeRadioCurrentAirTime	AirTime (in percent) of radio over the last second
1.3.6.1.4.1.56320.1.2.4 .streamscapeRadioCurrent.streamscapeRadioCurrentRate	current transmit data rate of radio over the last second
1.3.6.1.4.1.56320.1.2.5 streamscapeRadioCurrent.streamscapeRadioCurrentLoss	Number of transmitted packets lost from the radio over the last second
1.3.6.1.4.1.56320.1.2.6 .streamscapeRadioCurrent.streamscapeRadioCurrentNoise	Current Noise Level of the Node
1.3.6.1.4.1.56320.1.3 .streamscape.streamscapeCurrent	Subtree for current values (voltage, temperature)

1.3.6.1.4.1.56320.1.3.1 .streamscapeCurrent.streamscapeVoltageCurrent	Current voltage in mV
1.3.6.1.4.1.56320.1.3.2 .streamscapeCurrent.streamscapeTemperatureCurrent	Current CPU temperature in C
1.3.6.1.4.1.56320.1.5 .streamscape.streamscapeNeighbors	Subtree for neighbors table
1.3.6.1.4.1.56320.1.5.1 .streamscapeNeighbors.streamscapeNeighborTable	Structure (and OID) for the neighbor table
1.3.6.1.4.1.56320.1.5.1.1 .streamscapeNeighborTable.neighborEntry	Struct for a table row
1.3.6.1.4.1.56320.1.5.1.1.1.1 .neighborEntry.neighborEntryNodeid	Node id of the neighbor, this column is the index of the table
1.3.6.1.4.1.56320.1.5.1.1.1.2 .neighborEntry.neighborEntrySNR	SNR of local radio to the neighbor
1.3.6.1.4.1.56320.1.5.1.1.1.3 .neighborEntry.neighborEntryAirTime	Air time (in percent) of the transmission link to the neighbor within the last second
1.3.6.1.4.1.56320.1.5.1.1.1.4 .neighborEntry.neighborEntryRate	Data rate (in Byte) of the link to the neighbor within the last second
1.3.6.1.4.1.56320.1.5.1.1.1.5 .neighborEntry.neighborEntryLoss	Lost packets of the link to the neighbor within the last second
1.3.6.1.4.1.56320.1.5.1.1.1.6 .neighborEntry.neighborEntryStatus	The current operational state of the link (1=up, 2=down)

Table 26 Silvus SNMP OIDs

5.3 Spectrum Dominance

The Silvus radios come with special features that allow it to analyze the frequency spectrum as it is deployed in the field. This will give a network administrator some powerful tools to deploy a functioning network. If there is interference on a channel, the spectrum dominance features in the Silvus radios will allow a way to detect it, and find the channel with the least amount of interference.

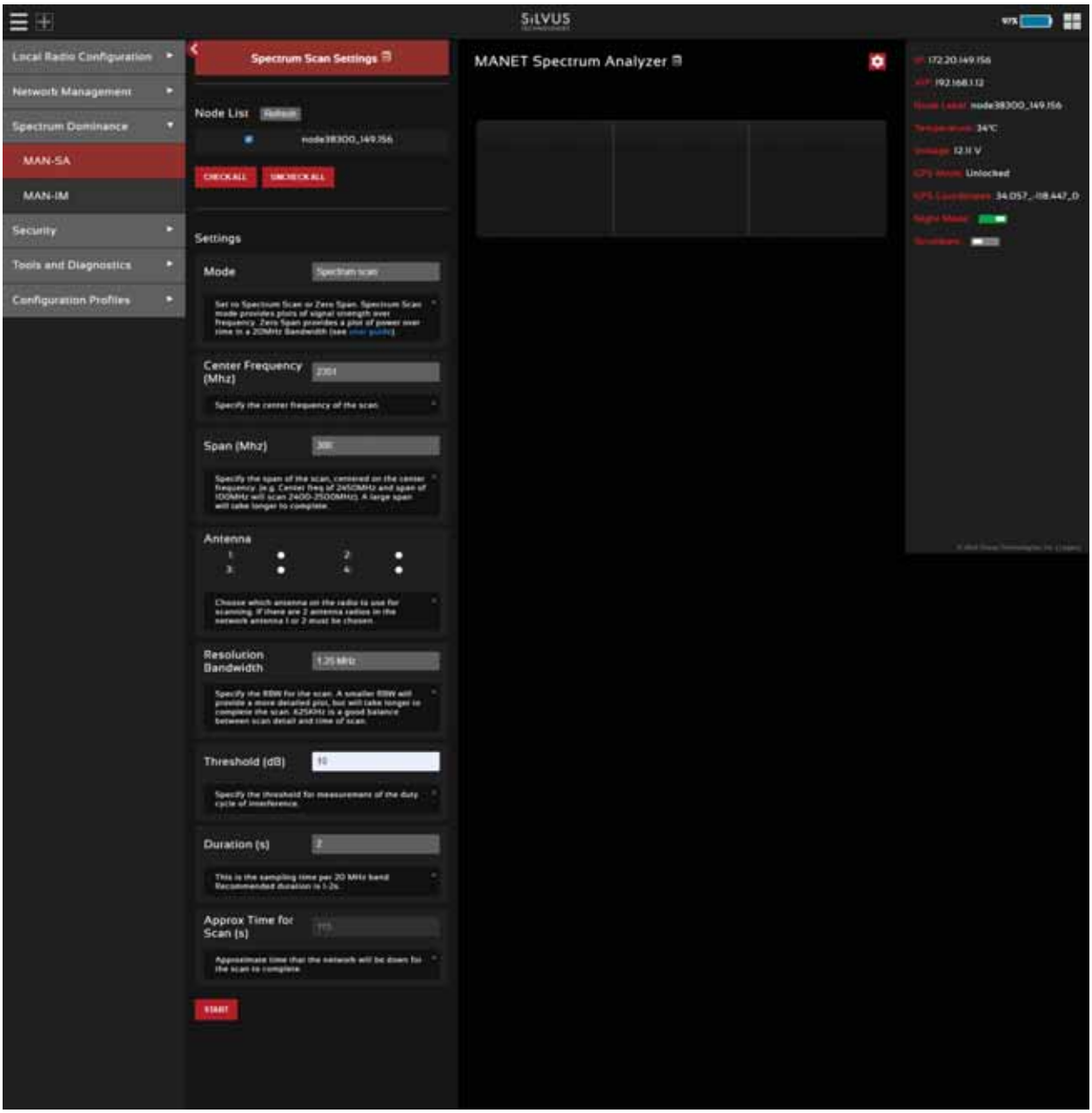


Figure 65 Spectrum Dominance

5.3.1 Spectrum Analyzer

The first tool in the Spectrum Dominance section is the spectrum analyzer. 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.

5.3.1.1 Spectrum Analyzer Settings

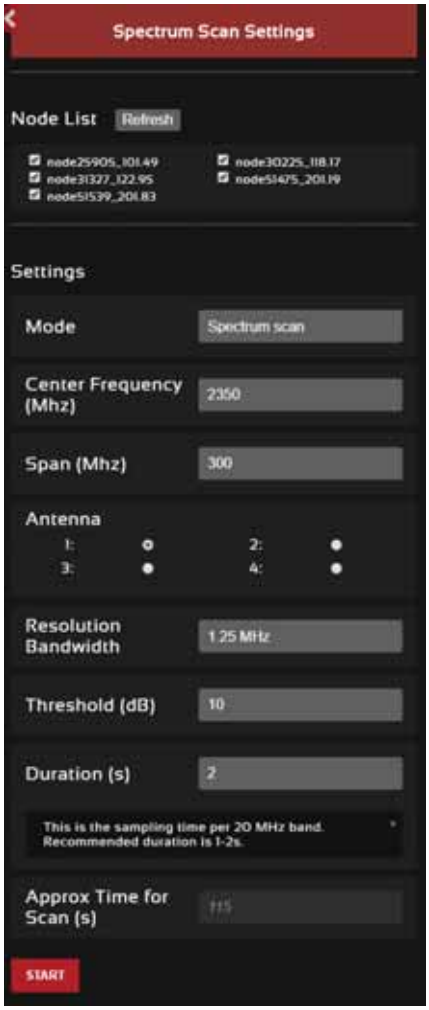


Figure 66 Spectrum Scan Settings

Clicking the settings icon ( ) at the top right of the window will show the settings panel as shown in **Figure 66 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 69 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.

5.3.1.2 Spectrum Scan Results

Figure 67 Spectrum Scan Results below 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.

Figure 67 Spectrum Scan Results

5.3.1.3 Zero Span Mode

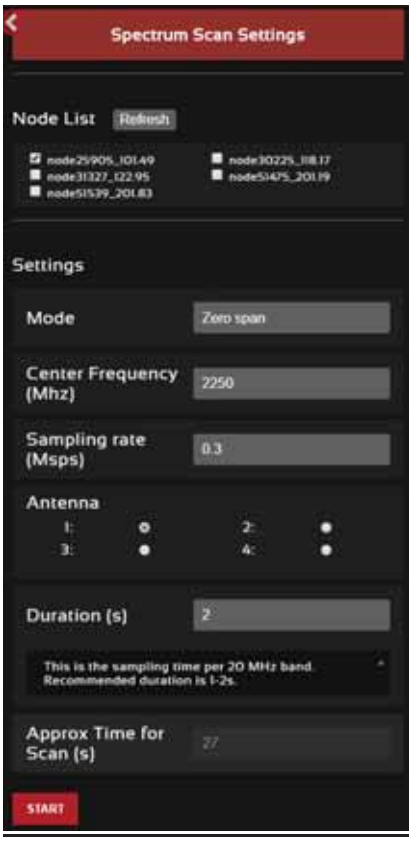


Figure 68 Zero Span Settings

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 69 Zero Span Results

5.3.2 MAN-IM (MANET Interference Monitoring)

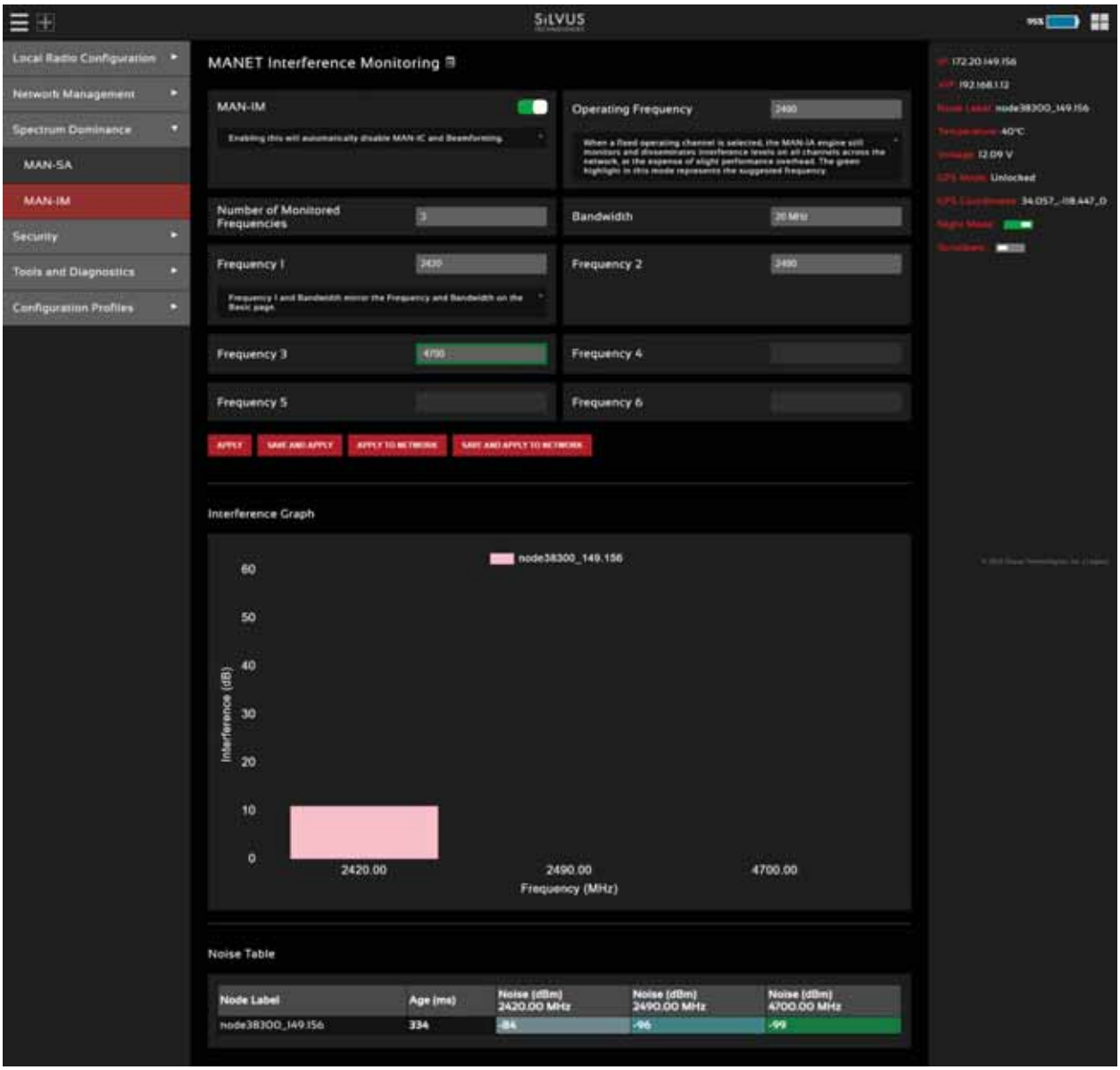


Figure 70 MAN-IM

MAN-IM is a feature that has been developed to help live monitor the interference levels on several frequencies. When monitoring these frequencies, you can decide whether the network would benefit from changing channels to a less congested frequency. When enabling MAN-IM you will automatically disable Tx beamforming.

Configuring MAN-IM:

MAN-IM- The first parameter in the menu allows enabling or disabling the MAN-IM feature. All radios within a network should have this enabled in order to operate properly.

Operating Frequency- You can quickly jump between operating frequencies that are listed in the MAN-IM frequency list. Select the operating frequency from the drop down menu and click apply or save and apply to change the operating frequency.

Number of Valid Frequencies- This configuration is the number of channels that the MAN-IM feature will monitor. All radios within a network should have this configured the same in order to operate properly.

Bandwidth- This is the bandwidth of the channels. All radios within a network should have this configured the same in order to operate properly. This setting will override the bandwidth setting on the 'Basic' page.

Frequencies- These are the center frequencies of the channels to be monitored. Frequency 1 will override the Frequency setting on the 'Basic' page. All radios within a network should have the same frequency set in order to operate properly.

Configuration changes can be propagated to the entire network by clicking 'Apply to Network' or 'Save and Apply to Network'. Note that this update will take around 1-2 minutes to take effect.

MAN-IM Metrics

Once configured, the MAN-IM functionality of the network can be monitored in real-time. The bar graph is a visual representation of the interference on each channel at each node. It will show the reported noise level measured by each radio in the network, in each channel being monitored.

The 'Age' field indicates the time since the last update received from each node in the network.

The frequency with the lowest reported amount of interference will be highlighted in green.

NOTE: transition time will get longer if the number of hops in the network increases and as traffic increases.

5.3.3 MAN-IA (MANET Interference Avoidance) (License enabled)

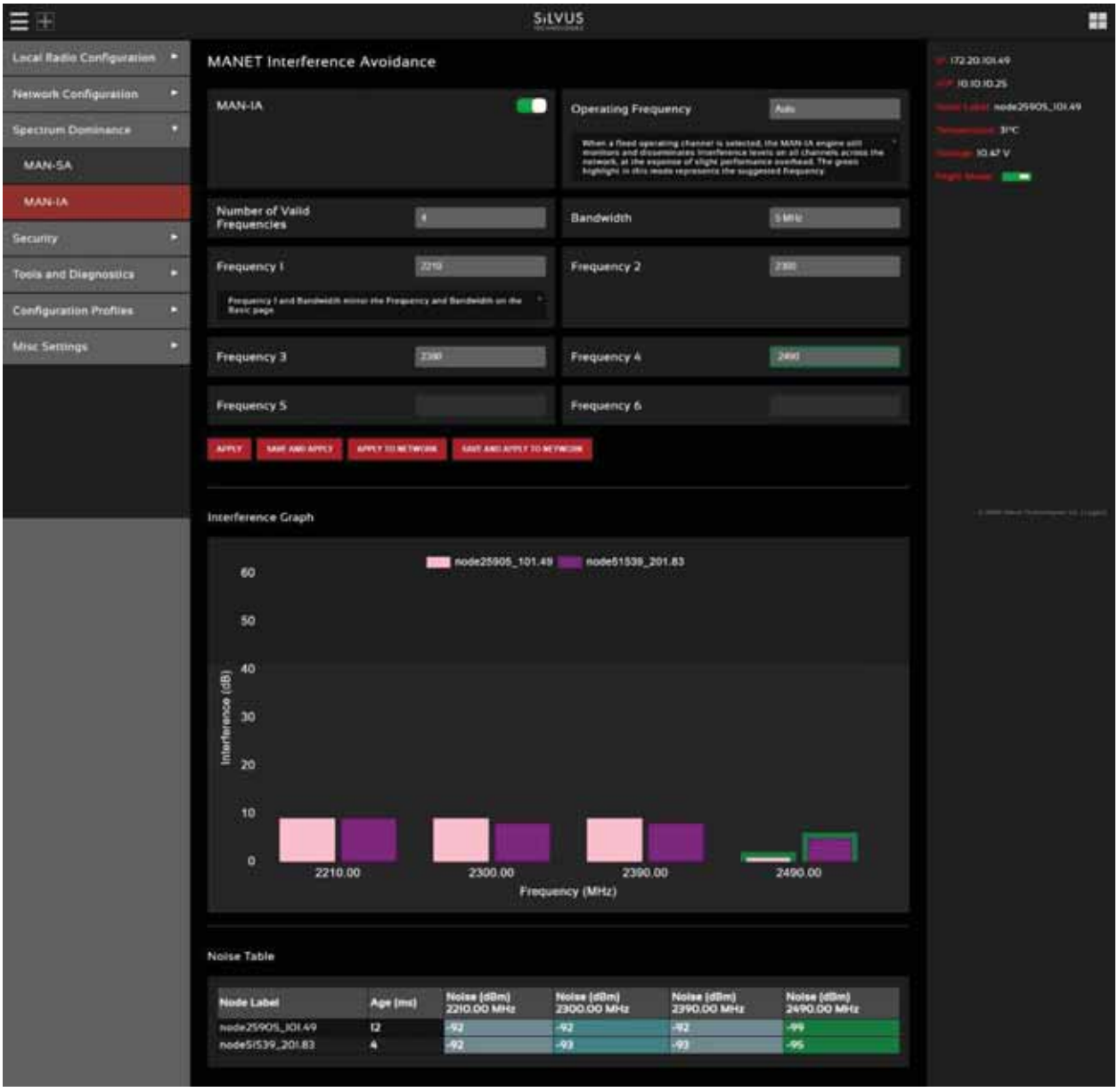


Figure 71 MAN-IA

MANET Interference Avoidance (MAN-IA) is a license enabled feature that provides Silvus radios the capability to monitor interference and dynamically configure the network to avoid congested spectrum. MAN-IA allows a network administrator to select up to 6 preset frequencies for each radio in the network to monitor in real-time, with no impact on normal network operations. If another channel is cleaner and has less interference then the current channel, the network will rapidly move to the better channel. MAN-IA will disable Tx beamforming.

Configuring MAN-IA:

The MAN-IA feature will require a software license on each node that will participate in the MAN-IA enabled network. The MAN-IA feature is not a part of the standard StreamScape release.

MAN-IA can be configured from the 'MAN-IA' tab in the radio GUI, as shown above.

MAN-IA- The first parameter in the menu allows enabling or disabling the MAN-IA feature. All radios within a network should have this enabled in order to operate properly.

Operating Frequency- When set to 'Auto' mode, the radios will share interference information and automatically change to the channel which is determined to be the best for the network to operate on. The chosen channel will be highlighted in green. Note that 'Auto' mode will have some additional network overhead. If this setting is set to a fixed frequency, the radios will no longer automatically change frequencies. In this case, the channel highlighted in green will be the suggested best channel. All radios within a network should have this configured the same in order to operate properly.

Number of Valid Frequencies- This configuration is the number of channels that the MAN-IA feature will monitor and jump between. All radios within a network should have this configured the same in order to operate properly.

Bandwidth- This is the bandwidth of the channels. All radios within a network should have this configured the same in order to operate properly. This setting will override the bandwidth setting on the 'Basic' page.

Frequencies- These are the center frequencies of the channels to be monitored and jump between. Frequency 1 will override the Frequency setting on the 'Basic' page. All radios within a network should have the same frequency set in order to operate properly.

Configuration changes can be propagated to the entire network by clicking 'Apply to Network' or 'Save and Apply to Network'. Note that this update will take around 1-2 minutes to take effect.

MAN-IA Metrics

Once configured, the MAN-IA functionality of the network can be monitored in real-time. The bar graph is a visual representation of the interference on each channel at each node. It will show the reported noise level measured by each radio in the network, in each channel being monitored.

The 'Age' field indicates the time since the last update received from each node in the network.

The frequency currently being occupied will be highlighted in green and will change as the network moves to different channels.

NOTE: MAN-IA currently only takes into account interference levels in making decisions for the best operating channel. The user will need to take into consideration propagation characteristics when operating across different bands.

NOTE: transition time will get longer if the number of hops in the network increases and as traffic increases.

5.3.4 MAN-IC (MANET Interference Cancellation) (License enabled)

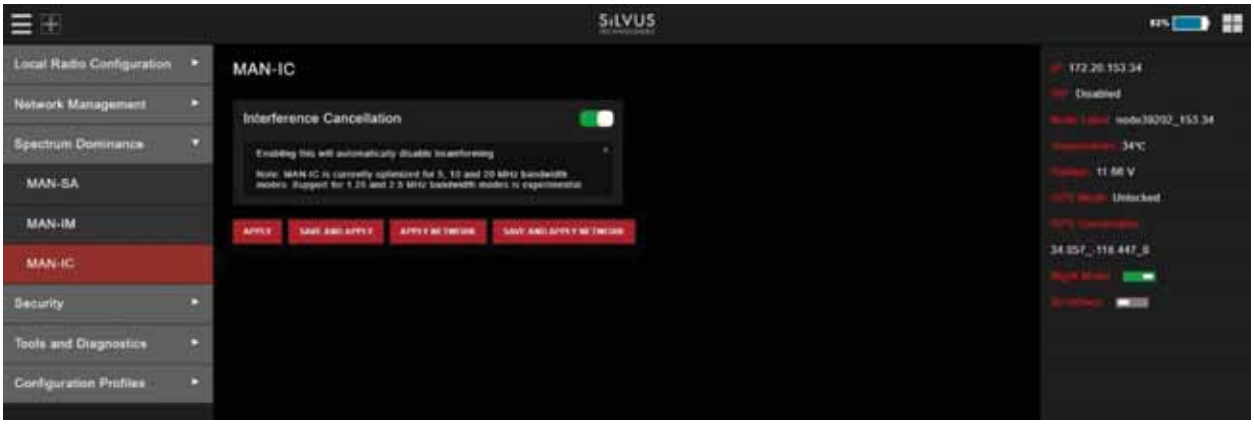


Figure 72: MAN-IC Configuration Page

MANET Interference Cancellation (MAN-IC) allows a Silvus network to maintain high throughput in the presence of otherwise harmful interference. This feature employs a sophisticated MIMO signal processing technique to nullify the offending interfering signals while maintaining reliable communications with other StreamCaster radios.

To enable MAN-IC, simply toggle the feature 'On' from the MAN-IC page in the Spectrum Dominance section of StreamScape. You can choose to enable it on only the local radio, or the entire network. A network-wide update of MAN-IC will take ~20 seconds with a brief drop in communication. Nodes with MAN-IC enabled will be displayed in the Network Topology as a triangle as shown in **Figure 73** below.

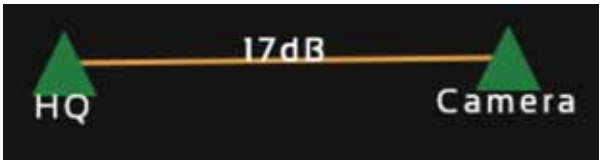


Figure 73: MAN-IC Nodes Displayed as Triangles in Network Topology

When hovering over a node with MAN-IC enabled, the Node Statistics Pop-up will report the Front-end interference and the Post MAN-IC interference. The difference between these two is roughly the amount of interference protection MAN-IC is providing. In **Figure 74** below there is 55dB of Front-end Interference and 32dB of Post MAN-IC interference. In this case, MAN-IC is providing ~23dB of interference suppression.

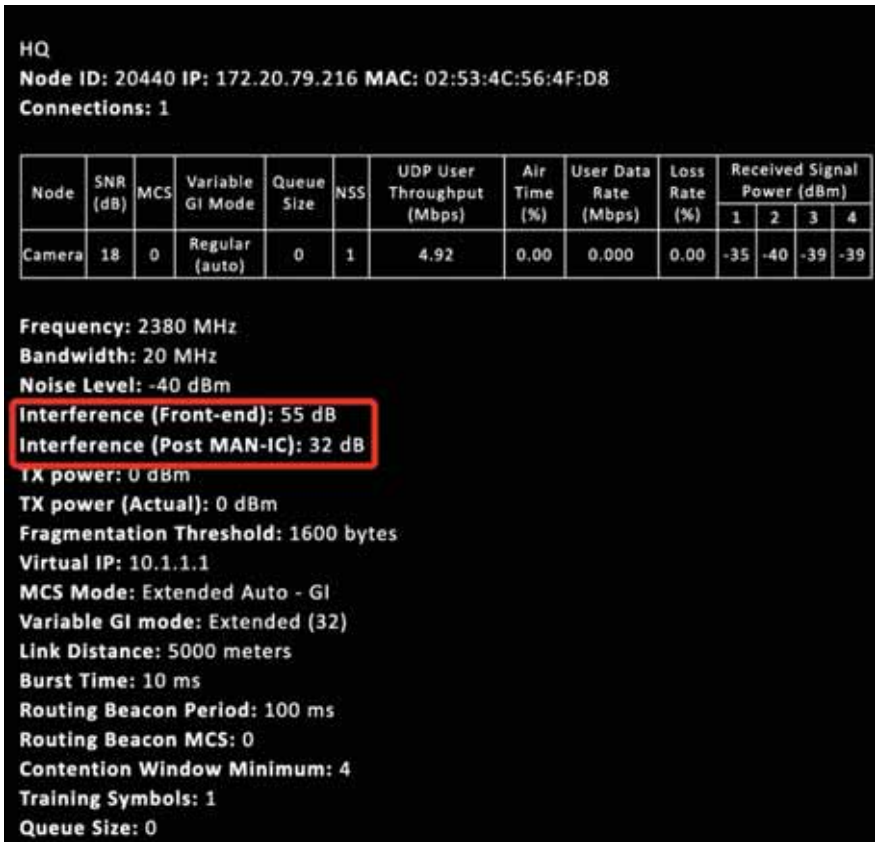


Figure 74: Node Statistics Pop-Up w/ MAN-IC Enabled

5.4 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.

5.4.1 Encryption

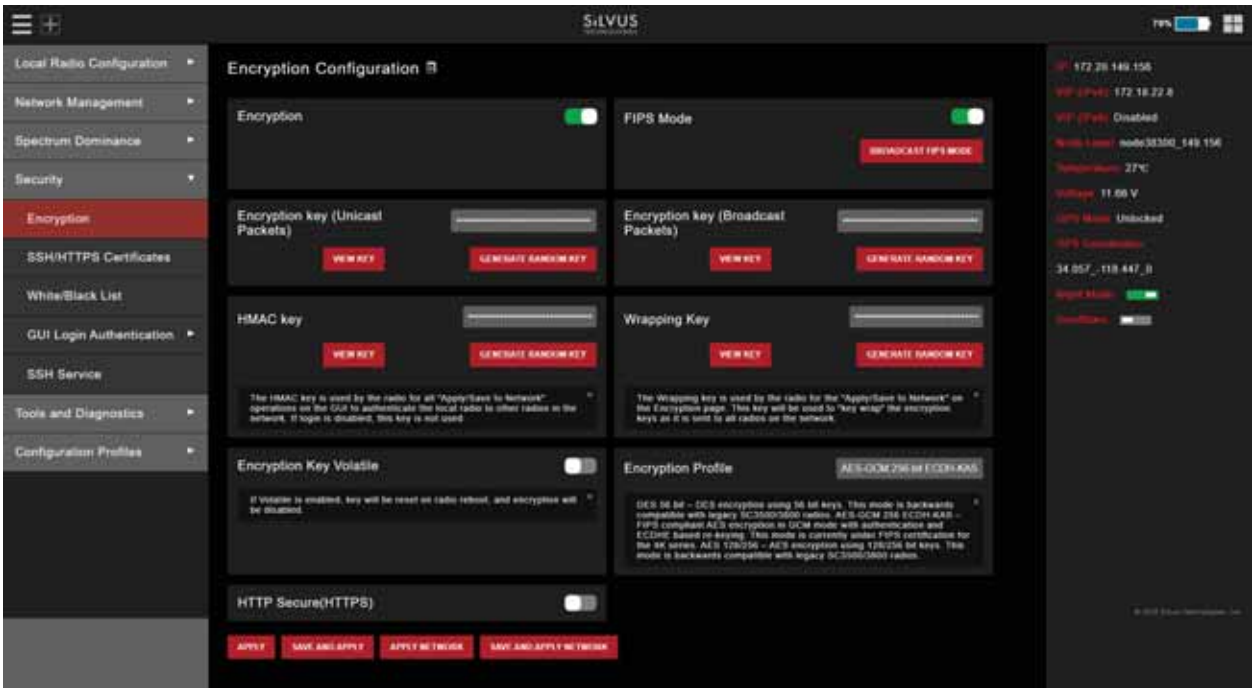


Figure 75 Security (Encryption)

- **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. There is also a broadcast FIPS mode button that will enable FIPS mode on every radio on the network, and then force a reboot with all passwords set to default.
    - 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. This needs to match on all radios that want to join the same network. If AES-GCM 256 is selected a key for unicast traffic as well as broadcast packets will need to be set. The generate random key button will generate a random key that could be used. The view button will display the key.
- **HMAC key:** used by the radio for all "apply/save to network" operations on the GUI to authenticate the local radio to other radios in the network. If login is disabled, this key is not used. The generate random key button will generate a random key that could be used. The view button will display the key.
- **Wrapping key:** used when you click on the apply and save to network on the encryption page. This key will be used to "key wrap" the encryption keys as it is sent to all radios on the network. The generate random key button will generate a random key that could be used. The view button will display the key.
- **Encryption Key Volatile:** If volatile is enabled, key will be reset on radio reboot, and encryption will be disabled.
- **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. FIPS certification for the 4C42/44 radio models.
- **HTTP Secure (HTTPS):** Enable or disable HTTPS access to StreamScape.

5.4.2 SSH/HTTPS Certificates

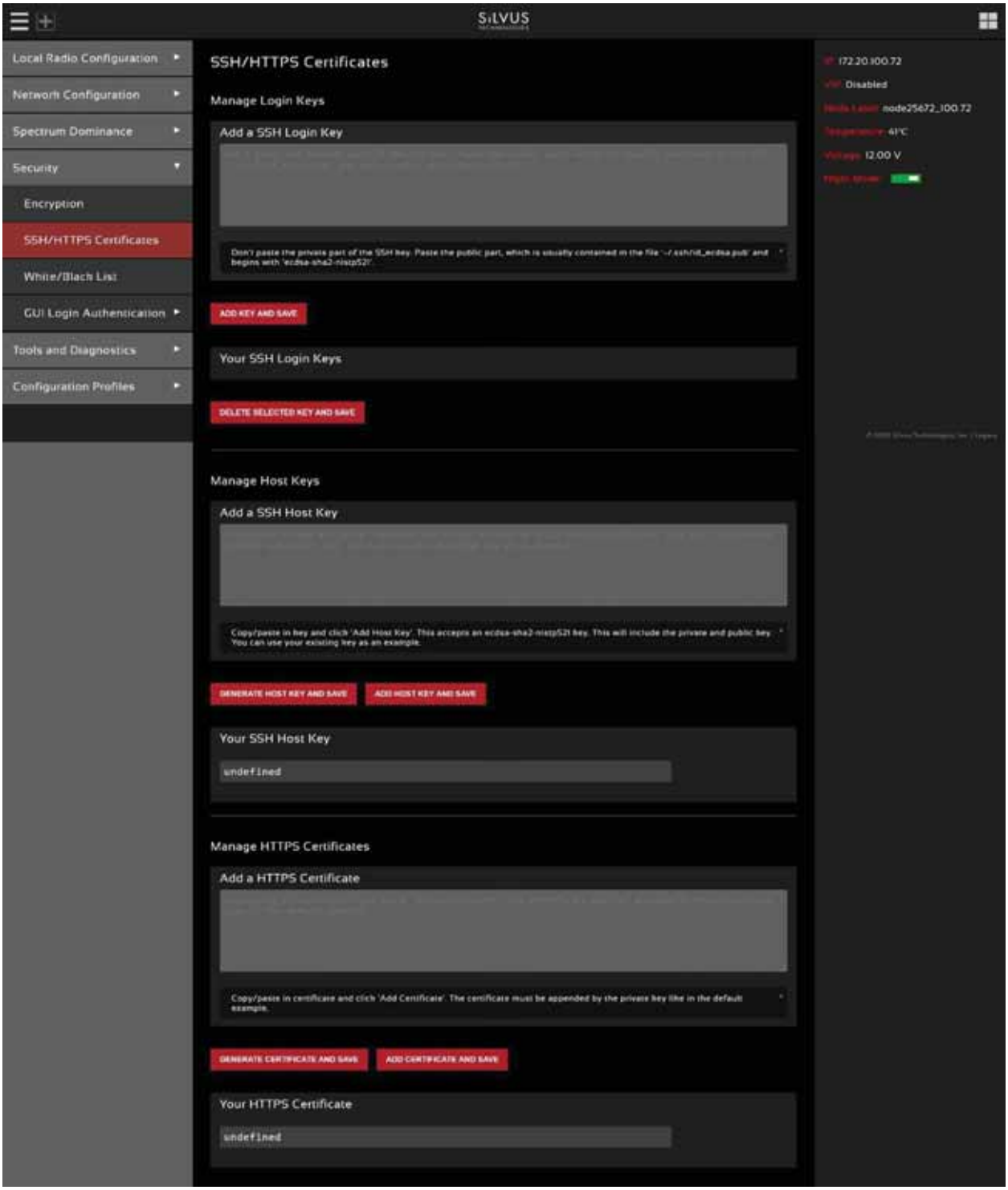


Figure 76 Security (SSH/HTTPS Certificates)

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."

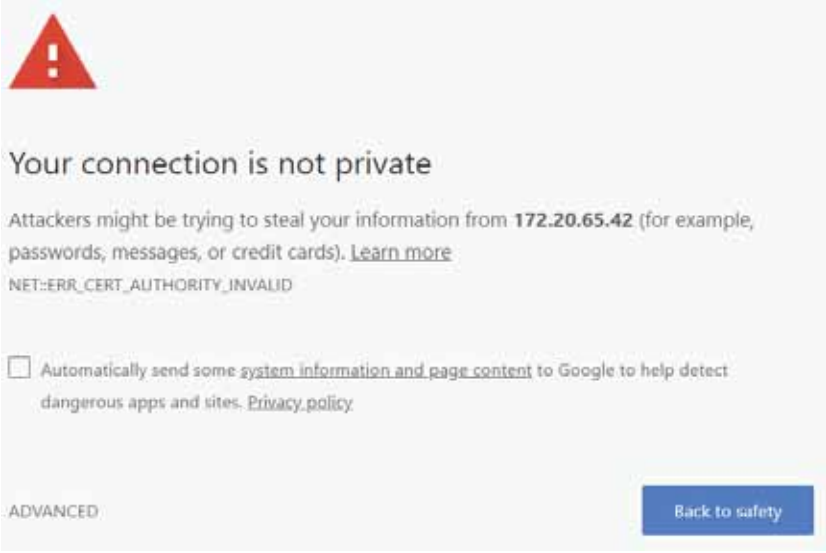


Figure 77 (Chrome Browser Warning)

5.4.3 White/Black List

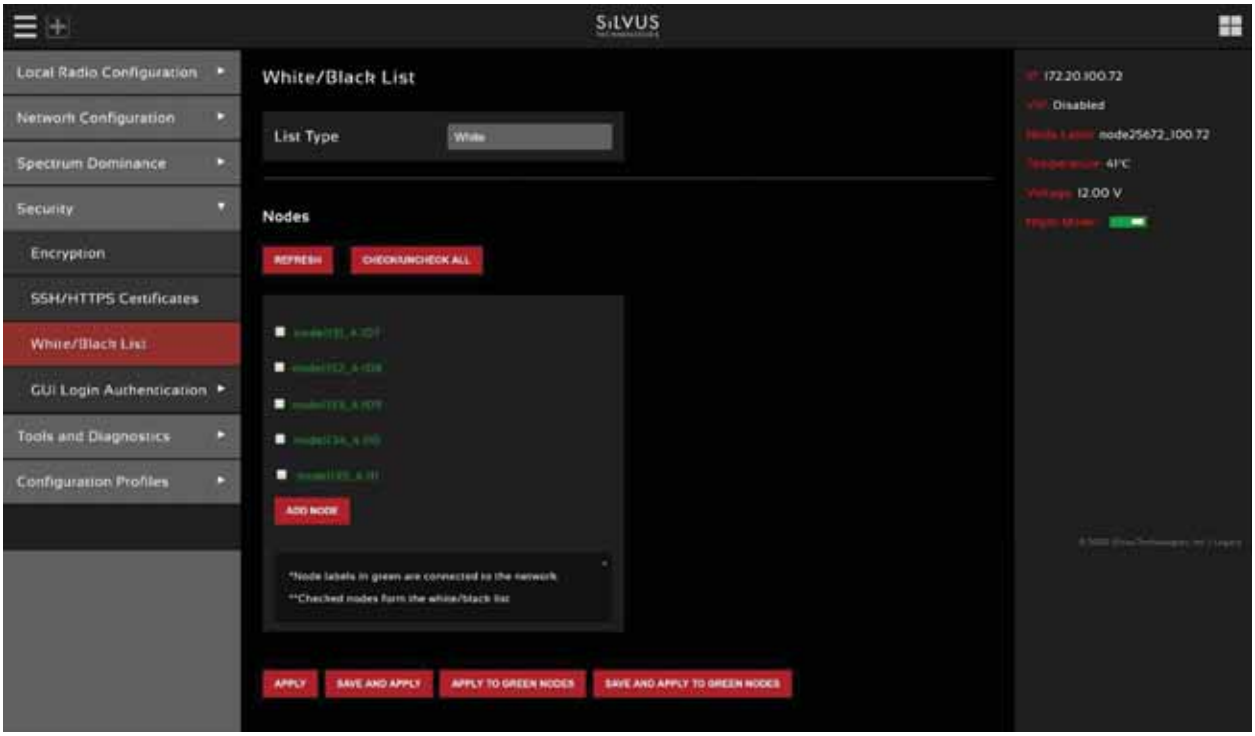


Figure 78 Security (White/Black List)

This page is to add a level of security in the mesh network. It will only allow the radio to mesh with radios on the white list, or to never mesh with radios on the black list.

White List: a list of radio IP addresses that you deem safe to connect to.

Black List: a list of radio IP addresses that you do not want to connect to.

While you can create either a White List or a Black List to reach the same result, you cannot use both lists at the same time. When you select the list type of either White or Black, it will automatically populate all radios that the radio is currently connected to. You can also add radios that are not currently connected to the network by adding the last two octets of the IP address of those radios.

5.4.4 GUI/Login Authentication

5.4.4.1 Admin

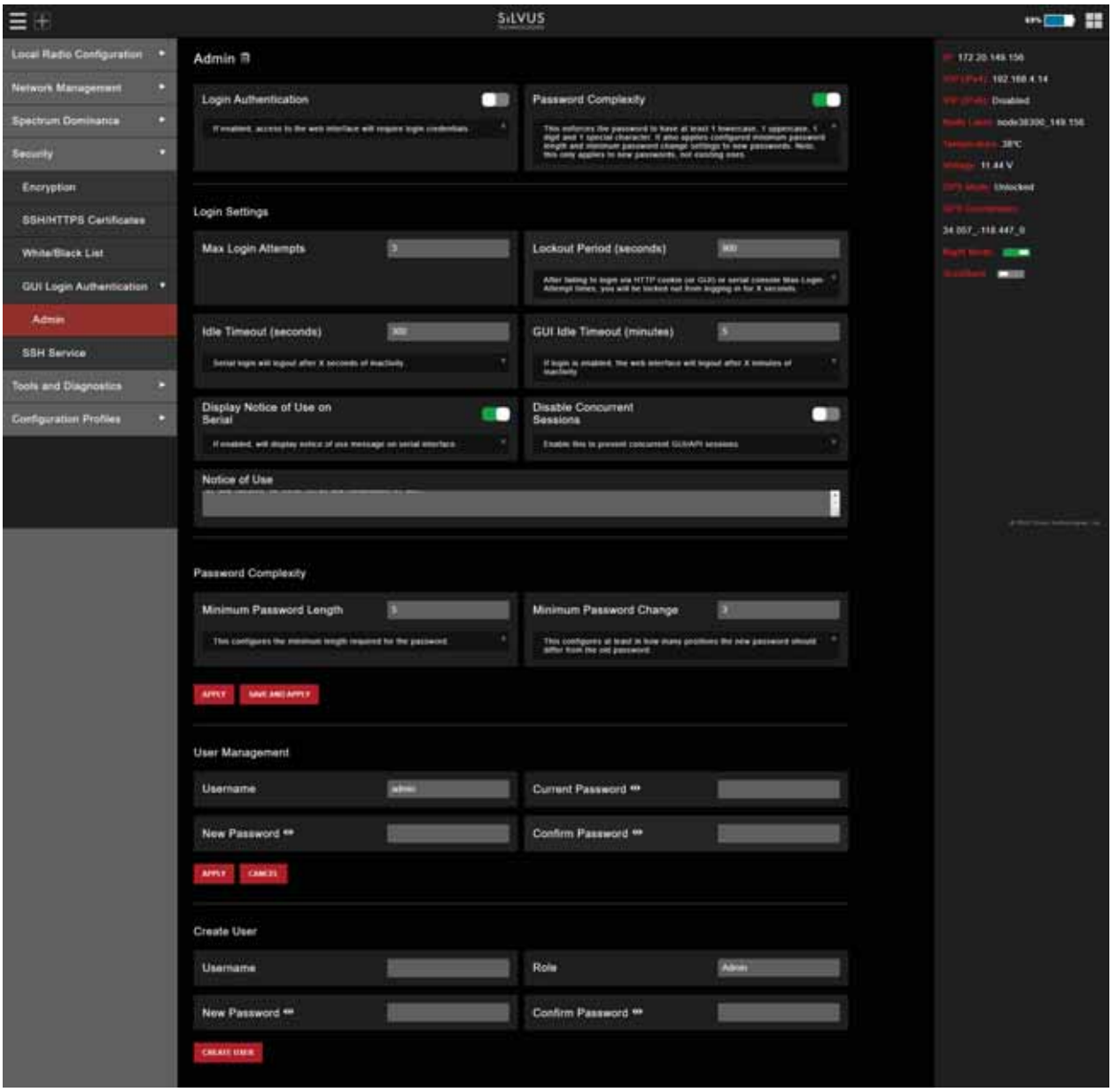


Figure 79 Admin page

The Admin page provides the option of password protecting access to Streamscape. There are several parameters that can enforce various security measures in regards with the Login Authentication. There are three levels of login authentication, Basic, Advanced, and Admin, each with increasing privileges on the GUI and backend API. The basic login would give access to local radio configs, network management, and tools and diagnostics. The Advanced login will give you everything in Basic plus spectrum dominance and configuration profiles (everything except security). The admin gives you full access to the GUI.

- Login Authentication: This will enable the requirement to enter a password in order to access the radio GUI.

- Password Complexity: This will enforce the password to have at least 1 lowercase, 1 uppercase, 1 digit, and 1 special character. It also applies configured minimum password length and minimum password change settings to new passwords. Note, this only applies to new passwords, not existing ones.

- Max Login Attempts: After failing to login via HTTP cookie (or GUI) or serial console Max-Login-Attempt times, you will be locked out from logging in for X seconds.

- Lockout Period: The amount of time that the radio login will be locked out if the max login attempts are reached.

- Idle Timeout: Serial login will logout after X seconds of inactivity.

- GUI Idle Timeout: If login is enabled, the web interface will logout after X minutes of inactivity.

- Display Notice of Use on Serial: If enabled, will display notice of use message on serial interface.

- Disable Concurrent Sessions: Enable this to prevent concurrent GUI/API sessions.

- Minimum Password Length: This configures the minimum length required for the password.

- Minimum Password Change: This configures at least in how many positions the new password should differ from the old password.

- User Management: This section allows you to reset the password for various user profiles.

- Create user: This section allows you to create new users and configure their role/permission levels.

To enable, set the Login Authentication to Enable and click apply or save and apply. 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.

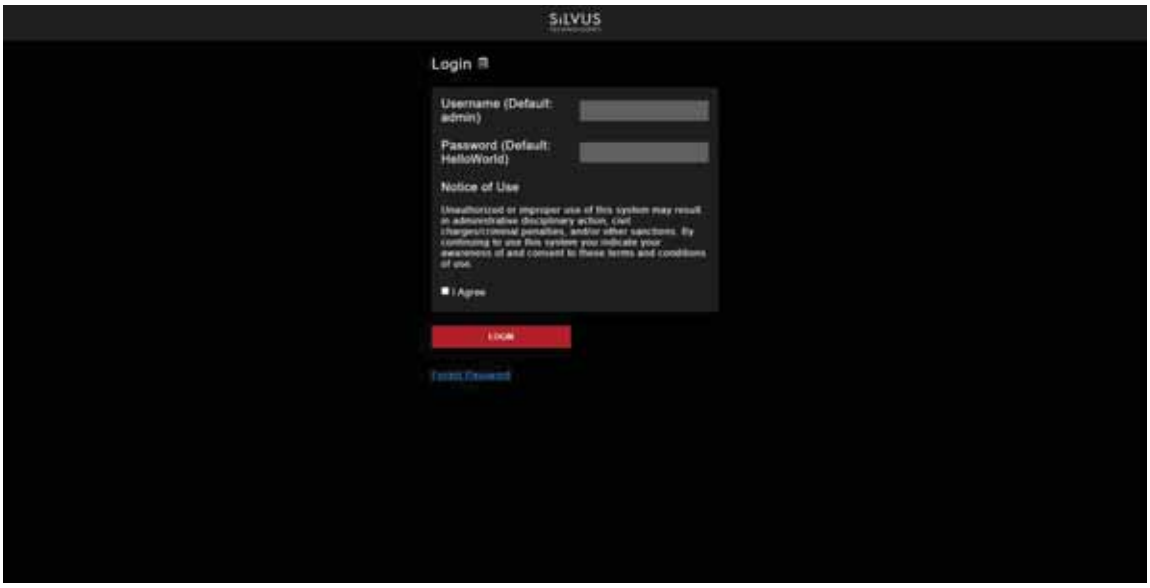


Figure 80 Login

Reset Password:

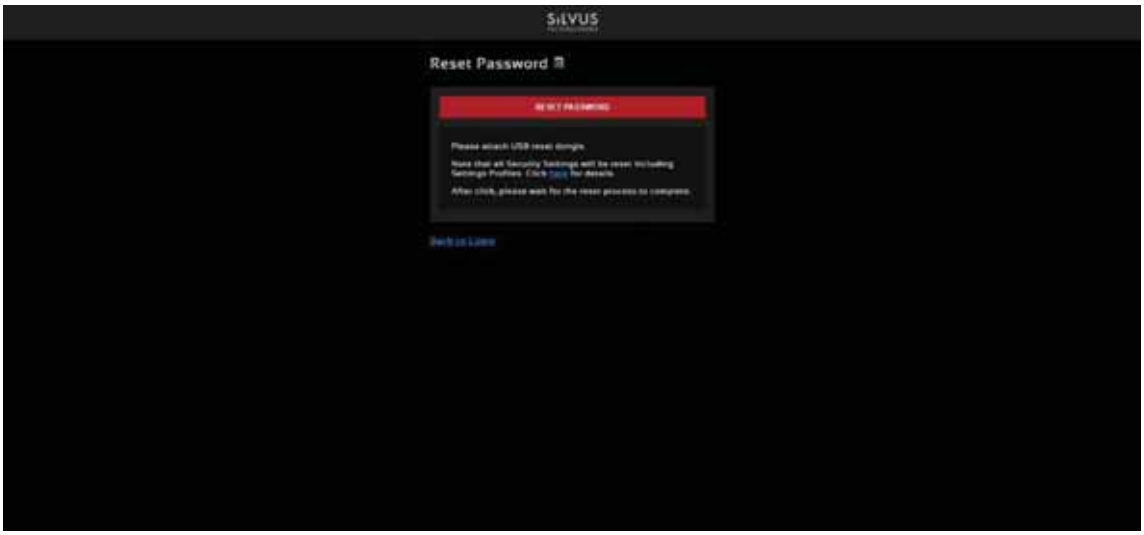


Figure 81 Reset Password

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.

5.5 Tools and Diagnostics

In this section, you will find the sections of the GUI that will provide you with details about the firmware version of the radio. You will also have the option to upload new firmware, as well as access some faults/indicators, factory reset, change languages, and a log tracking some security access to the radio.

5.5.1 Firmware and Licenses

5.5.1.1 Build Information

Figure 82 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. The current firmware version loaded on the radio will be listed under Build Tag line on this page.

5.5.1.2 Firmware Upgrade

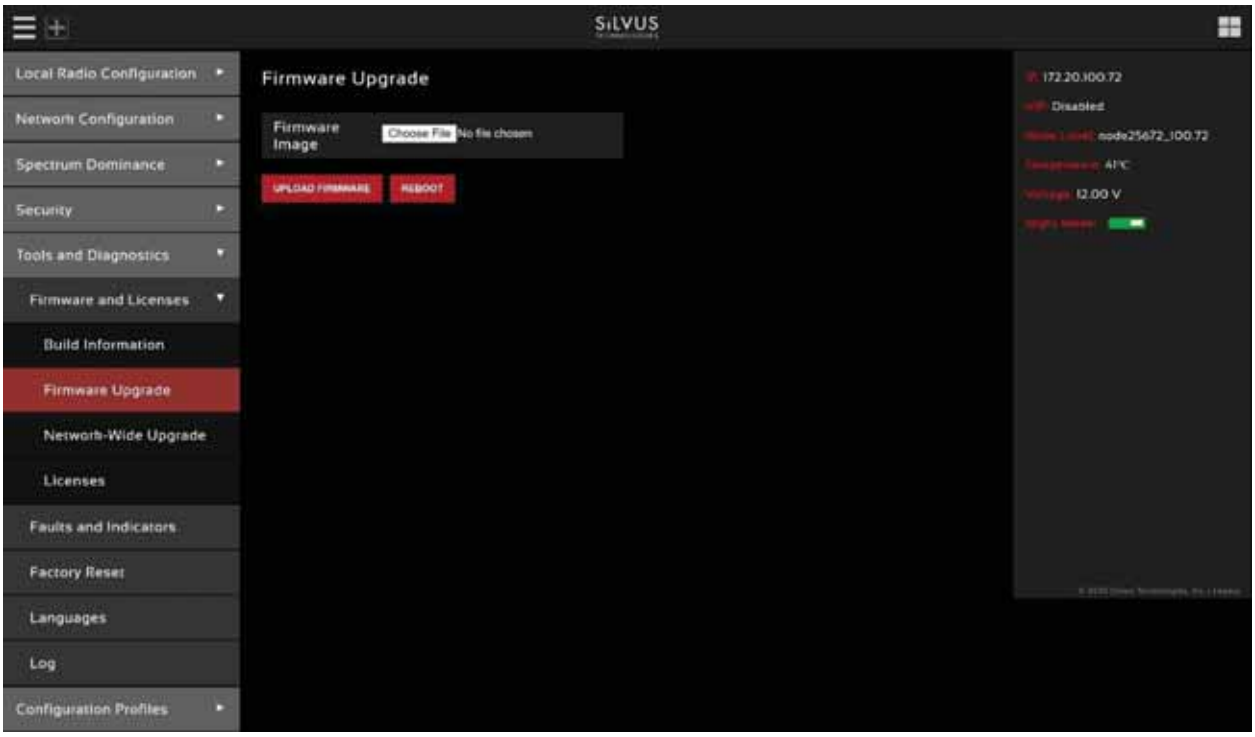


Figure 83 Tools and Diagnostics (Firmware Upgrade)

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.

5.5.1.3 Network-Wide Upgrade

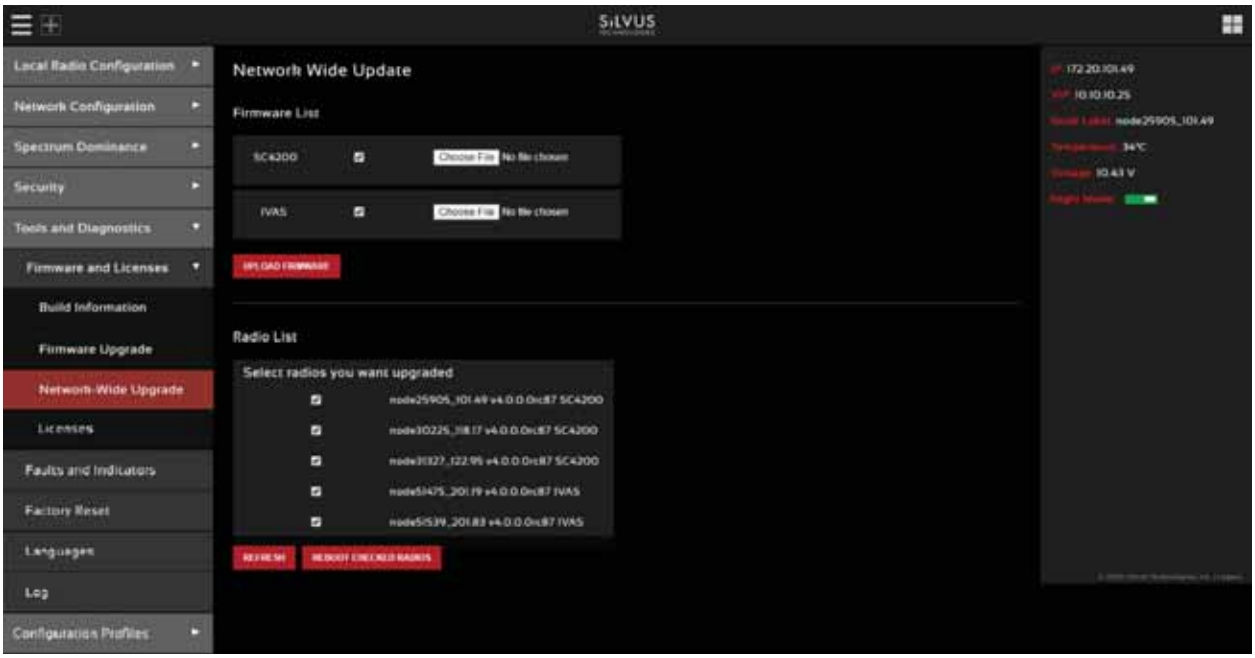


Figure 84 Tools and Diagnostics (Network-Wide Upgrade)

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.

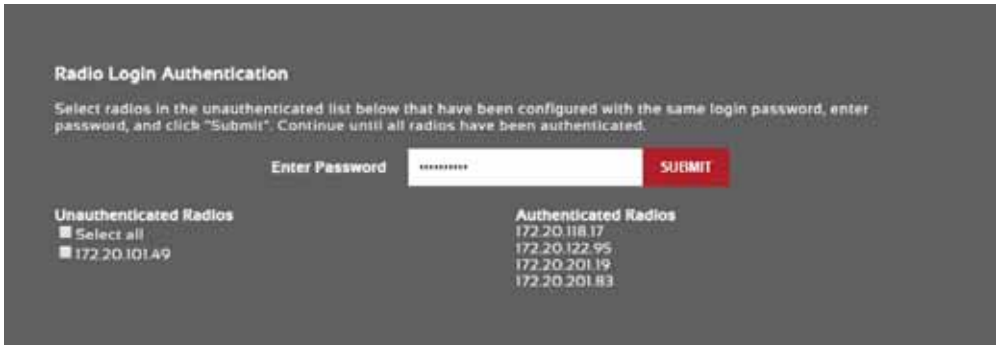


Figure 85 Radio Login Authentication during Network-Wide Upgrade

If you attempt a network wide update, and the login authentication is enabled on some radios, you will need to enter the radio's login authentication password in order to proceed. The window asking for the password can be seen on **Figure 85 Radio Login Authentication during Network-Wide Upgrade** above.

5.5.1.4 Licenses

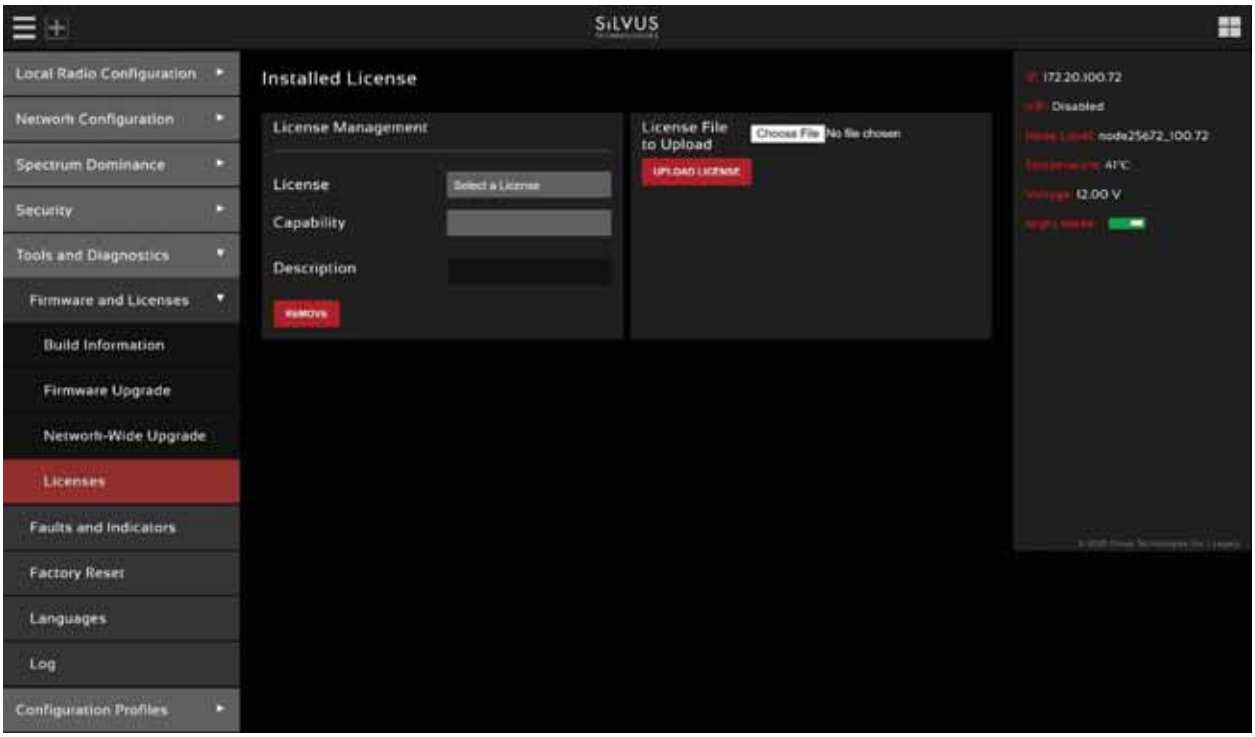


Figure 86 Tools and Diagnostics (Licenses)

Features such as encryption levels and frequency ranges can be enabled by licenses obtained from Silvus. New license keys can be uploaded to the radio on this page. Upload license button will load the license selected to the local radio only. The broadcast license button will load licenses to all radios on the network. Please note that the license files are targeted on an IP specific basis, so the license you use with this feature must incorporate all IP radios in the mesh. If there is a radio without the IP in that license, the upload will fail for that particular radio only.

5.5.2 Faults and Indicators

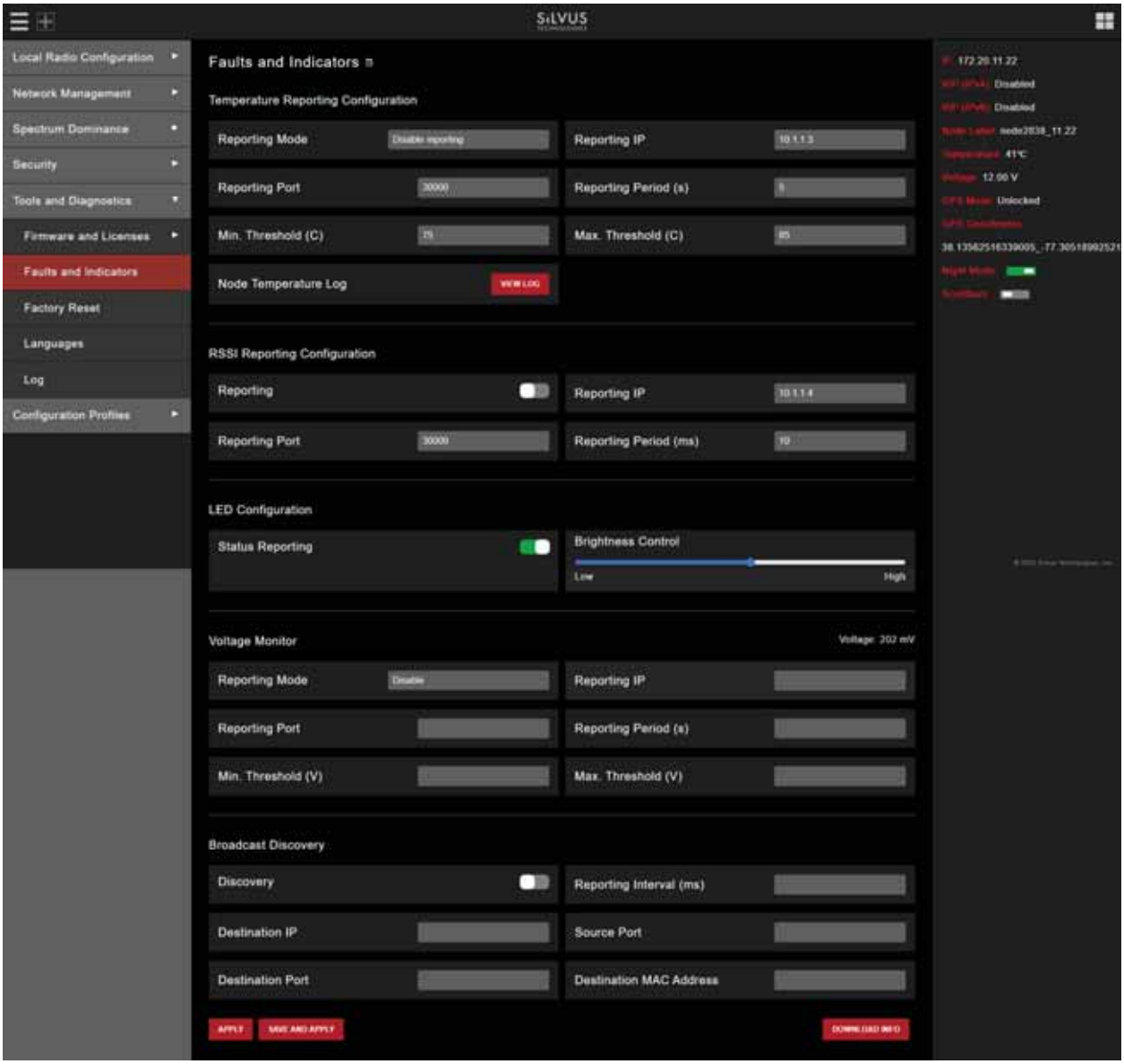


Figure 87 Faults and Indicators Page

The Faults and Indicators page allows the user to specify an IP and Port number for Temperature and RSSI (Receiver Signal Strength Indication) reports to be delivered to. This is useful for users that intend to feed this information into some other platform for analysis and recording. Section 9 gives more information on the format of streaming reports. You can also click on the node temperature log to open another window that shows the current output of what the temperature report would output.

Temperature Thresholds

In addition to receiving temperature reports, this page can be used to set minimum and maximum temperature thresholds for the radio. The StreamCaster™ family of radios is equipped with on board temperature sensors which are monitored to prevent overheating. Once a radio reaches the maximum temperature threshold, the radio will begin to reduce its transmission time until the temperature falls below the minimum temperature threshold. By default, the min and max values are 75C and 85C respectively.

RSSI Reporting Configuration

This setting allows the users to report the RSSI values every few milliseconds base on users setting.

LED Configuration

This setting allows the user to disable or enable the LED on the faceplate of the radio. Also has a slide bar to control LED brightness level.

Voltage Monitor

Radios built on or after Jan 1, 2015 have the ability to monitor the input voltage, displayed here.

Broadcast Discovery

This feature is used to send radio information packets periodically to a server. Information sent will include the node ID, virtual IP address, frequency, and bandwidth of the radio.

5.5.3 Factory Reset

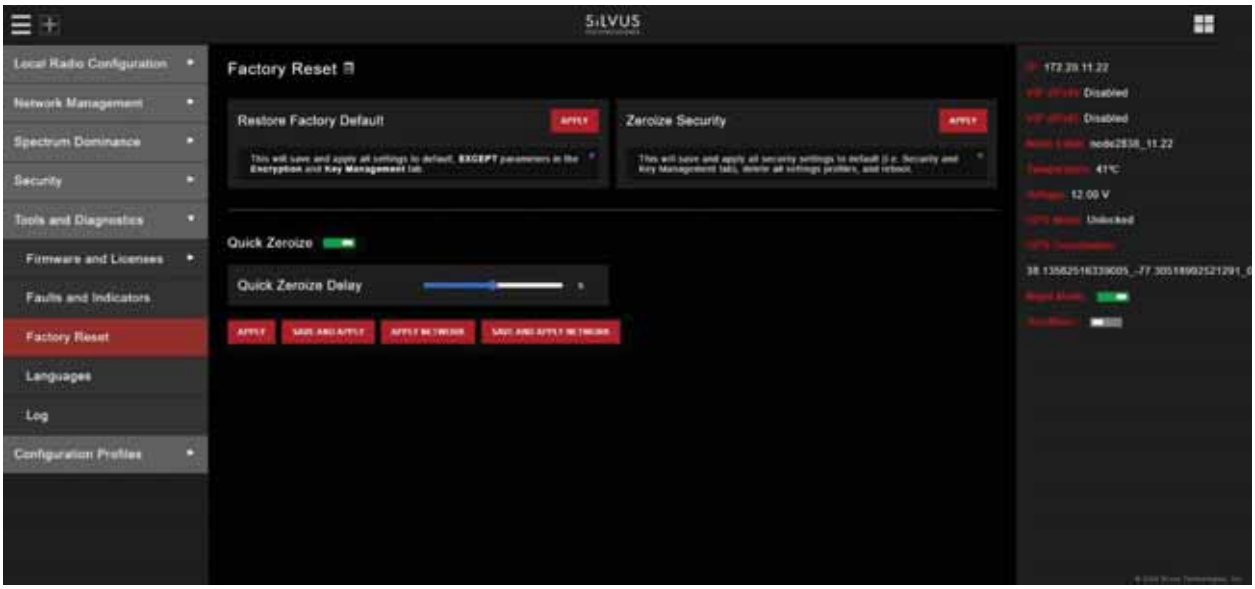


Figure 88 Tools and Diagnostics (Factory Reset)

- **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. Zeroize will require a reboot in order to ensure all settings are zeroized. If zeroize was initiated through the GUI, the radio will automatically reboot.

- **Quick Zeroize:** When enabled, the radio zeroize process will commence after the zeroize delay when the multi-position switch is turned to the "Z" position. When disabled the radio multi-position switch must be turned from the off position to "Z" during the boot sequence to initialize zeroize. The quick zeroize delay will wait to trigger the zeroize for the specified time.

5.5.4 Languages

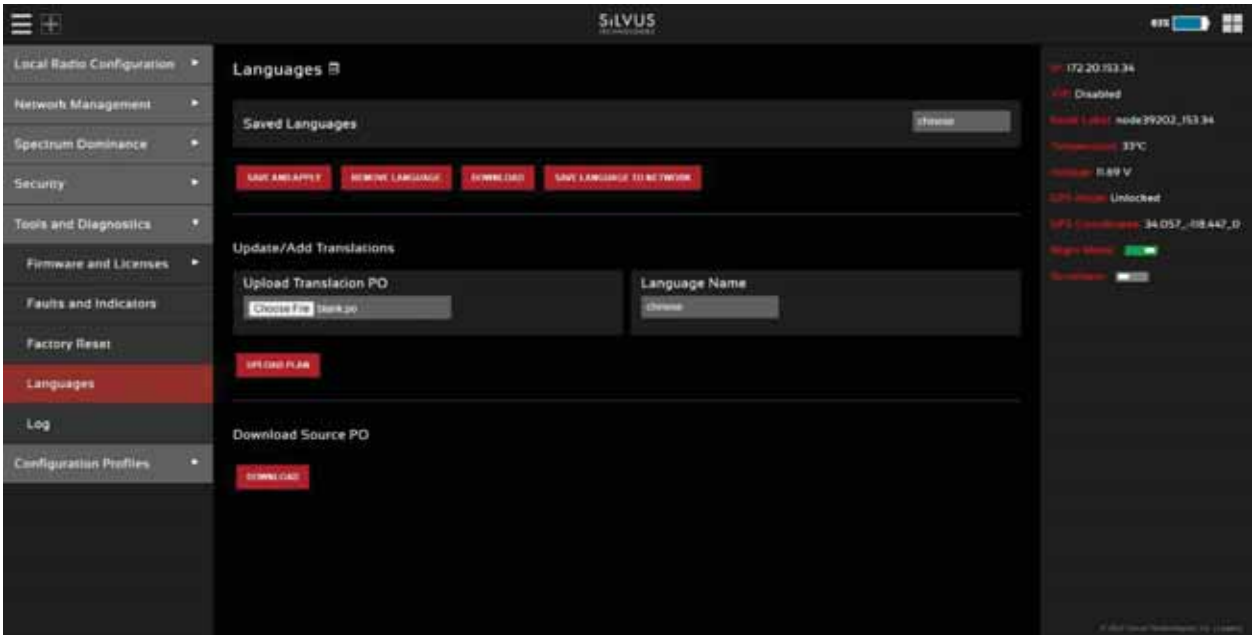


Figure 89 Tools and Diagnostics (Languages)

In this tab you will be able to edit and update the GUI into any language you choose. To do this, you would download the Source PO File as per the button on the bottom of this page. Once you have the source PO file, you can open it to edit in any plain text editor, however it may be easier to read in Notepad++.

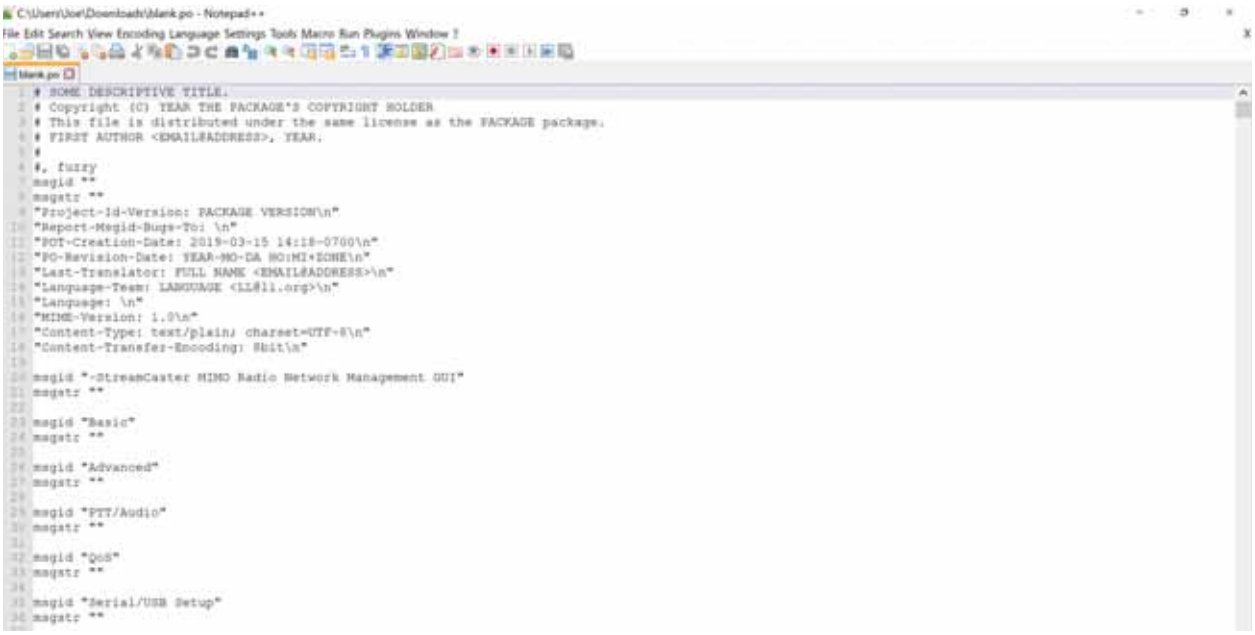


Figure 90 example Source PO file for custom languages

To create a language profile in another language other than English, please follow below steps:

1. Enter the translated words from msgid into the msgstr”” after the original word or phrase.
2. Save the revised source PO file
3. Enter the language you have translated the words for into the field labeled Language Name.
4. Click on choose file and select the source PO file that you revised and saved.
5. Click on upload plan.
6. After the plan has been uploaded, you should be able to select which language plan you would like to use under the drop-down menu of saved languages.
7. Select the language you would like viewed in the GUI, click save and apply.

To remove a previously saved language, please see below steps:

1. select the language that you want to remove from the drop-down menu of saved languages.
2. Click on remove language button to remove the selected saved language. That saved language will no longer be an option for you to view.

In order to download a previously loaded language file, see below steps:

1. Select the language file from the drop-down menu of saved languages.
2. Click on the download button. You will download the source PO file that is associated with the language you selected under saved languages.

When a new firmware edition for the Silvus radio is released, there may be new texts that will require updated language translation. In order to update the po file in a new firmware edition you would need to download the old translated file, then the new blank po file from the new firmware edition. The new appended entries should be seen at the bottom of the new po file. Copy paste these new entries to your translated file (append), and translate new entries.

5.5.5 Log

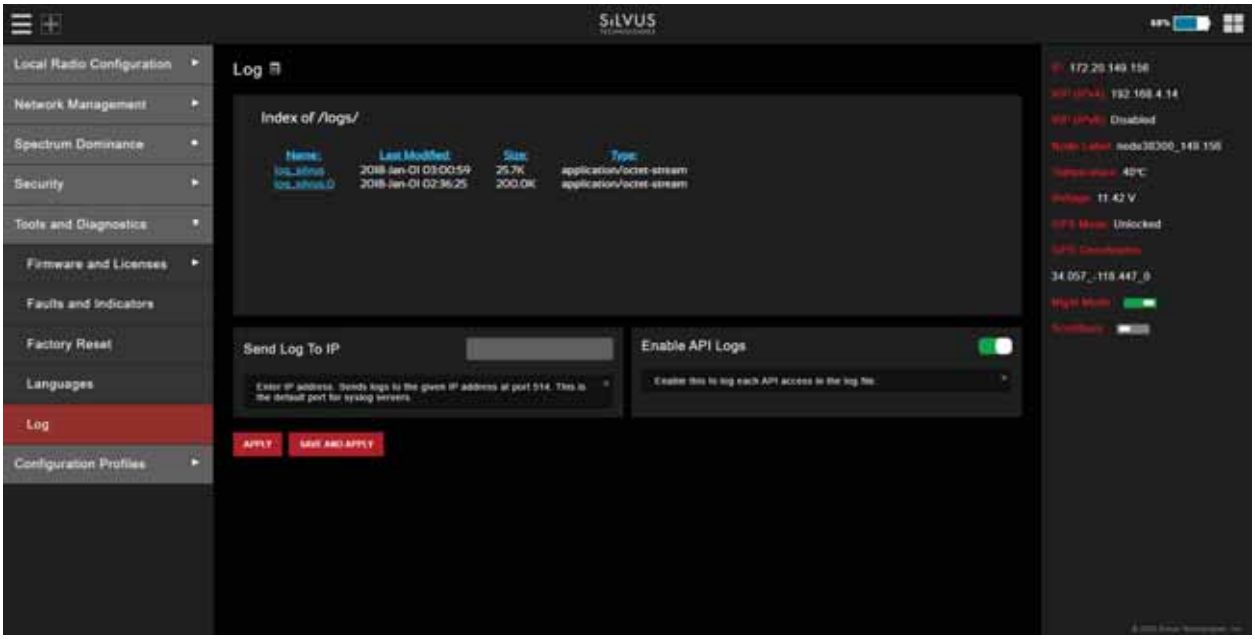


Figure 91 Security (Log)

The log tab tracks some security events that happen within the radio. Below is a list of events that the log keeps track of:

- Successful/unsuccessful login attempts when login authentication is turned on.
- Visits to the license tab (shown as secureinterface6.sh), upgrade tab (secureinterface3.sh) and encryption tab.
- Enable API log to include a detailed log of API access.

You can enter an ip address in the "Send Log to" text box. This will send the logs to that ip at port 514. It is compatible with Syslog servers.

Example of the log can be seen below.

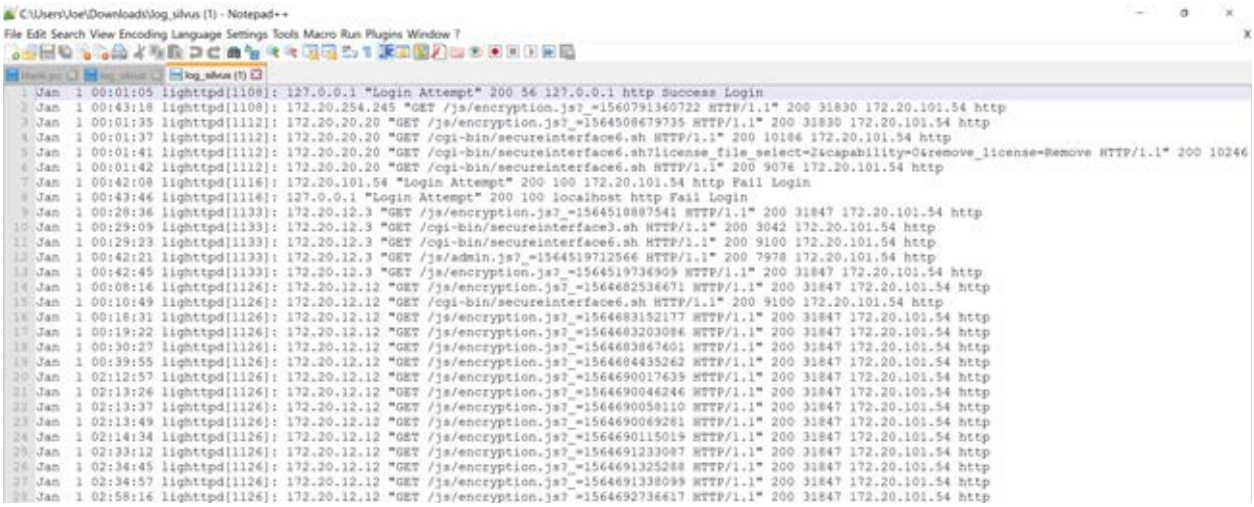


Figure 92 Example of security log

The first data listed in the log is the date and time that the occurrence happened. You can manually input the date and time of the radio under the Network Manager>Map Overlay tab under CoT feature. However, upon a reboot, the time will no longer be accurate.

Please disregard the lighttpd [xxxx] as this will be likely removed in updated firmware versions. The format of the details listed in the log after lighttpd [xxxx] is as follows:

"a b c d e http/https"
a = IP address of remote host
b = HTTP request-line
c = HTTP status code
d = bytes sent for the body
e = HTTP request host name

5.6 Configuration Profiles

Under the configuration profiles section you will be able to configure profile settings for the radio, and save them to a file to distribute to other radios. You will also be able to customize the multi-position switch in this section.

5.6.1 Settings profile

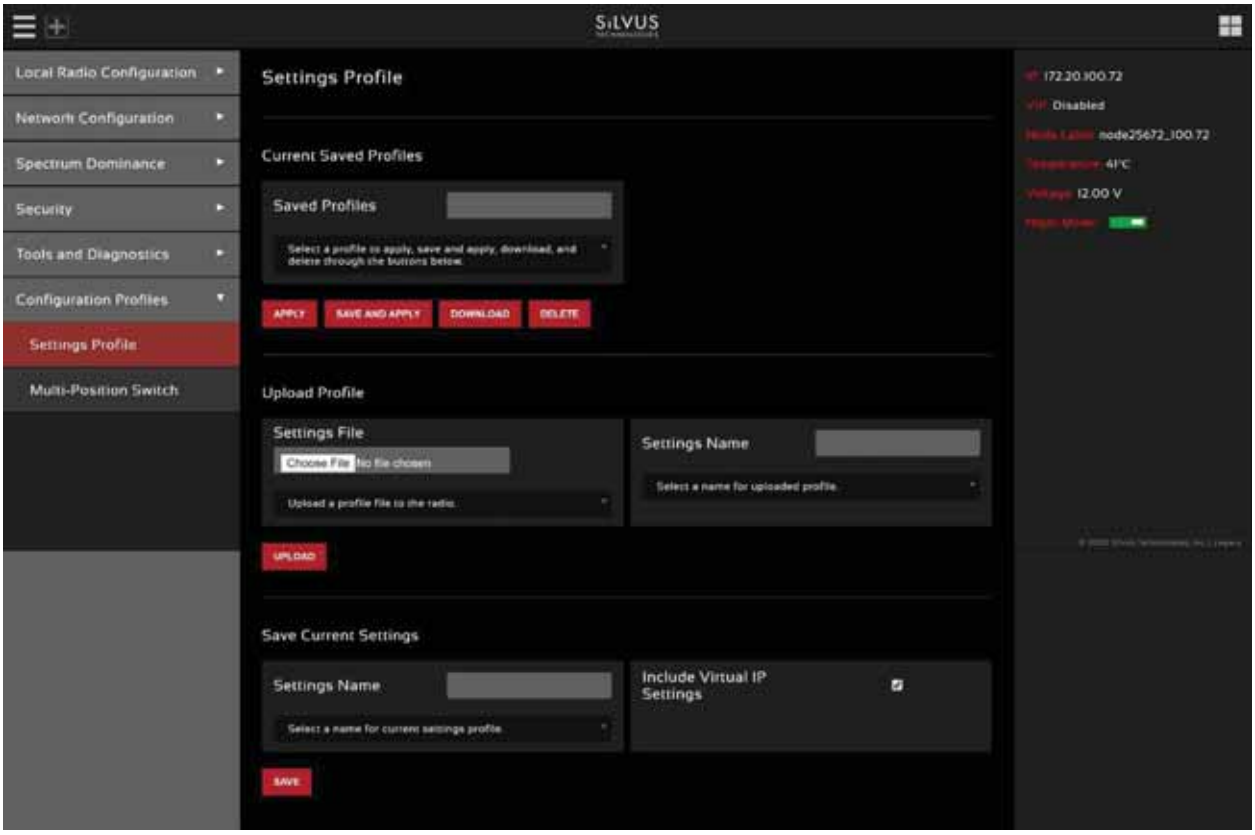


Figure 93 Configuration Profiles (Setting Profile)

- **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.

5.6.2 MPS (Multi-Position Switch) (not available on SL4200)

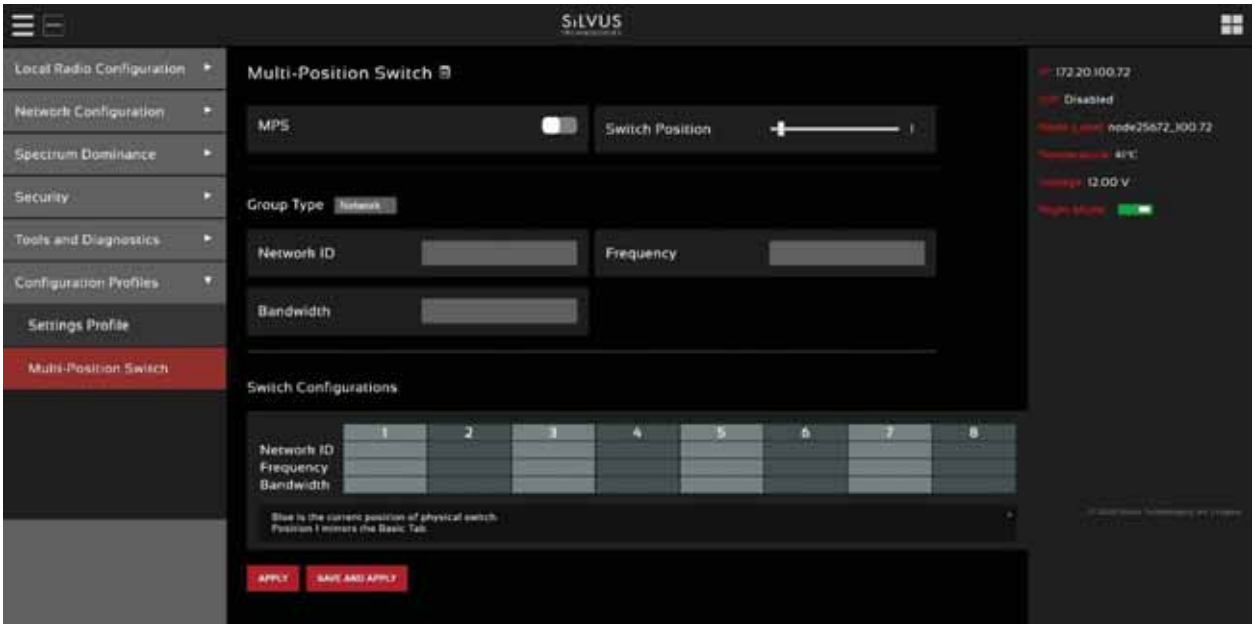


Figure 94 Multi-Position Switch

The Multi-Position Switch allows you to change various settings of the radio by using the new physical switch position, 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" (second to last position on the MPS), the radio will perform a physical MPS zeroize function. This action will reset all passwords, reset all settings in the Security tab to default, and performs a factory reset on all other settings. After zeroize has been completed, a radio reboot will be required to ensure all settings are zeroized.

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 5.4.4.1 Admin page.

3. Next go to Security -> SSH/HTTPS certificates. You must change the SSH Login Key, SSH Host Key, and HTTPS Certificate from their defaults. See section 5.4.2 under SSH/HTTPS certificates 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 the link label of “wired” and turn the link color black in order 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 80 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.

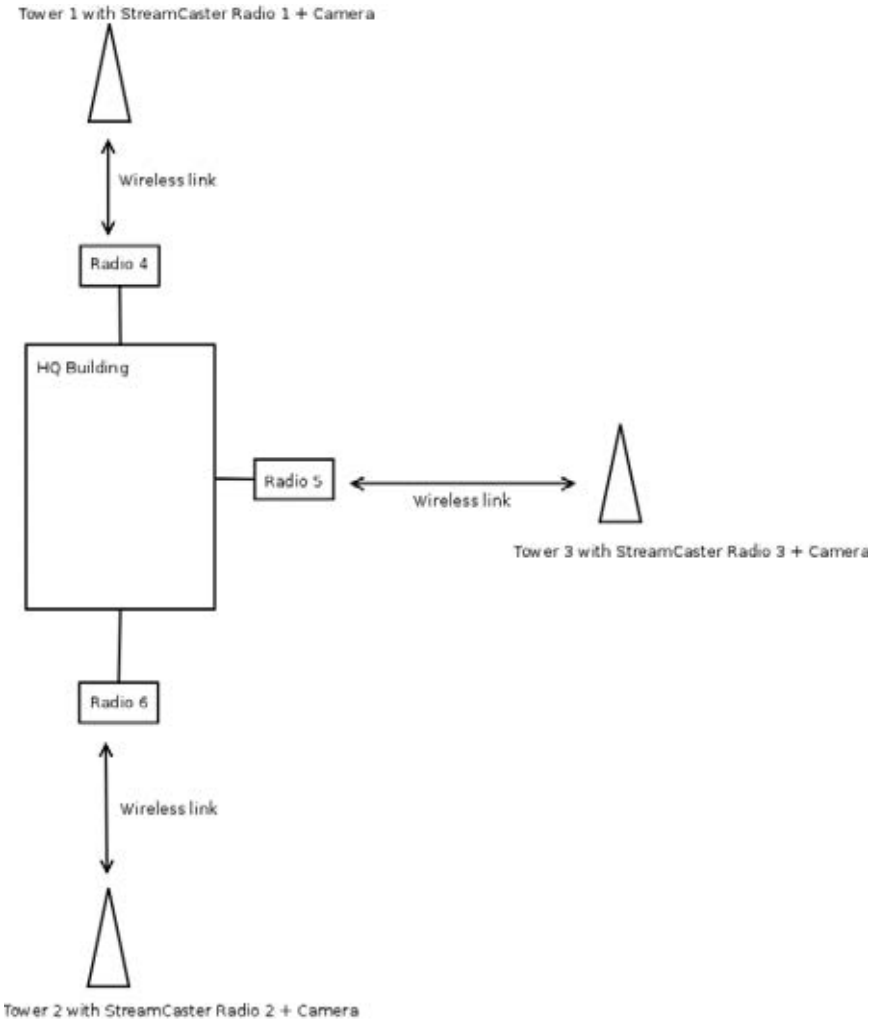


Figure 95 LAN Backbone Example

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 label of “wired” and turn the link color black in order to differentiate from 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 30 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.

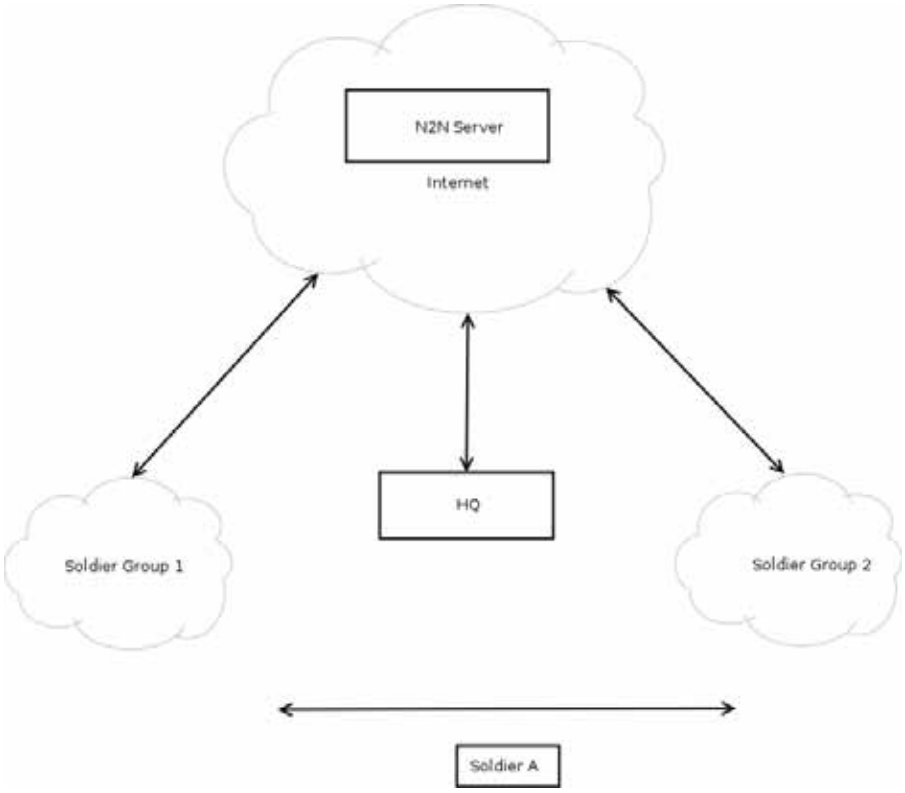


Figure 96 WAN Backbone Example

8. Custom Frequency Plan

8.1 Accessing and Installing CFP

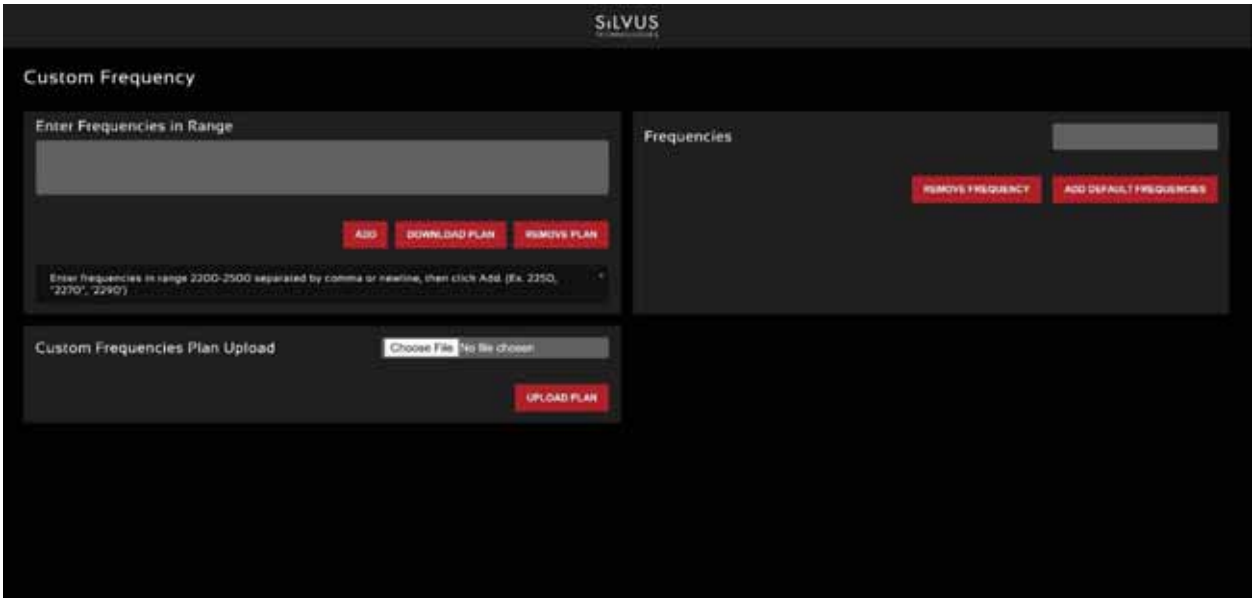


Figure 97 Custom Frequency Page

There are two ways to install the frequency plan. The first method is simpler. Users can simply click on *Create Custom Frequencies* below the frequency selection drop down to get to the custom frequency page shown in **Figure 97 Custom Frequency Page**.

- **Add:** Add the frequencies in the text box to the list
- **Download Plan:** Download the current frequency plan to a file that can be uploaded to other radios.
- **Remove Plan:** Removing the entire frequency plan. If this field is left empty, the radio will use the default frequency plan.
- **Remove Frequency:** Remove the currently selected frequency.
- **Add Default Frequencies:** The radios come with a list of default center frequencies. If you would like this list of default center frequencies in your custom list of frequencies, please select this button.
- **Custom Frequencies Plan Upload:** Upload a set of custom frequency plan from a file.

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
5011	String	172.20.xx.xx IP of radio
5012	String	Virtual IP of radio
5000	Integer	Raw signal power of first antenna, represented in full dBm steps.
5001	Integer	Raw signal power of second antenna represented in full dBm steps.
5002	Integer	Raw signal power of third antenna represented in full dBm steps.
5003	Integer	Raw signal power of fourth antenna represented in full dBm steps.
5004	Integer	Raw noise power represented in full 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 transmitter radio that triggered the receiver to send an RSSI report packet.
5008	32-bit integer	Report sequence number, increments for every report, resets after 9999.
1	Empty string ""	End of report.

Table 27 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 28 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 29 Temperature Reporting Format

9.3 Voltage Reporting

The type, length and value for voltage 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 voltage spiked above max threshold, as an integer string.

Table 30 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 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 FCC ID: N2S-SL42-245

Silvus model #: SL4210-245-SB

Equipment Class: Digital Transmission System

Antennas: 2.15 dBi Dipole Antennas (Silvus part# 1001-071)

Bandwidth: 1.25, 2.5 or 5MHz

Maximum 5MHz Bandwidth Output Power @ Frequency #1: 950.6mW @ 2412MHz

Maximum 5MHz Bandwidth Output Power @ Frequency #2: 862.98mW @ 2440MHz

Maximum 5MHz Bandwidth Output Power @ Frequency #3: 968.28mW @ 2462MHz

Maximum output power for 5MHz @ operating frequency spectrum should not exceed 27dBm/antenna

13.11 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 and must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

The user's manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.

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 SC4240E-206-BB

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, SC4240E-206-BB 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*!	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/ctu-ctu/rsup-p_06_09-2014-07_en_.pdf, new version is available 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 (Freq[*]) could be permitted for a limited time in accordance with §58 TKG. This is provided that the frequency usages indicated in the Frequency Ordinance (Freq[V]) 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*!	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*!	Cordless cameras, temporary use on a case- by-case basis. Standard EN 302064. Other use includes military use and space operation
	G	Y*!	Technology and application neutral but typically used for wireless cameras, typically licensed at 100 mW e.r.p.
	GEO	L*	
	GRC	L*!	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 ! – restrictions apply (e.g. geographical restrictions)

Table 31 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

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 SC4240E-206-BB
Additional information	SW version : v3.17.1.1 HW version : B7

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: 1-7-2020

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 SC24980-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 [identifier le dispostif par son numéro de certification d'ISED] 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.

16. MIC Japan Notice

16.1 ID: 211-210701

Silvus model #: SC4210P-245-O. Note that the SC4210P is a subset of the generic SC4200P, the "1" in the model # indicates it is a 1-watt maximum output power product or if lower the limits found by the MIC testing.

Equipment Class: 2.4GHz Band for Unmanned Mobile Image Transfer System

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

Antennas:

3dBi Omni Antennas (Silvus ABV3S235)

2.15dBi Omni Antennas (C-Astral OMNI2G4)

3dBi Omni Antennas (Silvus AO2D3S235F-SF)

3dBi Omni Antennas (Silvus AOM3S240F-SF)

1dBi Omni Antennas (Silvus AOV2D235515S-TM)

Bandwidth: 4.5MHz

Maximum 4.5MHz Bandwidth Output Power @ Frequency #1: 910mW @ 2486MHz

Maximum 4.5MHz Bandwidth Output Power @ Frequency #2: 870mW @ 2491MHz

Bandwidth: 9MHz

Maximum 9MHz Bandwidth Output Power @ Frequency #1: 880mW @ 2489MHz

Modulation and Coding Schemes tested: MCS0 to MCS15

16.2 ID: 011-210045

Silvus model #: SC4210P-576-O. Note that the SC4210P is a subset of the generic SC4200P, the "1" in the model # indicates it is a 1-watt maximum output power product or if lower the limits found by the MIC testing.

Equipment Class: 5.7GHz Band for Unmanned Mobile Image Transmission System

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

Antennas:

2.3dBi Omni Antennas (Silvus AOV2D235515S-TM, also Southwest Antenna 1001-253)

2.15dBi Omni Antennas (Silvus AOV2S520G-TM, also Southwest Antenna 1001-128)

2.15dBi Omni Antennas (C-Astral OMNI5G7)

3dBi Omni Antennas (Silvus AO2D3S)

3dBi Omni Antennas (Silvus AOV3T245515575-TM, also L-Com HG2458RD-TM)

Bandwidth: 4.5MHz

Maximum 4.5MHz Bandwidth Output Power @ Frequency Low: 29.78dBm @ 5625.5MHz

Maximum 4.5MHz Bandwidth Output Power @ Frequency Mid: 29.8dBm @ 5702.5MHz

Maximum 4.5MHz Bandwidth Output Power @ Frequency High: 29.76dBm @ 5752.5MHz

Bandwidth: 9MHz

Maximum 9MHz Bandwidth Output Power @ Frequency Low: 29.72dBm @ 5655MHz

Maximum 9MHz Bandwidth Output Power @ Frequency Mid: 29.82dBm @ 5695MHz

Maximum 9MHz Bandwidth Output Power @ Frequency Low: 29.82dBm @ 5750MHz

Bandwidth: 19.7MHz

Maximum 19.7MHz Bandwidth Output Power @ Frequency Low: 29.6dBm @ 5660MHz

Maximum 19.7MHz Bandwidth Output Power @ Frequency Mid: 29.74dBm @ 5700MHz

Maximum 19.7MHz Bandwidth Output Power @ Frequency High: 29.66dBm @ 5745MHz

Modulation and Coding Schemes tested: MCS0 to MCS15

16.3 Software License

A Software License is used to ensure only parameters and limits that are allowed by the MIC certificates shown in sections 16.1 & 16.2 can be selected. These parameters include Frequency, Output Power, Modulation and Bandwidth.

16.4 Firmware Encryption

The details of our Firmware Encryption are considered proprietary and are discussed in depth in the submitted document SC4210P-576-O Circuit Description v1.3 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 MIC certificate shown in section 16.1 & 16.2 can be selected.