

BlueTOAD[®] Spectra[™] CV

User Guide



© 2026 COPYRIGHT ITERIS, INC.

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the prior written permission of Iteris, Inc.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit, or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

The information contained in this document is subject to change without notice.



SOFTWARE LICENSE AGREEMENT

License Grant

DO NOT USE OR LOAD (AS APPLICABLE) THE SOFTWARE (DEFINED BELOW) UNTIL PURCHASER READS CAREFULLY THE FOLLOWING TERMS AND CONDITIONS. BY LOADING OR USING THE SOFTWARE, PURCHASER AGREES TO THE TERMS OF THIS AGREEMENT. IF PURCHASE DOES NOT AGREE WITH THIS AGREEMENT, DO NOT INSTALL OR USE THE SOFTWARE.

Iteris, Inc. ("Iteris") hereby grants a personal non-exclusive, nontransferable (except as expressly provided herein) license to the purchaser ("Licensee") of its Iteris Vantage® and/or Spectra™ ("System") to use the Iteris supplied software programs, algorithms, or firmware, and any updates, upgrades, enhancements or modifications thereto, whether delivered electronically or otherwise ("Software") and any User Documentation accompanying the Software ("Documentation") for its use, subject to the terms and conditions hereof, in conjunction with the Iteris System.

By purchase of the System, Licensee agrees to the terms of this Software License Agreement ("Agreement").

Iteris (and its suppliers) retains title to and ownership of the Software and Documentation, including all intellectual property rights (e.g., patents, copyright, trade secrets). Except for the express licenses granted under this Agreement, no other rights or licenses of any kind or nature are granted, either express or implied, to Licensee under any Iteris (or its suppliers) patents, copyrights, trademarks, or other intellectual property rights.

The Licensee may not either (i) copy or otherwise reproduce the Software or Documentation without prior written permission of Iteris, (ii) modify, decompile, disassemble or reverse engineer the Software or any part thereof, or attempt to do so, without the express written consent of an authorized officer of Iteris, (iii) remove any copyright or other proprietary notices from the Software, or (iv) except as set forth herein, may not rent, lease, sublicense, distribute or otherwise transfer the Software or Documentation. The Software and Documentation is licensed for use only in conjunction with the Iteris System. Use of the Software or Documentation in conjunction with non-Iteris products is not licensed hereunder.

Term of License

The License shall be effective from the date of shipment of the System and Software and shall remain in effect for the life of the System (subject to the terms and conditions of this Agreement) unless terminated sooner as provided in this Agreement. This Agreement terminates automatically if the Licensee fails to comply with any of the terms or conditions of this Agreement. Upon such termination, Licensee shall return Software and Documentation (including all permitted copies) to Iteris. Upon termination, Licensee will immediately stop using the Software and Documentation and destroy the Software and Documentation.

Provision for Transfer of License

In the event that substantially all of the assets of Licensee are sold, which transfer includes the System, to a third party ("transferee") and the System remains at the same location, this Agreement, including all the rights of Licensee herein, shall transfer automatically to the transferee provided that written notice of such transfer is given to Iteris and the transferee gives written notice to Iteris of its approval of this transfer of Agreement (contact Product Support Team, as described below, to begin this process).

In the event that the System is sold or transferred to a third-party, other than as set forth in the immediately preceding paragraph, the third-party transferee shall apply in writing to Iteris' Service Manager (contact Product Support Team, as described below) for approval of the transfer of the licenses under this Agreement. A license to use the Software installed in the System at the time of the sale or transfer shall be granted to the transferee, at no charge, provided the transferee gives written notice to Iteris of its approval to transfer the licenses under this Agreement.

In the event that the System is financed or leased, this Agreement may be assigned to the lessor or the third-party providing such financing, provided that (i) the financing arrangement or lease includes the complete System, (ii) prior written notice of such financing or lease is given to Iteris, and (iii) the party providing such financing or leasing gives written notice to Iteris of its approval of the Agreement. Any subsequent disposition of the System by such party shall be made subject to the terms of this Agreement, including the requirements set forth in the preceding paragraphs.



In the event of transfer or assignment of the System, the original Licensee shall retain no right to use the Software or Documentation, and all copies thereof shall either be delivered to the transferee or destroyed.

Software Limited Warranty

For a period of three years from the date of delivery of the System to the Licensee, Iteris warrants (i) that the Software will conform, in all material respects to the functional capacities described in the Documentation, provided that the Software is used as instructed; (ii) that the Documentation contains the necessary information to utilize the Software; and (iii) that the media on which the Software is supplied shall be free from defects in material and workmanship. In no event does Iteris warrant that the Software is error free or that Licensee will be able to operate the Software or System without problems or interruptions.

EXCEPT FOR THE LIMITED WARRANTY SET FORTH ABOVE, THE SOFTWARE AND THE DOCUMENTATION IS PROVIDED "AS IS." ITERIS MAKES NO OTHER WARRANTY, EITHER EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFTWARE AND/OR DOCUMENTATION AND SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ITERIS DOES NOT WARRANT THAT THE SOFTWARE AND/OR THE USER DOCUMENTATION WILL MEET SPECIFIC USER REQUIREMENTS OR EXPECTATIONS OR THAT THE OPERATION OF THE SOFTWARE SHALL BE UNINTERRUPTED AND/OR ERROR FREE.

Licensee's exclusive remedy and the entire liability of Iteris and its suppliers under this Software limited warranty will be, at Iteris' option, repair, replacement or refund of the Software portion, if report (or, upon request returned) to the party supplying the System to Licensee. Some states do not allow the exclusion or limitation of implied warranties, so the above exclusions and limitations may not apply. This limited warranty gives the Licensee specific rights, and there may be additional rights which vary from state to state.

Iteris' Responsibility

During the two-year warranty period and so long as Licensee is not threatening or actually in breach of the terms and conditions of this Agreement, if Iteris releases a general Software upgrade and Documentation revision ("Upgrade") to its other customers under the same conditions through its then-standard delivery process, Iteris shall provide the Upgrade to the Licensee at no additional charge. Iteris has sole discretion to provide a general Software Update or whether a specific Software Upgrade will be made and what constitutes a general release of such Upgrade as opposed to a limited release. Iteris does not imply or guarantee that a general Software release will be made by Iteris. Any such Upgrade shall be subject to the terms of this Agreement but shall not extend the original term of the limited Software warranty.

In order to ensure Iteris Customer Service Support, Licensee shall be required to maintain the System and the Software at the most recent, compatible versions. Iteris Customer Service Support will support only the current general Software releases. See additional resources below for Iteris Customer Service Support contact information.

Limitation of Remedies and Liability

The Software limited warranty shall not apply to any defect, failure or damage caused by (i) improper installation, (ii) improper use of the Software or System, (iii) accident, (iv) persons other than Iteris tampering, modifying or altering the Software or System; and (v) other reasons beyond Iteris' reasonable control.

Under no circumstances, and notwithstanding any failure of the essential purpose of any limited remedy provided for herein, shall Iteris be liable to the Licensee for any damages, claims or losses whatsoever, including but not limited to lost profits, lost savings or other special, incidental or consequential damages arising out of the use or inability to use the Software, Documentation, and or the System regardless of the circumstances. In no case shall Iteris' (or its suppliers') liability exceed the purchase price of the System.

Controlling Law

This Agreement shall be governed and construed according to the laws of the State of California without regard to principles of conflict of laws. However, if Licensee is a government body or agency, this Agreement shall be governed by and construed according to the laws of the state in which the Licensee is located without regard to the principles of conflict of laws.

Severability

In the event that any provision of this Agreement shall be deemed unenforceable or invalid, such unenforceability or invalidity shall not render this Agreement unenforceable or invalid as a whole, and the remainder of this Agreement shall remain enforceable and valid. The court or



determining body shall enforce and interpret the remainder of this Agreement so as to best accomplish the intended objectives and economic effects of the Agreement.

Entire Agreement

The Licensee acknowledges that he has read this Agreement, understands it and that it is the complete and exclusive statement of agreement with Iteris which supersedes any prior agreement, oral or written, between the Licensee and Iteris. No variation of the terms of this Agreement will be enforceable against Iteris unless Iteris gives its express written consent specifically intended to amend this Agreement and signed by a duly authorized signatory of Iteris.

Notwithstanding the foregoing, in the event Licensee purchases Subscription Services (defined below), such services are subject to a separate agreement that Licensee will be required to accept and agree, and nothing in the Subscription Services agreement shall be construed to modify the terms and conditions of this Agreement for other products and services subject to this Agreement. "Subscription Service(s)" means an Iteris-branded service offering, of which access and use is subject to a subscription fee, including without limitation, Iteris VantageLive!®, VantageCare®, VantageARGUS CV™, and all respective subsequent variations and versions.

U.S. GOVERNMENT RESTRICTED RIGHTS

The Software and Documentation are "commercial items" as that term is defined at 48 CFR 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in 48 CFR 12.212. Consistent with 48 CFR 12.212 and 48 CFR 227.7202-1 through 227.7202-4, U.S. Government end users acquire the Software and Documentation with only those rights set forth herein. Contractor/manufacturer is Iteris, Inc., 1700 Carnegie Ave., Suite 100, Santa Ana, CA 92705.

© Copyright 1998-2026 Iteris, Inc. All rights reserved.



Table of Contents

License Grant	3
Term of License	3
Provision for Transfer of License	3
Software Limited Warranty	4
Iteris' Responsibility	4
Limitation of Remedies and Liability	4
Controlling Law	4
Severability	4
Entire Agreement	5
U.S. GOVERNMENT RESTRICTED RIGHTS	5
Glossary	6
Introduction	10
Purpose	11
Components of the BlueTOAD Spectra and BlueTOAD Spectra CV	11
General Roadside Device Deployment Guidelines	12
Pre-Installation Testing	13
BlueTOAD Spectra CV Installation Procedures	14
Purpose	15
Supporting Equipment	15
Setup and Configuration Procedures	15
Layout Guidelines	15
Pre-Install Evaluation and Setup	16
How to Set Up the Traffic Controller Before Field Deployment	17
Configuration Procedures – using Browser-Based Configuration Utility	19

Configuration Settings Page.....	19
RSU Basic Settings.....	20
Advanced Network Settings	22
Active Message and Immediate Forward Settings	22
Stored Active Messages.....	23
Immediate Forward Settings	23
Intersection Settings	24
Signal Group Mappings	26
WSA Settings.....	27
Security Settings	27
Forward Message Settings.....	31
Advanced Config Settings	32
Status Menu	37
GNSS Detail.....	39
System Activity	39
Radio Detail	40
SPAT Detail	40
Ethernet Status	42
Advanced Status	43
Utilities.....	44
System Reboot.....	45
Firmware Update.....	45
Revert to Factory Defaults	47
Customer Defined Configuration.....	48
LED Test Utility.....	48

Device ID Utility	49
System Event Log	49
BlueTOAD Spectra Setup Procedures	50
Purpose.....	51
Supporting Equipment	51
System Setup Procedures	51
Pre-Install Evaluation	51
Network and Communications Setup Parameters	51
Traffic Network – Evaluate the existing network.....	52
How to Configure the BlueTOAD Web IP.....	52
BlueTOAD Web IP Configuration Menu.....	53
Installation & Maintenance of BlueTOAD Spectra (CV).....	53
Guidelines to install an RSU enclosure:.....	54
Testing a BlueTOAD Spectra RSU After Field Installation	58
Confirm Network Connectivity and Data Collection	59
Troubleshooting.....	60
Record Keeping.....	61
Data and Device Management via VantageARGUS CV	61
On-Going Operations / On-Going Customer Support	62
Appendix 1 – BlueTOAD Spectra RSU, Recommended Network Configuration	
Implementation Requirements	62
Local Network Settings	63
Network Overview Diagram	63
BlueTOAD Spectra RSU Communications Protocols and Usage Guide	63
Device Access - User Interface, terminal sessions, and file transfers	64

Agency Network Access for Data Management	64
Appendix 2 – BlueTOAD Spectra RSU C-V2X5.9 GHz Spectrum Specifications	65
Iteris C-V2X Roadside Unit – FCC Individual Device RSU License Details	66
Iteris RSU – Specifications	66
Standards Compliance	66
V2X Security.....	66
C-V2X	67
Power Specifications.....	67
Power over Ethernet (PoE)	67
Operating Temperature Range	67
Processor	67
Interface Options.....	67
Dual antenna supports two modes:.....	67
Antennae	68
Appendix 3 – Connected Vehicle In-Cabinet Processor Specifications	68
Specifications.....	69
Basic Iteris In-Cabinet Processor Setup Information	70
How to Configure the In-Cabinet Processor.....	70
Please contact Iteris Support for further information and/or assistance:	70
Appendix 4 – How to Create an RSU MAP File	70
Objective.....	71
Material Requirements.....	71
Map File Creation Procedure.....	71
Appendix 5 – How to Retrieve an Unknown BlueTOAD Spectra RSU IP Address....	81
Use Wireshark to Retrieve the BlueTOAD Spectra RSU assigned IP Address.....	82

Main Window, Packet List Pane Column Definitions	83
Appendix 6 – BlueTOAD Spectra CV RSU Site Requirements Form	83
System Evaluation Checklist	84
Appendix 7 - Regulatory Information	88
FCC Compliance Statement	88
FCC Label Information	88
FCC Part 15.21 – Modification Warning	88
FCC Part 15.25 – Operation Within Authorized Frequency Bands	88
FCC Part 15.27 – Special Operating Conditions	88
RF Exposure Information	88

Glossary

In the glossary below, terms are listed in alphabetical order along with their meanings. Below is an example of acronyms used in text.

Example: In the future, each automobile will be a Connected Vehicle (CV) equipped with an Onboard Unit (OBU) that will communicate with the external traffic infrastructure.

Term	Meaning
AGL	Above Ground Level
ATIS	American Traveler Information Systems
AWS	Amazon Web Services
VantageARGUS CV	Web-based software to monitor BlueTOAD detectors
BlueTOAD	Bluetooth® Travel time Origin And Destination
BSM	Basic Safety Message—every 0.10 second, a connected vehicle (CV) broadcasts its vehicle type, speed, location, direction and approach relative to an intersection.
CAT-5 Cable	Category 5 cable, a twisted pair cable for computer networks. The cable standard provides performance of up to 100 MHz and is suitable for 1000BASE-T (Gigabit Ethernet). This is also called an “Ethernet Cable” or a “LAN Cable.”
CV / CAV	Connected Vehicle / Connected and Autonomous Vehicles
C-V2X	Cellular Vehicle to Everything – Use of chipset for 5.9 GHz spectrum communications
Discoverable/ Non-Discoverable	Discoverable = Bluetooth device searching to Pair with another Bluetooth device Non-Discoverable = two Paired Bluetooth devices
DNS UDP	Domain Name System—a hierarchical and decentralized naming system for resources connected to the Internet or a private network. User Datagram Protocol—an alternative comm protocol to TCP
DSRC	Dedicated Short Range Communications
Egress	Going out of (leaving) an intersection
EIRP	Effective Isotropic Radiated Power
EMAC	Ethernet Media Access Controller
ERM	Event Reporting Message
FCC	Federal Communications Commission

Term	Meaning
Free-TEXT	Custom text you type to create a message or part of a message for a TIM
GPS	Global Positioning System
HTML	Hypertext Markup Language
IEEE	Institute of Electrical and Electronics Engineers
Index-phrase	Standard text used create a message or part of a message for a TIM, defined by ITIS and assigned a code number—whose meaning is known internationally.
Ingress	Going into (entering) an intersection
IoT	Internet of Things
IP address	Internet Protocol address—host or network interface identification and location addressing
ITIS	International Traveler Information Systems. For ITIS phrase lists to use in creation of TIMs, use SAE publication SAE J2540-2. To order a copy, go to https://www.sae.org/standards/content/j2540_200207/
ITS	Intelligent Transport System
LAN/WAN	Local Area Network/Wide Area Network
MAP	Map Data Message— intersection geography and line definitions of the intersection or street. An RSU transmits one MAP message per second to OBUs.
MIB	Management Information Base (MIB), an 'object' that resides within the device in a database is uniquely identified with an object identifier (OID)
NTCIP	National Transportation Communications for Intelligent Transportation System Protocol
NTCIP 1202 Support	ITS Standard NTCIP 1202 Object Definitions used for communication with Actuated Traffic Signal Controller (ASC) Units
NTP	Network Time Protocol
OBU	Onboard Unit
O/D	Origin/Destination
OID	Simple Network Management Protocol (SNMP) Object Identifier (OID) is an address used to uniquely identify managed devices
Omni-directional	Receiving signals from or transmitting in all directions
PCB	Printed Circuit Board
PoE	Power over Ethernet
PuTTY	SSH Client terminal program for Microsoft Windows

Term	Meaning
RDS	Radio Data Service (on FM 57 kHz subcarrier)
RJ-45 Port	Registered Jack (RJ) is a standardized telecommunication network interface
RSU	Road Side Unit
RTCM	Radio Technical Commission for Maritime services. In the United States, the Federal Communications Commission uses RTCM standards to specify Differential GPS systems for C-V2X.
SCMS	Security Certificate Management System—developed by a consortium of automakers and the United States Department of Transportation (USDOT) as a vehicle-to-vehicle (V2V) security system in the United States.
SNMP	Simple Network Management Protocol—used to monitor and manage devices on networks. Typically, SNMP uses User Datagram Protocol (UDP) transport layer (layer 4) as its transport protocol.
SPaT	Signal Phase and Timing
SRM	Signal Request Message
SSH Client	A software program which uses the Secure Shell protocol to connect to a remote computer.
SYSLOG	A way for network devices to send event messages to a logging server, known as a Syslog server
TCP	Transmission Control Protocol
TIM	Traveler Information Message—delivered to Connected Vehicles and Mobile App—a personal message board about local conditions. TIMs describe traffic-related events of interest to travelers and other traffic practitioners.
TIM Zone	A geographic area in the shape of a Polygon, Polyline or Circle, defined to receive TIMs
TMC	Traffic Management Center
UPER	Unaligned Packed Encoding Rules
URL	Uniform Resource Locator
Users	Authorized access through secure login to software application
WAVE	Wireless Access in Vehicular Environments
WinSCP	File transfer application
WSA	WAVE Service Advertisement messages

Introduction

Purpose

This *User Guide* outlines procedures to deploy Iteris BlueTOAD Spectra or BlueTOAD CV Connected Vehicle Roadside units or combined BlueTOAD Spectra CV devices. Included are procedures to confirm network connectivity and traffic data collection. *Chapter 3* thru *Chapter 5* explain how to deploy the BlueTOAD Spectra CV RSU. *Chapter 6* thru *Chapter 13* are Appendices, which contain supplemental system documentation.

The tables below describe the four BlueTOAD Spectra roadway sensor units and give their main features.

BlueTOAD Unit	Function
Spectra - Ethernet PoE	Detects and transmits Data for Speed and Travel Time
Spectra - Ethernet Cellular PoE	
Spectra - Solar Cellular	
CV - Ethernet PoE	Roadside unit for receiving and sending V2X messages
Spectra CV - Ethernet PoE	Receives and transmits Bluetooth Detection, and V2X messages

Components of the BlueTOAD Spectra and BlueTOAD Spectra CV

The table below shows hardware and software accessories for each of the four BlueTOAD Spectra units.

Item	BlueTOAD Spectra			BlueTOAD Spectra Roadside Units
	Ethernet PoE	Ethernet Cellular PoE	Solar Cellular	
PoE Injector + Power Supply	X	X		X
Shielded CAT-5 or CAT-6 Cable	X	X		X
Mounting Bracket + Fasteners	X	X	2	X
Cable Band	X	X	2	X
Solar Panel + Mounting Hardware			X	
Battery			X	
VantageARGUS CV Software	X	X	X	X
Support for Traffic Controller SPAT data (see next table)				X

An “X” under a unit indicates that the related **Item** is a component of that unit.

A “2” under a unit indicates that there are two of the related **Items** in that unit.

		BlueTOAD Spectra			Connected Vehicle Roadside Units	
		Ethernet PoE	Ethernet Cellular PoE	Solar Cellular	BlueTOAD Spectra CV	BlueTOAD CV
Features						
Types of Data Processed	Speed and Travel Time	X	X	X	X	
	Connected Vehicle SAE J2735 & J3224 messages				X	X
Data is Transmitted	Through Agency Network	X			X	X
	Through the Cellular Network		X	X		
Powered by	Power over Internet (PoE)	X	X		X	X
	Solar-Charged Battery			X		
Field Installation	Near Roadside Traffic Cabinet	X	X		X	X
	Stand-Alone			X		
Weight	Weights with brackets	<5 lbs.	<5 lbs.	<40 lbs.*	<9 lbs.	<9 lbs.

General Roadside Device Deployment Guidelines

After you select the target road segment for speed/travel time data collection, use the guidelines that follow to determine how many BlueTOAD detectors are necessary for your travel time study or reporting objectives.

The RSU has an effective C-V2X detection range of up to approximately 3,000 feet radius from the antennas (with direct line-of-sight).

BlueTOAD “Bluetooth” detection has an effective omni-directional detection range of an approximately 300-foot radius from the antenna.

The **minimum** recommended distance to space a BlueTOAD Spectra RSU is every 0.25 mile.

 **Note:** Power Control lets you reduce the detection zone to minimize overlap. Thus, with Power Control, the minimum spacing could be less than 0.25 mile.

The **maximum** distance to space BlueTOAD Spectra RSU is a function of the road type:

Road Type	Maximum Spacing, miles
Highway	4 to 5
Arterial (no traffic lights)	2 to 2 ½
Arterial (with traffic lights)	1 to 1 ½
Dense urban area*	1
* Note: The number of intersections, traffic signals, or exit ramps can affect the speed/travel time; thus, you should keep them to a minimum.	

In an Origin/Destination (O/D) deployment, you must install BlueTOAD detectors before the destination as well as after. The number of additional BlueTOAD detectors necessary is then based on driver options.

 **Example:** If a driver could turn either left or right at T intersection, you must install a BlueTOAD in each of the two possible directions of travel.



Pre-Installation Testing

Refer to section in the Appendix 6 – “BlueTOAD, RSU and/or ICP CV System Test Procedure” to follow steps that provide instructions to test the BlueTOAD Spectra CV before installed in the field.

The following topics are covered in Appendix 9:

- SPaT, MAP, TIM and BSM Data Broadcasting Verification
- Basic Security Credential Management System (SCMS) Validation
- OBU DSRC/C-V2X Message Verification Instruction
- Message Capture and Validation
- BlueTOAD Spectra RSU Site Requirements Form
- System Evaluation Checklist

BlueTOAD Spectra CV Installation Procedures

Purpose

The procedures in this chapter tell you what to do to deploy a BlueTOAD Spectra CV devices. We assume you are familiar with the BlueTOAD Spectra CV, supporting equipment, and the associated software listed below.

Supporting Equipment

- Windows PC and Ethernet Cables
- WinSCP or equivalent File Transfer Application
- PuTTY or equivalent SSH Client
- Iteris BlueTOAD Spectra CV
- PoE Injector
- Traffic Controller with Power Cable or Similar ATC Controller (Optional)
- 7-Zip Archiving Utility
- Advanced IP Scanner (Optional)
- Work area with adequate GPS reception

Setup and Configuration Procedures

The setup and configuration procedures that follow tell you how to deploy and test a BlueTOAD Spectra Connected Vehicle (CV) and 5.9 GHz Cellular Vehicle to Everything data collection and management system.

 **Note:** After notice to proceed is approved, Iteris and key collaborative team personnel will work with your Agency to create a formal deployment, implementation, and operations plan document for your BlueTOAD Spectra CV system.

 **Important:** FCC License: Each C-V2X-based RSU requires an FCC License to operate within a specific transportation agency jurisdiction. Only transportation agencies or transportation authorities can apply for and operate a 5.9 GHz C-V2X spectrum-based radio broadcast system.

Iteris can provide support for your Agency to acquire an FCC Regional License to manage and operate the C-V2X Network. We can also help you apply for required single FCC filings per RSU and RSU location. The Iteris RSU has been accepted by the FCC for deployment in the past, and we anticipate a successful outcome for your project.

Layout Guidelines

After you select the target road segment for CV and C-V2X data collection and management, use the guidelines that follow to determine how many Iteris BlueTOAD Spectra CV Roadside Units (RSUs) are necessary for your project.

- The RSU has an effective C-V2X detection range of up to approximately 3,000 feet radius from the antennas (with direct line-of-sight).
- You can install an RSU at each signalized intersection, mid-block or highway location that has an appropriate 120 VAC power source.
- The minimum recommended (but not limited) distance to space the Spectra CV RSU is every 0.25 mile; this is because of the minimum recommended distance to space the BlueTOAD detector part of the RSU.

 **Note:** *Power Control lets you reduce the detection zone to minimize overlap. Thus, with Power Control, the minimum spacing could be less than 0.25 mile.*

Pre-Install Evaluation and Setup

Before you install an RSU, make sure things are ready at the installation sites:

1. **Location** – Prepare a sight survey of all intersection locations that have been selected to deploy RSUs.
 - a. Identify power sources available in the traffic cabinets.
 - b. Make sure you have all the necessary parts for the system. Refer to the table on [Page 3-1](#) and information on [Page 6-44](#) for a list of the items needed and included with an RSU.
 - c. Are the Traffic Controllers in the traffic cabinets compatible with the RSU?
2. **Traffic Network** – Evaluate the existing network.
 - a. Confirm that the network settings (for example, IP address, gateway, subnet mask, and DNS) are correctly set and that all ports (69, 123, 443, 8010, 8892, 10001, 10002) are open and set for outbound data traffic.

 **Important:** *Confirm all necessary inbound/outbound network ports have been set up.*

- b. What are the IP addresses assigned to the Traffic Controller and to the RSU?

 **Note:** *If there is an In-Cabinet Processor - ICP (optional), it also has an IP address.*
3. **MAP File Creation** – For each intersection, create a MAP file; with Signal, Phase and Timing (SPaT) information if a location is a signalized intersection. For instructions, refer to Appendix 8, *How to Create an RSU MAP File*.
 4. Fill out the BlueTOAD Spectra RSU Site Requirements form on [Page 12-1](#).
 5. Power ON the RSU and confirm all LEDs are normal after the unit initializes:

BlueTOAD CV or Spectra CV (Bottom View)



LED Indicators

Green – Device operational

Amber – Device ON

Red - Fault

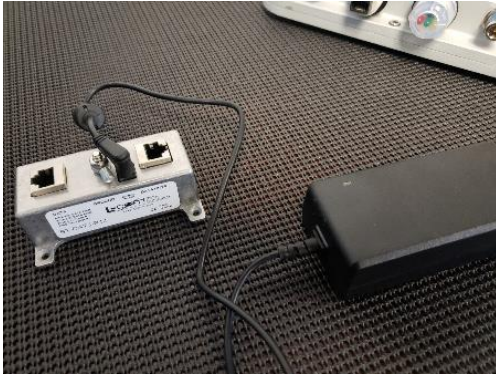
How to Set Up the Traffic Controller Before Field Deployment

This example uses an Econolite **traffic controller**, model Cobalt Advanced Traffic Controller (ATC). However, you can use ATC controllers (preferred) from other manufacturers that have Ethernet and IP interfaces and can send SPAT and/or MAP information to RSU in SAE J2735, TSCBM or in some cases proprietary formats. You can consult Iteris Support for models of traffic controllers supported.

1. Attach the Traffic Controller “A” power cable to the “A” connector of the controller.



2. Plug the “A” power cable into an AC power source. The controller should power ON.
3. Using the example default IP address of a stock BlueTOAD Spectra CV RSU device, 192.168.1.76, navigate to the Ethernet communications page of the controller.
4. Set the controller IP address to (recommended default) 192.168.1.32 and (default) Netmask to 255.255.255.0. Set the Ping Server to the IP address of the RSU (RSU Default IP Address: 192.168.1.76).
5. Plug the AC power cable of the POE injector AC adapter to an AC power source.
6. Plug the AC adapter output power cable into the POE injector. The AC adapter LED indicator should light up with power.



7. Connect the RSU to the Data+PWR port of the POE Injector with an Ethernet cable. The RSU Power LED indicator should light up with power.



8. Connect the POE Injector Data port to Port 1 of ENET-1 (WAN) of the controller with an Ethernet cable.



9. Connect the computer to Port 2 of ENET-1 (WAN) of the controller with an Ethernet cable.
10. Set the computer's IP address to match the subnet of the RSU and controller—for example, 192.168.1.100.

11. Program controller to send SPAT and in some cases MAP messages to RSU device. The steps depend on the manufacturer, model and software/firmware version. Please consult the controller manufacturer support or user guide documentation.

Configuration Procedures – using Browser-Based Configuration Utility

Log into BlueTOAD Spectra CV browser-based configuration utility. Open a Web Browser (Google Chrome or Microsoft Edge is preferred).

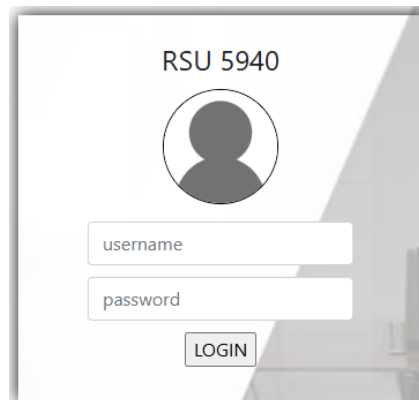
Enter the “default” BlueTOAD Spectra CV URL <https://192.168.1.76:4934>

 **Note:** If the IP address has been changed from the factory default, use the new IP address to access the login website.

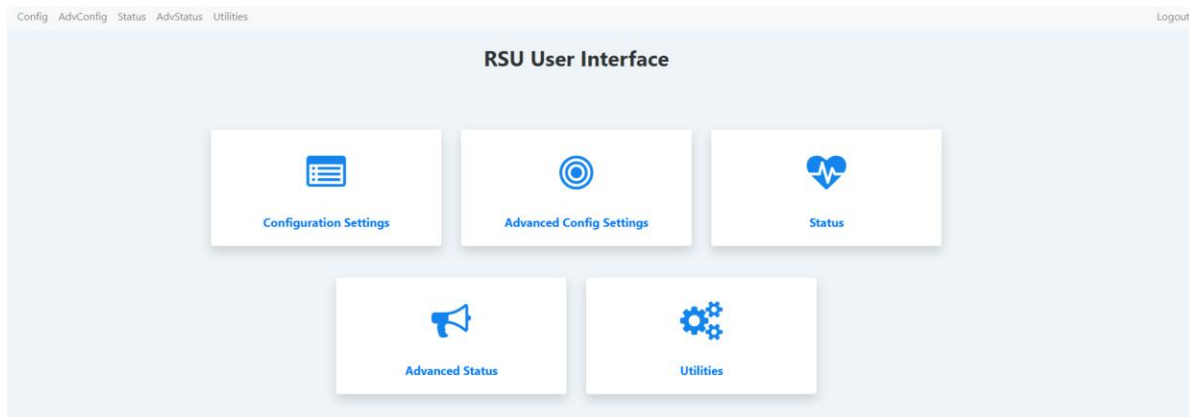
For the configuration tool to proceed, you must use the username and password given below at the default address:

- **RSU Root Username:** **rsuuser**
- **RSU Root Password:** **Heavyduty@2025!**

Select **Login** to log into the BlueTOAD RSU web-based configuration utility main menu



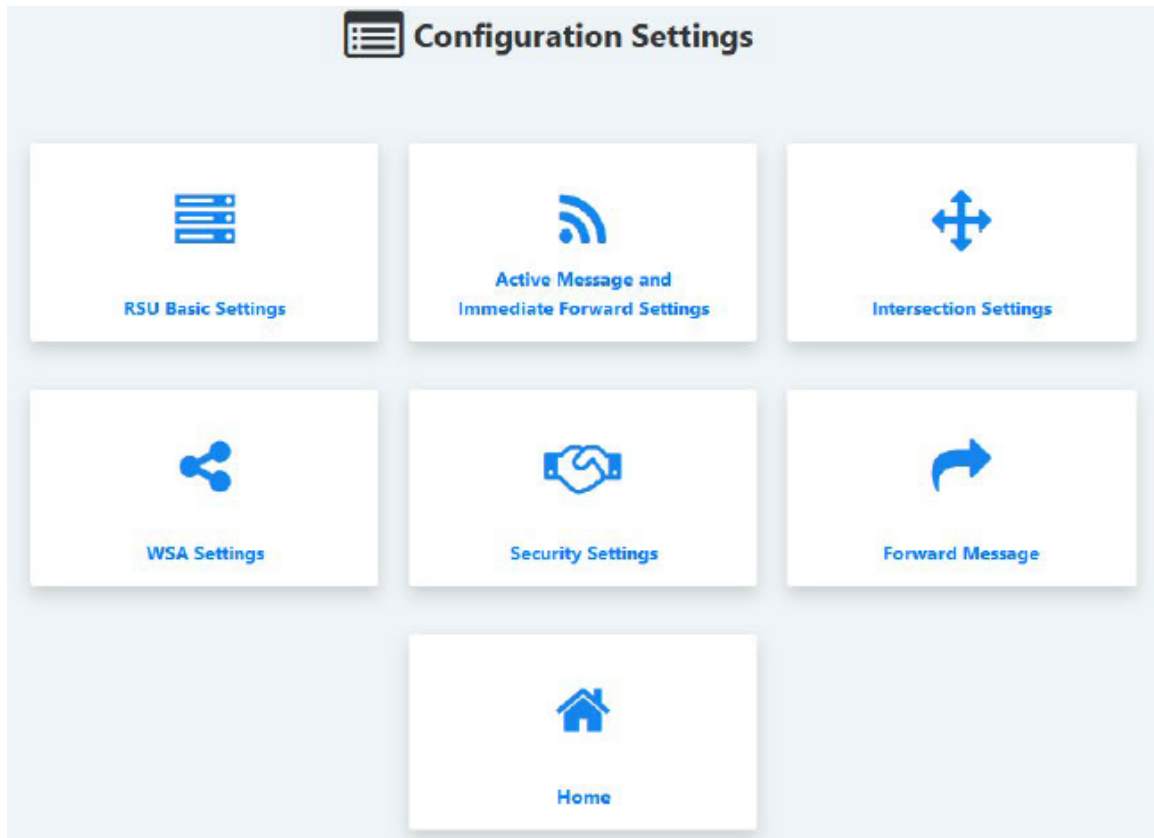
After Login, the BlueTOAD Spectra CV RSU Main Menu is available for selection. The Main Menu contains options about Configuration Settings, Status and Utilities as shown below.



Configuration Settings Page

This section provides the basic configuration options. Those range from basic networking settings, over the settings for active messages and immediate forward settings to intersection and security settings.

- Click on the Dashboard menu to view information about the System, as shown below:
- Click on the RSU Basic Settings to configure network settings.



RSU Basic Settings

Basic RSU network settings can be configured here.

Enable DHCP Checkbox - Select this checkbox to set the RSU to use DHCP instead of a static IP. Make sure to confirm if DHCP is supported ahead of time. Enable with care given that it can result in being locked out from the RSU if enabled on a non-DHCP network.

RSU IP Address - When using static IPs, this field displays the current IP address. If the user changes this value, it is not updated in the GUI until after a reboot.

RSU Address Mask - This field defines the netmask. The value is the leading bits set to 1 (e.g. 24 = FFFFFFF0, a mask of 255.255.255.0).

Enable Gateway - Select this checkbox to set a default gateway address to the static IP. This setting is ignored when DHCP is active.



RSU Basic Settings

Settings

☐ Enable DHCP

RSU IP Address

192.168.1.72

RSU Address Mask (bits)

24

☒ Enable Gateway

RSU Gateway IP Address

192.168.1.1

RSU Network MTU

1500

☐ Enable VLAN

VLAN IP Address

192.168.3.80

VLAN Address Mask (bits)

24

☐ Enable VLAN Gateway

RSU VLAN Gateway IP Address

192.168.3.1

VLAN Identifier

0

Webgui HTTPS Port

4934

SNMP Port

161

SSH Port

22

[Advanced Network Settings](#)

RSU Gateway IP Address - Fill this value with the proper gateway address when selecting the Enable Gateway checkbox.

RSU Network MTU - Set the value of the MTU using this field. Consult your network administrator when changing this field.

Enable VLAN - Select this checkbox when the RSU must communicate using a VLAN.

VLAN IP Address - Use this field to specify the IP address the RSU will use when VLAN is enabled. Only a static IP address is allowed for VLAN support. The IP address specified in this field may not be duplicate of the RSU IP address.

VLAN Address Mask(bits) - This field defines the VLAN address mask, similar to the RSU Address Mask.

Enable VLAN Gateway - Select this checkbox to enable the VLAN default gateway address field.

RSU VLAN Gateway IP Address - This field defines the VLAN gateway address, similar to the RSU Gateway IP Address. The VLAN Gateway may not be a duplicate of the RSU Gateway IP Address.

VLAN Identifier - This field represents the VLAN ID the RSU must use. Consult your network administrator when setting this value.

Webgui HTTPS Port - The port used for the HTTPS interface. Any unused port may be specified. Set the value to 0 to disable the interface.

SNMP Port - The port used for the SNMP interface. Any unused port may be specified.

SSH Port - The port used for the SSH interface. Any unused port may be specified.

Advanced Network Settings

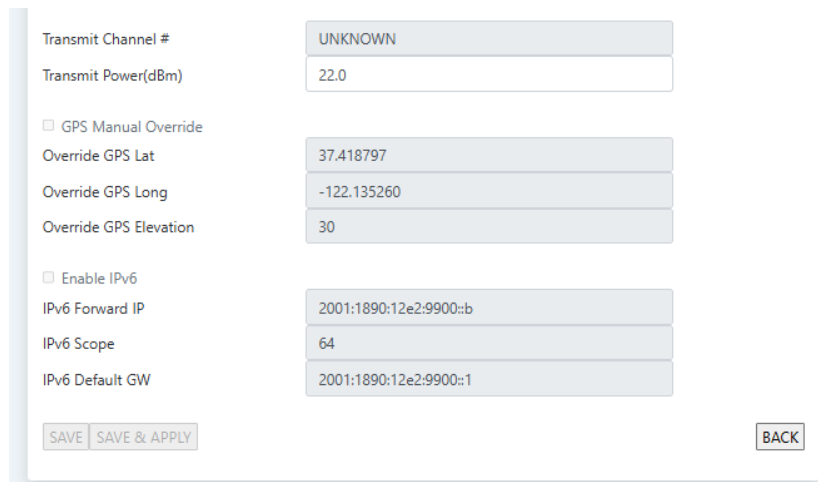
Transmit Channel # - Not to be used/changed. This is the V2X service channel used for activity. For C-V2X the channel is 183 (a 20 MHz channel) Modifications/editing may be allowed in future releases

Transmit Power - This is the power in dB that is used for broadcast. Values from 10 – 23 dBm are allowed. Ensure that both CV2X ANT ports are connected to V2X antennas (or RF equipment) before the transmitter is activated.

Save Button - Use the save button to save any changes. Once saved, the user remains on the same page. This describes the general behavior of Save button throughout the configuration webpage.

Save & Apply Button - Use the save and apply button to save changes and to initiate an immediate RSU reboot to apply the changes. This describes the general behavior of Save button throughout the configuration webpage.

Back Button - Use the back button to return to the configuration settings page. Selecting the back button before saving any changes clears any changes. This describes the general behavior of Save button throughout the configuration webpage.



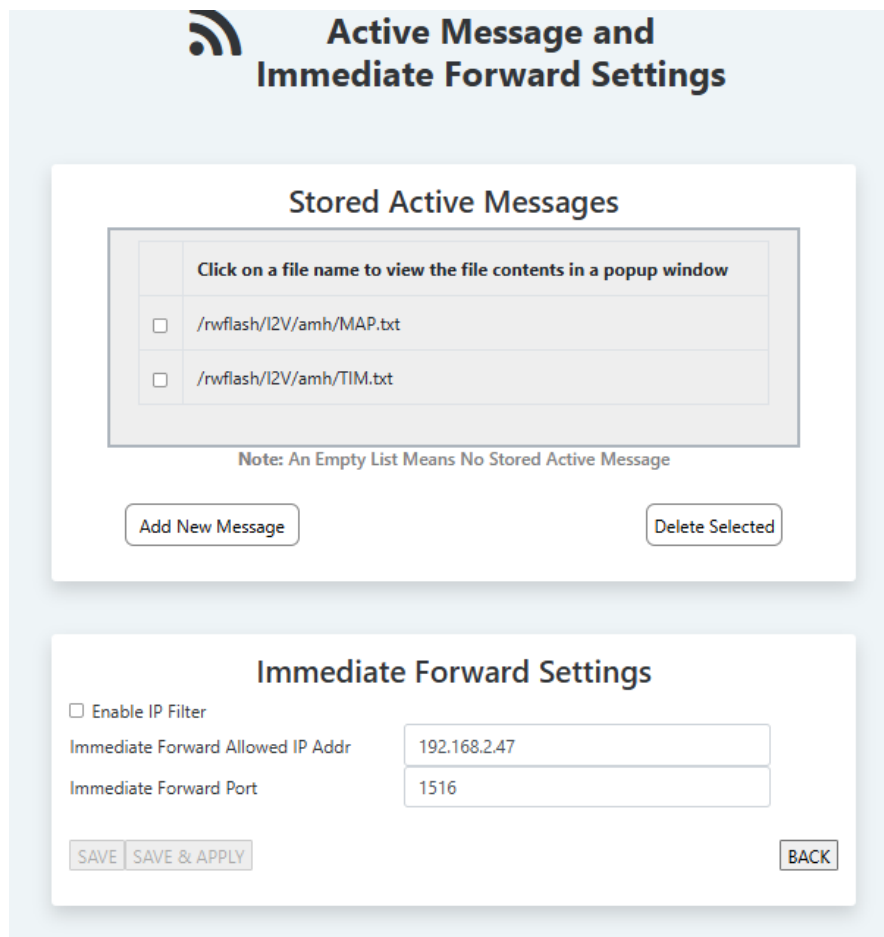
The screenshot shows a configuration page with the following fields and values:

Transmit Channel #	UNKNOWN
Transmit Power(dBm)	22.0
☐ GPS Manual Override	
Override GPS Lat	37.418797
Override GPS Long	-122.135260
Override GPS Elevation	30
☐ Enable IPv6	
IPv6 Forward IP	2001:1890:12e2:9900::b
IPv6 Scope	64
IPv6 Default GW	2001:1890:12e2:9900::1

At the bottom, there are three buttons: **SAVE**, **SAVE & APPLY**, and **BACK**.

Active Message and Immediate Forward Settings

The figure below shows the active message, immediate forward parameters available and a successful file upload. Active messages are either Store and Repeat messages or Immediate Forward messages. Store and Repeat messages are saved on the RSU and will be repeatedly broadcast. Immediate Forward messages are not saved on the RSU. Examples of active messages are MAP or TIM messages. A default active message file (MAP file) may be present on your device. The file is present so a user can see radio activity out of the box. You may wish to delete this file for your deployments, as it serves no purpose in your deployment.





Active Message and Immediate Forward Settings

Stored Active Messages

Click on a file name to view the file contents in a popup window	
☐	/rwflash/I2V/amh/MAP.txt
☐	/rwflash/I2V/amh/TIM.txt

Note: An Empty List Means No Stored Active Message

Immediate Forward Settings

☐ Enable IP Filter

Immediate Forward Allowed IP Addr:

Immediate Forward Port:

Stored Active Messages

This table shows any **stored** active messages on the RSU. The output is a list of files. If there is no listing, then there are no stored active messages. If files are listed, click a file to view the contents (see the example after this table).

Add New Message - Select this button to upload a new active message file.

Delete Selected - Select this button to delete all selected active messages in the list. Each active message has a checkbox next to the entry that can be clicked. If the user selects no files, this button has no effect.

Immediate Forward Settings

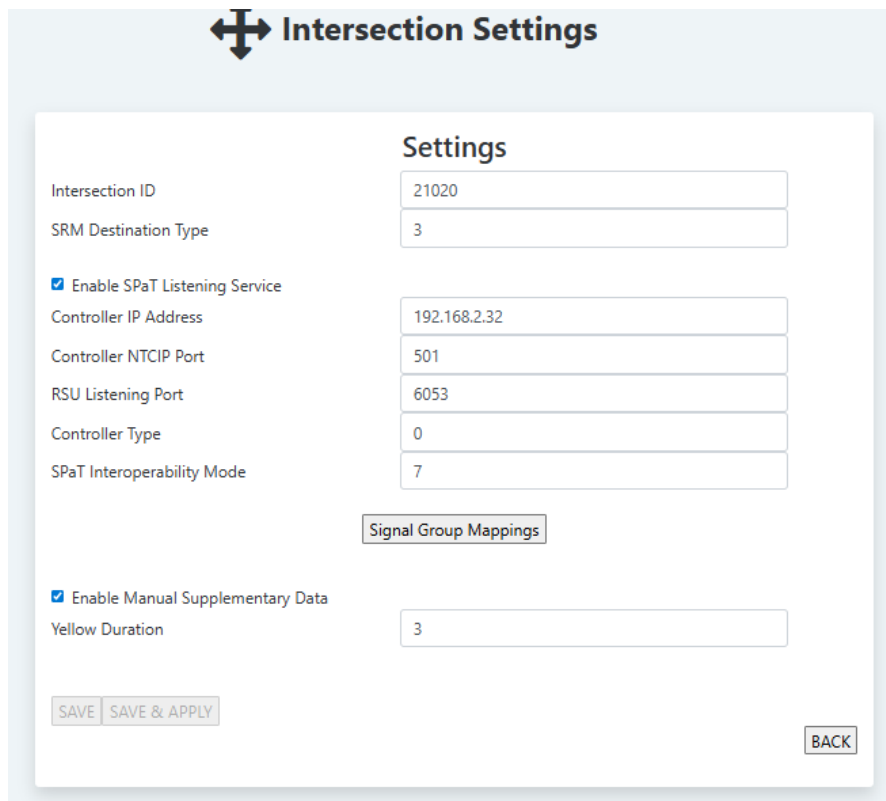
Enable IP Filter Checkbox - Select this checkbox to enable a single IP allowed to forward messages to the RSU.

Immediate Forward Allowed IP Addr - When the IP filter is enabled, use this field to define the allowed IP.

Immediate Forward Port - Use to define the listening port for receiving immediate forward messages.

Intersection Settings

The purpose of this menu is to configure intersection and settings for devices operating at the subject intersection.



The screenshot shows the 'Intersection Settings' web interface. At the top, there is a header with a double-headed arrow icon and the title 'Intersection Settings'. Below this is a 'Settings' section with various input fields and checkboxes. The fields are: 'Intersection ID' (21020), 'SRM Destination Type' (3), 'Controller IP Address' (192.168.2.32), 'Controller NTCIP Port' (501), 'RSU Listening Port' (6053), 'Controller Type' (0), and 'SPaT Interoperability Mode' (7). There are two checkboxes: 'Enable SPaT Listening Service' (checked) and 'Enable Manual Supplementary Data' (checked). Below the checkboxes is a 'Signal Group Mappings' section with a 'Yellow Duration' field (3). At the bottom, there are 'SAVE', 'SAVE & APPLY', and 'BACK' buttons.

Intersection ID – The intersection ID value.

SRM Destination Type - Use this field to specify the type of listener receiving the SRM (the format of the SRM sent, i.e. CSV or encoded). Supported Values:

1 = CSV output

2 = Proprietary (Reserved for most users)

3 = UPER encoded output

All other values are invalid

Enable SPaT Listening Service Checkbox - Select this checkbox when the RSU is connected directly to a TSC to enable SPaT to broadcast over the configured radio channel.

Controller IP Address - Use this field to specify the traffic signal controller IP address.

Controller NTCIP Port - Use this field to specify the traffic signal controller port that receives NTCIP requests.

RSU Listening Port - Use this field to define the RSU's listening port for SPaT data; only supports ports 6053 or 6054 for SPaT that is received as TSCMB or proprietary format that is to be converted to SAE J2735 SPaT format. If SPaT data is received from a traffic signal controller in SAE J2735 format, it would not be configured here. Instead, it would be routed via 1516 port and immediate forward functionality described in the Immediate Forward Settings menu. Setting different values results in RSU applications failing to start.

Controller Type - Use this field to specify the controller type. The Controller Type is used only for Traffic Signal Controllers (TSCs) that do not support the Battelle ICD packet. The only supported TSC that falls into this category is the Cubic Trafficware TSC. Changing this value from its default setting takes precedence for how the RSU accepts the input TSC data. When this value is set to a non-default value, the RSU no longer expects Battelle ICD data. Parameter values:

- 0 - Default setting; use this value for all controllers supporting the Battelle ICD.
- 1 - Basic mode for Trafficware controller support where phase detection is performed through time to change for either max or min values being set to value corresponding to unknown. Set the "Enable Manual Supplementary Data" checkbox when using this value.
- 2 - Secondary basic mode for Trafficware controller support where phase detection is performed through time to change for both max and min values being set to value corresponding to unknown. Set the "Enable Manual Supplementary Data" checkbox when using this value.
- 3 - Advanced mode for Trafficware controller support using phase enabled mask for detection of enabled phases. Be sure to deselect the checkbox for "Enable Manual Supplementary Data" when using this value.

SPaT Interoperability Mode - Use this field to define the broadcast SPaT definition; unless otherwise instructed, it is recommended not to change the default. The setting is a bitmask where a bit set to 1 enables an alteration to the SPaT message. Hex values and descriptions are provided below:

- 0x08 - Enables pedestrian/bicyclist detection presence to be transmitted in the SPaT message. Set bit to 0 to disable. The detection information is retrieved from the TSC, if supported. At the current time, only detection information from a TrafficWare controller is obtained.
- 0x04 - Enables UTC time to be presented in SPaT message. Set bit to 0 to switch to a non-J2735 defined countdown for the SPaT timing. In this case, the hex value is 0x05
- 0x02 - Enables SPaT messages to be broadcast with both minimum and maximum SPaT timing durations. Set bit to 0 to broadcast a single value (either minimum or maximum) defined by UseMaxTimeToChange setting in /rwflash/configs/scs.conf. In general, this bit should always be set to 1.
- 0x01 - Enables simplified SPaT messages. Set bit to 0 to enable messages to all simple phase count down. In general this bit 0 should always be set to 1.
- Note: 1. Only the lower nibble is defined. The upper nibble is always 0. 2. The lower nibble bits may be OR'ed or combined as required.
 - ♦ a. Example: 0x04 + 0x01 = 0x05
 - ♦ b. Example: 0x02 + 0x01 = 0x03

- ♦ c. Example: 0x08 + 0x04 + 0x02 = 0x0E and so on.

Enable Manual Supplementary Data Checkbox - Select this checkbox to enable hard-coded values for additional TSC data undefined in the SPaT message and suppress NTCIP requests from the RSU to the TSC.

Yellow Duration - When using hard-coded values, this field defines the yellow duration in seconds for the intersection.

Signal Group Mappings

The Signal Group Mappings Editor is used to define vehicle phases and overlap phases as Signal Group IDs for intersection's SPaT data. The user is responsible for ensuring the settings align with the intersection and any MAP broadcast by the RSU. The editor allows the User the option to create up to 32 total signal groups between Vehicle and Overlap phases (16 each).

Signal Group Mappings Editor

Signal Group Mappings

Phase Type	Phase #	Signal Group ID	Green Means	Delete Row
Vehicle ▼	1	1	Protected ▼	Delete
Vehicle ▼	2	2	Protected ▼	Delete
Vehicle ▼	3	3	Protected ▼	Delete
Vehicle ▼	4	4	Protected ▼	Delete
Vehicle ▼	5	5	Protected ▼	Delete
Vehicle ▼	6	6	Protected ▼	Delete
Overlap ▼	7	7	Permitted ▼	Delete
Overlap ▼	8	8	Permitted ▼	Delete

+ ADD

SAVE
SAVE & APPLY

BACK

Phase Type - The Phase Type section box in each row allows the user to choose whether the configured values are for a Vehicle Phase or an Overlap. Click the drop-down icon in the box to choose between Vehicle and Overlap.

Phase # - Each row contains a Phase number field where the user can define the associated phase or overlap number as defined for the intersection.

Signal Group ID - Each row contains a Signal Group ID field that allows the user to define which signal group used in the SPAT message is connected to the phase.

Green Means – protected = exclusive right-of-way, permitted = proceed when safe after yielding

Delete Row - The Delete button in each row is provided to allow a user to remove the settings for a given phase (if there is a change or if the user entered the data incorrectly). Deletion of the row is reflected in the GUI immediately.

Add - The Add button is used to create a new row. The GUI defaults to showing only what is configured which is nothing by default.

WSA Settings

WSA support is not yet implemented so users should ignore the fields under this menu until further notice.

Security Settings

The BlueTOAD CV or BlueTOAD Spectra CV RSU devices support V2X security. The default configuration is with security disabled as depicted in the screenshot below. The Security Configuration page allows a user to enable or disable security, as well as upload security credentials. The page also displays the current status of the security module. The Security Metrics and Security Certificate Status blocks show the current activity and status for the security module.

Security Settings

☐ Enable Security

SPAT Security PSID

SPAT Ssp String

SPAT SspMask String

MAP Security PSID

MAP Ssp String

MAP SspMask String

TIM Security PSID

TIM Ssp String

TIM SspMask String

SSM Security PSID

SSM Ssp String

SSM SspMask String

☐ Enable VOD

VTP in Milliseconds

☐ Enable Proxy

☐ Enable HTTP Proxy

Proxy IP

Proxy Port

HTTP Proxy Port

☒ Enable SPAT Ssp

☐ Enable SPAT Bitmap Ssp

☒ Enable MAP Ssp

☐ Enable MAP Bitmap Ssp

☒ Enable TIM Ssp

☐ Enable TIM Bitmap Ssp

☒ Enable SSM Ssp

☐ Enable SSM Bitmap Ssp

Security Metrics

	Requests	Successes	Failures	Err.Code
Message Signs	0	0	0	0
Security Strips	170285	170285	0	0
Message Verifies	167035	56223	110812	20

Security Certificate Status

Enrollment Requests: **1**

Signed Enrollment Responses: **1**

Total Number of .OER Files: **11**

Weeks of Downloaded Certs: **2**

ISS Certificate Management Status

Upload results will appear here

Enable Security - Select the checkbox to activate security. Deselect the checkbox to disable security.

SPAT Security PSID - The PSID to be used for SPAT messages when security is enabled. This value must match the V2X certificate for which the RSU is enrolled.

SPAT Ssp String - The SSP value to be used with the PSID for SPAT messages when security is enabled. If defined by the V2X certificate, this value must match the certificate. The value is a hex value but do not use the 0x qualifier when specifying the hex value.

SPAT SspMask String - The SSP mask value to be used with the SSP for SPAT messages when security is enabled. If defined by the V2X certificate, this value must match the certificate. The value is a hex value but do not use the 0x qualifier when specifying the hex value.

MAP Security PSID - The PSID to be used for MAP messages when security is enabled. This value must match the V2X certificate for which the RSU is enrolled.

MAP Ssp String - The SSP value to be used with the PSID for MAP messages when security is enabled. If defined by the V2X certificate, this value must match the certificate. The value is a hex value but do not use the 0x qualifier when specifying the hex value.

MAP SspMask String - The SSP mask value to be used with the SSP for MAP messages when security is enabled. If defined by the V2X certificate, this value must match the certificate. The value is a hex value but do not use the 0x qualifier when specifying the hex value.

TIM Security PSID - The PSID to be used for TIM messages when security is enabled. This value must match the V2X certificate for which the RSU is enrolled.

TIM Ssp String - The SSP value to be used with the PSID for TIM messages when security is enabled. If defined by the V2X certificate, this value must match the certificate. The value is a hex value but do not use the 0x qualifier when specifying the hex value.

TIM SspMask String - The SSP mask value to be used with the SSP for TIM messages when security is enabled. If defined by the V2X certificate, this value must match the certificate. The value is a hex value but do not use the 0x qualifier when specifying the hex value.

SSM Security PSID - The PSID to be used for SSM messages when security is enabled. This value must match the V2X certificate for which the RSU is enrolled.

SSM Ssp String - The SSP value to be used with the PSID for SSM messages when security is enabled. If defined by the V2X certificate, this value must match the certificate. The value is a hex value but do not use the 0x qualifier when specifying the hex value.

SSM SspMask String - The SSP mask value to be used with the SSP for SSM messages when security is enabled. If defined by the V2X certificate, this value must match the certificate. The value is a hex value but do not use the 0x qualifier when specifying the hex value.

Enable VOD - Enable Verify On Demand for incoming messages by the security module.

VTP in Milliseconds - Time in milliseconds in which incoming messages are verified by the security module.

Enable Proxy - Enable Proxy for security communication with SCMS server.

Enable HTTP Proxy - Enable HTTP Proxy for HTTP tunneling.

Proxy IP - Proxy Server IP address.

Proxy Port - Port for communication with Proxy Server.

HTTP Proxy Port - Port for HTTP tunneling with Proxy Server.

Setting PSID, SSP, and SSP mask values, values incorrectly when security is enabled prevents the RSU from transmitting.

The Security Metrics details are displayed below Security Settings.

Security Metrics					Security Certificate Status	
	Requests	Successes	Failures	Err.Code		
Message Signs	0	0	0	0	Enrollment Requests: 1	
Security Strips	170285	170285	0	0	Signed Enrollment Responses: 1	
Message Verifies	167035	56223	110812	20	Total Number of .OER Files: 11	
					Weeks of Downloaded Certs: 2	

Message Signs

Requests - The number of requests by the RSU services to sign messages. Signing is applied to messages transmitted by the RSU.

Successes - The number of successful message signings by the security module relative to the number of requests.

Failures - The failing number of message signings by the security module relative to the number of requests. Failed signed messages are not transmitted from the RSU.

Err.Code - Error code when the signing of messages failed. It is used for debugging the signing failure.

Security Strips

Successes - The successful number of strips. A strip means the security header of received messages is removed.

Failures - The failing number of strips for received messages.

Message Verifies

Requests - The number of requests by the RSU services to verify signed messages. Verification of signed messages applies to received messages. Message verification is configurable, and not all received messages may be verified.

Successes - The successful number of message verifications by the security module relative to the number of requests.

Failures – The failing number of message verifications by the security module relative to the number of requests. Failed verification messages are an indicator of a corrupt or invalid received messages and the RSU services may reject the message.

Err.Code - Error code when the signing of messages failed. It is used for debugging the signing failure.

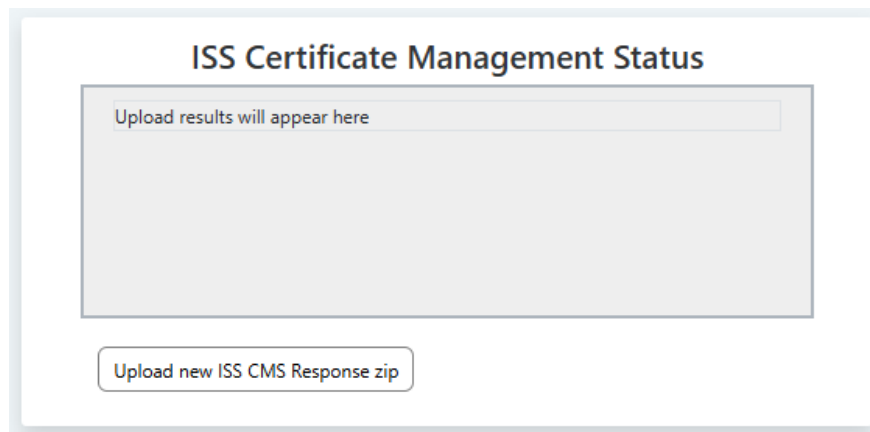
The Security Certificate Status table contains the following details.

Enrollment Requests - The number of requests generated by the security module.

Signed Enrollment Responses - The number of enrollment responses processed by the security module.

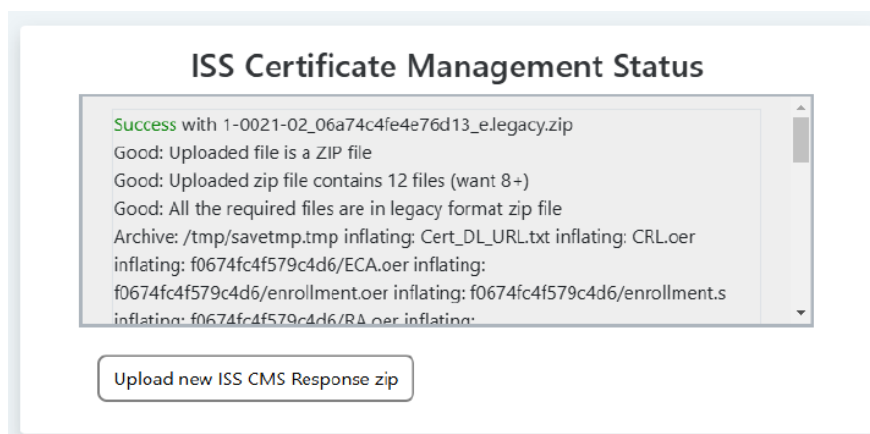
Total Number of .OER Files - The security related files contained within the response.

Weeks of Downloaded Certs - The number of weeks the RSU has valid certificates to cover broadcasting signed messages (and performing verification on received messages).



For the ISS CMS Response upload, a user may overwrite any existing files with a new package. If a user selects to upload a new zip package, the user is presented with a window to search for the zip on the user's local system.

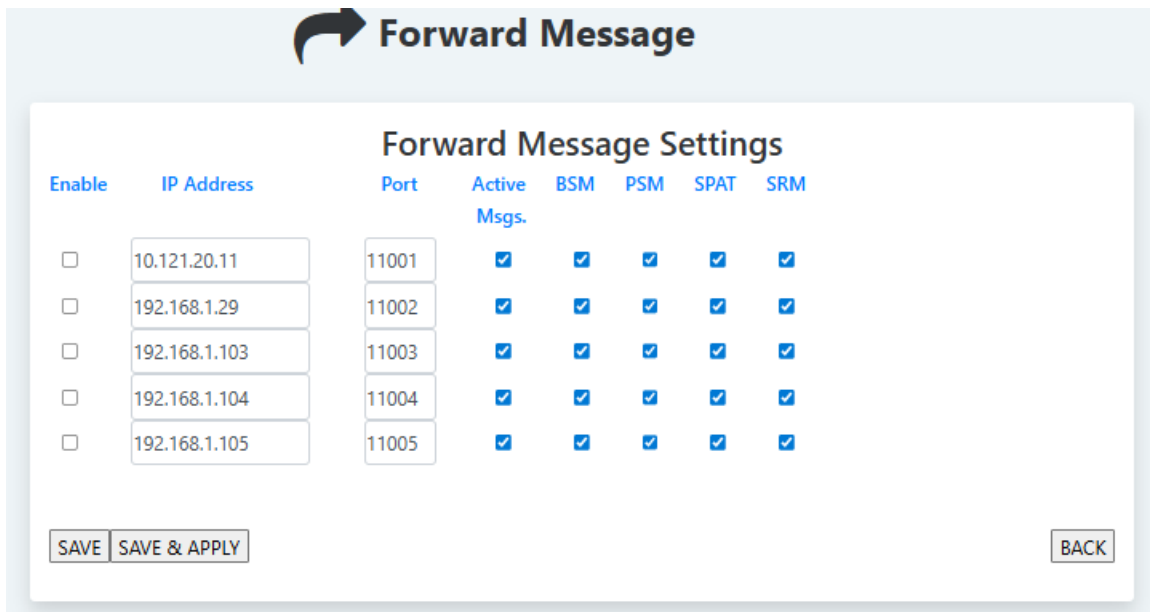
The GUI page updates immediately and shows success or failure once the user selects the Open button in the pop up search window.



Forward Message Settings

The RSU supports forwarding selected V2X data to up to five distinct endpoints. Settings are provided such that a user may choose which data elements are forwarded to each destination.

For each element check the box or enter text shown as examples. If fields are not applicable or no change is desired, please keep them blank.



The screenshot shows a web interface titled "Forward Message" with a curved arrow icon. Below the title is a form titled "Forward Message Settings". The form contains a table with the following columns: Enable, IP Address, Port, Active Msgs., BSM, PSM, SPAT, and SRM. There are five rows of settings, each with an "Enable" checkbox, an "IP Address" field, a "Port" field, and five selection boxes for "Active Msgs.", "BSM", "PSM", "SPAT", and "SRM". All checkboxes and selection boxes are currently checked. At the bottom of the form are three buttons: "SAVE", "SAVE & APPLY", and "BACK".

Enable	IP Address	Port	Active Msgs.	BSM	PSM	SPAT	SRM
☐	10.121.20.11	11001	☒	☒	☒	☒	☒
☐	192.168.1.29	11002	☒	☒	☒	☒	☒
☐	192.168.1.103	11003	☒	☒	☒	☒	☒
☐	192.168.1.104	11004	☒	☒	☒	☒	☒
☐	192.168.1.105	11005	☒	☒	☒	☒	☒

SAVE SAVE & APPLY BACK

Enable - The enable selection box determines if the target destination defined for the row is activated for receiving forward messages.

IP Address - The IP address of the target destination. The address is an IPv4 address in numerical format. When configuring multiple destinations please ensure that there are no duplicate IP addresses.

Port - The IP port of the target destination. This is the listening port on the target device.

Active Msgs. - The selection box determines if V2X active messages (immediate forward or store and repeat) are forwarded to the configured target destination.

BSM - The selection box determines if BSMs are to be forwarded to the configured target destination. The BSMs forwarded are all BSMs an RSU receives.

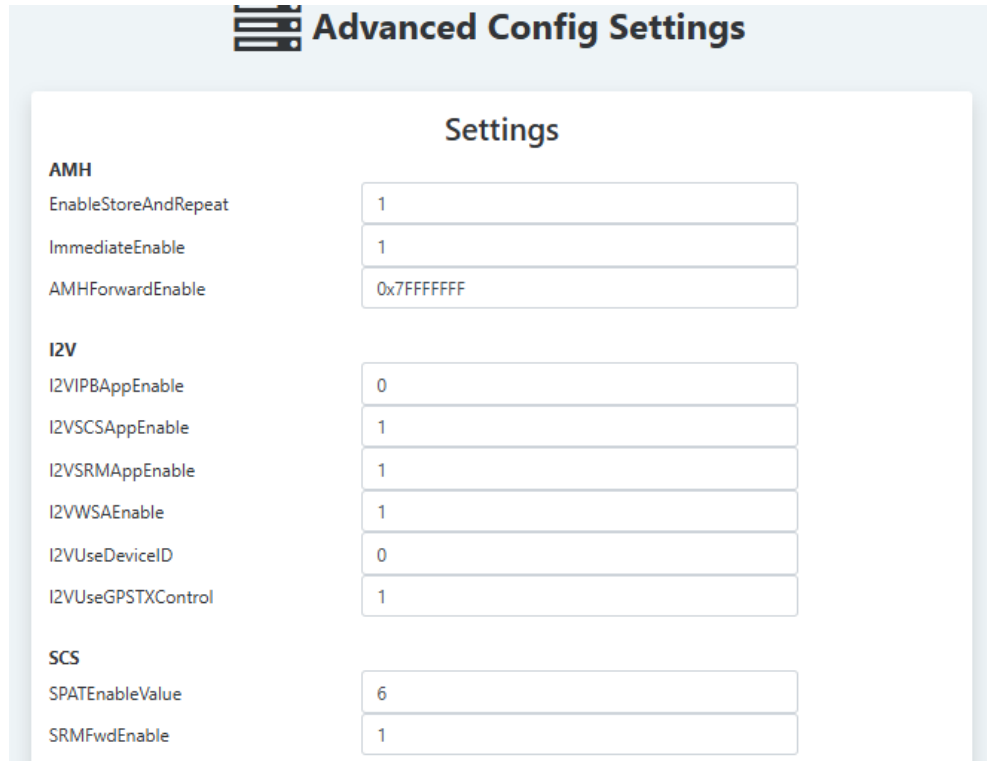
PSM - The selection box determines if PSMs are to be forwarded to the configured target destination. The PSMs forwarded are all PSMs the RSU receives.

SPAT - The selection box determines if SPAT messages are to be forwarded to the configured target destination.

SRM - The selection box determines if SRMs are to be forwarded to the configured target destination. The SRMs forwarded are all SRMs the RSU receives.

Advanced Config Settings

The Advanced Config Settings provide configuration that should only be modified by experienced users who need to adjust the RSU behavior to meet specific deployment goals. The settings are grouped according to the corresponding use case referenced in bold on the page. Since these are advanced settings, not all configs are elaborated in detail in this document. Consult your local Iteris representative if a justified need arises to inquire about these parameters. Most users do not need to change these settings.



Advanced Config Settings

Settings

Category	Setting Name	Value
AMH	EnableStoreAndRepeat	1
	ImmediateEnable	1
	AMHForwardEnable	0x7FFFFFFF
I2V	I2VIPBAppEnable	0
	I2VSCSAppEnable	1
	I2VSRMAppEnable	1
	I2VWSAEnable	1
	I2VUSeDeviceID	0
	I2VUSeGPSTXControl	1
SCS	SPATEnableValue	6
	SRMFwdEnable	1

AMH

EnableStoreAndRepeat - Default set to 1; set to 0 to disable allowing senders to submit active messages through the Immediate Forward interface that are stored and retransmitted by the RSU.

ImmediateEnable - Default set to 1; set to 0 to disable the Immediate Forward interface.

AMHForwardEnable - Default set to 0x7FFFFFFF; a bitmask of supported J2735 messages that are forwarded to a target. Set the value to 0 to disable this forwarding. Disable select bits to limit the messages that are forwarded. Bit mapping:

MAP = 0x1
 SPAT = 0x2
 CSR = 0x4
 EVA = 0x8
 ICA = 0x10
 NMEA = 0x20



PDM = 0x40
PVD = 0x80
RSA = 0x100
RTCM = 0x200
SRM = 0x400
SSM = 0x800
TIM = 0x1000
PSM = 0x2000
TEST00 = 0x4000
TEST01 = 0x8000
TEST02 = 0x10000
TEST03 = 0x20000
TEST04 = 0x40000
TEST05 = 0x80000
TEST06 = 0x100000
TEST07 = 0x200000
TEST08 = 0x400000
TEST09 = 0x800000
TEST10 = 0x1000000
TEST11 = 0x2000000
TEST12 = 0x4000000
TEST13 = 0x8000000
TEST14 = 0x10000000
TEST15 = 0x20000000
BSM = 0x40000000

AMHForwardIP – as defined in the [Forward Message Settings](#) above

AMHForwardPort – as defined in the [Forward Message Settings](#) above

I2V

I2VSCSAppEnable – Default set to 1; set to 0 to disable the interface to a traffic signal controller.

I2VSRMAppEnable - Default set to 1; set to 0 to disable support for handling SRMs.

I2VWSAEnable - Default set to 1; set to 0 to disable WSA broadcasts

I2VUseDeviceID - Default set to 0; set to 1 to enable. Used in Forward Message to tag each message. If set to zero then message tagging is not used. If non-zero integer is entered then each message forwarded will have this id added to the front of the message followed by a time tag. This allows data from one RSU to be distinguished from another.

I2VUseGPSTXControl - Default set to 1; set to 0 to disable. If enabled radio will only transmit if it has a valid GNSS fix. For CV2X is recommended to leave this enabled. With no GNSS fix the radio will not transmit and errors will be seen in the System Event Log.

SCS

SPATEnableValue - Default set to 6; used only when RSU must enable TSCBM on supported traffic signal controllers.

SRMFwdEnable - Default set to 1; set to 0 to disable SRM forwarding to an Ethernet target if the RSU receives SRMs from OBUs.

SPAT16	
BSMRxEnable	1
BSMRxPSIDPERU	0x20
I2VSPATSecPSID	0x8002
NSCONFIG	
AC_BE_CCH_RADIO_0	15,1023,6,0
AC_BK_CCH_RADIO_0	15,1023,9,0
AC_VI_CCH_RADIO_0	15,1023,4,0
AC_VO_CCH_RADIO_0	3,7,2,0
AC_BE_SCH_RADIO_0	15,1023,6,0
AC_BK_SCH_RADIO_0	15,1023,9,0
AC_VI_SCH_RADIO_0	15,1023,4,0
AC_VO_SCH_RADIO_0	3,7,2,0
AC_BE_CCH_RADIO_1	15,1023,6,0
AC_BK_CCH_RADIO_1	15,1023,9,0
AC_VI_CCH_RADIO_1	15,1023,4,0
AC_VO_CCH_RADIO_1	3,7,2,0
AC_BE_SCH_RADIO_1	15,1023,6,0
AC_BK_SCH_RADIO_1	15,1023,9,0
AC_VI_SCH_RADIO_1	15,1023,4,0
AC_VO_SCH_RADIO_1	3,7,2,0

SPAT16

BSMRxEnable - Default set to 1; set to 0 to disable support for the RSU listening to BSMs.

BSMRxPSIDPERU - PSID for BSM message.

2VSPATSecPSID - PSID for SPaT message.

SRM_RX	
SRMPermissive	1
SRMTXVehBasicRole	0xFFFFFFFF
SRMVODMsgVerifyCount	10
NTCIP-1218	
rsuSysRetriesEnable	1
rsuSnmpTrapsEnable	1
SAVE SAVE & APPLY BACK	

SRM_RX

SRMPermissive - Default set to 1 to enabled; RSU will not use IntersectionID to reject SRM it sees. Will process any it sees regardless of IntersectionID.

SRMTXVehBasicRole - Default is 0xFFFFFFFF; bitmask of SRM roles RSU will accept & forward to ATC.

J2735 2016 defines (32 bits)

- basicVehicle = 0,
- publicTransport = 1,
- specialTransport = 2,
- dangerousGoods = 3,
- roadWork = 4,
- roadRescue = 5,
- emergency = 6,
- safetyCar = 7,
- none_unknown = 8,
- truck = 9,
- motorcycle = 10,
- roadSideSource = 11,
- police = 12,
- fire = 13,
- ambulance = 14,
- dot = 15,
- transit_1 = 16,
- slowMoving = 17,
- stopNgo = 18,
- cyclist = 19,
- pedestrian = 20,
- nonMotorized = 21,
- military = 22



Some examples:

0x0 = NO ROLES ACCEPTED : will NOT forward anything to ATC. Will make SRM look "off".

0xFFFFFFFF = ALL ROLES ACCEPTED : will forward ALL roles to ATC.

0x1 = basicVehicle

0x2 = publicTransport

0x4 = specialTransport

0x8 = dangerousGoods

0x10 = roadWork

0x20 = roadRescue

0x40 = emergency

0x80 = safetyCar

0x100 = none_unknown

0x200 = truck

0x240 = truck & emergency

0x280 = truck & safety

SRMVODMsgVerifyCount - Default is 10; Verify one in this many SRM messages when VOD is enabled. Min is zero and Max is 65535

NTCIP 1218

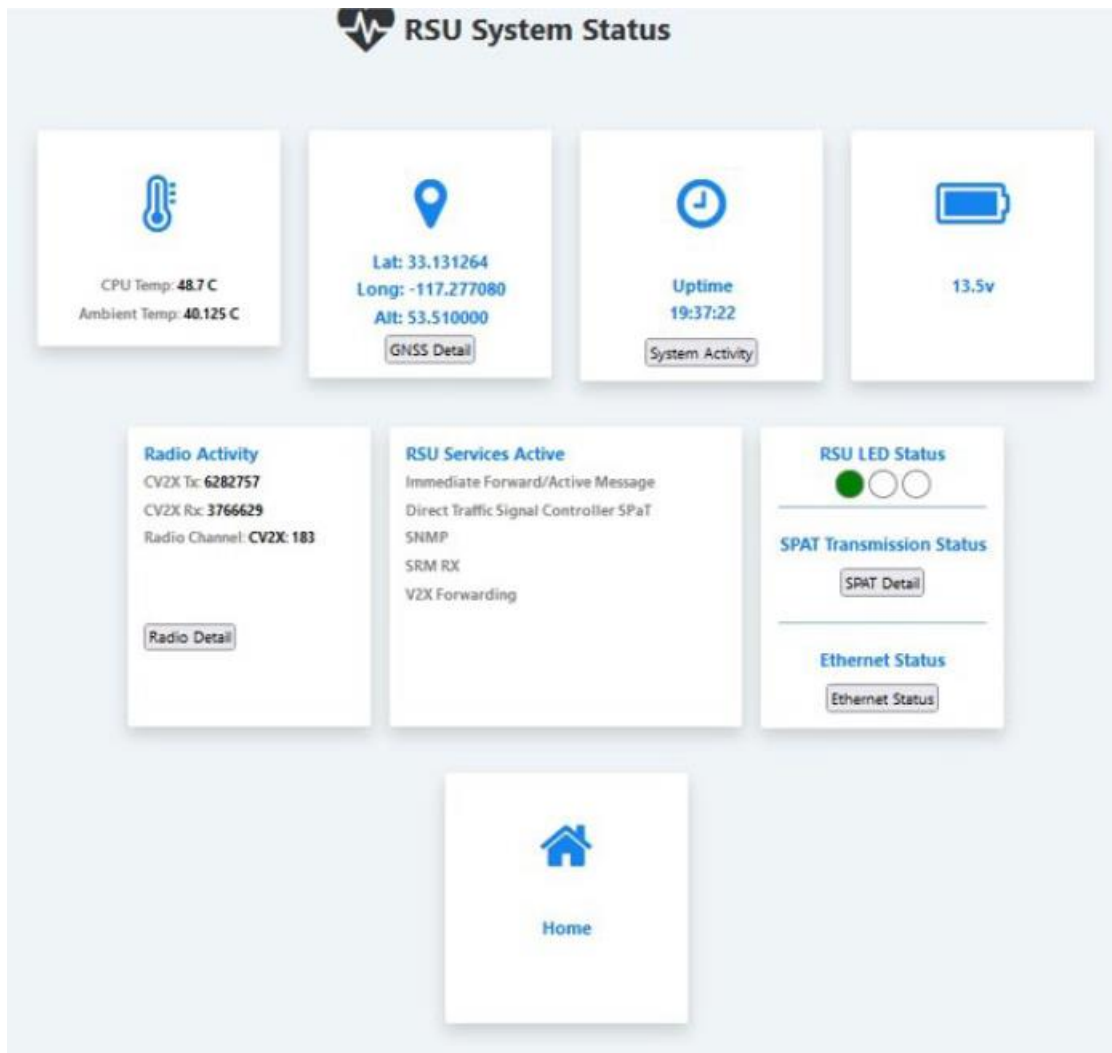
rsuSysRetriesEnable – Default is 1; 0 to disable. 1 to enable (rsuSysRetries == 15 attempts, rsuSysRetryPeriod == 5 minutes). No reboot required. Hit <SAVE> button to apply.

rsuSnmptTrapsEnable – Default is 0 to disable; 1 to enable. Reboot is required. Hit <SAVE & APPLY> button to apply, otherwise hit <SAVE> to continue and reboot later.

Status Menu

The page shows key details related to the current runtime execution of the RSU, including temperature, position information, and system activity.

The list of RSU services depends on the components active on the RSU but does not change dynamically (unless something fails). The temperature information, radio statistics, GPS information, and UTC timestamps all update on the page dynamically. The UTC clock updates each second while the rest of the dynamic items update at approximately 3 to 4 second intervals.



CPU temp - indicates the temperature of the processor of the RSU in Celsius.

Ambient Temp - indicates the temperature in the device environment.

Latitude, longitude and altitude - coordinates are provided to define a location of a subject device.

Uptime – The time elapsed since a subject device was turned on or restarted.

Battery - icon on the right of the page represents the system voltage indication. If the icon is not displayed, then the system does not have appropriate input voltage.

The radio stats shown on the page reflect activity only for the active radio interface.

CV2X Tx – Number of transmitted messages

CV2X Rx – number of received messages

Radio Channel CV2X – The number of the radio channel in use

RSU LED Status - indicate the status of the device

The page contains links to other pages with additional information. Those will be described below.

GNSS Detail

The GNSS Detail page displays additional information about the GNSS status for the RSU. The Ublox GNSS section describes the GNSS information for the RSU applications. The information in this section is also used for the system time.

The Status Detail section describes additional basic information. The GPS Antenna value may be one of the following: SupplyFail, NotConnected, Short, and Connected. The value depends on the GPS antenna hardware.

The Signal/Jamming section describes diagnostic information for the u-blox behavior.

RSU GNSS Detail

UBlox GNSS

```

source_msg_type: 000
fix_quality: 2
fix_mode: 3
date: 121224
time: 196004.00
latitude: 33.1313468
longitude: -117.2770224
altitude: 65.57
groundspeed: 0.033
course: 0.0
hdop: 0.89
pdop: 1.56
laterr: 2.13
lonerr: 2.13
alterr: 5.00
sens-major_err: 2.13
sens-minor_err: 2.13
sens-major_orient: 0.0000
numats: 13
diffage: 0.00
leap_seconds: 18
coding_is_change: 0
secs_to_1schange: -24000763

```

* Note: This GPS data is used for V2X messaging and RSU time and location

Status Detail

GPS Antenna: **Connected**

Boot to Position Fix: **35** seconds

Boot to Time Fix: **21** seconds

Boot to Time Accuracy of Cv2x: **21** seconds

UBlox Firmware version: **SPG 3.01**

UBlox Config: **DENSO RSU-S940 v1.1.0**

20220817

Signal / Jamming Detail

UBlox Noise Level: **104**

UBlox Jamming Indicator: **3.9%**

UBlox Jamming Status: **OK - no significant jamming**

[← Back](#)

 **Note:** The RSU application functionality depends on GNSS availability. When the RSU does not have a GNSS fix, it will not transmit. GNSS availability requires open sky conditions in the absence of a GNSS repeater. Be sure to confirm the system has GNSS when troubleshooting any RSU behaviors.

System Activity

The System Activity page shows the actively running tasks on the system as output using the ‘top’ Linux command. This page is useful to observe potential resource issues, such as high CPU utilization or lack of available system memory. The page updates dynamically every few seconds.


RSU System Activity

System Activity

```
top - 16:33:09 up 23:18, 0 users, load average: 0.98, 1.02, 1.05
Tasks: 111 total, 1 running, 67 sleeping, 0 stopped, 0 zombie
%Cpu(s): 1.9 us, 6.2 sy, 0.0 ni, 89.8 id, 0.0 wa, 1.6 hi, 0.5 si, 0.0 st
KiB Mem : 2735176 total, 2478048 free, 90148 used, 166980 buff/cache
KiB Swap: 0 total, 0 free, 0 used. 2468036 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3352	root	20	0	514904	19456	5932	S	11.8	0.7	168:26.44	radioServices
6276	root	20	0	3532	1652	1304	R	11.8	0.1	0:00.04	top
6215	root	20	0	38016	1712	1448	S	5.9	0.1	12:56.85	spat_app
1	root	20	0	8448	4808	3184	S	0.0	0.2	0:29.74	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.13	kthreadd
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker/0:0H
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_percpu_wq
7	root	20	0	0	0	0	S	0.0	0.0	0:05.30	ksoftirqd/0
8	root	20	0	0	0	0	I	0.0	0.0	0:30.85	rcu_preempt
9	root	20	0	0	0	0	I	0.0	0.0	0:17.75	rcu_sched
10	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_bh
11	root	rt	0	0	0	0	S	0.0	0.0	0:00.14	migration/0
12	root	20	0	0	0	0	S	0.0	0.0	0:00.00	cpuhp/0



[Back](#)

Radio Detail

The Radio Detail page shows expanded radio activity beyond the basic statistics shown on the main status page. The page displays antenna status, however, this information depends on the type of antenna connected.

If the user has enabled security, security statistics update on this page. Radio configuration and temperatures are also displayed on the page with the temperatures dynamically updating.


RSU Radio Detail

Radio Status

CVZX Tx Status: **Active**

CVZX Rx Status: **Active**

Radio Activity

CVZX Tx: **48910**

CVZX Rx: **35890**

Radio Channel: **CVZX: 183**

Antenna Status

CVZX Antenna 1: **Not Connected**

CVZX Antenna 2: **Not Connected**

Radio Message Security Activity

	Requests	Successes	Failures
Signs	0	0	0
Strips	4952	4952	0
Verifies	0	0	0

Radio Configuration

Radio Mode: **CVZX**

CVZX Transmit Channel: **183**

Transmit Power(dB): **5.0**



[Back](#)

SPAT Detail

This page will be in use only if SPAT data is sent from a traffic signal controller to the RSU device as TSCBM or Trafficware proprietary format to port 6053 or 6054. If traffic signal controller sends SPAT data in SAE J2735 format to the port 1516 to be immediately forwarded, this page will not be populated with data as the conversion is not occurring as it is not needed. Another case where this page will not be populated with data is if a user improperly configures the Signal Phase Mappings such that the input TSCBM data does not correctly match, the page shows a warning message. If the RSU has not been properly configured to receive TSCBM data or if the TSC has not been properly configured to send data to the RSU, the SPAT detail page remains empty.

Below both the Input and Output tables are additional Boolean values that may be set by the Traffic Signal Controller (TSC) when providing the TSCBM message. These Booleans indicate status messages from the TSC that may be activated in select scenarios. If a condition is active, the corresponding radio button for the status indication is selected. The TSC fully controls the status indications and the RSU only displays any values parsed. The meaning of these Booleans is appropriate for individuals familiar with traffic management, such as Traffic Engineers. The fields are not explained in this guide.


RSU SPAT Detail
Tin


Invalid Data

TSCBM Input

Phase	Vehicle	Min Time to Change	Max Time to Change	Flashing	Overlap	Min Time to Change	Max Time to Change	Flashing
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								

☐ Manual Control
 ☐ Fault Flash
 ☐ Priority (TSP)
 ☐ Coordination In-Transition
 ☐ Stop Time
 ☐ Preempt
 ☐ Coordination
 ☐ Programmed Flash

J2735 Output

Signal Group ID	Event State	Min End Time	Max End Time	Phase Source

☐ Manual Control
 ☐ Signal Priority
 ☐ Failure Mode
 ☐ No Valid MAP
 ☐ Stop Time
 ☐ Fixed Time Operation
 ☐ Controller Off
 ☐ No Valid SPaT
 ☐ Failure Flash
 ☐ Traffic Dependent Operation
 ☐ Recent MAP Message Update
 ☐ Reserved
 ☐ Preempt
 ☐ Standby Operation
 ☐ Recent Change in MAP Assigned Lanes Used
 ☐ Reserved

Revision: 127

The final data element is the Revision counter shown at the bottom of the page. This revision is parsed from the TSCBM provided by the traffic signal controller.

If everything is configured correctly, the SPAT detail page describes the dynamically updating SPAT data the system is processing. The user should select the Back link at the top of the page (not the Web browser Back button) to return to the main status page. The top of the page reflects the Traffic Signal Controller Broadcast Message (TSCBM) input data fed to the RSU. The J2735 Output table on the page shows the corresponding J2735 message that is transmitted based on the input TSCBM data after the message conversion is complete.

TSCBM Input									
Phase	Vehicle	Min Time to Change	Max Time to Change	Flashing	Overlap	Min Time to Change	Max Time to Change	Flashing	
1	Red	110	121	No	Dark	0	0	No	
2	Green	45	45	No	Dark	0	0	No	
3	Red	51	51	No	Dark	0	0	No	
4	Red	59	70	No	Dark	0	0	No	
5	Red	110	121	No	Dark	0	0	No	
6	Green	45	45	No	Dark	0	0	No	
7	Red	51	51	No	Dark	0	0	No	
8	Red	59	70	No	Red	51	51	No	
9	Dark	0	0	No	Dark	0	0	No	
10	Dark	0	0	No	Dark	0	0	No	
11	Dark	0	0	No	Dark	0	0	No	
12	Dark	0	0	No	Dark	0	0	No	
13	Dark	0	0	No	Dark	0	0	No	
14	Dark	0	0	No	Dark	0	0	No	
15	Dark	0	0	No	Dark	0	0	No	
16	Dark	0	0	No	Dark	0	0	No	

J2735 Output				
Signal Group ID	Event State	Min End Time	Max End Time	Phase Source
1	STOP_AND_REMAIN	1849	1860	Vehicle 1
2	PROTECTED_MOVEMENT_ALLOWED	1784	1784	Vehicle 2
3	STOP_AND_REMAIN	1790	1790	Vehicle 3
4	STOP_AND_REMAIN	1798	1809	Vehicle 4
5	STOP_AND_REMAIN	1849	1860	Vehicle 5
6	PROTECTED_MOVEMENT_ALLOWED	1784	1784	Vehicle 6
7	STOP_AND_REMAIN	1790	1790	Vehicle 7
8	STOP_AND_REMAIN	1798	1809	Vehicle 8
9	STOP_AND_REMAIN	1790	1790	Overlap 8

 **Note:** A user *MUST* first configure the Signal Phase Mappings for the RSU to transmit J2735 encoded SPAT messages.

Ethernet Status

The Ethernet Detail page shows additional information about the network interface. The information on this page dynamically updates every two seconds while viewing the page. Items displayed relate to Ethernet activity, the IP addresses and routes, and the speed of the network link. The user should use the Back button on the bottom of the page to return to the main status page.

 **RSU Ethernet Detail**

Ethernet Properties

Active NIC: **eth0**

Link Detected: **yes**

Link Speed: **100Mb/s**

Ethernet Interface Activity

```
eth0      Link encap:Ethernet  HWaddr b2:f2:a9:80:4f:a7
          inet addr:192.168.1.76  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::b0f2:a9ff:fe80:4fa7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:51421 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7332 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6097338 (5.8 MiB)  TX bytes:2048433 (1.9 MiB)
```

IP Show Dev

```
2: eth0:  mtu 1500 qdisc mq state UP group default qlen 1000
   inet 192.168.1.76/24 brd 192.168.1.255 scope global eth0
        valid_lft forever preferred_lft forever
```

IP Route

```
default via 192.168.1.1 dev eth0
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.76
192.168.2.0/24 dev eth0 scope link
```



Back

Advanced Status

The Advanced Status page provides version information about various components of the RSU device with limited meaning to end users (the Ethernet MAC is displayed on this page, which is a useful item for end users). Use this page when instructed by Iteris to collect data for debug purposes.

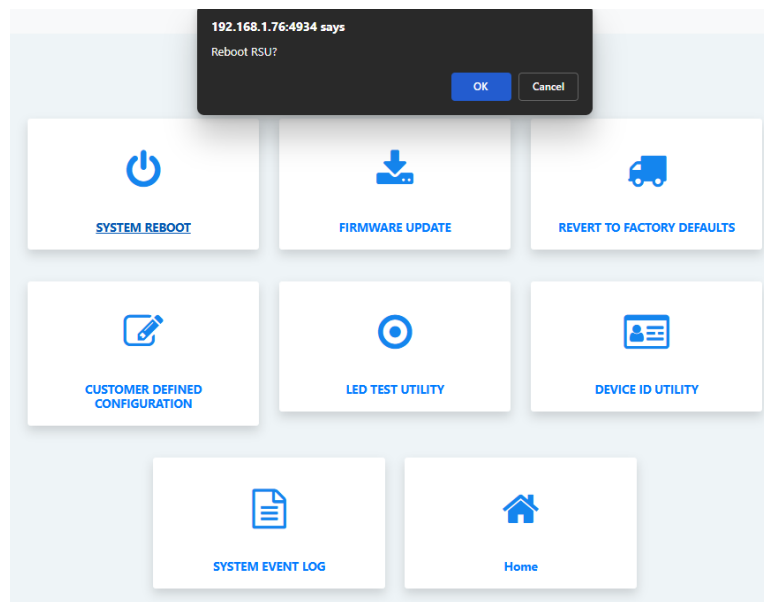


Utilities

The Utilities section provides operators with a consolidated control surface for essential device maintenance and lifecycle actions. From this module, users can initiate a controlled reboot of the device, apply software or firmware updates, and perform a full or partial revert to factory defaults when recovery or reconfiguration is required. The section also offers direct access to system and application logs, enabling efficient troubleshooting and diagnostics

System Reboot

A user can initiate a device reboot from the Utilities page. After initiating the reboot procedure, a user is asked to confirm the intent before proceeding.



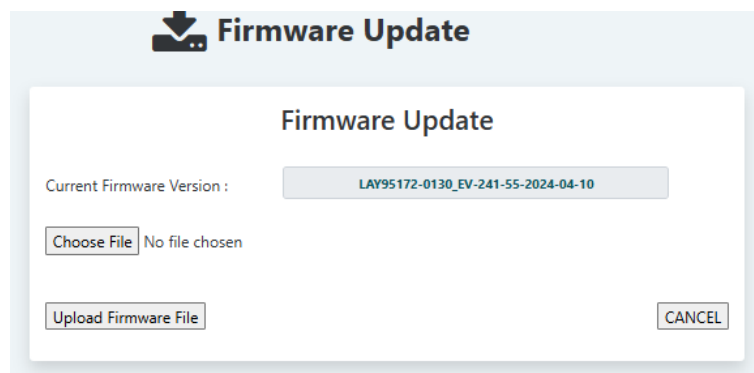
After a user triggers the reboot process, the user interface cannot provide access to an RSU device until the reboot is completed. A countdown appears indicating the remaining time until a reboot is completed, and finally a confirmation that the reboot is performed with a link to log back into a device appears.



A user must select the link displayed on the GUI to return to the log in screen to resume a GUI session. The browser does not automatically redirect to the login page once the RSU reboots. Please allow a few seconds after the page above is shown before attempting to log in again.

Firmware Update

When a user selects the Firmware Update option through the UI, the following page is displayed. It is recommended that a user reboot the system prior to launching a firmware update. Depending on how long the RSU has been operational, a system reboot may clear potential performance problems that could interfere with the firmware update.



Browse - Use this button to select the firmware image from the local system.

Upload Firmware File - Once an image is selected, press this button to begin transfer of the file to the RSU. An example is shown in the following graphics of the GUI display during the transfer.

Once a user selects an appropriate image file, press the Upload Firmware File button when ready to begin the firmware upgrade process. The firmware file uploaded is first validated before the upgrade proceeds. Once properly validated, the update process continues.



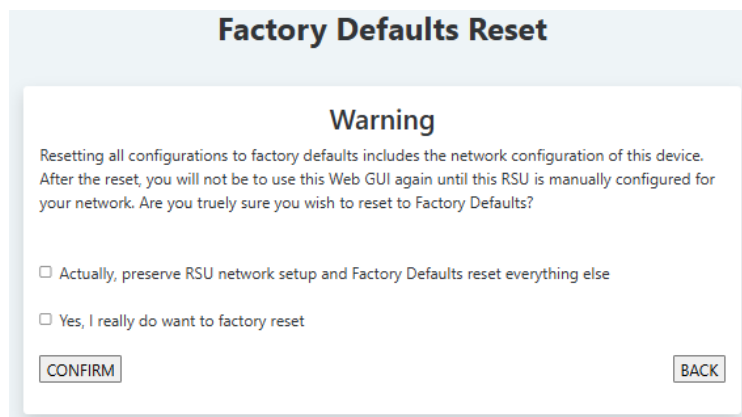
When the process is complete a user is notified about the outcome. Upon the successful completion of the firmware update process, the button at the bottom of the page transitions to Reboot. The user may choose to reboot the RSU immediately or use the Back button to continue RSU operation. The firmware upgrade process, once completed, does not require an immediate reboot. The RSU applies the new firmware after the next reboot, whether triggered immediately, or manually invoked by the user at a later time.

If there is an error in the firmware update process, an appropriate message is displayed. The user should review the message and if necessary seek additional support. If the message does not reflect a critical failure, the user may retry the update. The firmware update process has no impact on the currently executing firmware on the RSU device. If a unit fails to upgrade, the unit may be rebooted without side effects before retrying the update.



Revert to Factory Defaults

Reverting to factory defaults is useful when a user is experiencing problems and is unsure of configuration changes that were applied, or for when a user wants to reuse an RSU device for a different installation. A user must first check the 'Yes, I really do want to factory reset' selection box to proceed. Because all settings are erased, the process is designed to minimize the likelihood of a user erasing the configuration by accident.



By default, the factory reset operation resets all network settings, including the IP address, to their default values. However, this may result in the RSU being unusable immediately after performing the action depending on the managed network. Hence, a selection box is also available to preserve the RSU network settings when performing a reset to allow the RSU to be accessible at the existing

IP address. A user may want to choose this option when performing a reset if he/she wishes to have access to the GUI immediately after the reset. In addition to the static IP address and subnet mask, network settings that are preserved when this option is chosen are: DHCP enable, Gateway settings, Network MTU, VLAN settings, Proxy server settings, and SSH port.

The rsuuser account password, the Web GUI port, and all other configurable settings, including NCTIP-1218 settings, are always reset to their default values. If a user selects to revert a device to factory defaults, the device will reboot so the default settings take effect.

Customer Defined Configuration

The current device configuration can be saved so it can be restored in the future if desired. All settings available for configuration in the Web UI are included in the customer defined configuration. A user should first perform any desired configuration changes for the RSU. When complete, the user may then save the configuration as the customer baseline. If additional configuration changes are performed in the future, a user may return and update the baseline. Additionally, a user may choose to restore previously saved baseline configuration using this utility page.

Customer Defined Configuration: Backup and Restore

Backup Current Configuration

Backing up the current RSU configuration will overwrite any previously backed up customer defined configuration.

☐ Yes, I really do want to backup the current configuration

CONFIRM

Restore Customer Configuration

Restoring a customer defined configuration includes the network settings of this device. After the reset, you will not be able to use this Web GUI again until manually resetting network settings, unless the backed up settings are configured for your network. Are you sure you wish to restore the backed up customer defined configuration?

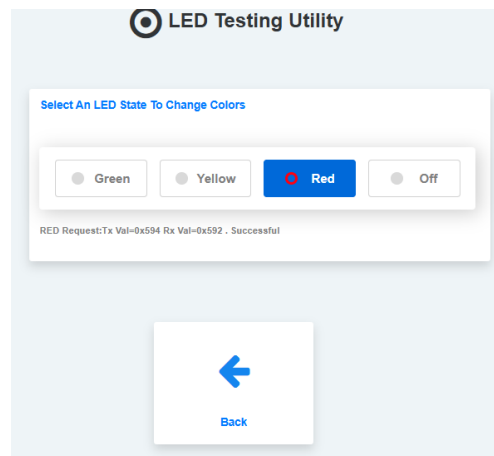
☐ Yes, I really do want to restore the previously backed up customer defined configuration

CONFIRM

BACK

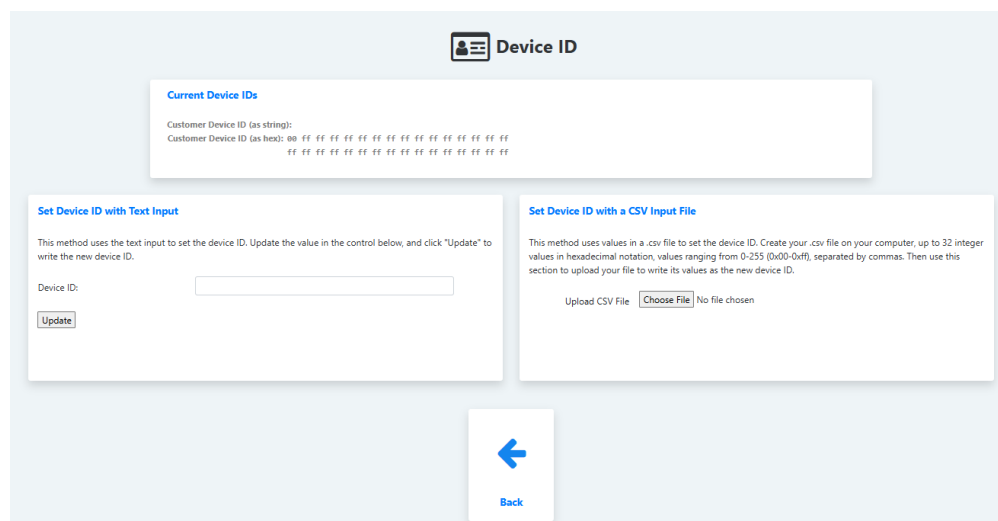
LED Test Utility

The LED Test Utility page allows a user to perform a visual diagnostic for installed devices with appropriate LED hardware. The utility allows the user to activate the color of the LED that is displayed in the field. Select from the Green, Yellow, or Red buttons to activate the associated LED. Select the Off button to deactivate all the LED indications.



Device ID Utility

The Device ID page allows a user to change the customer reserved portion of the platform's device ID. A device ID is preprogrammed and allows a user to program a customer identification as a string with up to 32 characters or as a hex value. The Current Device IDs table displays the values that are already programmed, where the customer ID displays ASCII (when possible) and hex.



The text or CSV upload options overwrite any customer device ID that is already present. Be aware that the device has a limited number of writes in its lifetime, so frequent changes to the device ID are not recommended.

If a provided Customer Device ID is too long, the user interface will indicate that.

System Event Log

The System Event Log contains the logs collected while a device was operational between power ups. A user can enable the logging when desired. The available logs are displayed in the Stored Logfiles table on the page. Select any log to see the content. The page defaults to Sort Ascending whenever it is loaded. When a log file is selected, the Logfile Content table shows the log data

System Event Log

Settings

☒ Enable Enhanced Logging

Stored Logfiles

Click on a file name to view the file contents in a popup window

☒	i2vstat_20240410_000628--0000000038--1.0.log
☐	i2vstat_20240410_000629--0000000036--1.0.log
☐	i2vstat_20240410_000632--0000000032--1.0.log

Logfile Content - i2vstat_20240410_000628--0000000038--1.0.log

```

*****
/rwflash/I2V/syslog/i2vstat_20240410_000628--0000000038--1.0.log
*****

EVENT TIME | NAME | LEVEL | DETAIL
*****
20240410_000637 | dnnet | INFO | MTU applied to interface (eth0): 1500
20240410_000637 | dnnet | INFO | No VLAN to activate
20240410_000637 | dnnet | CRIT | dnnetcfg: ERROR: invalid rule: ()
20240410_000639 | rsu_table | DBG | rsuAsync start file does not exist. No traps enabled.
20240410_000639 | rh850 | DBG | Count of watchdog timeout resets since last power cycle: 0
20240410_000639 | rh850 | DBG | Count of total watchdog timeout resets: 3
20240410_000639 | cv2x | DBG | Host:
20240410_000639 | cv2x | DBG | CV2X version: 5.17.0 (SPI)
20240410_000639 | cv2x | DBG | Software version: section-5.17.0-rel
20240410_000639 | cv2x | DBG | Device:
20240410_000639 | cv2x | DBG | SDK version: 5.17.0 (SPI)
20240410_000639 | cv2x | DBG | Software version: section-5.17.0-rel
20240410_000639 | cv2x | DBG | DSP:
20240410_000639 | cv2x | DBG | Software version: 3.10.0 rc1-bld7
20240410_000639 | cv2x | DBG | Baseband V2X:
20240410_000639 | cv2x | DBG | Hardware version: 3.0
20240410_000639 | cv2x | DBG | MAC CV2X Version: 3.9.0-0 (5.17.0 (SPI))
20240410_000640 | rsk | DBG | rsk(0x2) wsm(0x0)
20240410_000648 | i2v | INFO | i2v waiting for iwmh on radio0 to start up
20240410_000648 | iwmh | INFO | i2v operating on radio 0 in continuous mode
20240410_000648 | iwmh | INFO | (6206) ready to operate (5, 0)
20240410_000648 | i2v | INFO | i2v done waiting for iwmh
20240410_000648 | i2v | DBG | i2v (3393) executing fwdmsg (6213). errno=0.
20240410_000648 | i2v | DBG | i2v (3393) executing scs (6214). errno=0.
20240410_000648 | i2v | INFO | number of processes loaded is 5.

```

By default, the Enhanced Logging is not enabled. The content in the logs contained on the device is limited if enhanced logging is not enabled. Select the Enable Enhanced Logging checkbox and then click either the Save or Save & Apply buttons in the Settings table. The RSU must be rebooted for the setting to be adjusted and it is a persistent setting. Use the Save & Apply button to immediately trigger the RSU reboot.

BlueTOAD Spectra Setup Procedures

 **Important:** Contact Iteris support, 1 (888) 254-5487, before you install any equipment to make sure all devices have been correctly tested and operate using the latest firmware and application software.

Purpose

The procedures in this chapter tell you how to deploy a Iteris BlueTOAD Spectra speed/travel time detector system and then start to collect data. We assume you are familiar with the Ethernet-based communications network of your Agency and the supporting equipment listed below.

Supporting Equipment

- Windows PC and Ethernet Cables¹
- Portable Laptop, Apple iPad or Android-based tablet with wireless Internet access
- Web browser – Google Chrome or Windows Edge are preferred
- Iteris BlueTOAD Spectra detector

System Setup Procedures

The procedures that follow tell you how to deploy and test a BlueTOAD Spectra speed/travel time detector system.

 **Note:** After notice to proceed is approved, Iteris and key collaborative team personnel will work with your Agency to create a formal deployment, implementation and operations plan document for your BlueTOAD system.

Pre-Install Evaluation

Before you install a BlueTOAD system, make sure things are ready at the installation sites.

Location – Prepare a sight survey of intersection locations that have been selected to deploy BlueTOAD Spectra detectors.

Identify power sources available in the traffic cabinets.

Before you install a BlueTOAD Spectra:

Make sure a site survey checklist has been completed for all locations.

Make sure you have all the necessary parts for the system. Refer to the table on [Page 3-1](#) for a list of the items included with your BlueTOAD Spectra RSU.

¹ Ethernet Cables are NOT necessary for the BlueTOAD Spectra Solar Cellular detector.

Network and Communications Setup Parameters

Traffic Network – Evaluate the existing network.

1. Fiber and/or Ethernet based? Or no network communications?
2. Confirm that the network settings (for example, IP address, gateway, subnet mask, and DNS) are correctly set and that all ports (see below) are open and set for outbound data traffic.
3. What is the IP address assigned to the BlueTOAD Spectra and BlueTOAD Spectra RSU?
4. Port 10001 needs to be open to 52.39.79.127 (to collect DSRC Connected Vehicle specific data – to be deprecated)
5. Port 10002 needs to be open to 52.39.79.127 (to collect C-V2X Connected Vehicle specific data)
6. Port 8010 needs to be open to btserver.trafficcast.com
7. Port 8892 needs to be open to SCMS enrollment
8. Port 443 needs to be open to bluetoad.iteris.com for HTTPS
9. Port 123 needs to be open, only if using an external NTP server.
10. Required DNS entries for btserver.trafficcast.com:
 - ♦ 18.220.189.165
 - ♦ 3.18.180.164
 - ♦ 3.18.166.19

How to Configure the BlueTOAD Web IP

To configure the Web IP of the BlueTOAD Spectra or the BlueTOAD Spectra component of the BlueTOAD Spectra CV²:

1. Connect the Ethernet BlueTOAD™ to a switch or laptop Ethernet port.

 **Note:** *With this connection, an Ethernet BlueTOAD can auto-negotiate.*

2. Power ON the Ethernet BlueTOAD™.
3. Log into the BlueTOAD Spectra detector:
 - a. Open a Web Browser (Google Chrome or Microsoft Edge is preferred).

² You configure the Web IP for a BlueTOAD Spectra travel time component of the BlueTOAD Spectra RSU. The BlueTOAD Spectra RSU is a dual radio system that includes both a BlueTOAD 2.4 GHz Bluetooth detector unit, as well as a BlueTOAD DSRC, 5.9 GHz radio system unit.

- b. Enter the default BlueTOAD Spectra IP address (192.168.1.77) and URL (<http://192.168.1.77:8080/admin.cgi>)

 **Note:** If the IP address has been changed from the factory default, use the new IP address to access the login website.

- c. For the configuration tool to proceed, you must use the username and password given below at the default address:

Username: **admin**

Password: **77admin77**

After login, the **BlueTOAD Device Administration** screen will open.

- d. To change any of the fields in the **System Settings** area:

- i. Enter the new value into each field.

 **Note:** For a helpful workbook to keep a record of the values in each field, consult *Preprogramming installation cheat sheet*.

In the middle left of the page, select BlueTOAD Programming Cheat Sheet.xlsx At the bottom left of the Excel page, select the Pre Installation Sheet tab.

- ii. When done, click Submit Changes. The BlueTOAD Spectra resets automatically.

 **Important:** If you change the IP address, **keep a record of the new BlueTOAD Spectra IP address** because you must use the new IP address to log back into this same device! Without the correct IP, you CANNOT log in.

BlueToad Device Administration

Device Info

Device Id: 2136174
GMT System Time: 01/01/07 00:01:08
Firmware Version: 04.00.01.543
Ethernet MAC Address: fc:c2:3d:20:98:6e

System Settings

IP Type: ☒ static ☐ dhcp
Cellular System: ☐ on ☒ off
Cellular APN: **broadband**
Static IP Address: **172.20.5.91**
Static Netmask: **255.255.255.0**
Static Gateway: **172.20.5.1**
Static DNS Server: **8.8.8.8**
NTP Server: **192.168.1.5**
BT Server: **btserver.trafficcast.com**
Update Server: **btserver.trafficcast.com**

Radio Detector Settings

BT Classic Radio1: ☒ on ☐ off
Spectra Radio: ☒ on ☐ off

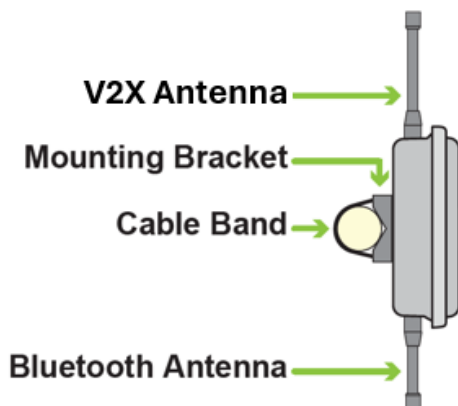
Submit Changes

Installation & Maintenance of BlueTOAD Spectra (CV)

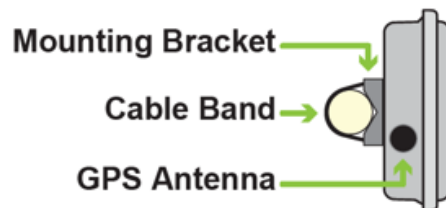
Guidelines to install an RSU enclosure:

1. **Mounting Structure** - Mast Arm or Roadside Pole that:
 - a. Is near the roadside traffic signal cabinet, or appropriate 120 VAC power source
☒ **Note:** *The mounting pole should be near the cabinet for easy conduit access.*
 - b. Has a mounting location with a clear line-of-sight from the RSU antennas to the target road segment
 - c. **Mounting Height** - 8 meters (26.3 feet) to 15 meters (49.2 feet) above the roadbed
2. Mount the Enclosure to a Signal Mast Arm, Mast Arm³ or Pole
 - a. Insert the two metal Cable Bands through their slots in the Mounting Bracket.
☒ **Note:** *The Mounting Bracket is “dual-direction,” designed to mount on either a horizontal or vertical pole.*
3. Wrap the Cable Bands around the pole.
☒ **Note:** *The Cable Bands are designed for mounting on Mast Arms, Poles, I-Beams or other support structures up to 14” in diameter.*
4. Use a drill to tighten the Cable Bands with a 5/16” nut driver bit or equivalent.

**Mast Arm (Horizontal) Mount
- Side View**



**Pole (Vertical) Mount
- Top View**

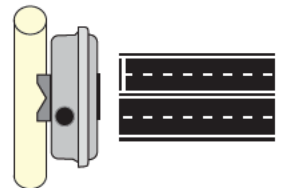


³ The preferred installation is on a Mast Arm, as shown on the next page.

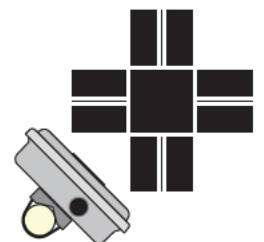


5. Align the Enclosure per your installation as shown below:

Mast Arm Installation - To achieve optimal line-of-sight, RSU should be mounted near as possible to center of intersection.



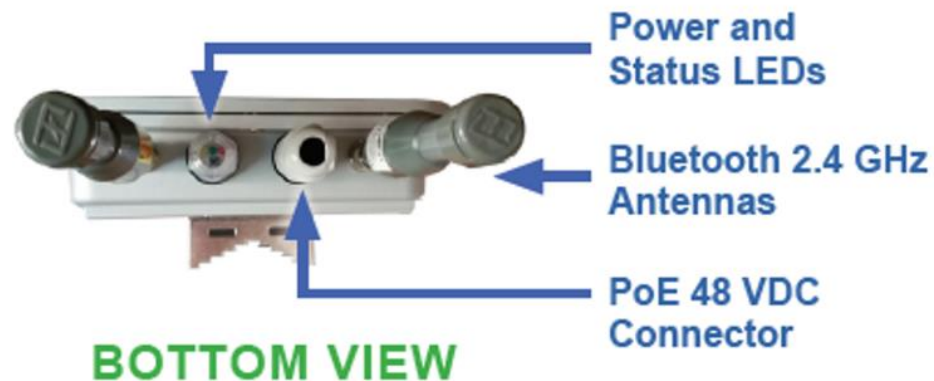
Pole Mount Installation - To achieve optimal line-of-sight, RSU should be mounted at 45 Degree angle, pointed at center of intersection.



6. Guidelines to route and connect the cables:

- a. Traffic Closure—Close traffic lanes as necessary to pull cable.
- b. CAT-5 Ethernet Cable
 - ♦ Pull the main CAT-5 Ethernet Cable through the roadside conduit from the roadside cabinet to the enclosure.
 - ♦ Connect the Ethernet cable to the PoE 48 VDC Connector on the bottom of the enclosure.

✓ **Note:** The PoE 48 VDC connector goes to the PoE Splitter that also sends data from the Spectra RSU to the PoE Injector inside the cabinet.



✎ **Important:** To seal the antenna (lightening suppression) connectors against rust and corrosion, protect them per the Required Best Practice instructions shown below.

✓ **Note:** The BlueTOAD Spectra RSU ships with the antenna connectors pre-wrapped with watertight sheathing.

NOTE: Required Best Practice!

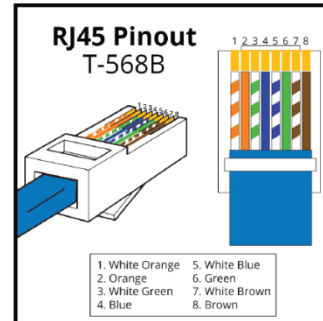
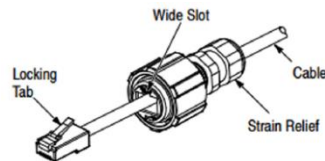
It is required to wrap antenna metal connectors with Hand Moldable Plastic COAX-SEAL. Seals connectors from moisture and corrosion.

ALL Iteris RSU installations will utilize Plastic COAX-SEAL for antenna connectors.



- ♦ Pass the cable through the Liquid-Tight Cable Gland of the Ethernet cable Coupler and terminate it to an RJ45 connector per the pinout shown.

✓ **Note:** You will have to remove the Strain Relief on the cable to pass it through the Cable Gland. However, you can slide the Strain Relief away from the RJ-45 connector without cutting the Strain Relief.

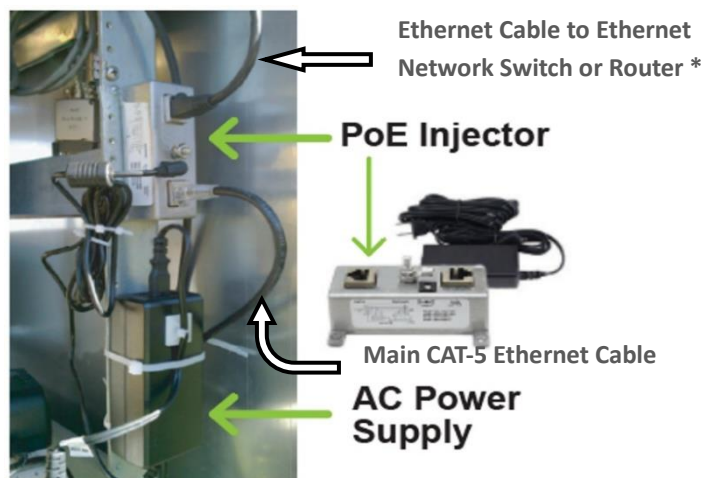


7. Install the PoE Injector in the roadside cabinet:

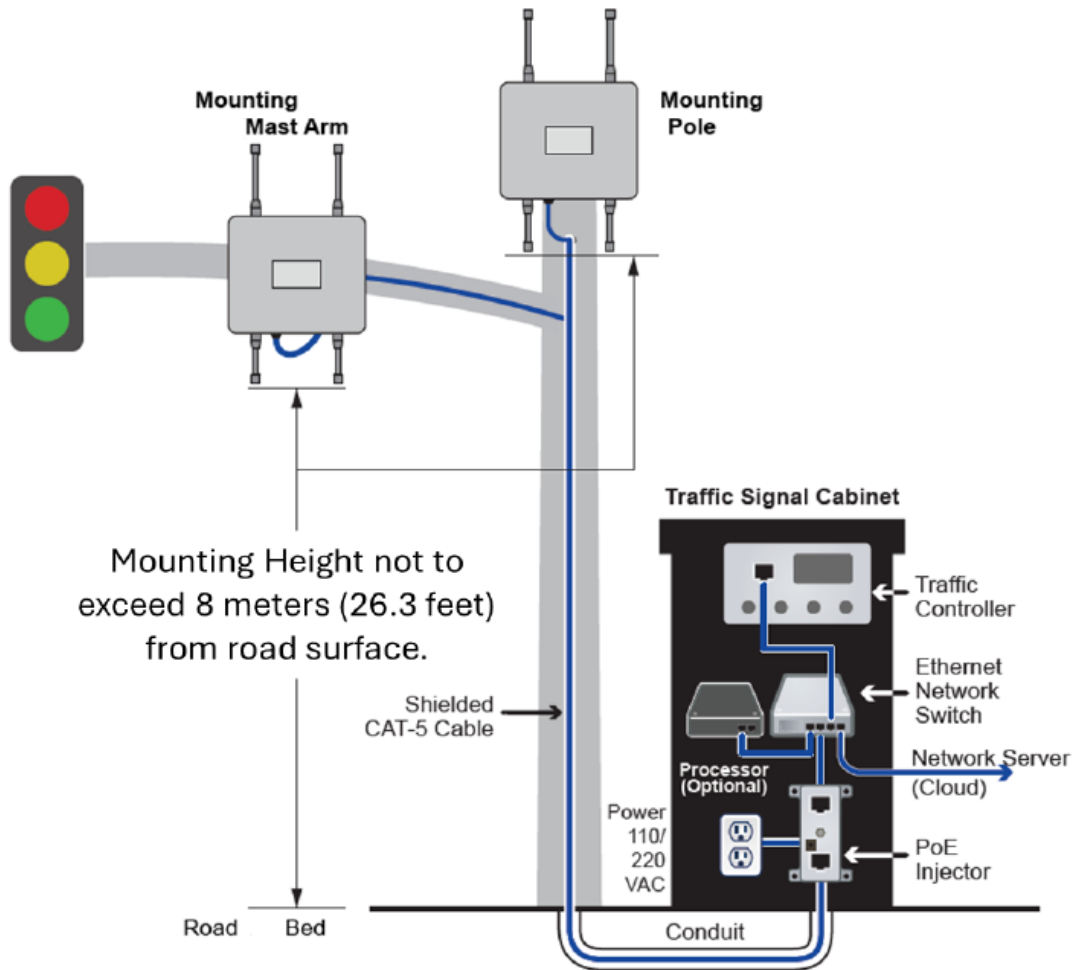
- Secure the PoE injector onto a flat surface inside the roadside cabinet.

✓ **Note:** The PoE Injector has two RJ-45 ports: Data—connects to the network Ethernet switch, router or hub; Data and Power—connects to the device

- Connect the ground wire.
- Connect the Main CAT-5 Ethernet Cable to the PoE Injector.
- Connect an Ethernet cable from the PoE Injector to the cabinet LAN/WAN Ethernet Network Switch or Router.
- Connect the Ethernet Network Switch to the Traffic Controller.
- Connect the AC Power Supply to the PoE Injector.
- Plug the 110 VAC cord into an AC power outlet receptacle.



8. This is the completed installation of a Spectra CV that shows both possible ways to mount the enclosure—on a Mast Arm and a Pole:



Testing a BlueTOAD Spectra RSU After Field Installation

1. Plug the Ethernet cable into the PoE Injector to power ON the Spectra RSU.
2. Confirm that all LEDs are normal after the unit initializes:

RSU Bottom View



LED Indicators

Green – Device operational

Amber – Device ON

Red - Fault

3. Before leaving the location:
 - a. After the unit is Powered ON, call Iteris Customer Support at **(888) 254-5487**.
 - i. Tell Iteris the device ID number and that the LEDs are normal.
 - ii. Confirm from Iteris that the network is transmitting the SPaT and MAP data from this unit.
 - b. Access Iteris RSU status using the web based VantageARGUS CV software.
 - i. Login credentials (Username and Password) are provided to each User, based on their predetermined Role (Admin or User) when the Account is initially setup.
 - ii. VantageARGUS CV Website: <https://vantagearguscv.iteris.com/>
4. Add each installed Iteris RSU unit to a compiled list of unit location data. For each unit, keep a record of device ID, location, and installation date.

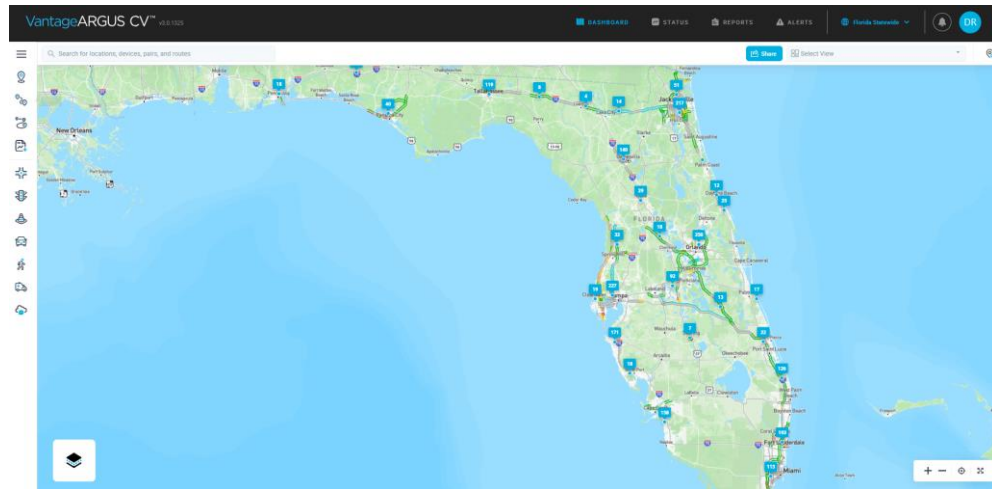
Important: Contact Iteris support, (888) 254-5487, before you install any equipment to make sure all devices have been correctly deployed and tested.

Confirm Network Connectivity and Data Collection

Now that you have tested the LEDs, make sure that data is being received by Iteris:

- a. Using a laptop, iPad or Android tablet with access to the Internet, launch Google Chrome or Microsoft Edge web browser.
- b. Log in to VantageARGUS CV (Iteris will provide login Username and Password before installation).

VantageARGUS CV Login page: <https://vantagearguscv.iteris.com/>



- Go to the Data Explorer page under Account information by clicking on the user icon with initials in the upper right corner to test that data collection is active and generate a diagnostics report: <https://vantagearguscv.iteris.com/account/data-explorer>
- For BlueTOAD Spectra detections, select Detections from the Table dropdown.
- Insert the BlueTOAD Device serial number or location ID if a device is assigned to a location.
- Click the Explore button to open the diagnostics report. BlueTOAD Spectra should start to collect data within 2-5 minutes after you enable power connections.

VantageARGUS CV™ v3.0.1259

DASHBOARD STATUS

Account

- Profile
- Organization

Access

- Users
- Recipients
- API Token

Configuration

- Locations
- Devices
- Pairs
- Routes
- CV Fleet
- Speed Thresholds
- Diagnostics
- Data Explorer**

Data Explorer

Table: Detections Location ID or Serial Number: 9361 Period: Last 24 hours Explore

Location ID	Serial Number	MAC Address	RSSI	Type	Created At
9361	1596964	41:42:73:62:40:bd	87		11/14/2025, 12:11:00 PM
9361	1596964	00:00:00:7b:72:be	92		11/14/2025, 12:11:00 PM
9361	1596964	74:d7:ca:ed:02:00	80		11/14/2025, 12:11:00 PM
9361	1596964	00:00:00:4f:76:ac	93		11/14/2025, 12:11:00 PM
9361	1596964	14:13:0b:1fb7:cc	79		11/14/2025, 12:11:00 PM
9361	1596964	00:00:00:1fb7:cc	94		11/14/2025, 12:11:00 PM
9361	1596964	00:00:00:7d:82:fa	81		11/14/2025, 12:11:00 PM
9361	1596964	00:00:00:7d:82:fa	87		11/14/2025, 12:11:00 PM
9361	1596964	00:00:00:1fb7:cc	90		11/14/2025, 12:11:00 PM
9361	1596964	00:00:00:1fb7:cc	88		11/14/2025, 12:11:00 PM
9361	1596964	14:8f:21:ed:3a:bd	82		11/14/2025, 12:11:00 PM
9361	1596964	14:13:0b:1fb7:cc	82		11/14/2025, 12:11:00 PM
9361	1596964	14:13:0b:1fb7:cc	85		11/14/2025, 12:11:00 PM
9361	1596964	10:a8:82:ad:6d:69	68		11/14/2025, 12:11:00 PM

Troubleshooting

Troubleshooting BlueTOAD Spectra Connectivity

After the detector has started detecting Bluetooth signals, communicated the device ID number, and the LEDs are normal:

1. Call the Iteris **Customer Support Number**, (888) 254-5487.
2. Confirm from Iteris that the network is transmitting the data from this detector.
3. Possible issues include:
4. Network Port settings are incorrect – confirm the settings with the Agency IT department (as above)
5. Ethernet switch port not active or communicating
6. BlueTOAD Spectra not powered – check PoE connections

Troubleshooting of Server Errors

Error Message	Possible Issues
NTP Server Error	Port 123 is not open NTP server address is not correct
BlueTOAD Server Error	Port 8010 or 443 is not open TCP protocol not allowed BlueTOAD server address is not correct
NTP Server Error – or – BlueTOAD Server Error	IP address is not correct Gateway address is not correct DNS address is not correct Port 53 for DNS is not open DSN UDP protocol not allowed EMAC address is blocked

Record Keeping

In the pre-installation process, Iteris adds each installed BlueTOAD detector to a list of detector locations within the VantageARGUS CV web-based reporting application (for your records, also keep a list of device ID, location, and installation date for each detector).

 **Note:** For a helpful workbook to keep a record of information for each detector, use *BlueTOAD Programming Cheat Sheet.xlsx*

Customer Support Number: (888) 254-5487

Iteris Support email address: iteris-techsupport@iteris.com



Data and Device Management via VantageARGUS CV

Iteris Support will set up and configure Agency access to VantageARGUS CV data collection and management system.

- You can monitor each BlueTOAD detector using the web-based VantageARGUS CV software.
- You will be given login credentials (Username and Password) before field installation, based on your predetermined Role (Administrator or User) when the Account was initially set up.

VantageARGUS CV Website: <https://vantagearguscv.iteris.com/>

On-Going Operations / On-Going Customer Support

Each Connected Vehicle system deployed will have access to the full suite of support resources available through the Iteris and BlueARGUS system management software:

Iteris Support email address: iteris-techsupport@iteris.com

Iteris Support Phone Number: (888) 254-5487

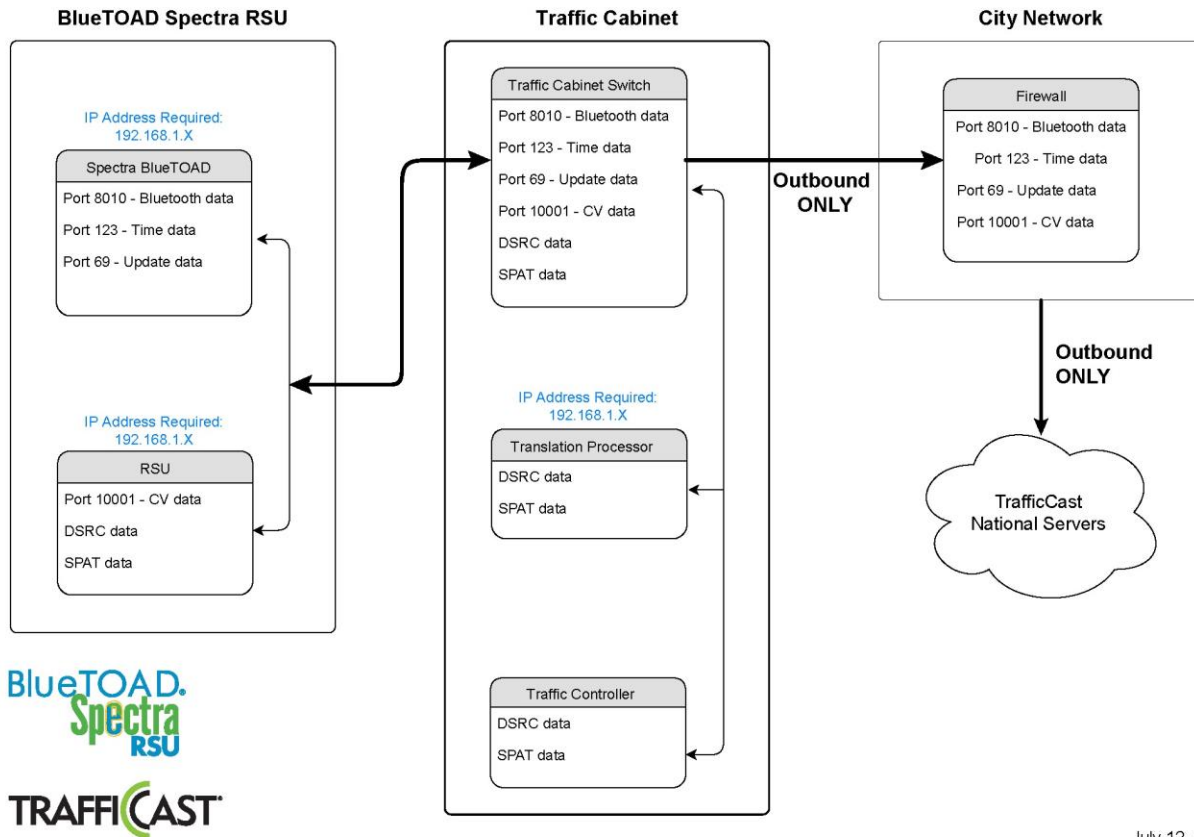
Appendix 1 – BlueTOAD Spectra RSU, Recommended Network Configuration Implementation Requirements

Local Network Settings

Local network settings requirements for data collection and management:

1. BlueTOAD Module assigned: IP Address, Subnet Mask and Gateway
2. C-V2X Module assigned: IP Address, Subnet Mask and Gateway
3. In-Cabinet Processor assigned: IP Address, Subnet Mask and Gateway Network Port Configuration:
4. Port 10002 needs to be open to 52.39.79.127 (C-V2X Connected Vehicle specific data)
5. Port 8010 needs to be open to btserver.trafficcast.com
6. Port 8892 needs to be open to SCMS provider
7. Port 443 needs to be open to <http://bluetoad.iteris.com/>
8. Port 123 needs to be open, only if using an external NTP server.
9. Required DNS entries for btserver.trafficcast.com:
 - a. 18.220.189.165
 - b. 3.18.180.164
 - c. 3.18.166.19

Network Overview Diagram



July 12, 2018

BlueTOAD Spectra RSU Communications Protocols and Usage Guide

Device Access - User Interface, terminal sessions, and file transfers

Remote Access (Device)	VPN/Admin network --> Traffic Device Network (Port)	TCP/UDP	Description (Protocols/Usage)
RSU	443	TCP	HTTPS interface
RSU	1516	UDP	Used for immediate forward
RSU	4934	TCP	HTTP (GUI for RSU config web page)
RSU	5922	TCP	RSU SSH port
RSU	6053 or 6054		Used for TSC communication – mainly conversion from TSCBM or proprietary SPaT formats into SAE J2735
RSU	161 and 162	UDP	SNMP/SNMPTRAP
BlueTOAD	22	TCP	SSH
BlueTOAD	80	TCP	HTTP
BlueTOAD	443	TCP	HTTPS
In-Cabinet Processor	22	TCP	SSH
In-Cabinet Processor	80	TCP	PedSafe Web UI
In-Cabinet Processor	443	TCP	PedSafe Web UI
In-Cabinet Processor	161	TCP and UDP	SNMP
In-Cabinet Processor	1883	TCP	MQTT (Message Queuing Telemetry Transport) publish-subscribe network protocol for interaction with Iteris detection system APIS
In-Cabinet Processor	8883	TCP	MQTT for interaction with Iteris detection system APIS
In-Cabinet Processor	4442	TCP	SSH

Agency Network Access for Data Management

Remote Access (Device)	VPN/Admin network --> Traffic Device Network (Port)	TCP/UDP	Description
RSU	10001	UDP	DSRC Data
RSU	10002	UDP	CV2X Data
RSU	53	TCP and UDP	DNS
RSU	8892	TCP and UDP	SCMS - TLS over TCP/IP for SCMS functions (e.g., enrollment and certificate top-offs) with Green Hills/ISS server addresses (possible range from 64.22.157.96 - 64.22.157.111 - the SpectraRSU uses 64.22.157.108 exclusively)
BlueTOAD	8010	TCP	Bluetooth Detection Data - Outbound data to btserver.trafficcast.com (if future BlueTOAD/BlueARGUS functionality required/desired by Agency)
BlueTOAD	53	TCP and UDP	DNS
BlueTOAD	123	UDP	NTP
In-Cabinet Processor	443-450	TCP	TCI Amazon Service Access
In-Cabinet Processor	53	TCP and UDP	DNS
In-Cabinet Processor	123	UDP	NTP
In-Cabinet Processor	443	TCP	api.twilio.com
In-Cabinet Processor	8086	TCP	metiri.mhcorbin.com (PedSafe)
In-Cabinet Processor	22	TCP	metiri.mhcorbin.com (PedSafe)
In-Cabinet Processor	587	TCP	express-relay.jangosmtp.net
In-Cabinet Processor	1883	TCP	mqtt.mhcorbin.com (PedSafe)
In-Cabinet Processor	8883	TCP	mqtt.mhcorbin.com (PedSafe)

Appendix 2 – BlueTOAD Spectra RSU C-V2X 5.9 GHz Spectrum Specifications

Iteris C-V2X Roadside Unit – FCC Individual Device RSU License Details

The Iteris RSU specifications for FCC authorization include:

1. **Manufacturer and model of the RSU Module: MFG=Iteris MODEL_# = BTSPCV2X54940**
2. **FCC ID numbers: OVH-BTSPCV2X54940**
3. **Manufacturer and model of the Antenna – L-Comm HGV-4958-06U**
4. **Antenna gain in dBi - 6 dBi**
5. **Antenna Beamwidth in degrees - Omni-directional (360 degree)**
6. **Center Line of the antenna Above Ground Level (AGL) in meters – Note: antenna base mounting height of up to 8 Meters (26.3 Feet) from roadway bed surface.**
7. **RSU Equipment Class - C = 23 dBm Max. Output Power**
8. **Effective Isotropic Radiated Power (EIRP) in dBm - 27.6dBm max for 33 dBm-rated channels; 22.6 dBm max for 23 dBm-rated channels (configuration parameters must be properly set to reduce max TX power on 23 dBm-rated channels) – 20 dBm for C-V2X.**
9. **Operating channel numbers:**
 - a. 180 – 5895-5905MHz (Max EIRP = 23 dBm)
 - b. 182 – 5905-5915MHz (Max EIRP = 23 dBm)
 - c. 184 – 5915-5925MHz (Max EIRP = 33/40 dBm) (Government entities)

 **Note:** The Iteris RSU by default supports channel 183 that contains channels 182 and 184.

Iteris RSU – Specifications

Standards Compliance

- SAE J2735 and SAE J2945/1
- SAE 3161/1
- IEEE 1609
- 3GPP, Release 14/15 for C-V2X
- NTCIP 1218 v01.38
- CTI 4001
- CTI 4501

V2X Security

- Based on industry best practice ISO 21434
- NIST/Brainpool ECC up to 512b
- V2X-embedded HSM (Hardware Security Module) with storage up to 10k keys
- FIPS 140-2 Level 3 / EAL6+
- Secure Boot

C-V2X

- LTE-V2X: 5.9GHz ITS (5895 – 5925 MHz)
- 3GPP Release 14/15 C-V2X PC5

Power Specifications

- 12V $\pm 10\%$ (< 12 Watts)

Power over Ethernet (PoE)

- 110/220 VAC supply to external POE injector and splitter

Operating Temperature Range

- -40°C (-40° Fahrenheit) to +85°C (185° Fahrenheit)

Processor

- Quad-core ARM A35 @ 1.2GHz + M4 (~9000DMIPS)
- 2GB LPDDR4 SDRAM
- 256MB QSPI NOR flash
- 8GB eMMC mass storage
- Embedded Linux OS

Interface Options

- PoE - Ethernet 10 BASE-T / 100 BASE-T
- Static IP Addressing, DHCP
- IPv6, IPv4
- 2.4 GHz Bluetooth Demodulator
- Bluetooth Radio (adjustable) Transmit Power Range: -90 dBm to +20 dBm

Dual antenna supports two modes:

- Single DSRC channel (2 antenna diversity operation possible) or use a single antenna for Tx and Rx
- C-V2X with 2 antennas (for Tx & Rx) on upper 30 MHz band of 5.9 GHz spectrum.
- miniPCIe slot for optional LTE radio interface

Antennae

- 2 - 8 dBi (5.9 GHz C-V2X antennas)
- 2 - 2 dBi Omni (Bluetooth Discoverable and Non-Discoverable Detector)
- LNA active GNSS external antenna

For Your Notes:

Appendix 3 – Connected Vehicle In-Cabinet Processor Specifications



The Iteris In-Cabinet Processor (ICP) is an Industrial Computer suitable to host and manage Connected Vehicle (CV) applications. The Iteris In-Cabinet Processor is a ruggedized roadside field device intended to send and receive data and information to meet the requirements of a variety of CV infrastructure and host various applications. The industrial computer is a commercial-off-the-shelf product with a Linux operating system that provides a platform for hosting and executing CV applications and other related software.

The ICP is an embedded device also used to help facilitate integration between multiple different types of traffic controllers and the C-V2X based Roadside Units. It is required for the implementation of certain Connected Vehicle applications such as "Traveler Information Messages" (TIM), "Transit Signal Priority" (TSP) and "Emergency Vehicle Preemption"(EVP). The ICP is an in-traffic cabinet processor that operates within the same network as the RSU and traffic controller. It can translate certain messages to meet traffic signal control (NTCIP) and Society of Automotive Engineers (SAE J2735 – March 2016) standards and send the translation to one or more destinations. It hosts a configuration and monitoring web page called CV App Manager.

In the event of cabinet power interruptions, the Iteris In-Cabinet Processor automatically recovers from power failure after power is restored. All applications hosted on the industrial computer automatically start using their previous configurations and the system resumes proper operation.

Specifications

Base System: (UNO2372GE1212001-T) Compact Modular Box Platform with Intel® Atom® Processor

- **CPU built-in:** Intel® Atom® E3940 quad-core processor with 4G DDR3L memory
- **Operating System:** Ubuntu 22.04 Linux Desktop Version
- **Memory:** up to 8GB RAM
- **I/O Interface:** 2 x GbE, 4 x USB 3.0, 4 x COM, 2 x mPCIe, 1 x HDMI 1.4b, 1 x DP 1.2
- **Certification:** CE, FCC, UL, CCC, BSMI
- **Dimensions:** (W x D x H) Single-stack model: 150 x 105 x 35 mm (5.8 x 4.2 x 1.4 in)
- **Enclosure:** Aluminum housing
- **Mount Options:** Stand, wall, VESA (optional), DIN rail (optional)



- **Weight:** (Net) Single-stack model: 0.8 kg (1.8 lb)
- **Power Requirement:** 10 ~ 36 VDC
- **Power Consumption:** 18.36W (typical)
- **Operating Temperature:** -40 ~ 70 °C/-40 ~ 158 °F with 0.7m/s airflow, with wide-temperature (-40 ~ 85 °C/-40 ~ 185 °F) peripherals (e.g., SSD, wireless modules)
- **Storage Temperature:** - 40 ~ 85 °C/-40 ~ 185 °F
- **Relative Humidity:** 10 ~ 95% RH @ 40 °C/104 °F, non-condensing
- **Shock Protection:** Operating, IEC 60068-2-27, 50G, half sine, 11ms
- **Vibration Protection:** Operating, IEC 60068-2-64, 2Grms, random, 5 ~ 500Hz, 1hr/axis (mSATA)
- Operating, IEC 60068-2-64, 0.75Grms, random, 5 ~ 500Hz, 1hr/axis (HDD)
- **Available Wireless Modules:**
 - **Cellular (C-PCM-24S24G):** iDoor Communication Module with a MultiTech Dragonfly™ embedded cellular modem, LTE/HSPA+ Support, Dual Antennas, and AT&T and Verizon Certification for US/Canadian Networks
 - **Wi-Fi/Bluetooth (PCM-24S2WF):** WiFi 802.11 ac/a/b/g/n 2T2R w/Bluetooth 4.1, M.2/Full-size mPCIe, Antennas
- **Assembly and Testing:** Standard Assembly, Functional Testing, SW installation

Basic Iteris In-Cabinet Processor Setup Information

The Iteris In-Cabinet Processor is a ruggedized roadside field device to send and receive data and information to meet the requirements of a variety of Connected Vehicle infrastructure and vehicle systems applications.

- Ubuntu 22.04 Desktop Version
- Default Login information: Username / Password
(Contact your account manager to receive Username and Password information or see Iteris Support contact information below)

How to Configure the In-Cabinet Processor

For more information about the configuring the ICP and applications it hosts, please download and consult the CV App Manager User Guide from Iteris Resource Center

<https://www.iteris.com/resource-center>

Please contact Iteris Support for further information and/or assistance:

- Iteris Support Phone: +1 (888) 254-5487
- Iteris Support email address: iteris-techsupport@iteris.com

Appendix 4 – How to Create an RSU MAP File

Objective

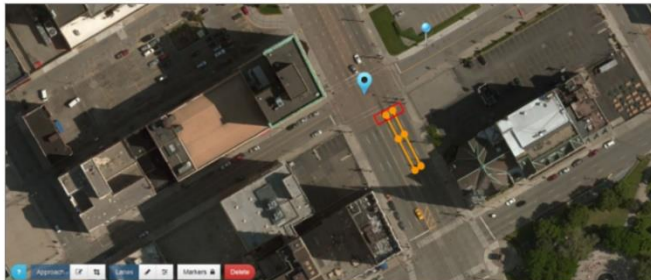
This procedure outlines the steps to produce an SAE J2735 compliant MAP file. J2735 messages are encoded using unaligned packed encoding rules (UPER) when transmitted from the roadside unit. This procedure assumes that you are familiar with traffic control terminology, intersection geometry and layout.

Material Requirements

- Windows PC with internet connection and web browser
- Customer intersection location
- Intersection diagram or equivalent

Map File Creation Procedure

1. Open the USDOT Connected Vehicles Tools website: <https://webapp.connectedvcs.com/>
2. Click **View Tool** to open the ISD Message Creator.



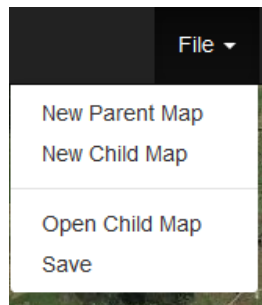
ISD Message Creator

Intersection MAP and SPaT

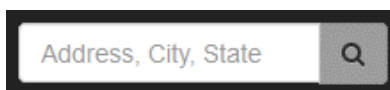
This tool allows a user to define the lanes and approaches of an intersection using a graphical interface. Once designed, the user can encode an ISD, MAP, or SPaT message as an ASN.1 UPER Hex string.

[View Tool >](#)

3. Click **File > New Parent Map** to start a new parent map.



4. In the search bar, enter an address near the intersection location.



- Center the view on the intersection and click the **Builder** icon.



- Put the **Reference Point Marker** in the center of the intersection.



- The Reference Point Configuration menu should open after you place the **Reference Point Marker**. If the menu does not open, left click on the **Reference Point Marker** to open it.

Reference Point Configuration

Marker Info

Type:

Select an Intersection Type ▾

Intersection Name:

Temporary Name

?

Revision:

0

?

Latitude:

28.61199484747454

?

Longitude:

-81.19190954374331

?

Intersection ID:

30615

?

Elevation:

-14

?

Master Lane Width:

366

?

Done

Cancel

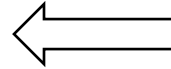
8. In the **Type** field, select **(1) Signal** as the Intersection Type and click **Done**.

Type: Select an Intersection Type ▾

Intersection Name: (1) Signal

Revision: (2) Metal Sign

Latitude: (3) Railroad



9. Put the Verified Point Marker in an accessible and measurable location such as the traffic cabinet or measured on-site field survey point if available.



10. The Verified Point Configuration menu should open when you place the **Verified Point Marker**. If the menu does not open, left click on the **Reference Point Marker** to open it.

Verified Point Configuration

Marker Info

Latitude:

28.611834730131644

?

Longitude:

-81.19165741609609

?

Elevation:

-14

?

Verified Latitude:

28.611834730131644

?

Verified Longitude:

-81.19165741609609

?

Verified Elevation:

-14

?

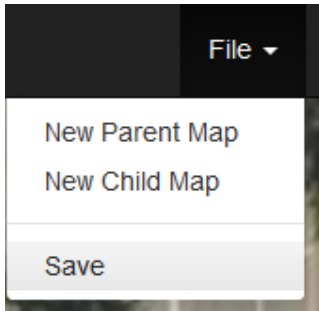
Done

Cancel

11. If the **Verified Latitude** and **Verified Longitude** values are available from on-site field surveys, enter them in the noted fields then click **Done**. If verified values are not available, just click **Done**.

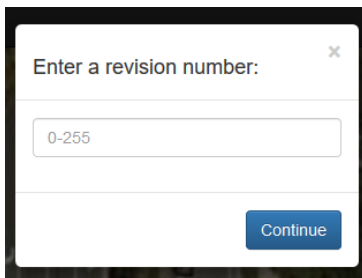
 **Note:** The internal GPS of the BlueTOAD Spectra RSU automatically calculates its Elevation.

12. Click **File > Save** to save the Parent Map. Then click **Continue**.

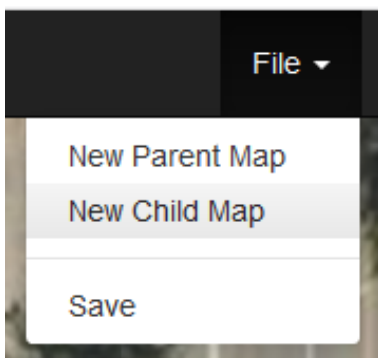


✓ **Note:** Do NOT press Enter—make sure you click *Continue*.

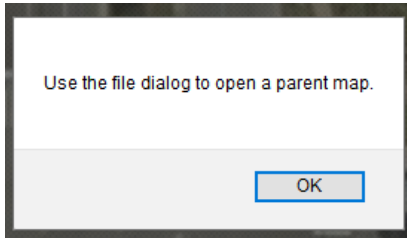
13. When prompted to enter a revision number, enter **0**, click **Continue**, and save the Parent Map to the local disk.



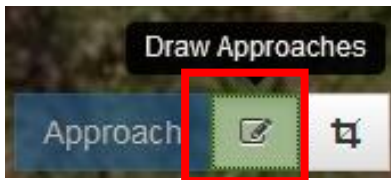
14. Click **File > New Child Map** to start building the Child Map.



15. Click **OK** on the file dialog notice to open the parent map; locate, select and open the Parent Map created in the previous steps.



16. Click on the **Draw Approaches** button in the bottom left corner to select the draw approach boxes.



17. Draw approach boxes across every Ingress and Egress⁴ approach relative to the intersection over the stop bar and across every lane as shown.



18. Use the **Edit Approaches** button to rotate, expand or contract the approach boxes as needed.

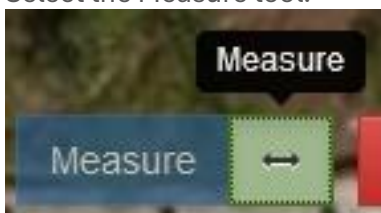
⁴ **Ingress** = Going into (entering) an intersection; **Egress** = Going out of (leaving) an intersection



19. Starting with the northmost approach, left click on each **Approach box** to open the Approach Configuration Menu.

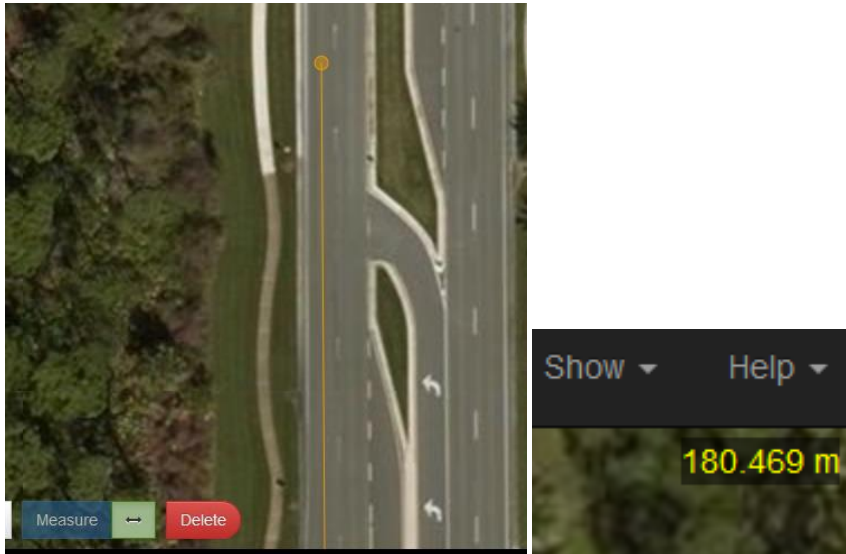
 A screenshot of a dialog box titled 'Approach Configuration'. It has a tab labeled 'Approach Info'. Below the tab, there are two dropdown menus: 'Approach Type:' with the option 'Select an Approach Type' and a question mark icon, and 'Approach ID:' with the option 'Select an Approach ID' and a question mark icon. At the bottom, there are two buttons: 'Done' and 'Cancel'.

20. Under **Approach Type**, select **Ingress** if the lanes are directed into the intersection and **Egress** if the lanes are directed out of the intersection; select the lowest **Approach ID** available starting at **01** then click **Done**.
21. Repeat Step 19 and Step 20 for all Approaches in a clockwise order until all approaches are drawn.
22. Select the Measure tool.



23. Left click on the **stop bar** of an approach, measure the distance from the stop bar to at least 180 meters away using the measured distance on the upper right, and note the

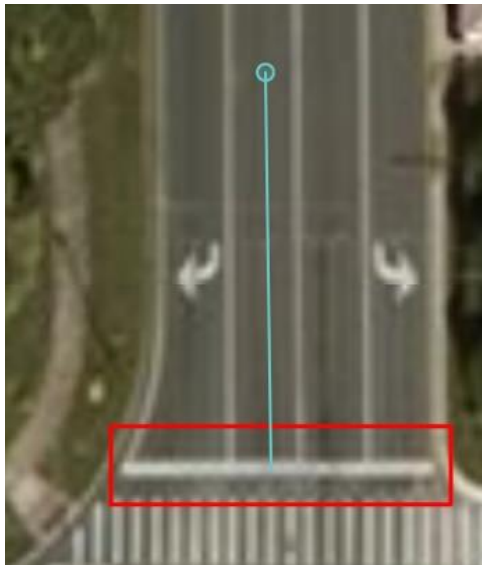
location with a landmark.



24. Left click on the **Draw Lanes** button.

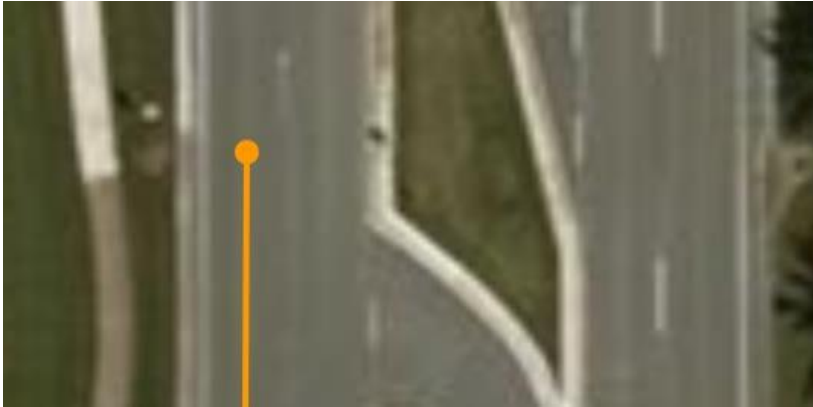


25. Left click on the **center** of the lane at the stop bar to start drawing lanes.



26. Use the **middle mouse button** to drag the view out to the measured landmark. Left click on the **center** of the lane as needed to remain in the center.

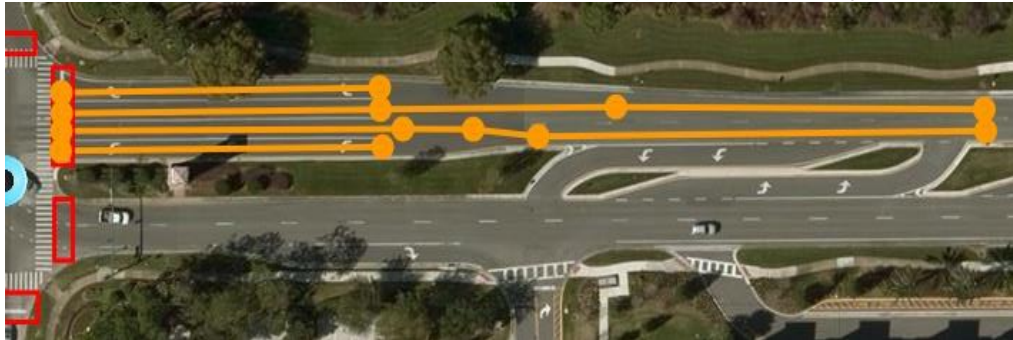
27. Double click on the desired **endpoint** of the lane to terminate the lane.



28. As needed to edit, left click on the **Edit Lanes** button and select the drawn lane. Click on the opaque midpoints to add nodes and use the **Delete** key to delete nodes.



29. Repeat the process for other individual lanes of the approach. For dedicated right and left turn lanes, span the entirety of the lanes until completed as shown (Rotated 90° CW).

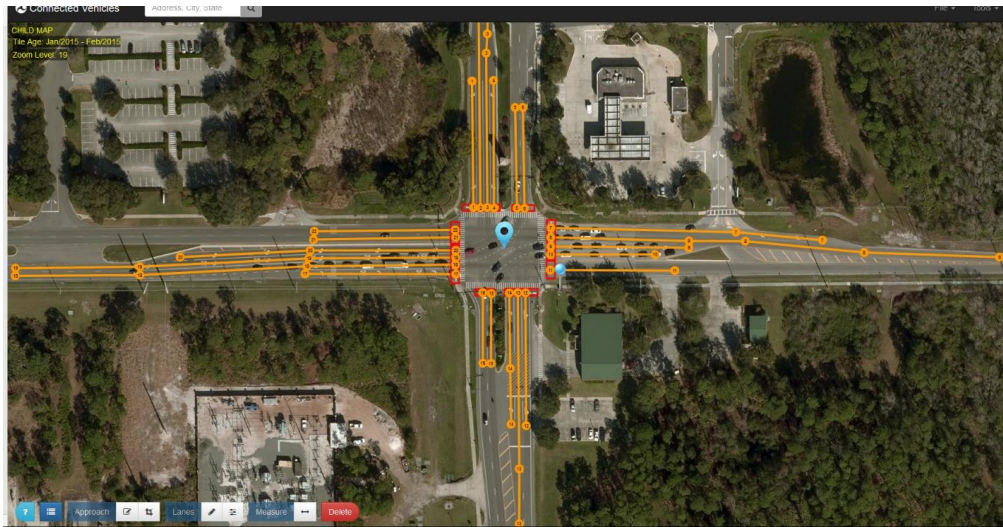


30. To draw the Egress lane, click on the **Draw Lanes** button, click on the center of the Egress lane within the approach box, draw the egress lane to at least the same length as the left turn lane, and double click on the **endpoint** to terminate the lane; repeat this process for all

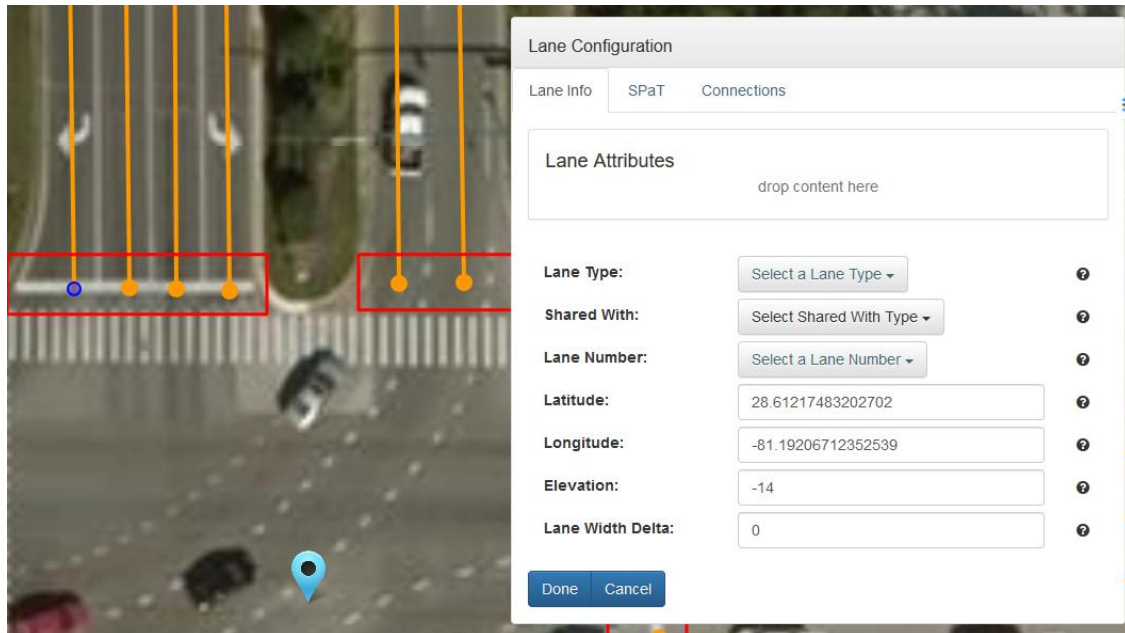
Egress lanes in the approach box until completed as shown (Rotated 90° CW).



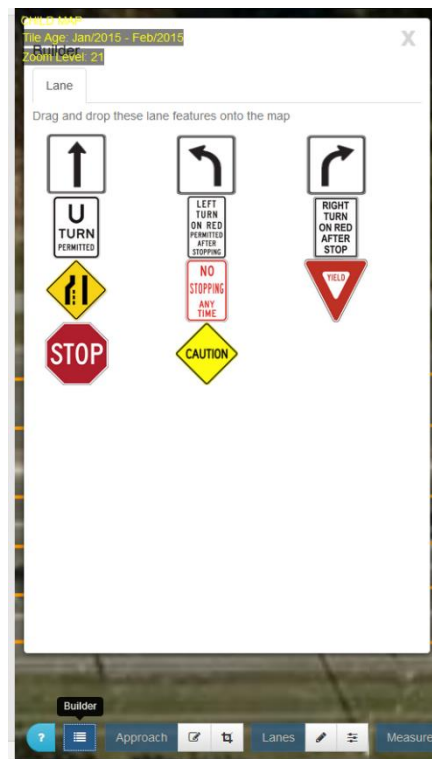
31. Repeat the process of drawing lanes until all lanes of the intersection are completely drawn as shown.



32. Click on the **starting point** of the left-most lane in the northern Ingress approach box to open the Lane Configuration menu.



33. Left click on the **Builder Menu** to open the **Lane** tab.



34. Drag and drop the **allowed maneuvers** from the appropriate icons in the Lane tab to the Lane Attributes box in the Lane Configuration menu; to determine the allowed maneuvers, refer to the intersection diagram, lane markings, and signage.

Lane Configuration

Lane Info SPaT Connections

Lane Attributes



Lane Type: Select a Lane Type

Shared With: Select Shared With Type

Lane Number: Select a Lane Number

Latitude: 28.61217483202702

Longitude: -81.19206712352539

Elevation: -14

Lane Width Delta: 0

Done Cancel

35. In the Lane Type field, select **Vehicle**; in the Type Attributes field, select **(0) Vehicle Revocable Lane**; in the Shared With field, select **(3) Individual Motorized (4) Bus (5) Taxi**; and, in the Lane Number, select the lowest available lane number starting with **01**; when done, click **Done**.

Lane Configuration

Lane Info SPaT Connections

Lane Attributes



Lane Type: Vehicle

Type Attributes: (0) Vehicle Revocable Lane

Shared With: 3 selected

Lane Number: 01

Latitude: 28.61217483202702

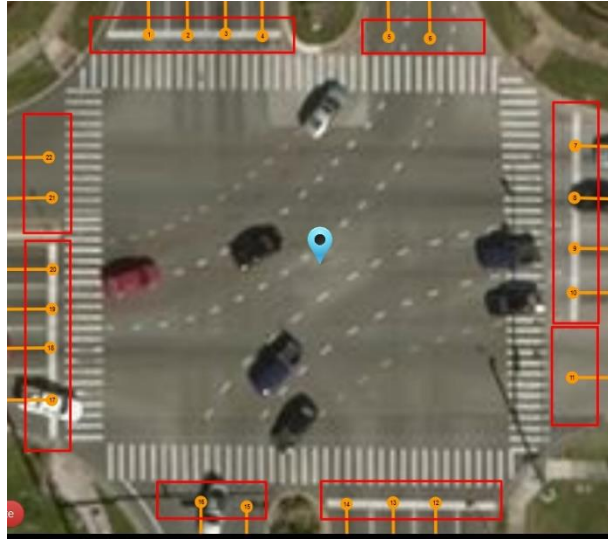
Longitude: -81.19206712352539

Elevation: -14

Lane Width Delta: 0

Done Cancel

36. Repeat this process for all remaining lanes in the intersection. When you are done, the starting node in each lane will be identified with its number as shown.



37. Click on **node** designated **1** to open the Lane Configuration menu and click the **Connections** tab.

Lane Configuration

Lane Info

SPaT

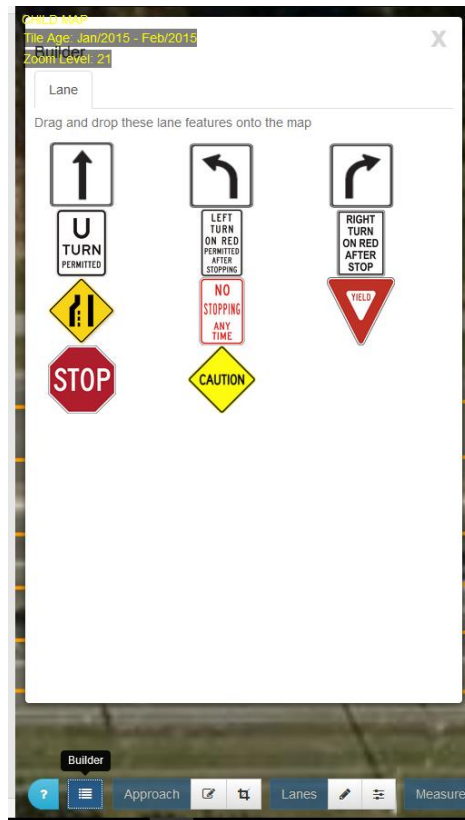
Connections

"To" Lane Number	Signal Group ID	Allowed Maneuvers	+
0 to 255	0 to 255	drop content here	🗑️

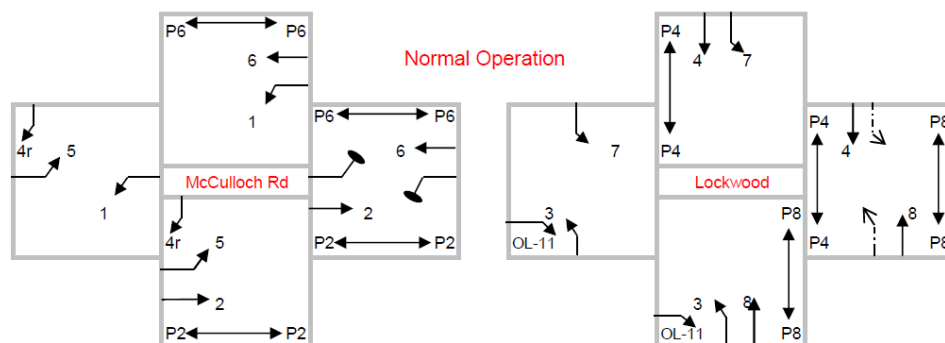
Done

Cancel

38. Left click on the **Builder Menu** to open the **Lane** tab.



39. You should have a diagram of the intersection provided by a traffic engineer. Open the file of the intersection diagram. An example diagram is shown below.



40. Using the intersection diagram as a reference, enter the destination lane number in the **“To” Lane Number** field and the phase number associated with the movement in the **Signal Group ID** field.

Lane Configuration			
Lane Info		SPaT	Connections
"To" Lane Number	Signal Group ID	Allowed Maneuvers	
22	4	drop content here	+
			trash
Done Cancel			

41. Drag and drop the **allowed maneuvers** for the given phase and lane number from the Lane tab of the Builder menu to the **Allowed Maneuvers** Box in the **Connections** tab window.

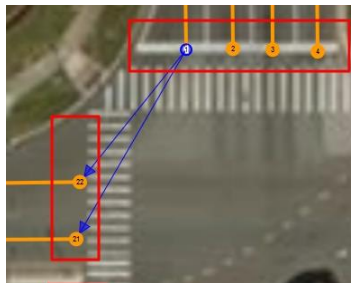
Lane Configuration			
Lane Info		SPaT	Connections
"To" Lane Number	Signal Group ID	Allowed Maneuvers	
22	4	RIGHT TURN ON RED AFTER STOP	+
			trash
Done Cancel			

42. Use the + button in the **Connections** tab window to add more connections and repeat the process as needed. When done, click **Done**.

The screenshot shows the 'Lane Configuration' dialog box with the 'Connections' tab selected. It contains a table with two rows of lane configurations. Each row has a 'To' Lane Number, a Signal Group ID, and Allowed Maneuvers. A '+' button is in the top right, and a trash icon is in the right margin of each row. 'Done' and 'Cancel' buttons are at the bottom.

"To" Lane Number	Signal Group ID	Allowed Maneuvers
22	4	RIGHT TURN ON RED AFTER STOP
21	4	RIGHT TURN ON RED AFTER STOP

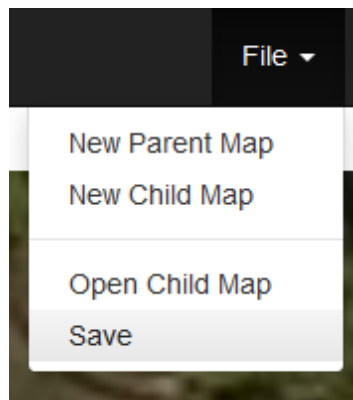
43. Click again on **node 1**. Blue arrows will be visible to show established connections.



44. Repeat this process for every **Ingress** lane in the intersection.

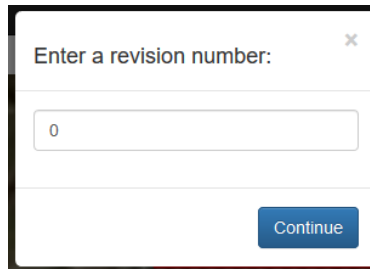
✓ **Note:** *Egress lanes do not need connections.*

45. Click **File > Save** to save the Child Map.



46. When prompted, enter the revision number starting with **0**. Then click **Continue**.

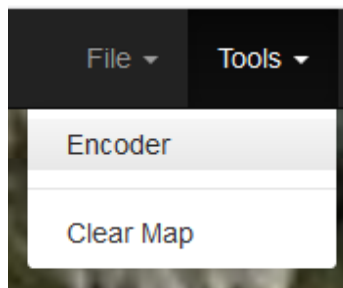
✓ **Note:** Do NOT press Enter—make sure you click Continue.



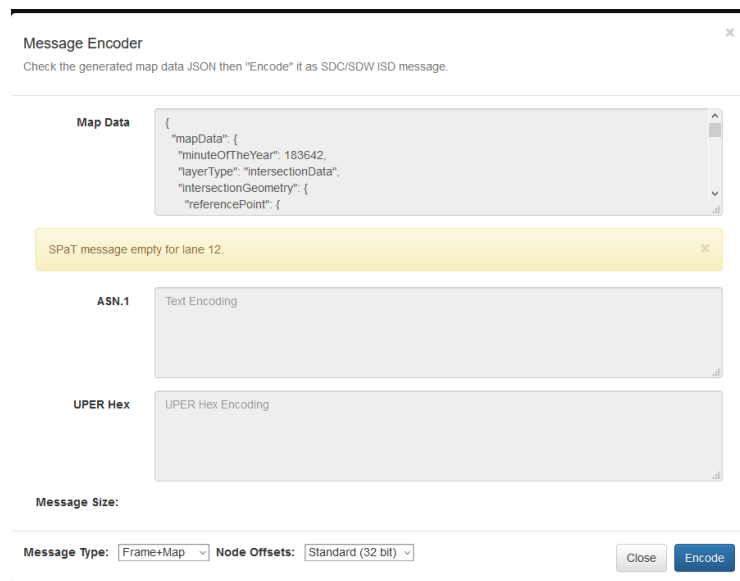
A dialog box with the title "Enter a revision number:". It contains a text input field with the number "0" and a blue "Continue" button at the bottom right.

47. Save the Child Map to the same directory on the local disk as the Parent Map. Whenever you make significant edits and revisions to the Child Map, increment the revision number by **1**.

48. Click **Tools > Encoder** to open the Message Encoder.



49. For Message Type, select Frame+Map and, for Node Offsets, select Standard (32 bit)



A screenshot of the "Message Encoder" dialog box. It contains a "Map Data" section with a JSON object, a "SPaT message empty for lane 12" warning, and two encoding options: "ASN.1 Text Encoding" and "UPER Hex Encoding". At the bottom, there are dropdowns for "Message Type" (set to "Frame+Map") and "Node Offsets" (set to "Standard (32 bit)"), along with "Close" and "Encode" buttons.

50. Click **Encode**. Ignore the warning for the SPaT message because this instruction is for building MAP messages. If there are no errors, the UPER Hex string will populate as shown.

Message Encoder
Check the generated map data JSON then "Encode" it as SDC/SDW/ISD message.

Map Data

```
{
  "mapData": {
    "minuteOfTheYear": 183642,
    "layerType": "IntersectionData",
    "intersectionGeometry": {
      "referencePoint": {
```

SPaT message empty for lane 12.

ASN.1

```
value MessageFrame ::= {
  messageId 16,
  value MapData : {
    msgIssueRevision 2,
    layerType IntersectionData,
```

UPER Hex

```
001282ba3802302030f12e0946b2c14b3ae4eaa00f7402dc051f70a9608ba1c0203240006bb973dc81
414d64b5800d02828d2204800490f2400248812001a43c9000cb049d0e0101c000135dc85f5400a0a2
b28bbfd93586f9b00a0a2b4bb3fe18242e00008b04dd0e0101a000135dc85f5400a0a2b2b33fecb5858
df9fc0a0a2b4be3fd8241900014b051d0e0101a8000b5dc85f5400a0a2b2cd3ffcb5a1ddfb340a0a1482a
0002a45842014b00450e01019200015e97e1e54aff8b2d9e69162400448a9200224589001522a4800a
```

Message Size: 702 bytes

Message Type: Frame+Map **Node Offsets:** Standard (32 bit)

Close Encode

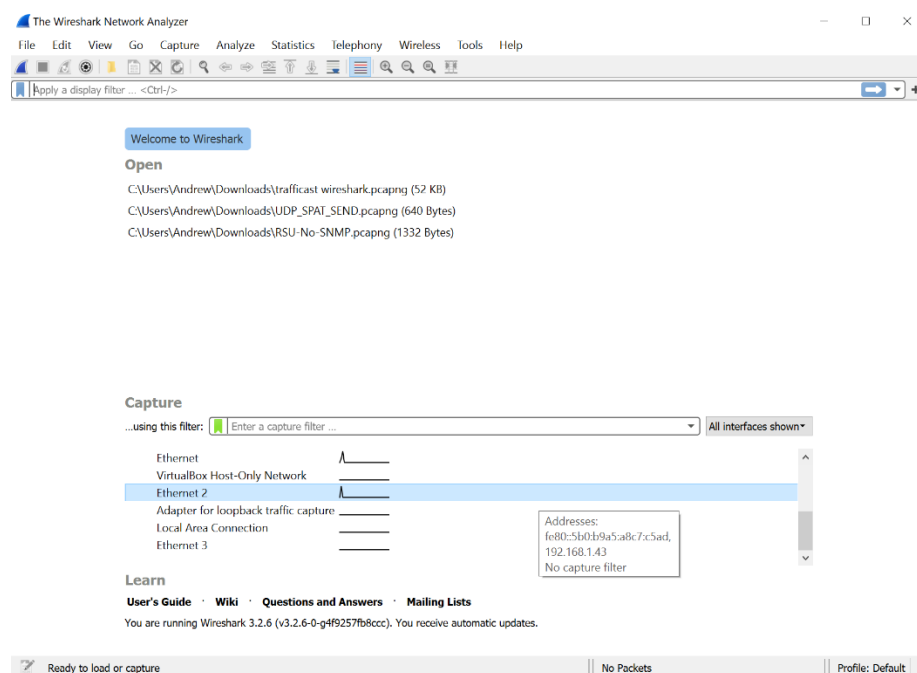
- ✓ **Note:** If the message size exceeds 1400 bytes, the RSU will not be able to support the payload size. Reduce the size by deleting excess points in lanes.

Appendix 5 – How to Retrieve an Unknown BlueTOAD Spectra RSU IP Address

Use the Wireshark utility to capture packet data in detail to ascertain the IP Addresses used by the BlueTOAD Spectra (CV). Wireshark is a free opensource application that serves as a network packet analyzer, which displays packets with detailed protocol information. The Wireshark utility can be obtained from the following website: <https://www.wireshark.org/download.html>

Use Wireshark to Retrieve the BlueTOAD Spectra RSU assigned IP Address

1. Connect the BlueToad Spectra RSU and/or Iteris RSU device via Ethernet directly to a Windows laptop or desktop. Ideally this should be a direct connection; do not use any Ethernet switch or hub as you will also detect any additional network traffic from those devices.
2. Start Wireshark and capture all traffic from the Ethernet interface that is connected to the BlueTOAD Spectra RSU device. You can start Wireshark from the command line, but in this example, Wireshark was started from the Wireshark Microsoft Windows app.



3. In this example, the device is connected to “Ethernet 2”. By double-clicking on “Ethernet 2” it will begin capturing packets from that device.
4. Let the capture run for a minute. Then select the Capture Tab and select the “Stop” menu item to stop capturing network traffic. You will see traffic appear in the Wireshark window.

You will be able to see ARP traffic coming from the RSU or BlueTOAD Spectra device(s). See example below.

- As shown in the screenshot below, you can see traffic coming from two remote IPs, 192.168.1.77 and 192.168.13.112. Once you have found these IPs, you can configure the local computer's network interface with a Static IP in the same range and then browse or SSH to each IP to confirm and log in.

Capturing from Ethernet 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
6270	5011.501517	Atmel_29:b4:72	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.77
6271	5012.501493	Atmel_29:b4:72	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.77
6272	5013.501466	Atmel_29:b4:72	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.77
6273	5017.500961	Atmel_29:b4:72	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.77
6274	5018.501374	Atmel_29:b4:72	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.77
6275	5019.501372	Atmel_29:b4:72	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.77
6276	5019.708673	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x6acd442b
6277	5019.730192	169.254.197.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
6278	5022.511287	Atmel_29:b4:72	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.77
6279	5022.719844	169.254.197.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
6280	5023.324166	169.254.197.173	169.254.255.255	DB-LSP...	211	Dropbox LAN sync Discovery Protocol
6281	5023.511284	Atmel_29:b4:72	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.77
6282	5024.511274	Atmel_29:b4:72	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.77
6283	5024.522834	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x6acd442b
6284	5025.720784	169.254.197.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
6285	5028.728866	169.254.197.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
6286	5029.887595	fe:ff:ea:9a:10:37	Broadcast	ARP	60	Who has 192.168.13.31? Tell 192.168.13.112
6287	5030.668152	fe:ff:ea:9a:10:37	Broadcast	ARP	60	Who has 192.168.13.111? Tell 192.168.13.112
6288	5031.009713	fe:ff:ea:9a:10:37	Broadcast	ARP	60	Who has 192.168.13.31? Tell 192.168.13.112
6289	5031.528883	Atmel_29:b4:72	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.77
6290	5031.667132	fe:ff:ea:9a:10:37	Broadcast	ARP	60	Who has 192.168.13.111? Tell 192.168.13.112
6291	5031.728441	169.254.197.173	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
6292	5032.107816	fe:ff:ea:9a:10:37	Broadcast	ARP	60	Who has 192.168.13.31? Tell 192.168.13.112
6293	5032.521126	Atmel_29:b4:72	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.77
6294	5032.645742	fe:ff:ea:9a:10:37	Broadcast	ARP	60	Who has 192.168.13.111? Tell 192.168.13.112
6295	5033.106836	fe:ff:ea:9a:10:37	Broadcast	ARP	60	Who has 192.168.13.31? Tell 192.168.13.112
6296	5033.446705	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x6acd442b
6297	5033.521125	Atmel_29:b4:72	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.77
6298	5033.667366	fe:ff:ea:9a:10:37	Broadcast	ARP	60	Who has 192.168.13.111? Tell 192.168.13.112

The Main Window (Packet List Pane)

Main Window, Packet List Pane Column Definitions

No. – the number of the packet in the capture file.

Time – the timestamp of the packet.

Source – the address where this packet is coming from. This is where we can identify the BlueTOAD Spectra RSU's MAC Address.

Destination – the address where this packet is going to.



Protocol – the protocol name in a short (abbreviated) version. The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.

Length – the length of each packet.

Info – additional information about the packet content. This is where we can find the current IP Addresses used by the BlueTOAD Spectra RSU.

Appendix 6 – BlueTOAD Spectra CV RSU Site Requirements Form

This form must be printed for each RSU along with the Sign-Off Checklist below.

SPECTRA RSU SITE REQUIREMENTS

Thank you for choosing the Spectra RSU. To ensure the best possible field deployment experience, please provide the information below. All fields are required and must be complete prior to scheduling your installation.

CONTACT INFORMATION

Agency Name
 Agency Phone Number
 Agency E-mail

INTERSECTION INFORMATION

The Spectra RSU requires a supported ATC 5.2b (or higher) compliant traffic controller with compatible software to generate Signal Phase and Timing messages. Intersection diagrams are required to generate MAP messages. FCC site licenses are required by law (47 C.F.R, Parts 90 and 95). Intersection latitude and longitude shall be in Decimal Degrees.

Intersection Location
 Intersection Latitude Intersection Longitude
 Intersection Diagram Provided ☐ Intersection Timing Plan Provided ☐
 Traffic Controller Brand Traffic Controller Model
 Traffic Controller Software Version
 Traffic Controller IP Address
 Traffic Controller Subnet Mask
 Traffic Controller Gateway
 ATMS Software Version
 FCC Site License Registered ☐ FCC Call Sign
 FCC File Number

SPECTRA RSU INFORMATION

The Spectra RSU requires two IP addresses for Bluetooth and DSRC functionality. Serial numbers are found on device or packaging. Serial numbers may be left blank if unknown.

Bluetooth Module Serial Number
 Bluetooth Module IP Address
 Bluetooth Module Subnet Mask
 Bluetooth Module Gateway
 DSRC Module Serial Number
 DSRC Module IP Address
 DSRC Module Subnet Mask
 DSRC Module Gateway

TRAFFICCAST SERVER ACCESS

The Spectra RSU requires internet access to the TrafficCast servers for collection and processing of Bluetooth data. Refer to Tech Bulletin TCI-FSB-ET-2011-01 (available on request) for more information.

Port 69 Opened ☐
 Port 123 Opened ☐
 Port 8010 Opened ☐
 Port 10001 Opened ☐

System Evaluation Checklist

BlueTOAD, RSU and/or ICP CV System Test Procedure

This form must be printed for each RSU or ICP device.

Location:

Date:

Iteris Enclosure Serial Number:

RSU Serial Number:

BlueTOAD Spectra Serial Number:

RSU IP Address:

BlueTOAD Spectra IP Address:

ICP Device Serial Number:

ICP Device IP Address:

Category	Items verified	Date & Time	Pass	Signature of Evaluator
BlueTOAD Spectra & RSU				
Visual Inspection	Confirm condition of hardware enclosure: - Antennas with Connectors - Enclosure Ports - LEDs - Enclosure			
Confirm Power Up	Power up unit and confirm all LEDs are normal after the unit initializes. LED Indicators: Green – Device operational Amber – Device ON Red - Fault			
Confirm Network Configuration Settings	1. Network settings configuration <u>BlueTOAD Spectra</u> IP Address: Netmask: Gateway: DNS: NTP:			

Category	Items verified		Date & Time	Pass	Signature of Evaluator
		<u>RSU</u> IP Address: Netmask: Gateway:			
	2.	Configure IP Address settings for traffic controller (if applicable) IP Address: Netmask: Gateway:			
		MAP file Uploaded MAP file ID:			
	3.	Is the following network configuration done? 1.Connected Vehicle Data - Port 10002 – UDP egress (outbound) to 52.39.79.127 (Iteris VantageARGUS Cloud). 3. Travel Time Data - Port 8010 – TCP egress (outbound) to btserver.trafficcast.com / IP addresses			
Confirm Iteris System Data Collection	1.	RSU SPaT Data collection and display in VantageARGUS Travel Time system. (Signalized Intersection Locations ONLY)			
	2.	Bluetooth Data collection and display in VantageARGUS Travel Time system. (BlueTOAD Spectra RSU ONLY)			
Confirm Operation	1.	GPS Functionality Verified via RSU Statistics or Status page.			
	2.	MAP Broadcasting (Radio) Verification (generated by RSU). Check via RSU Statistics or Status page.			
	3.	SPaT, MAP, TIM, SSM, SRM and BSM message data validation – USDOT / SAE J2735 (March 2016 or greater)			
		Using Iteris V2X Connect Validation App on tablet (if applicable). 1. Verify if MAP messages are being			

Category	Items verified		Date & Time	Pass	Signature of Evaluator
		received and are correct. 2. Check if SPAT Messages are received (if a location is signaled intersection) and are correct 3. Verify if BSM messages are received in VantageARGUS CV by having a vehicle equipped with OBU traverse the network where RSU devices are installed. 4. Verify if TIM messages are received (TIM message added into RSU as store and repeat or activating an input on traffic signal controller that would trigger TIM message from ICPs TIMs application)			
		Using VantageARGUS data collection (if applicable). 5. Verify if MAP messages are being received and are correct. 6. Check if SPAT Messages are received (if a location is signaled intersection) and are correct 7. Verify if BSM messages are received in VACV by having a vehicle equipped with OBU traverse the network where RSU devices are installed. 8. Verify if TIM messages are received (TIM message added into RSU as store and repeat or activating an input on traffic signal controller that would trigger TIM message from ICPs TIMs application)			
ICP Device					
Visual Inspection	Confirm condition of hardware enclosure: - Power cable firmly connected - Connectivity cable is properly in place - Enclosure does not have physical damage				

Category	Items verified		Date & Time	Pass	Signature of Evaluator
Confirm Power Up	Verify that the power LED indicator (PWR) is illuminated.				
Confirm Network Configuration Settings	IP Address: Netmask: Gateway: DNS:				
Applications Inspection		N/A			

GLOSSARY:

RSU - Road Side Unit

OBU - On-Board Unit

ICP - In-Cabinet Processor (Advantech)

VACV - VantageARGUS Connected Vehicle

SCMS - Security Credentials Management System

BSM - Basic Safety Messages

SPAT - Signal Phase and Timing

MAP - Map Data Message— intersection geography and line definitions of the intersection or street.

SSM - Signal Status Message

SRM - Signal Request Message

TIM - Traveler Information Message

Inspector: _____ Date: _____

Appendix 7 - Regulatory Information

FCC Compliance Statement

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.

FCC Label Information

The FCC identification label is permanently affixed to the device and is visible to the user. The label contains the following information:

FCC ID: OVH-BTSPCV2X54940

Model: BTSPCV2X54940

The label is permanently attached to the device enclosure and is designed to remain legible for the life of the product.

FCC Part 15.21 – Modification Warning

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



FCC Part 15.25 – Operation Within Authorized Frequency Bands

This device has been evaluated to ensure compliance with the applicable requirements of FCC Part 15. Operation of this device is restricted to the frequency bands and power levels specified by the manufacturer.

The device shall not be operated outside of the authorized parameters defined by the FCC.

FCC Part 15.27 – Special Operating Conditions

This device is designed to operate in accordance with FCC rules governing unlicensed radio frequency devices.

The equipment must be installed and operated in a manner that ensures compliance with all applicable FCC requirements.

If the device incorporates an external antenna, only antennas approved by the manufacturer may be used.

Use of unauthorized antennas or modifications to the antenna system may result in non-compliance with FCC regulations.

RF Exposure Information

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment.

The device must be installed and operated with a minimum separation distance as specified by the manufacturer to ensure compliance with RF exposure requirements.

