BlueTOAD® Spectra CV

User Guide

BlueTOAD® Spectra™ CV (Connected Vehicle) Roadside Unit – DSRC/C-V2X RSU Installation, Operation and Maintenance

Revision 03, February 2021

iteris®

Copyright and Trademarks

Published: February 2021

Contact Information

Headquarters

Iteris, Inc.
1700 Carnegie Ave, Suite 100
Santa Ana, CA 92705

Support

BlueARGUS On-Going Operations Website: https://bluetoad.trafficcast.com/

Iteris Support Website: https://trafficcast.zendesk.com

Iteris Support Telephone: 1-608-713-9299

1. Table of Contents

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
BlueARGUS	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 Qualcomm chipset for 5.9 GHz spectrum WAVE 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
Free-TEXT	Custom text you type to create a message or part of a message for a TIM
GPS	Global Positioning System

Term	Meaning
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 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
RDS	Radio Data Service (on FM 57 kHz subcarrier)
RJ-45 Port	Registered Jack (RJ) is a standardized telecommunication network interface

Term	Meaning
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 DSRC/C-V2X.
SCMS	Security Certificate Management System—developed by a consortium of automakers and the United States Department of Transportation (USDOT) as a leading candidate for 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 TravelSMART 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

2. Introduction

Purpose

This *User Guide* outlines procedures to deploy Iteris BlueTOAD Spectra Roadside units. Included are procedures to confirm network connectivity and traffic data collection. *Chapter 3* thru *Chapter 5* explain how to deploy the BlueTOAD Spectra RSU. *Chapter* 6 thru *Chapter 14* are Appendices, which contain supplemental system documentation.

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

BlueTOAD Spectra Unit	Function	Part Number
Ethernet PoE	Detects and transmits Data for Speed and Travel Time	BT-ETH-SPECTRA-POE
Ethernet Cellular PoE		BT-CELL-SPECTRA-POE
Solar Cellular		BT-CELL-SPECTRA-85
RSU Ethernet PoE	Receives and transmits Detection, CV and SPaT Data	SPECTRA-DSRC-C-V2X SPECTRA-C-V2X BT-RSU-C-V2X

Components of the BlueTOAD Spectra and BlueTOAD Spectra RSU

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

	BlueTOAD Spectra			BlueTOAD Spectra Roadside Units
Item	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	
BlueARGUS Software	X	X	X	X
Traffic Controller (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 **Item**s in that unit.

		BlueTOAD Spectra			Connected Vehicle Roadside Units		
		Ethernet PoE	**Ethernet Cellular PoE**	**Solar Cellular**	**BlueTOAD Spectra RSU BT/DSRC/ C-V2X (Spectra-DSRC-C-V2X)**	**BlueTOAD Spectra RSU BT/C-V2X (Spectra-C-V2X)**	**BlueTOAD RSU (BT-RSU-C-V2X)**
Features							
Types of Data Processed	Speed and Travel Time	X	X	X	X	X	
	Connected Vehicle BSM				X	X	X
	Traffic Controller SPaT				X	X	X
	Traveler Information Messages (TIM)				X	X	X
Data is Transmitted	Through Agency Network	X			X	X	X
	Through the Cellular Network		X	X			
Powered by	Power over Internet (PoE)	X	X		X	X	X
	Solar-Charged Battery			X			
Field Installation	Near Roadside Traffic Cabinet	X	X		X	X	X
	Stand-Alone			X			
Weight	Weights with brackets	<5 lbs.	<5 lbs.	<40 lbs.	<9 lbs.	<9 lbs.	<9 lbs.

Compatible Traffic Controllers

For operation of the BlueTOAD Spectra RSU Ethernet PoE, you must have a connection to a Traffic Controller when deployed at signalized intersections.
The table below lists the Traffic Controllers that you can use with the BlueTOAD Spectra RSU.

Manufacturer	Model	Software	SPaT Support	NTCIP1202 Support
Econolite	ASC3/Cobalt-2100/1000/RM	Asc3app/Cobalt/EOS	Yes	Yes/Yes
Intelight	2070LDX ATC	Maxtime CV	Yes	Yes
McCain	NEMA ATC	FlexRM	Yes	Yes
Siemens	2070-1C/M60	SEPAC ECOM/ SEPAC NTCIP	Yes	No/Yes
Trafficware	980/NEMA ATC/2070-1C	Apogee	Yes	Yes

General Roadside Device Deployment Guidelines

1. 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 DSRC/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: “Appendix 9 – BlueTOAD Spectra RSU System Requirements and Validation Process” to follow steps that provide instructions to test the BlueTOAD Spectra RSU 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

3. BlueTOAD Spectra RSU Installation Procedures

Purpose

The procedures in this chapter tell you what to do to deploy a BlueTOAD Spectra RSU. We assume you are familiar with the BlueTOAD Spectra RSU, supporting equipment, and the associated software listed below. This documentation has been updated to support the new browser-based configuration application suitable for ITERIS RSU module firmware Version: I2V STANDARD SECURE 2020-03-13 1.x or greater.

Supporting Equipment

- Windows PC and Ethernet Cables
- BlueTOAD Spectra RSU Configuration Utility (Microsoft Windows 10 App)
- WinSCP or equivalent File Transfer Application
- PuTTY or equivalent SSH Client
- Iteris BlueTOAD Spectra RSU
- LCOM PoE Injector
- Traffic Controller with Power Cable or Similar ATC Controller1
- 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 RSU Connected Vehicle (CV) and 5.9 GHz wireless-based Dedicated Short Range Communications (DSRC) and 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 RSU system.

FCC License: Each DSRC/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 DSRC/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 DSRC/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.

[1] Refer to the table of Compatible Traffic Controllers on Page 1-2.

Layout Guidelines

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

2. Before you install an RSU, make sure things are ready at the installation sites:
   a. **Location** – Prepare a sight survey of all intersection locations that have been selected to deploy RSUs.
      - Identify power sources available in the traffic cabinets.
      - Make sure you have all the necessary parts for the system. Refer to the table on Page 2-2 and information on Page 5-23 for a list of the items needed and included with an RSU.
      - Are the Traffic Controllers in the traffic cabinets compatible with the RSU? Refer to the table of Compatible Traffic Controllers on Page 2-2.

   b. **Traffic Network** – Evaluate the existing network.
      - Confirm that the network settings (for example, IP address, gateway, subnet mask, and DNS) are correctly set and that all ports (69, 123, 8010, 10001) are open and set for outbound data traffic.

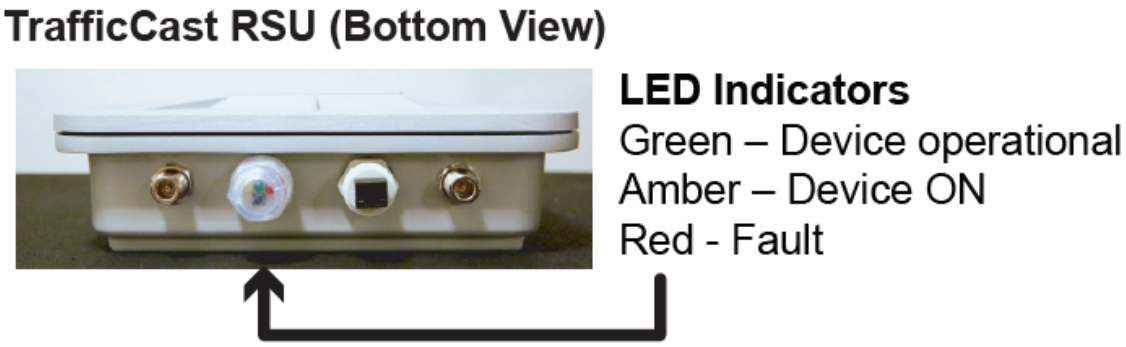
      > **Important**: Confirm all necessary inbound/outbound network ports have been set up.

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

      > **Note**: If there is a Processor (optional), it also has an IP address.

   c. **MAP File Creation** – For each intersection, create a MAP file with Signal, Phase and Timing (SPaT) information. For instructions, refer to Appendix 8, *How to Create an RSU MAP File*.
   d. Fill out the BlueTOAD *Spectra RSU Site Requirements* form on Page 9-14.
   e. Notify the **Iteris support team** to schedule a date for remote support for installation.
      Iteris Support Website: https://trafficcast.zendesk.com
      Iteris Support Telephone: 1-608-713-9299

f. Power ON the RSU and confirm all LEDs are normal after the unit initializes:

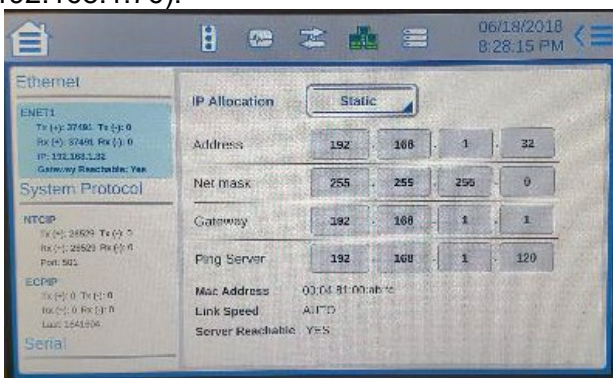


How to Set Up the Traffic Controller Before Field Deployment

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. Refer to the table on Page 2-2 for Compatible Traffic Controllers. Also, you can consult Iteris Support for models of traffic controllers supported; these include McCain (software Version 1.10.2.6705-2018-03-23), Siemens (software Version 3.59+), Trafficware (software Version 76.15N+) and Intelight (Maxtime CV).

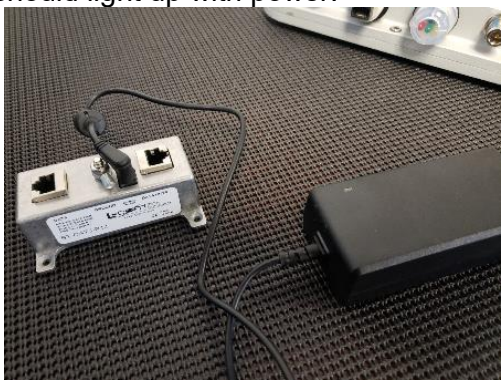
1. Attach the Traffic Controller "**A**" power cable to the "**A**" connector of the controller.

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 RSU, 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).

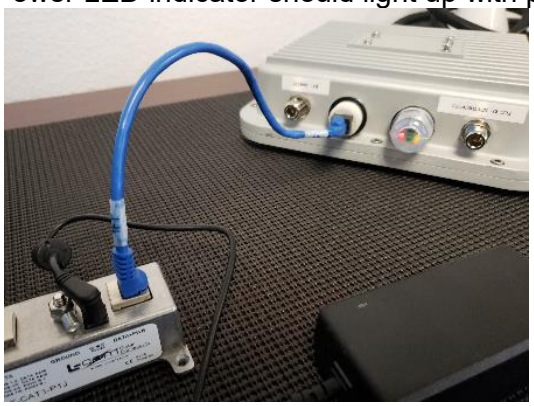


5. Plug the AC power cable of the POE injector AC adapter to an AC power source.

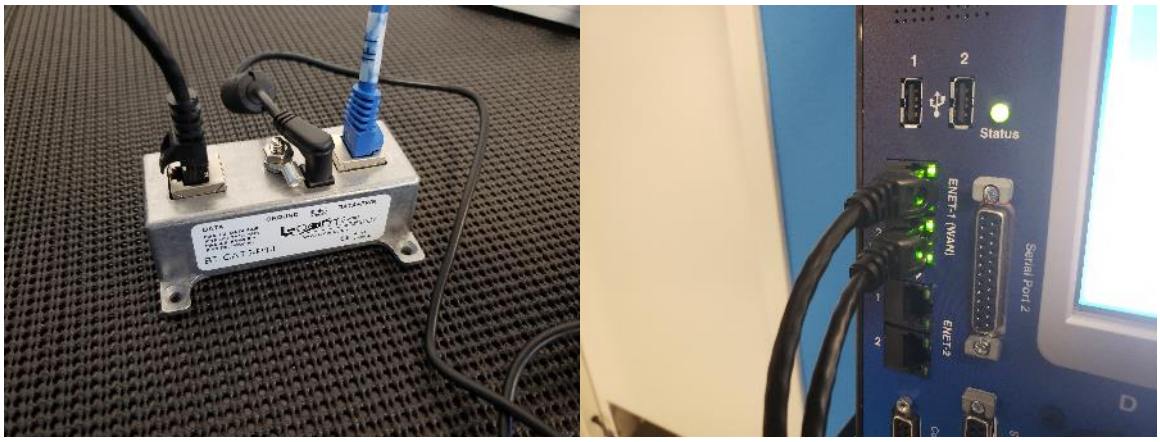
6. Plug the AC adapter output power cable into the POE injector. The AC adapter LED indicator should light up with power.



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 IP address to match the subnet of the RSU and controller—for example, 192.168.1.100.

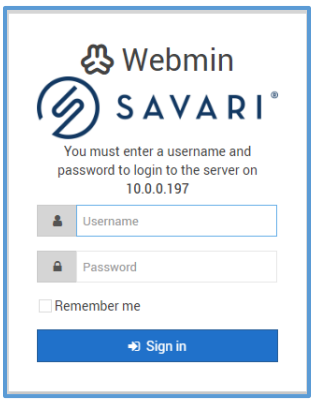
Iteris RSU Configuration Procedures – using *Browser-Based Configuration Utility – Webmin*

11. Log into BlueTOAD Spectra RSU browser-based configuration utility.
    - Open a Web Browser (Google Chrome or Microsoft Edge is preferred).
    - **Enter the "default"** BlueTOAD Spectra RSU IP address (192.168.1.76) and URL (<eth0 IP Address>:10000 – 192.168.1.76:10000)

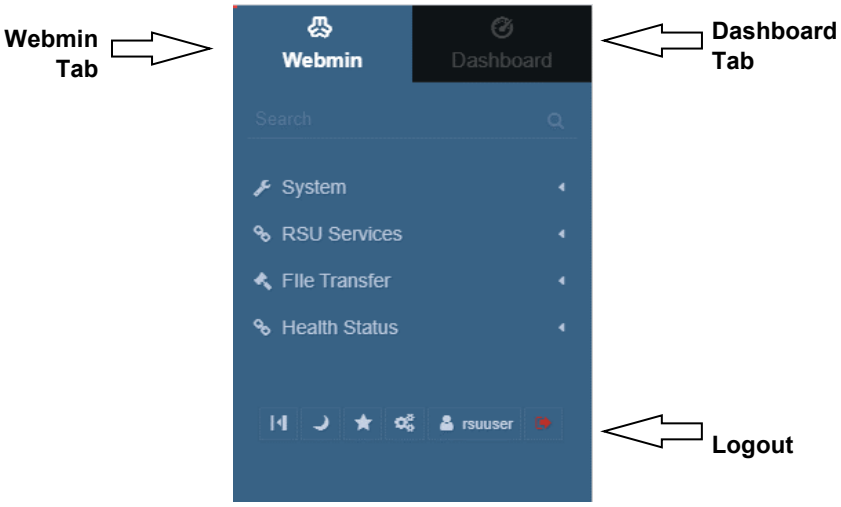
      Note: If the IP address has been changed from the factory default, use the new IP address to access the login website.

    - For the configuration tool to proceed, you must use the username and password given below at the default address:
      i. **RSU Root Username**: **rsuuser**
      ii. **RSU Root Password**: **6efre#ESpe**

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



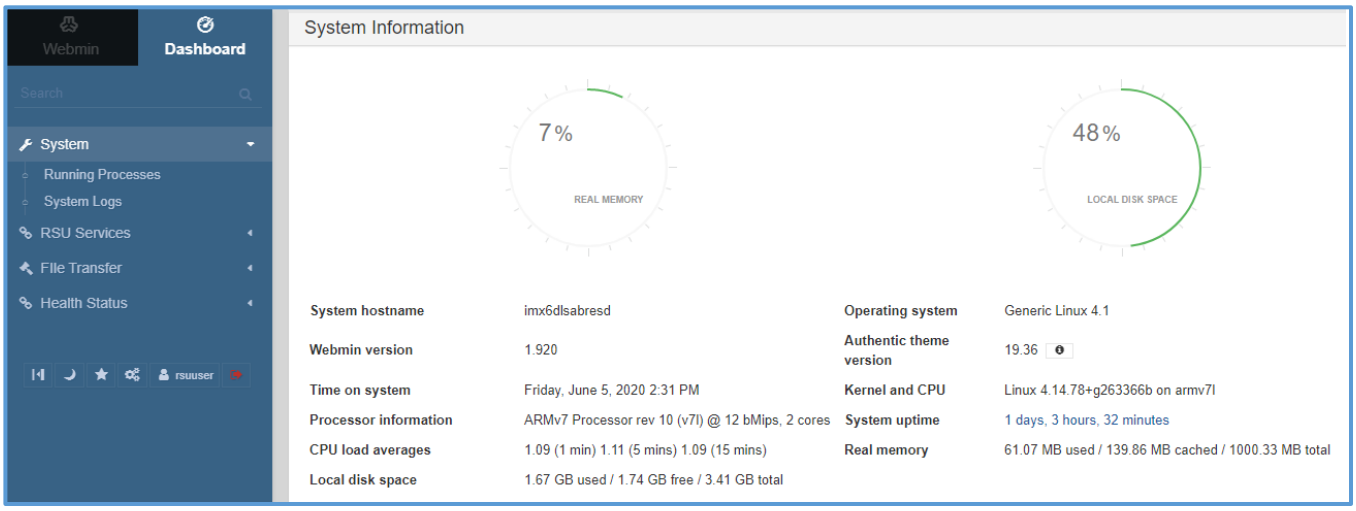
h. After Login, the BlueTOAD Spectra (Savari) RSU Main Menu is available for selection. SW2000 Webmin interface has two tabs, the Webmin and Dashboard Tabs. The Webmin tab contains information about System, RSU Services, File Transfer and Health Status as shown below. The Dashboard Tab provides the system information and the status of the running processes.



Iteris RSU Webmin System Overview

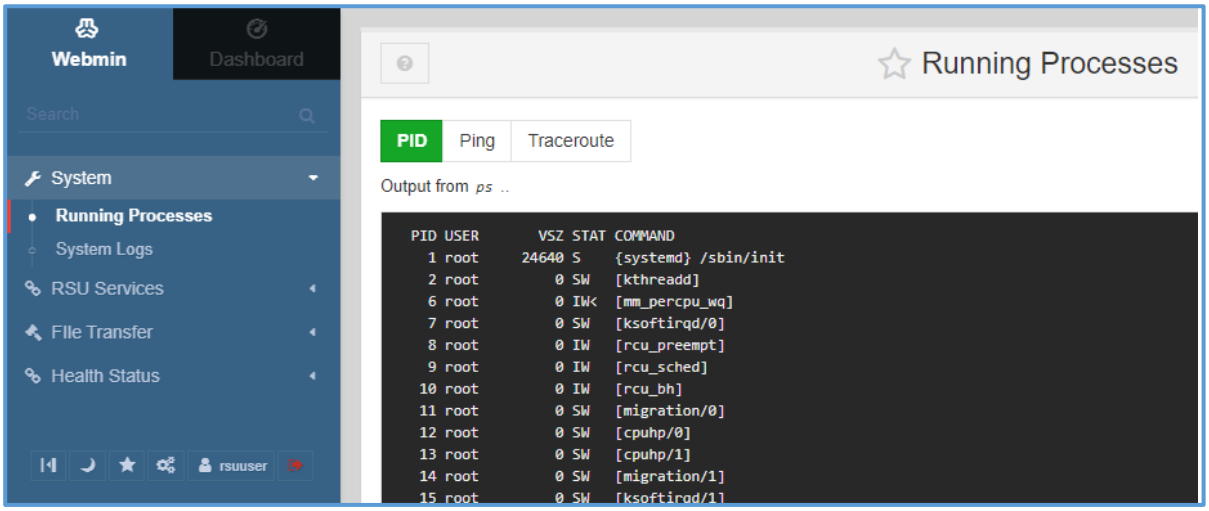
This section provides the system information and the status of the running processes.

1. Click on the Dashboard menu to view information about the System, as shown below:

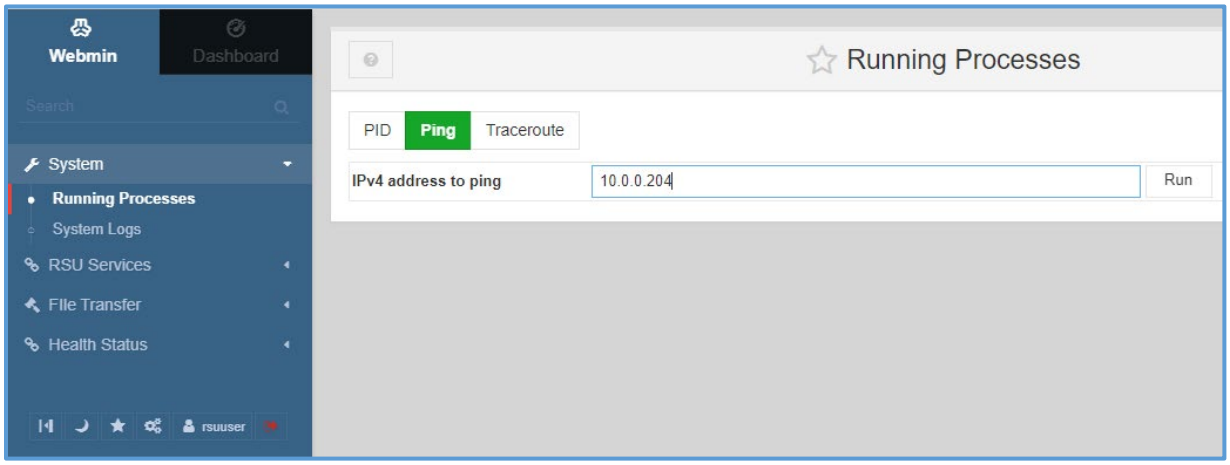


System Overview Information

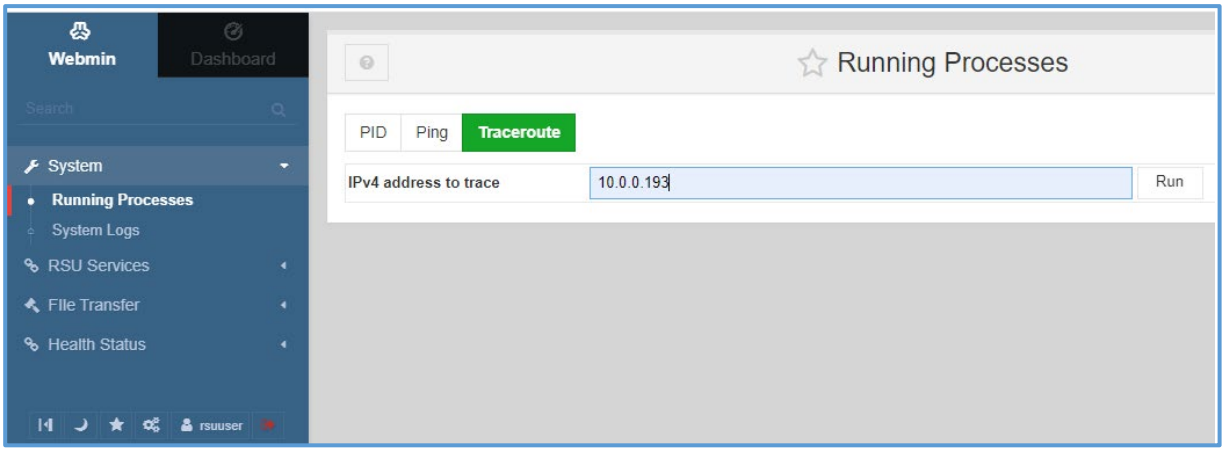
2. Click on the Running Processes to view the output of PID, Ping and Traceroute process. Click on the PID process it displays the list of all the running processes as shown below.



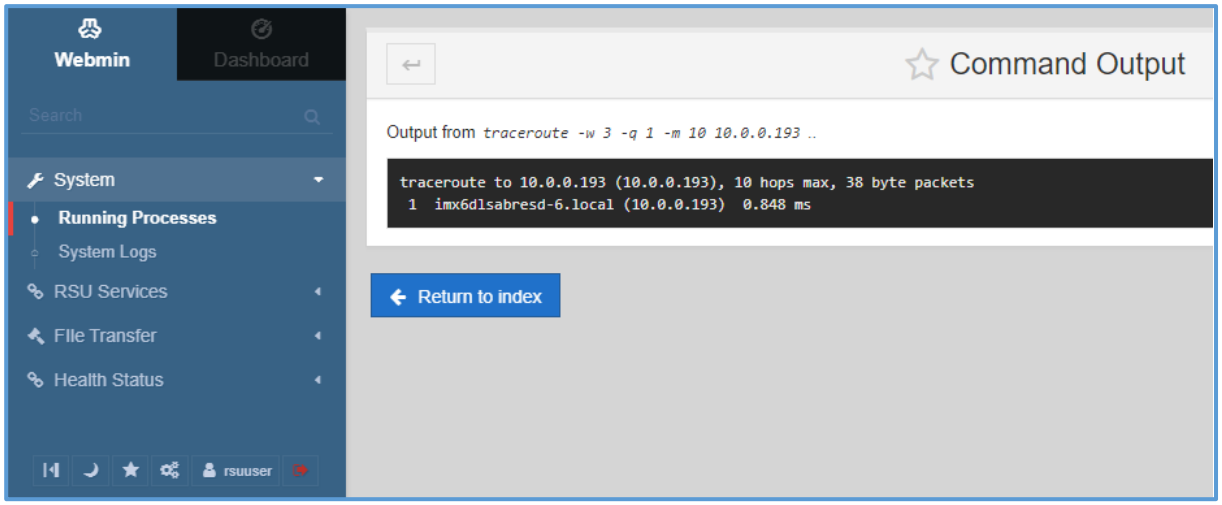
3. Click on the Ping tab in the Running Processes to check if a particular device is reachable or not



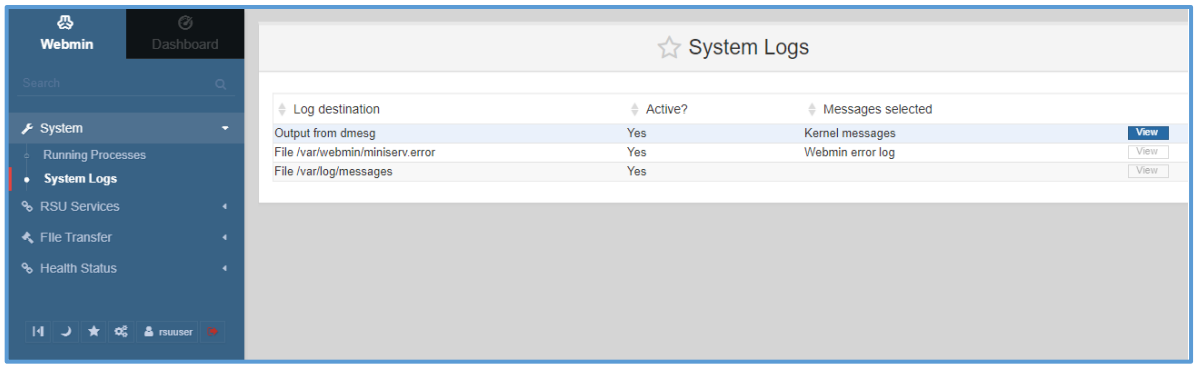
4. Click on the Traceroute tab in the Running Processes to trace the route of the machine/device.



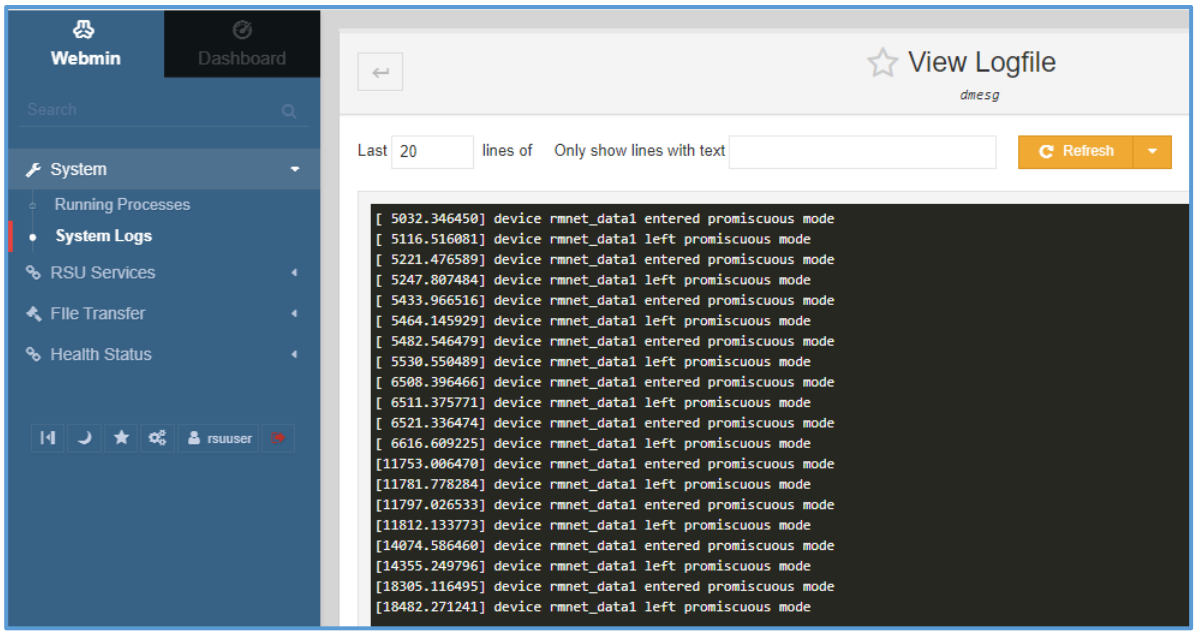
5. The Traceroute traces the IP hops and displays the output as shown below.



6. The System Logs displays the Log destination, along with their status as shown below. The system logs indicate Yes for Active and No for Not Active logs.



7. Click the View button to view more information about the system logs. The Log file information will be displayed as shown in the screen below:



OPERATIONS – How to Set RSU Services Parameters

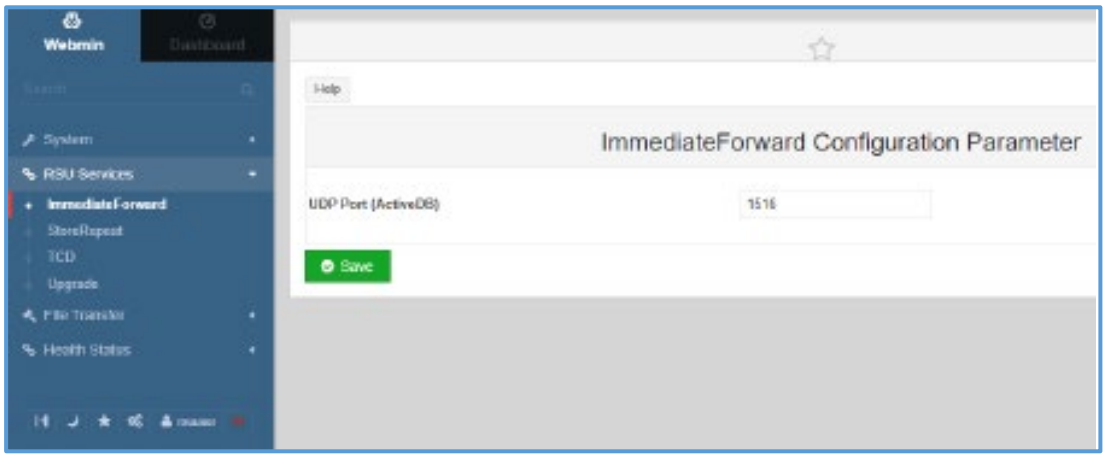
This section explains the parameters and statistical counters of individual RSU services. These counters get reset when the user places the SW2000 into a 'operate' state from a corresponding "standby" state or if configuration changes for individual applications. In the SW2000 Webmin Interface, Click on the RSU Services. ImmediateForward, StoreRepeat, or Traffic Controller (TCD) Tabs to access the lists of features supported by SW2000.

The following are the services supported by SW2000:

- Store-Repeat services, which includes MAP and TIM messages.
- Immediate-Forward services, including SPaT, MAP and TIM
- Traffic Controller Data, which includes SPaT

Immediate-Forward Service

In the SW2000 Webmin Interface, click on the ImmediateForward to modify the UDP Port. Click Save to save your changes, as shown in the screen below.



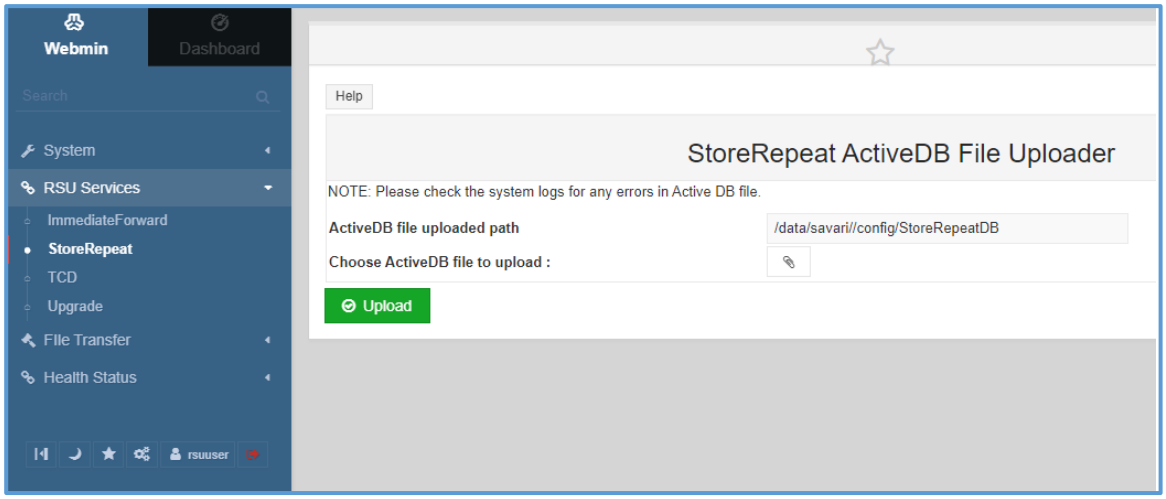
Immediate Forward Configuration Parameters

The following table lists the Immediate Forward configuration parameters which may be configured using the Webmin Interface.

No.	Parameter	Supported Values	Description
1	UDP Port	1516, 1024, 65535	UDP port on which the external server is listening (Configurable Port Range: 1024 - 65535)

StoreRepeat Service

In the SW2000 Webmin Interface, click on the StoreRepeat to modify the ActiveDB file uploaded path and upload the ActiveDB file. Click Upload to upload your changes, as shown in the screen below.



Store and Repeat Configuration Parameters

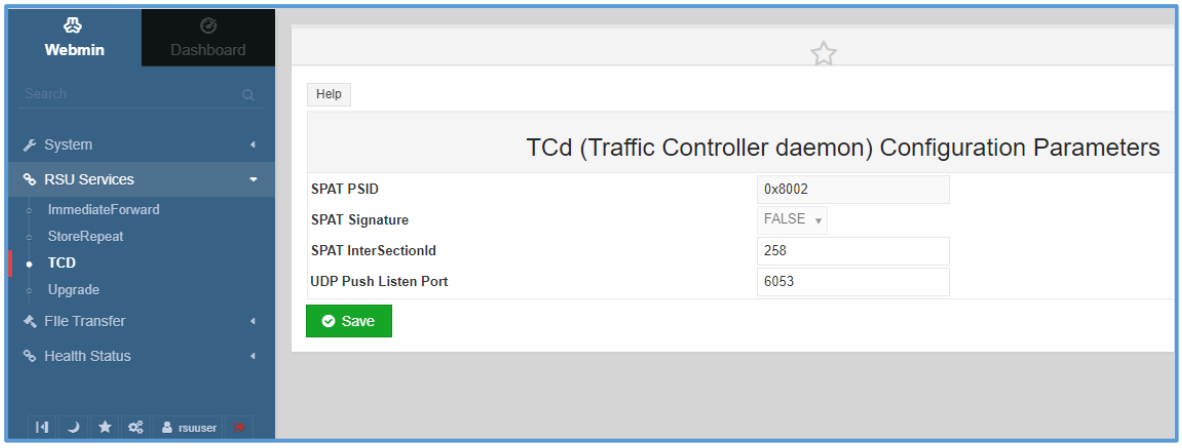
The following table lists the Store and Repeat configuration parameters which may be configured using the Webmin Interface.

No.	Parameter	Path	Description
1	ActiveDB file upload path	"/data/savari/config/ STOREREPEATDB/"	Always set to /data/savari/config/StoreRepeat DB/ Note: This path cannot be modified
2	Chose ActiveDB file to upload	"/data/savari/config/ STOREREPEATDB/"	

Traffic Controller Data (TCD) Service

In the SW2000 Webmin Interface, click on the TCD to modify the SPaT PSID, SPaT Intersection Id, SPaT Signature, and UDP Push Listen Port. Click Save to save your changes, as shown in the screen below.

The following table lists the TCD configuration parameters which may be configured using the Webmin Interface.



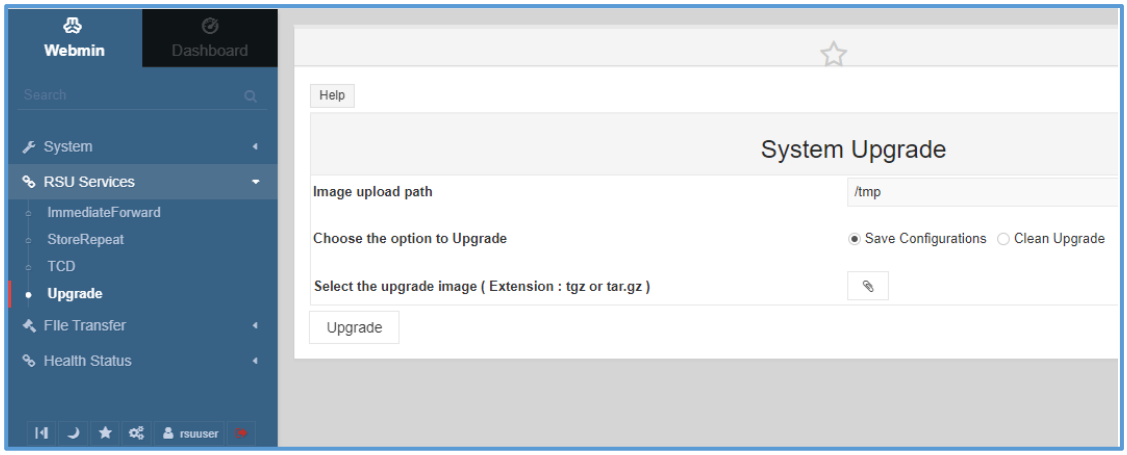
TCD Configuration

The following table lists the TCD configuration parameters. Access the **/savari/confconfig/Tcd.conf** file to configure TCD parameter values.

Parameter	Default	Range Min	Range / Max	Description
SPATPSID	0x8002			PSID/AID/V2XID with which the SPaT message is transmitted. byte AID: 0x00- 0x7F bytes AID: 0x8000 - 0xBFFF 3 bytes AID: 0xC00000 - 0xDFFFFF 4 bytes AID: 0xE0000000 -0xEFFFFFFF **Note**: Valid values are subject to standards and radio limitations.
SPATInterSectionId	258	0	65535 (US)	ID range of US: 0 to 65535 This must match with the corresponding ID with which MAP is being transmitted by Store and Repeat. Otherwise, SPaT messages are not transmitted.
SPaT Signature	False			SPaT signature indicates the security signature Supported values are “False” – True (Not supported in this release)
UDPListenerPort	1516, 1024, 65535			UDP port on which the external server is listening (Configurable Port Range: 1024 65535)
UDPPushListenPort	1516, 1024, 65535	1024	65535	UDP port on which the external server is listening

How to Upgrade the Iteris RSU Firmware

Click on the Upgrade Tab to perform system upgrade. Enter the System upgrade path (\tmp), choose the option to upgrade and select the upgrade image from your local folder as shown in the screen below. Once complete, click Upgrade for the upgrade to complete.

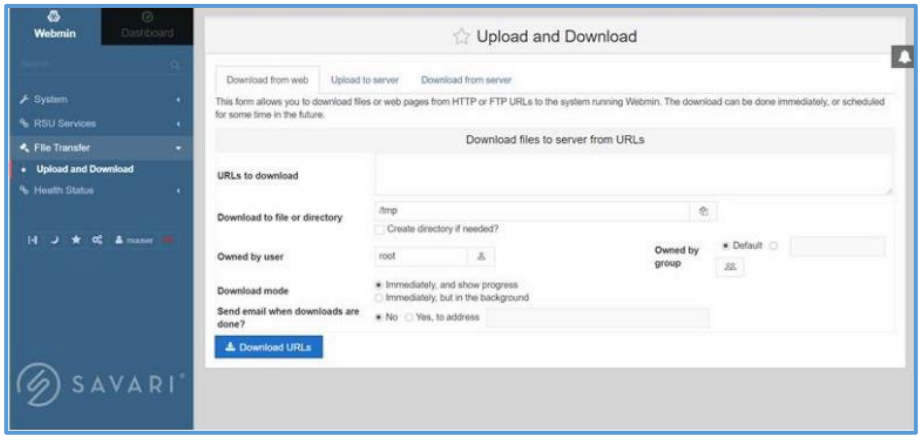


Parameter	Options	Description
Image upload path	Default path is /tmp	Indicates the path where the image file may be placed in the board
upgrade		Provides the option to save the existing configuration or clean the existing configuration and set to default
Select the upgrade image		the image from the

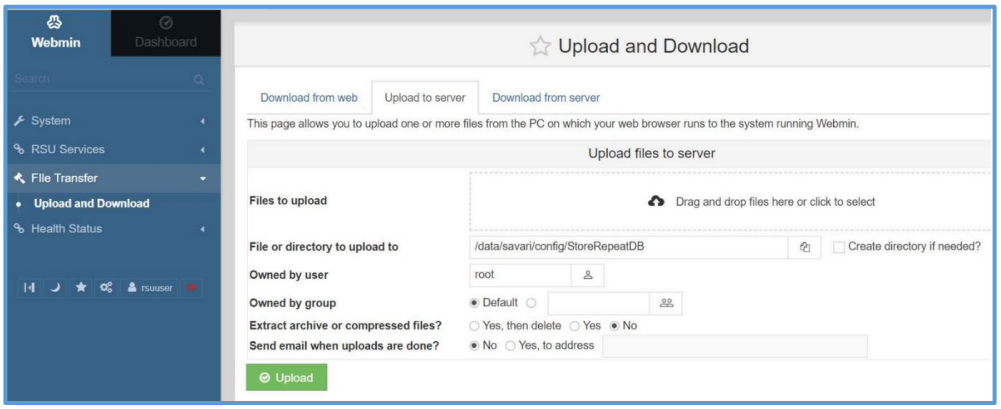
How to Transfer a File To/From RSU – File Transfer

This section provides details on the procedure to upload files to RSU (server), download files from RSU (server) and Download from web.

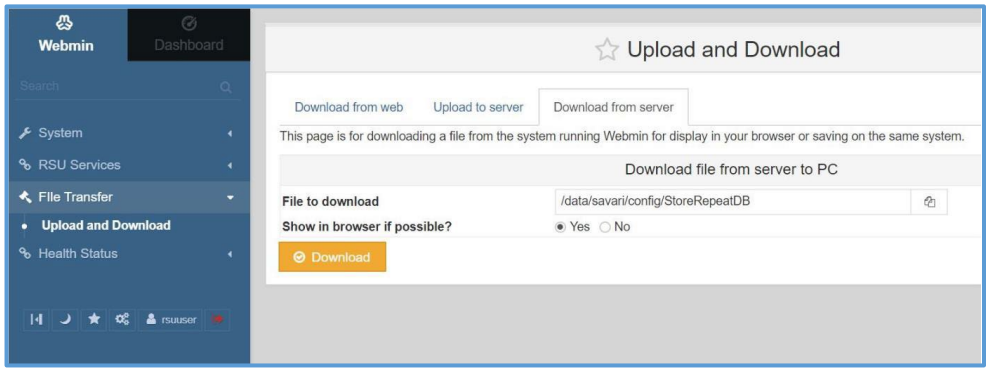
1. Download from web option is not supported in this release.



2. Click Upload to server to upload your files from local PC to the server. Click Upload to upload your files.



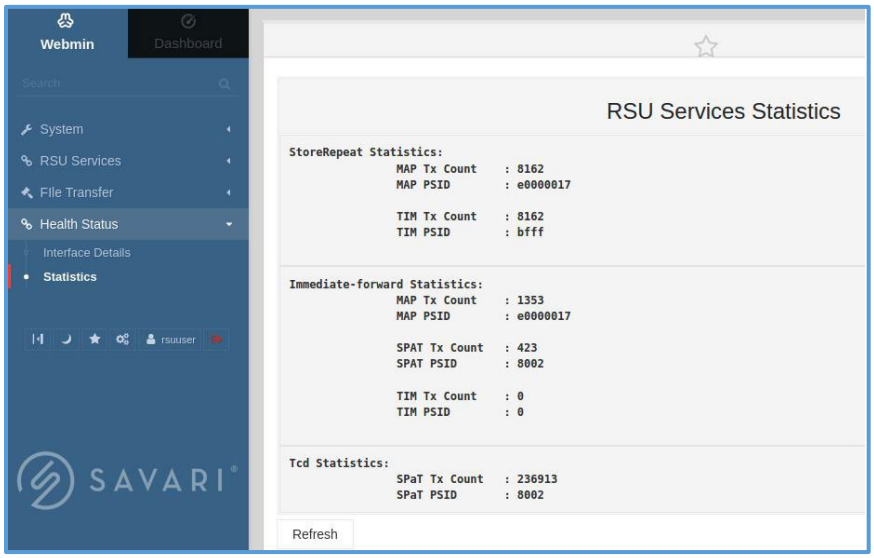
3. Click Download from server for downloading a file from the system running Webmin for viewing or saving on the local system. Click Download to download the file.



RSU Health Status Diagnostics Display

The Health Status menu helps to view Statistics. The Health Status provides service statistics details of StoreRepeat, ImmediateForward and TCD as shown in the screen below.

1. Click the Refresh button to view the updated service statistics details.

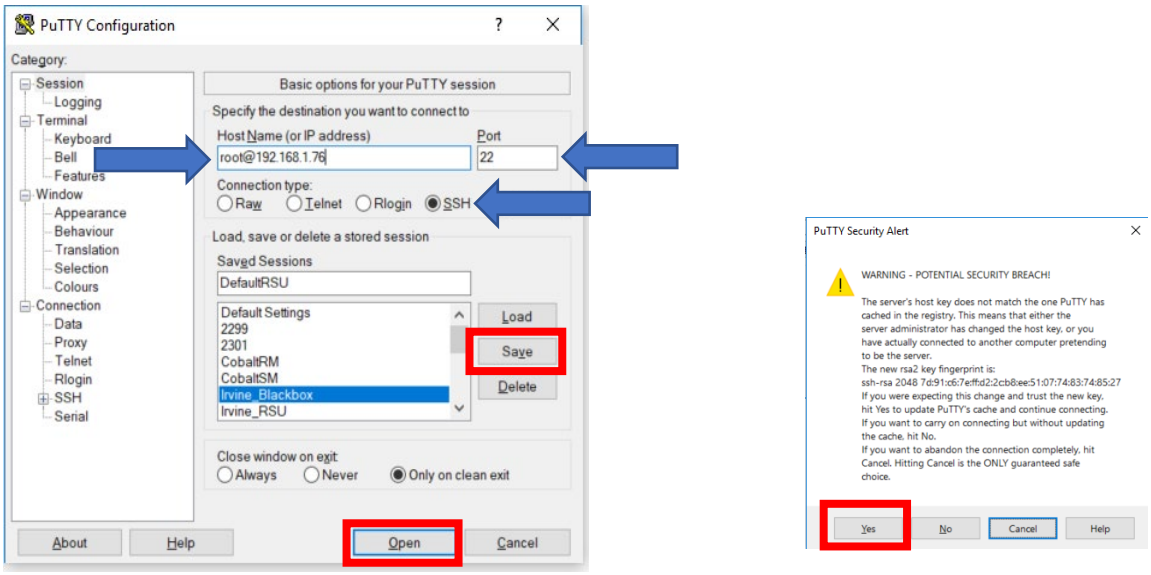


MAINTENANCE – Using the Command-Line Interface to Retrieve Diagnostics Statistics

This section provides access to RSU configuration parameters information using a CLI interface. The CLI Interface provides a series of Command-Line utilities to view specific RSU diagnostics information.

How to Access RSU Using CLI Commands

1. Open PuTTY to start an SSH session into the RSU. Set the Host Name to **root@192.168.1.76**, Port to **22**, Connection Type to **SSH**, and save the session as "**DefaultRSU**" for future use.



2. If prompted to accept the RSA key of the RSU click Yes.
3. When prompted, enter Default Password: **6efre#ESpe**
4. Once the BASH shell is available, you can begin retrieving RSU information.

Store and Repeat Messages

The following parameters get displayed in the Store and Repeat application status command:

/ # rsu_stats -s

Sample output as shown gets displayed. This example displays the Store and Repeat application in 'Running' state for 1 Active Message List.

```
StoreRepeat Statistics:
        TIM Tx Count   : 240268
        TIM PSID       : 8003

        MAP Tx Count   : 240268
        MAP PSID       : e0000017
```

Immediate Forward Message

Execute the following commands to display the parameters and counters in the Immediate Forward status

/ # rsu_stats -i

Sample output as shown below gets displayed.

```
Immediate-forward Statistics:
        TIM Tx Count   : 0
        TIM PSID       : 0

        MAP Tx Count   : 0
        MAP PSID       : 0

        SPAT Tx Count  : 0
        SPAT PSID      : 0
```

Traffic Controller Data (TCD)

Execute the following command to display the TCD app status parameters:

/ # rsu_stats -t

Sample output as shown gets displayed.

```
Tcd Statistics:
        SPaT Tx Count  : 0
        SPaT PSID      : 0
```

V2X Message Forward

1. Execute the following command to fetch statistics at the Network Proxy Forwarding layer

   /# savapp_us -p

   Sample output as shown gets displayed.

2. Execute the following command to reset statistics at the Network Proxy Forwarding layer

   /# savapp_us -z

   Sample output:

   ```
   CV2X Network Proxy reset successfully
   ```

```
NETWORK PROXY STATISTICS
**********Service 1 **********:
    Service ID              : 0x8002
    Service Direction       : TRX
    Transmit Count          : 0
    Receive Count           : 0
    Signing Failure Count   : 0
    Verification Failure Count : 0
**********Service 2 **********:
    Service ID              : 0x2
    Service Direction       : TRX
    Transmit Count          : 0
    Receive Count           : 0
    Signing Failure Count   : 0
    Verification Failure Count : 0
**********Service 3 **********:
    Service ID              : 0x8003
    Service Direction       : TRX
    Transmit Count          : 240362
    Receive Count           : 0
    Signing Failure Count   : 0
    Verification Failure Count : 0
**********Service 4 **********:
    Service ID              : 0x4
    Service Direction       : TRX
    Transmit Count          : 0
    Receive Count           : 0
    Signing Failure Count   : 0
    Verification Failure Count : 0
**********Service 5 **********:
    Service ID              : 0xe0000017
    Service Direction       : TRX
```

How to modify the 5.9 GHz Spectrum Radio Channel

1. Stop the RSU by executing “**systemctl stop rsu**”
2. Open **/data/savari/config/Radio.conf**
3. Search for “**Radio1_Continouous_Channel**” and replace the value with the required channel number
4. Use the same channel in “**TxChannel**” parameter in the Active DB files for StoreRepeat and Active DB data transmitted external server to ImmediateForward application.
5. Start the RSU by executing “**systemctl start rsu**”

4. BlueTOAD Spectra Setup Procedures

Important: Contact Iteris BlueTOAD support, 1-608-713-9299, **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 Cables[2]
- 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:
        i. Make sure a site survey checklist has been completed for all locations.
        ii. Make sure you have all the necessary parts for the system. Refer to the table on Page 2-2 for a list of the items included with your BlueTOAD Spectra RSU.

Network and Communications Setup Parameters

Traffic Network – Evaluate the existing network.

- Fiber and/or Ethernet based? Or no network communications?
- 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.
- What is the IP address assigned to the BlueTOAD Spectra and BlueTOAD Spectra RSU?
- Port 10001 needs to be open to 52.39.79.127 (to collect Connected Vehicle specific data)

[2] Ethernet Cables are NOT necessary for the BlueTOAD Spectra Solar Cellular detector.

- Port 8010 needs to be open to btserver.trafficcast.com
- Port 123 needs to be open, only if using an external NTP server.
- 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

12. To configure the Web IP of the BlueTOAD Spectra component of the BlueTOAD Spectra RSU[3]:
    a. Connect the Ethernet BlueTOAD™ to a switch or laptop Ethernet port.

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

    b. Power ON the Ethernet BlueTOAD™.
    c. Log into the BlueTOAD Spectra detector:
        iii. Open a Web Browser (Google Chrome or Microsoft Edge is preferred).
        iv. 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. **Important:** Make sure that you keep a record of the new settings. If you do not know the Static RSU IP address, you CANNOT log back into the RSU!

        v. 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.

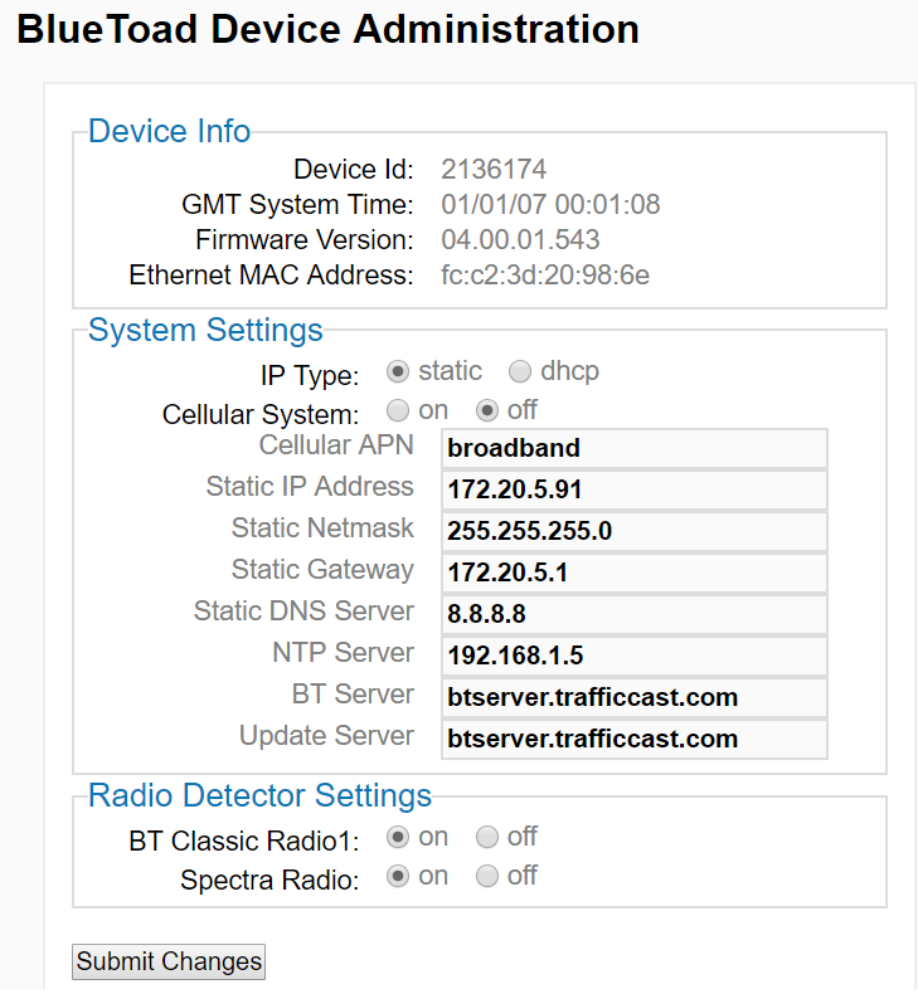
> **Note**: For a helpful workbook to keep a record of the values in each field, go to https:// https://trafficcast.zendesk.com/hc/en-us/articles/360015177732-Preprogramming-installation-cheat-sheet
> In the middle left of the page, select **BlueTOAD Programming Cheat Sheet.xlsx** At the bottom left 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.

[3] 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.

BlueTOAD Web IP Configuration Menu



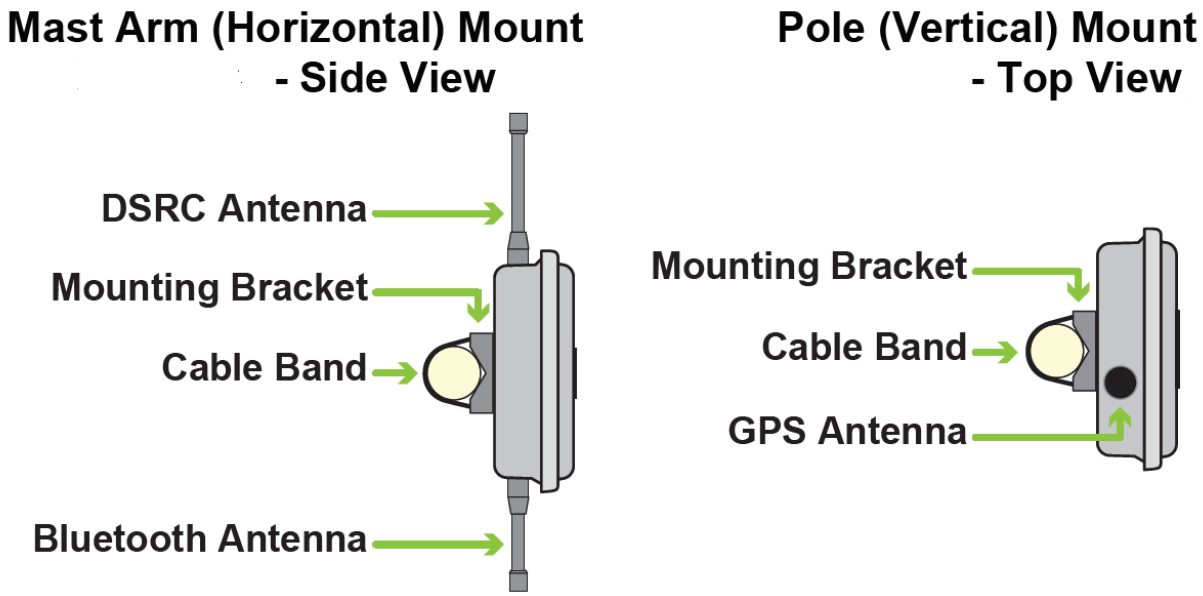
5. Installation & Maintenance of BlueTOAD Spectra RSU

Guidelines to install an RSU enclosure:

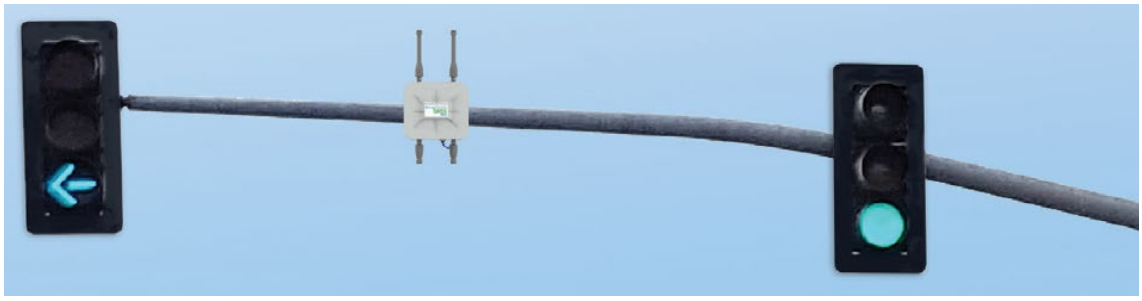
1. **Mounting Structure**—a Mast Arm or Roadside Pole that:
   - Is near the roadside traffic signal cabinet, or appropriate 120 VAC power source

   Note: The mounting pole should be near the cabinet for easy conduit access.
   - Has a mounting location with a clear line-of-sight from the RSU antennas to the target road segment
   - **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 Arm[4] or Pole
   - 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.

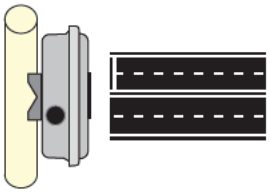


[4] The preferred installation is on a Mast Arm, as shown on the next page.

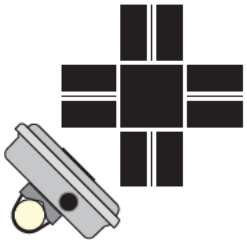


5. Align the Enclosure per your installation as shown below:

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.



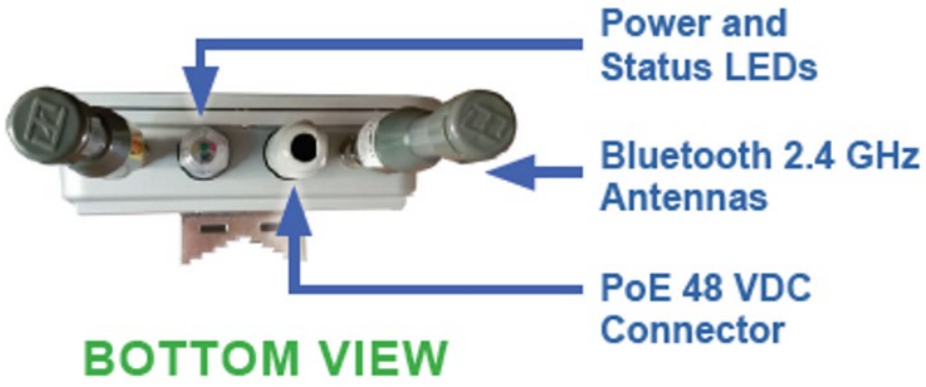
6. Guidelines to route and connect the cables:
    a. **Traffic Closure**—Close traffic lanes as necessary to pull cable.

b. **CAT-5 Ethernet Cable**

i. Pull the main CAT-5 Ethernet Cable through the roadside conduit from the roadside cabinet to the RSU enclosure.

ii. Connect the Ethernet cable to the PoE 48 VDC Connector on the bottom of the RSU 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-

NOTE: Required Best Practice!

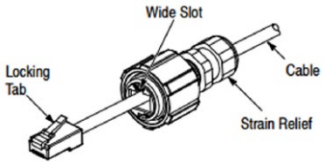
It is required to wrap antenna metal connectors with Hand Moldable Plastic COAX-SEAL. Seals connectors from moisture and corrosion.

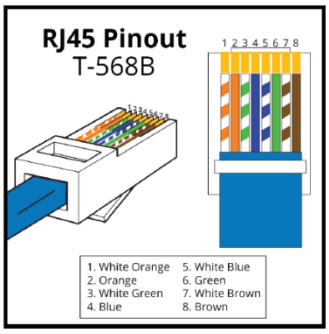
ALL TrafficCast RSU installations will utilize Plastic COAX-SEAL for antenna connectors.

wrapped with watertight sheathing.

iii. 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.

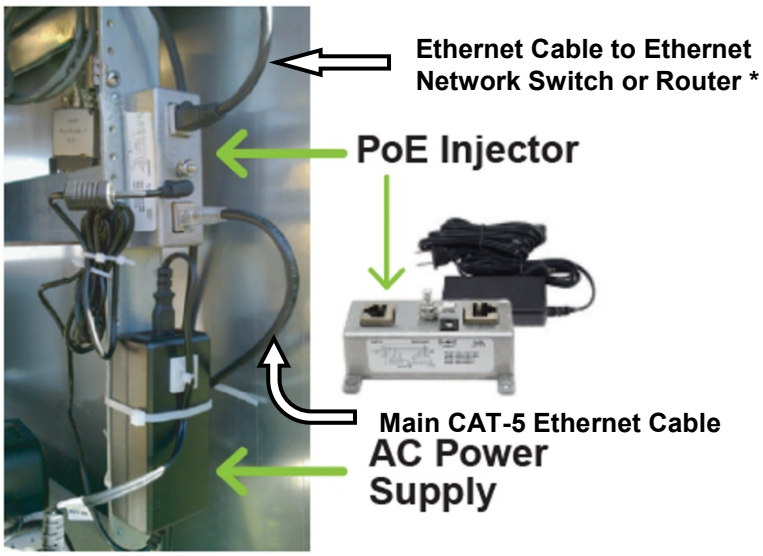




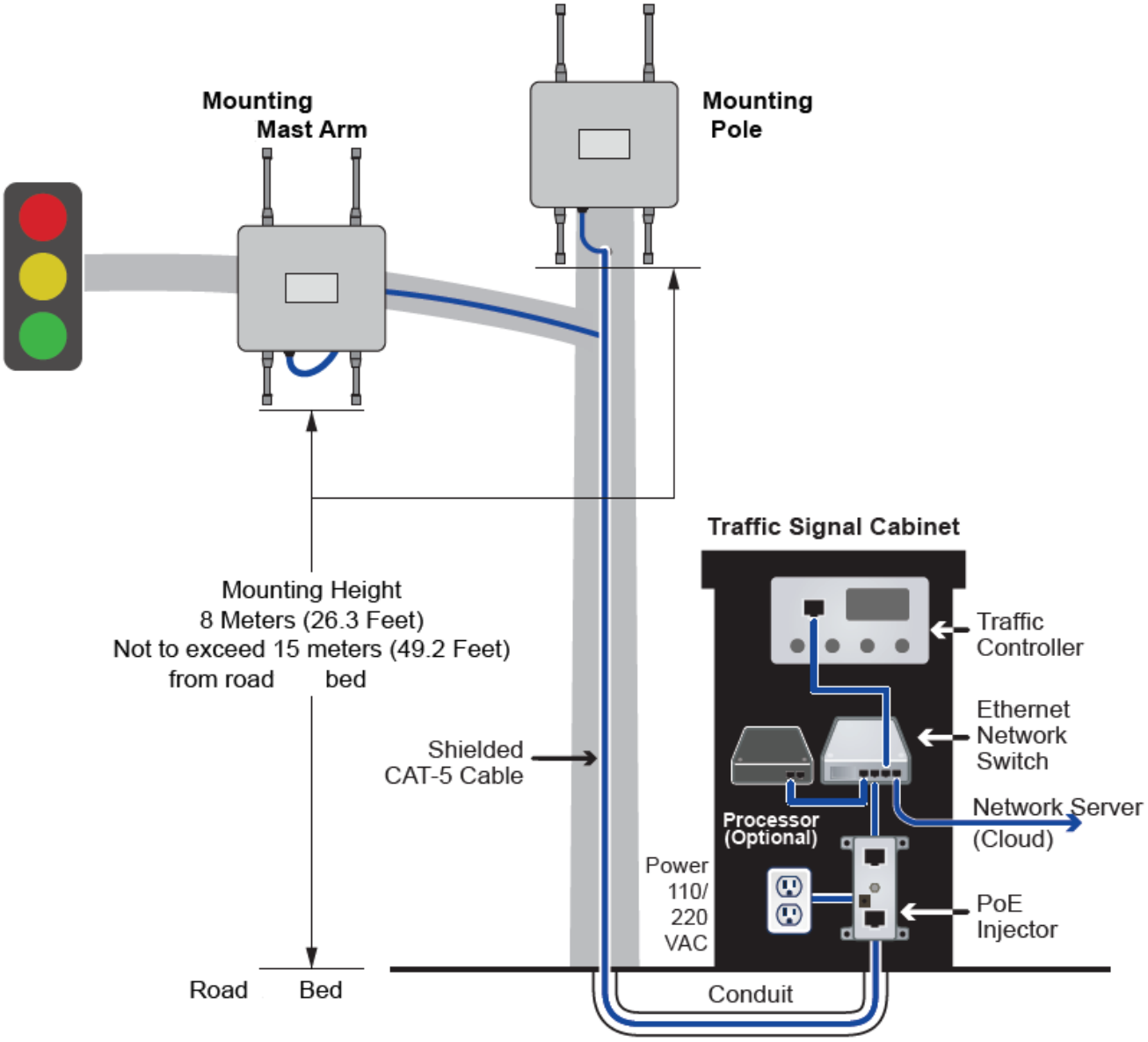
7. Install the PoE Injector in the roadside cabinet:
   i. Secure the PoE injector onto a flat surface inside the roadside cabinet.

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 PCB of the RSU, i.e. to the PoE Splitter

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

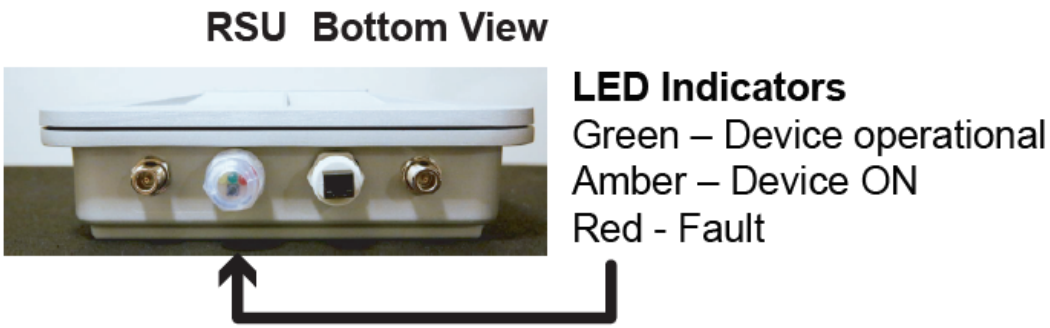


8. This is the completed installation of a Spectra RSU that shows both possible ways to mount the enclosure—on a Mast Arm and a Pole:



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:



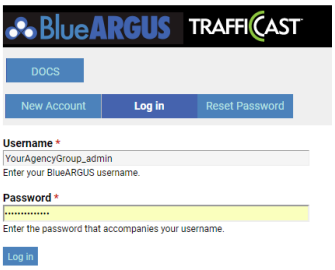
3. Before leaving the location:
   a. After the unit is Powered ON, call Iteris Customer Support at **(608) 713-9299**. Also refer to Iteris support website: https://bluetoad.zendesk.com
      i. Tell Iteris the device ID number and that the LEDs are normal.
      ii. Confirm from Iteris that the network is transmitting the SPaT and MAP data from this unit.
   b. Access Iteris RSU status using the web based BlueARGUS 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. BlueARGUS Website: https://trafficcast.zendesk.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 BlueTOAD support, 1-608-713-9299, **before** you install any equipment to make sure all devices have been correctly deployed and tested.

Confirm Network Connectivity and Data Collection

5. Now that you have tested the LEDs, make sure that data is being received by the Iteris National Servers:
   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 BlueARGUS (Iteris will provide login Username and Password before installation).

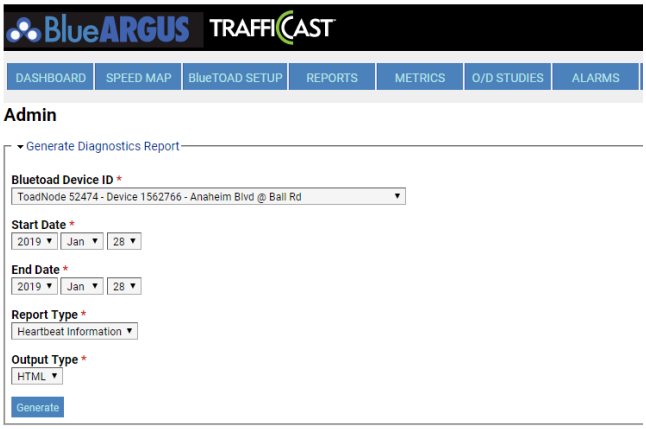
BlueARGUS Login page: https://trafficcast.zendesk.com/

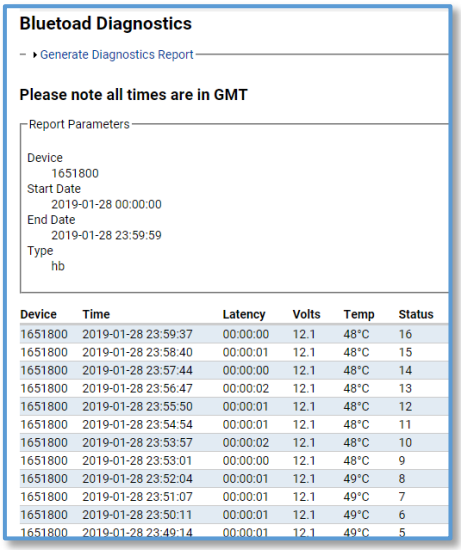


   c. Enter Diagnostics URL to test that data collection is active and generate a diagnostics report:

   - https://trafficcast.zendesk.com/diagnostics

   d. Select BlueTOAD Device ID from the dropdown list.
   e. From Report Type dropdown list, select Heartbeat Information.
   f. From **Output Type** dropdown list, select **HTML**.
   g. Select **Generate** to open the diagnostics report. BlueTOAD Spectra should start to collect data within 2-5 minutes after you enable power connections.





Troubleshooting

6. **Troubleshooting BlueTOAD Spectra Connectivity**
   After the detector has started detecting Bluetooth signals, communicated the device ID number, and the LEDs are normal:
   a. Call the Iteris **Customer Support Number**, (608) 713-9299.
   b. Confirm from Iteris that the network is transmitting the data from this detector.
   c. Possible issues include:
   - Network Port settings are incorrect – confirm the settings with the Agency IT department (as above)
   - Ethernet switch port not active or communicating
   - 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 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

7. In the pre-installation process, Iteris adds each installed BlueTOAD detector to a list of detector locations within the BlueARGUS 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, go to https:// https://trafficcast.zendesk.com/hc/en-us/articles/360015177732-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, notice the **Pre Installation Sheet** and **Field Installation Check List** tabs.

Customer Support Number: (608) 713-9299
Iteris Support Website: https://bluetoad.zendesk.com (Iteris will schedule an installation appointment.)

Data and Device Management via BlueARGUS

8. Iteris Support will set up and configure Agency access to BlueARGUS data collection and management system.
    - You can monitor each BlueTOAD detector using the web-based BlueARGUS 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. BlueARGUS Website: https://trafficcast.zendesk.com

On-Going Operations / On-Going Customer Support

9. Each Connected Vehicle system deployed will have access to the full suite of support resources available through the Iteris and BlueARGUS system management software:
    - **BlueARGUS On-Going Operations Website:** https://trafficcast.zendesk.com
    - **Iteris Support Website:** https://trafficcast.zendesk.com
    - **Iteris Support Number: 608-713-9299**

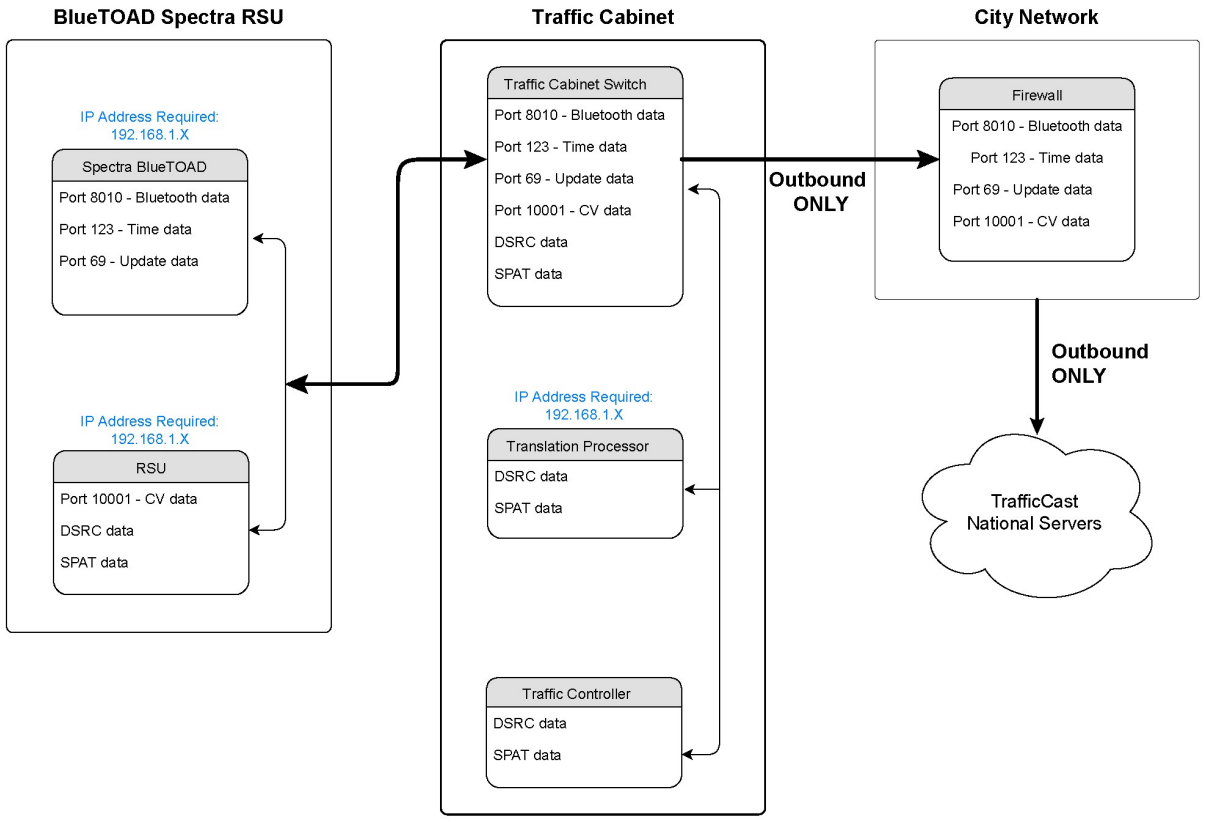
6. Appendix – BlueTOAD Spectra RSU, Recommended Network Configuration Implementation Requirements

Local Network Settings

Local network settings requirements for data collection and management:

1. BlueTOAD Module assigned: IP Address, Subnet Mask and Gateway
2. DSRC/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 10001 needs to be open to 52.39.79.127 (Connected Vehicle specific data)
5. Port 8010 needs to be open to btserver.trafficcast.com
6. Port 123 needs to be open, only if using an external NTP server.
7. Required DNS entries for btserver.trafficcast.com:
    - 18.220.189.165
    - 3.18.180.164
    - 3.18.166.19

Network Overview Diagram



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	22	TCP	SSH - SCP, SSH, and SFTP for remote terminal sessions and file transfers
RSU	80	TCP	HTTP
RSU	443	TCP	HTTPS - https to access web-based configuration GUI
RSU	9000	TCP	https to access (DSRC) web-based configuration GUI
RSU	10000	TCP	HTTP (Webmin - C-V2X)
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.
In-Cabinet Processor	8883	TCP	MQTT
In-Cabinet Processor	8081	TCP	PedSafe Web UI
In-Cabinet Processor	8082	TCP	PedSafe Web UI
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/CV2X Data
RSU	10002	UDP	DSRC/CV2X Data
RSU	53	TCP and UDP	DNS
RSU	123	UDP	NTP
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)

7. Appendix – BlueTOAD Spectra RSU DSRC and C-V2X, 5.9 GHz Spectrum Specifications

Iteris DSRC/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** – SW2100-qmxxxx
2. **FCC ID numbers:** FCC certified - 2AADT-SDR1000 plus C-V2X module (certification pending)
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: USDOT RSU Specification V4.1 Req_432-v004 references antenna centerline Mounting Height of 8 Meters (26.3 Feet), not to exceed 15 meters (49.2 Feet) from roadway bed surface.
7. **RSU Equipment Class** - C = 20 dBm Max. Output Power (400-meter communication zone)
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. 172 – 5855-5865MHz (Max EIRP = 33 dBm) (Public Safety)
    b. 174 – 5865-5875MHz (Max EIRP = 33 dBm)
    c. 176 – 5875-5885MHz (Max EIRP = 33 dBm)
    d. 178 – 5885-5895MHz (Max EIRP = 33 dBm) (Control Channel)
    e. 180 – 5895-5905MHz (Max EIRP = 23 dBm)
    f. 182 – 5905-5915MHz (Max EIRP = 23 dBm)
    g. 184 – 5915-5925MHz (Max EIRP = 33/40 dBm) (Government entities)

NOTE: The Iteris RSU shall support use of all the above channels. However, Iteris will follow the latest FCC draft proposal guidelines for new experimental/deployment licensing requirements.

Iteris RSU – Specifications

Standards Compliance

- DSRC Roadside Unit (RSU) Specifications Version 4.1
- 2016 SAE-J2735 specifications and SAE-J2945/1
- IEEE 802.11p, 1609.3 (WSMP), 1609.4, 802.3at Standards
- IEEE 1609.2, Draft ETSI EN 302 571 and
- 3GPP, Release 14/15 for C-V2X

V2X Security

- NIST/Brainpool ECC up to 384b
- V2X-embedded HSM (Hardware Security Module) with storage up to 500-plus keys.

C-V2X

- C-V2X Qualcomm® QC 9150 Chipset
- 3GPP Release 14/15 C-V2X PC5 (5G Upgradeable via module replacement possible when available – factory upgrade)

Power Specifications

- Operating Voltage: DC 12V – 24V (max 12W).

Power over Ethernet (PoE)

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

Operating Range

- -34 degrees C (-30 degrees F) to +74 degrees C (+165 degrees F)

Processor

- ARMv9 32-bit Co-Processor
- NXP i.MX6 Processor
- 2GB DDR Memory
- 4GB Flash Onboard Storage
- Linux Yocto v4.14

Interface Options

- PoE - Ethernet 10 BASE-T / 100 BASE-T
- Static IP Addressing, DHCP
- IPv6, IPv4
- Dual antenna supports two modes:
    - 1. Single-channel mode (2 antenna diversity operation)
    - 2. Dual-channel mode (1 antenna per channel), 2 independent IEEE 802.11p radios operating on different radio channels.
- IEEE 802.11p Class C (5 GHz band)
- 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 GHz DSRC/C-V2X antennas)
- 2 - 2 dBi Omni (Bluetooth Discoverable and Non-Discoverable Detector)
- Dual-Channel 5.x GHz RF paths (5.18 GHz to 5.93 GHz)
- LNA active GNSS and LTE external antenna

For Your Notes:

8. Appendix – Connected Vehicle In-Cabinet Processor Specifications

The Iteris In-Cabinet Processor is an Industrial Computer suitable to host and manage Connected Vehicle (CV) applications via an Infrastructure-to-Vehicle Hub (I2V Hub). 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 CV infrastructure and vehicle systems 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 Traffic Controller Translator (TCT) is an embedded device used to help facilitate integration between multiple different types of traffic controllers and the DSRC/C-V2X based Roadside Unit. 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 TCT 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 has the added functionality of providing debugging tools with GUI visualizations for applications such as emergency vehicle preemption and transit signal priority.

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 18.04 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 18.04 Desktop Version
- Default Login information: Username / Password
  (Contact your account manager to receive Username and Password information or see Iteris Support contact information below)

Unique Iteris Directory Structure Elements

In addition to the standard Ubuntu Operating System and basic applications that are installed on the processor, Iteris provides a set of basic configuration and management utilities to enable default Roadside Unit functionality and specific Connected Vehicle Applications.

The following folders contain critical configuration information, translators and software utilities to manage communications between the traffic controller and BlueTOAD Spectra RSU. The processor also contains unique Traveler Information Message (TIM) translators to support RSU message developed for use by the Iteris TravelSmart iOS and Android based smartphone applications.

Please DO NOT DELETE or DO NOT MANIPULATE IN WHOLE OR IN PART
these Critical Iteris folders:
/home/user/TCT and **/home/user/TCT-Configs**

Changing the contents of this folder **WILL adversely affect** the operations of the RSU!
Contact your Iteris account manager for more information.

How to Configure Network Settings in Ubuntu

In Ubuntu, basic network configuration changes can be made by either using the Command line or the Ubuntu Network Manager GUI (enabled using the Processor's VGA Monitor Port and USB Keyboard Port). See the following link for specific Ubuntu network configuration instructions:
https://vitux.com/ubuntu-network-configuration/

The Iteris in-cabinet processor is preset using the following network parameters:

- Default IP Address as set by Iteris: 192.168.1.xxx with Default Subnet Mask (255.255.255.0)
- The Processor's unique Default IP Address can be found on an external label affixed to the enclosure of the processor.

To facilitate DSRC/C-V2X Traveler Information Message (TIM) broadcast by RSU and TIM posts created by Iteris TIM composition services, the TCT needs access through the following two IPs and TCP ports to enable secure HTTP/HTTPS via Iteris' REST API: **52.39.79.127:60001 / 52.35.172.198:443**

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

- BlueToad Support Hotline: +1-608-713-9299
- General Information: info@iteris.com
- BlueToad Support: bluetoad-help@trafficcast.com

9. Appendix – How to Create an RSU MAP File

Objective

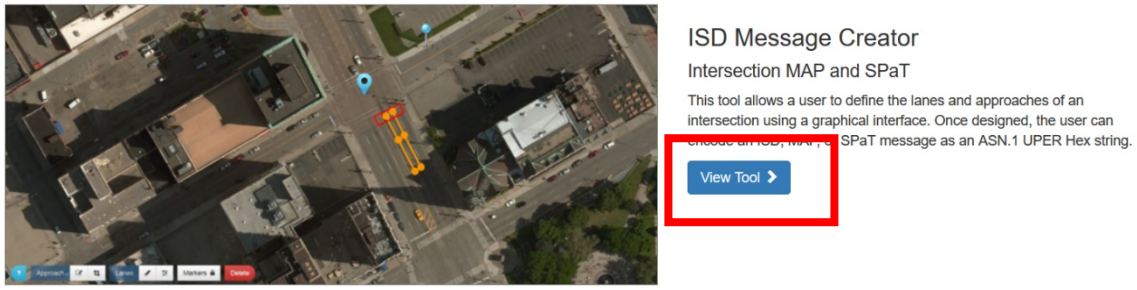
This procedure outlines the steps to produce an SAE J2735 compliant MAP file. J2735 messages are encoded using unaligned packed encoding rules (UPER) when transmitted from the roadside unit based on the 2016 standard's requirements. This procedure assumes that you are familiar with traffic control terminology, intersection geometry and layout.

Material Requirements

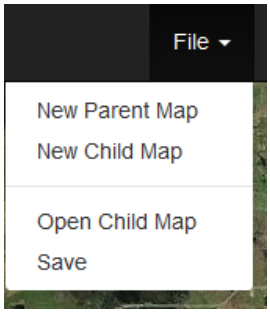
- Windows PC with internet connection and web browser
- Customer intersection location
- Intersection diagram or equivalent

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.

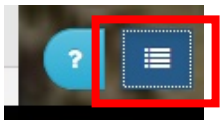


3. Click **File > New Parent Map** to start a new parent map.



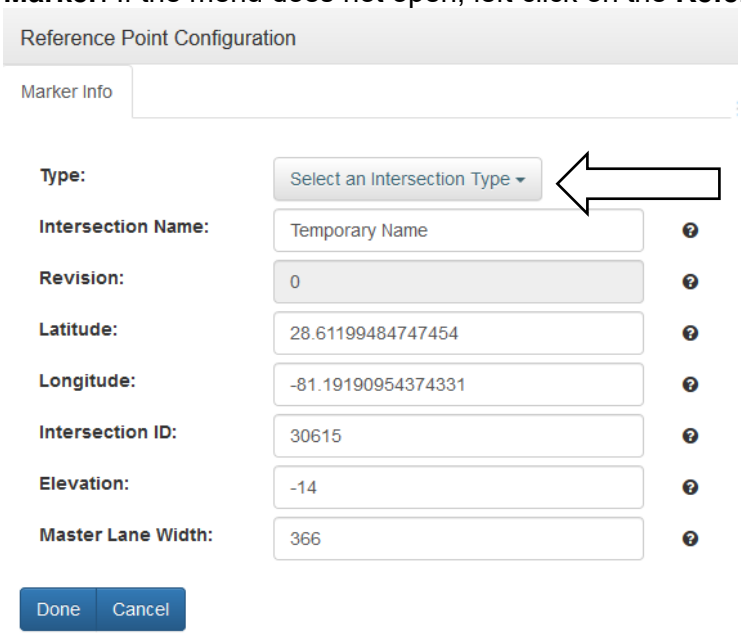
4. In the search bar, enter an address near the intersection location.

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

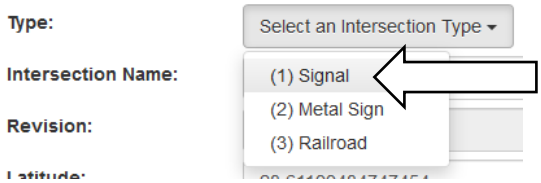


6. Put the **Reference Point Marker** in the center of the intersection.

7. 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.

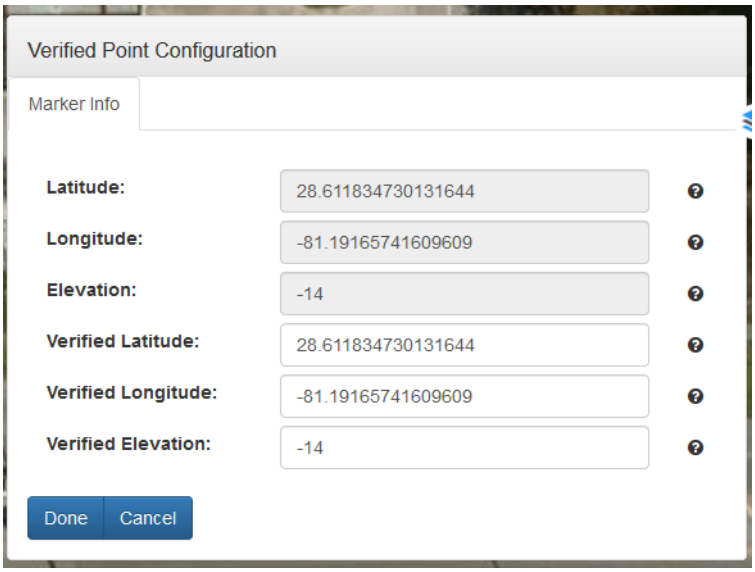


8. In the **Type** field, select **(1) Signal** as the Intersection Type and click **Done**.



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.

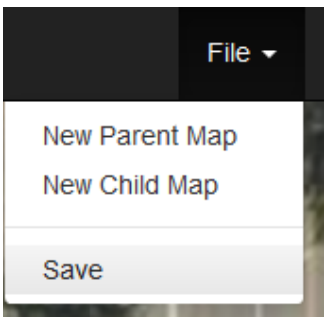


11. If the **Verified Latitude** and **Verified Longitude** values are available from on-site field surveys, enter them in the noted fields then click **Done**. If verified values are not available, just click **Done**.

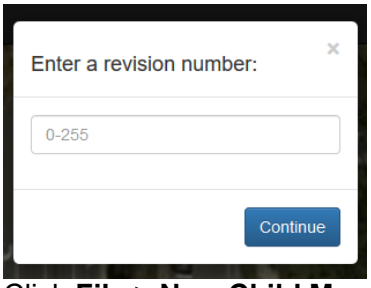
Note: The internal GPS of the BlueTOAD Spectra RSU automatically calculates its Elevation.

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

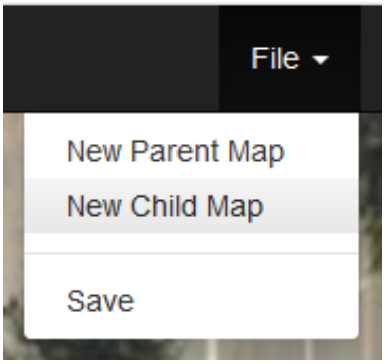
Note: Do NOT press **Enter**—make sure you click **Continue**.



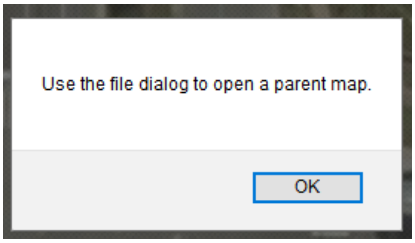
13. When prompted to enter a revision number, enter **0**, click **Continue**, and save the Parent Map to the local disk.



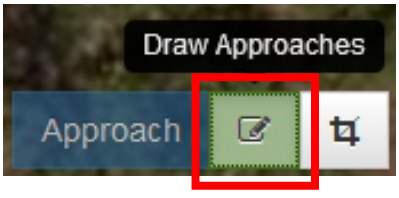
14. Click **File > New Child Map** to start building the Child Map.



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.

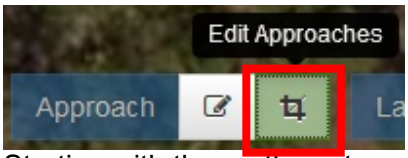


16. Click on the **Draw Approaches** button in the bottom left corner to select the draw approach boxes.

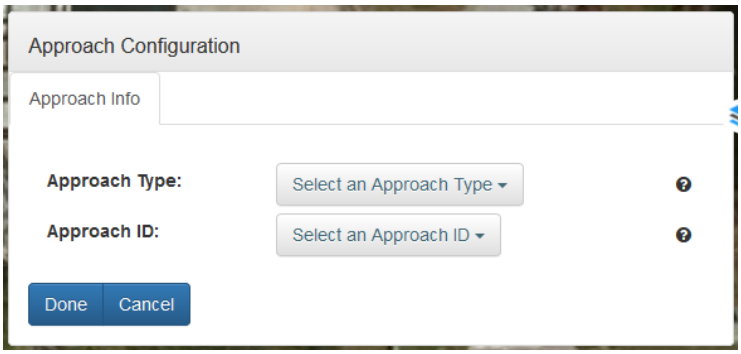


17. Draw approach boxes across every Ingress and Egress[5] approach relative to the intersection over the stop bar and across every lane as shown.

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



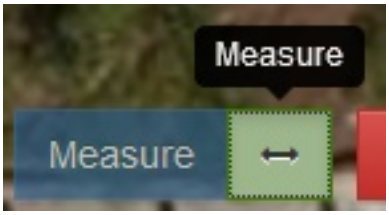
19. Starting with the northmost approach, left click on each **Approach box** to open the Approach Configuration Menu.



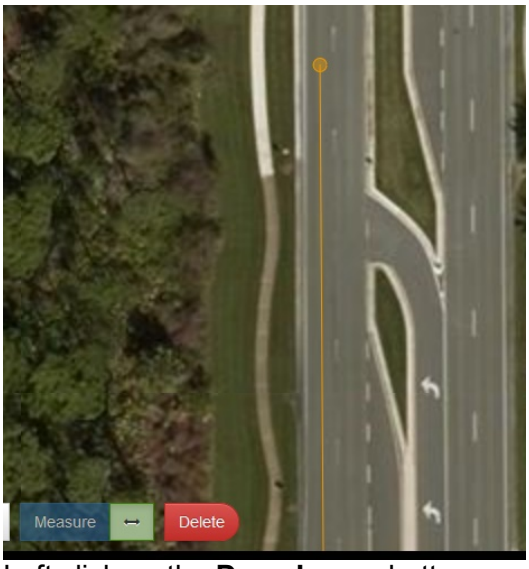
20. Under **Approach Type**, select **Ingress** if the lanes are directed into the intersection and **Egress** if the lanes are directed out of the intersection; select the lowest **Approach ID** available starting at **01** then click **Done**.
21. Repeat Step 19 and Step 20 for all Approaches in a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

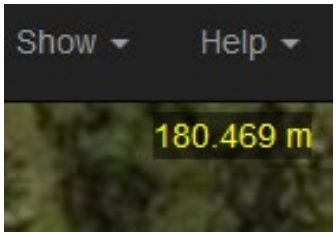
[5] **Ingress** = Going into (entering) an intersection; **Egress** = Going out of (leaving) an intersection

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.

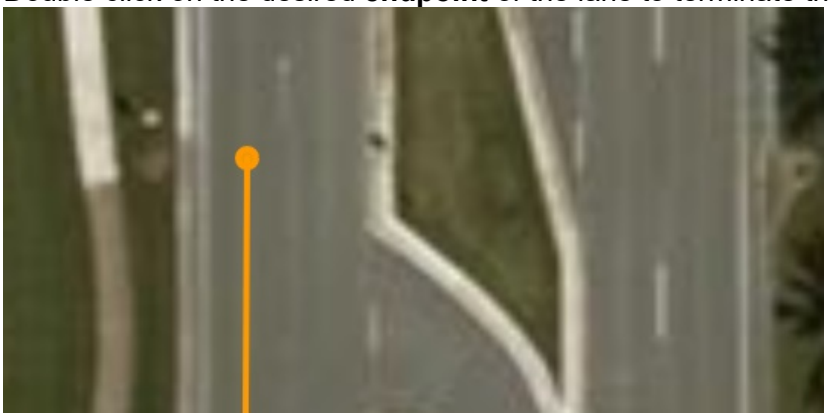




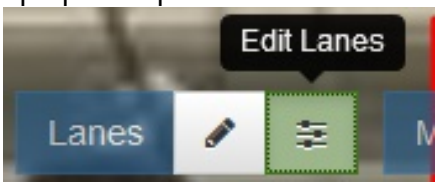
24. Left click on the **Draw Lanes** button.

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

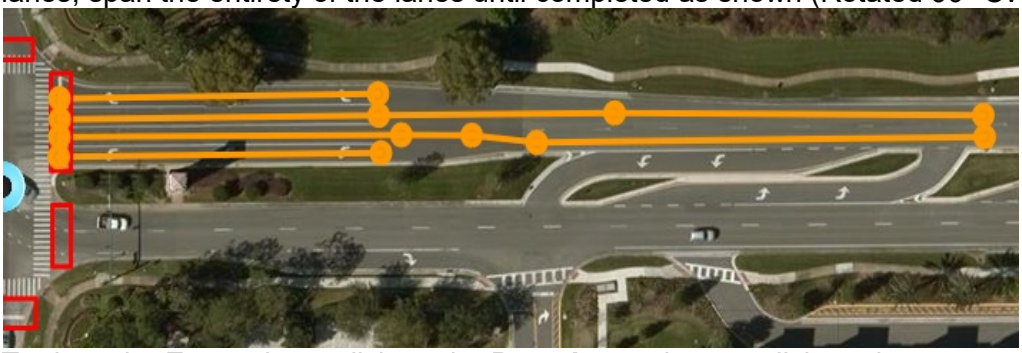
26. Use the **middle mouse button** to drag the view out to the measured landmark. Left click on the **center** of the lane as needed to remain in the center.
27. Double click on the desired **endpoint** of the lane to terminate the lane.



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.

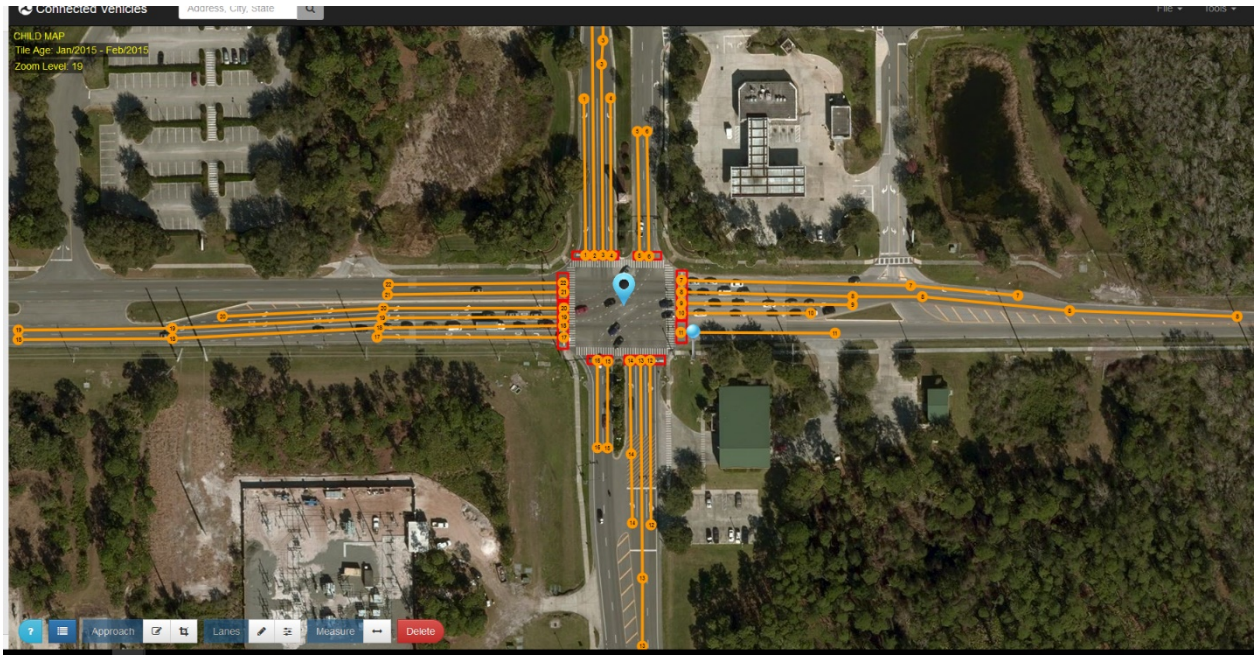


29. Repeat the process for other individual lanes of the approach. For dedicated right and left turn lanes, span the entirety of the lanes until completed as shown (Rotated 90° CW).

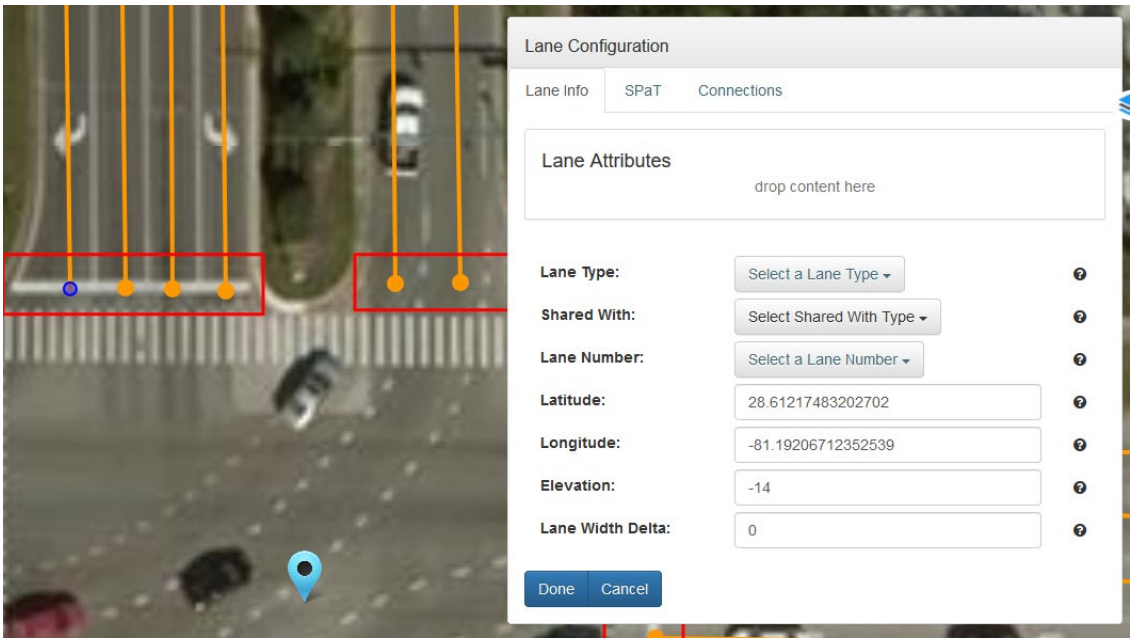


30. To draw the Egress lane, click on the **Draw Lanes** button, click on the center of the Egress lane within the approach box, draw the egress lane to at least the same length as the left turn lane, and double click on the **endpoint** to terminate the lane; repeat this process for all Egress lanes in the approach box until completed as shown (Rotated 90° CW).

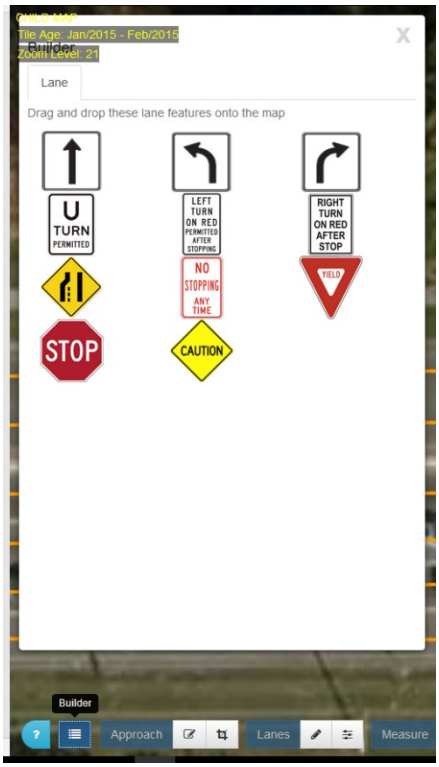
31. Repeat the process of drawing lanes until all lanes of the intersection are completely drawn as shown.



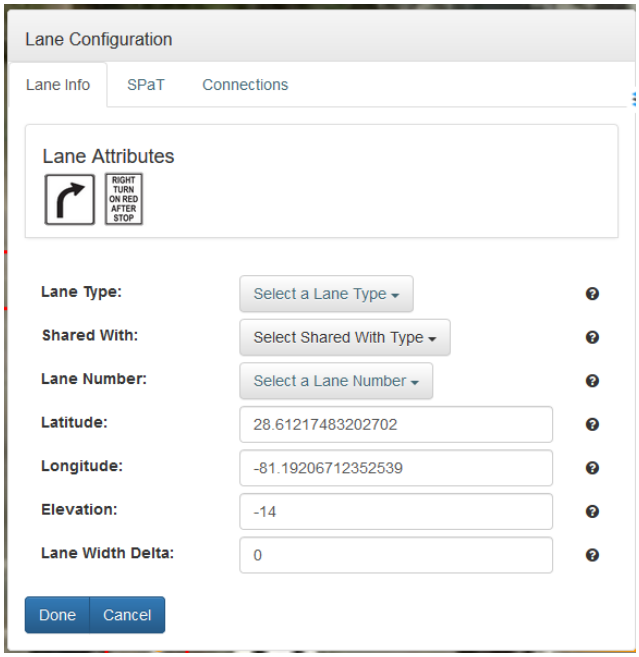
32. Click on the **starting point** of the left-most lane in the northern Ingress approach box to open the Lane Configuration menu.



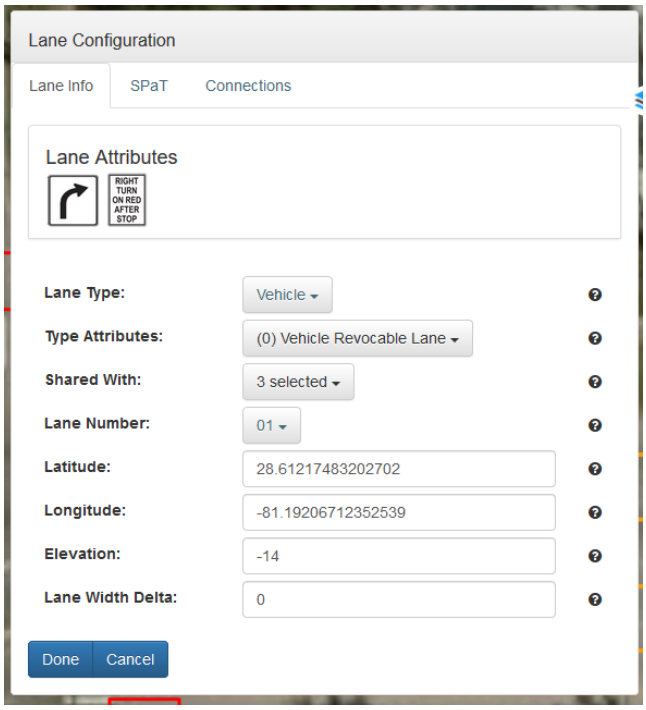
33. Left click on the **Builder Menu** to open the **Lane** tab.



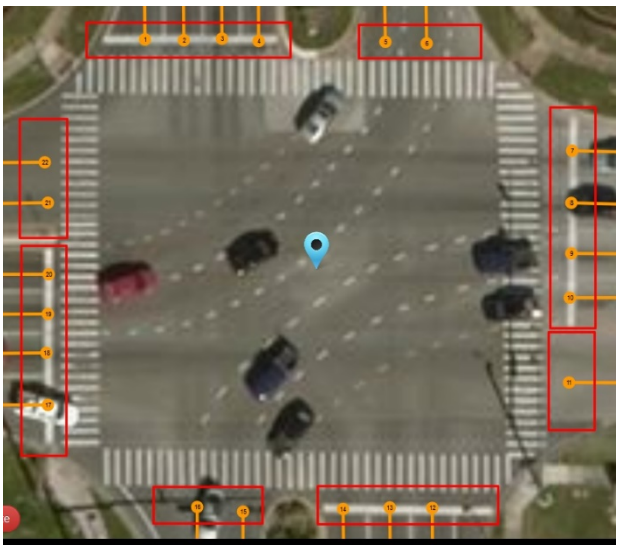
34. Drag and drop the **allowed maneuvers** from the appropriate icons in the Lane tab to the Lane Attributes box in the Lane Configuration menu; to determine the allowed maneuvers, refer to the intersection diagram, lane markings, and signage.



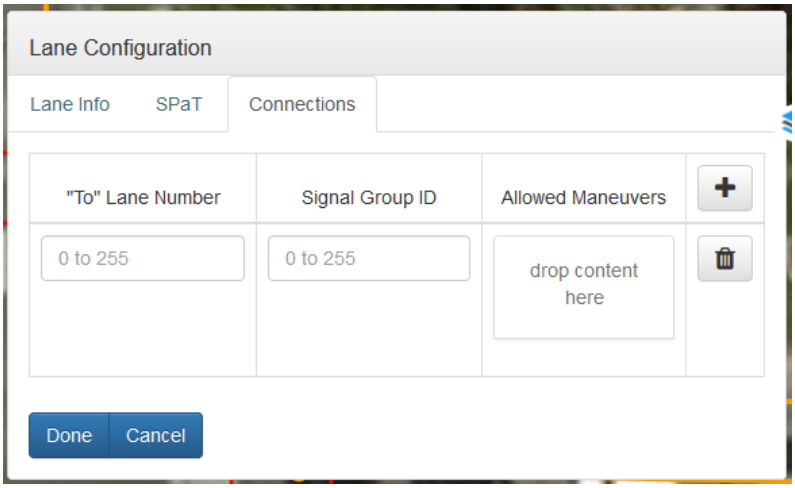
35. In the Lane Type field, select **Vehicle**; in the Type Attributes field, select **(0) Vehicle Revocable Lane**; in the Shared With field, select **(3) Individual Motorized (4) Bus (5) Taxi**; and, in the Lane Number, select the lowest available lane number starting with **01**; when done, click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



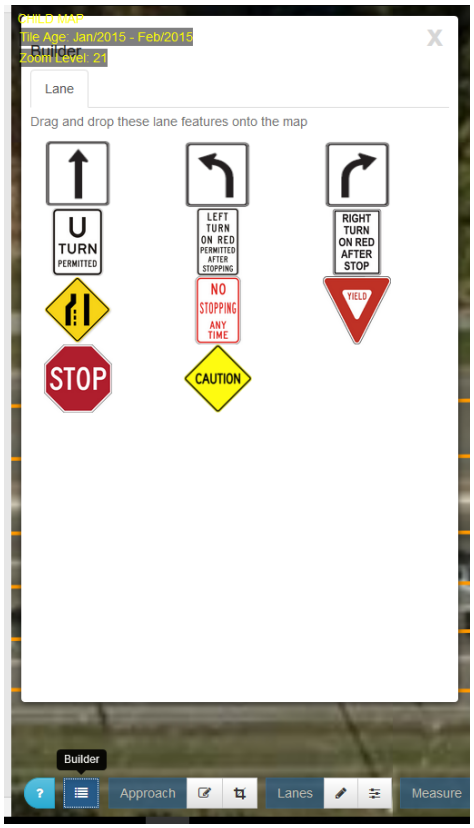
36. Repeat this process for all remaining lanes in the intersection. When you are done, the starting node in each lane will be identified with its number as shown.



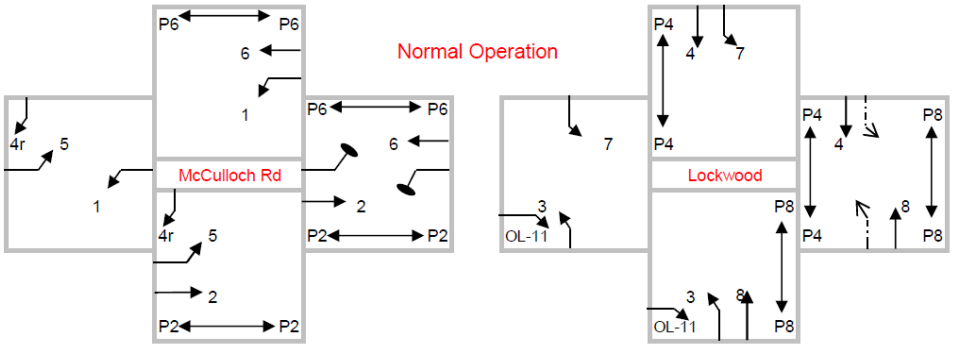
37. Click on **node** designated **1** to open the Lane Configuration menu and click the **Connections** tab.



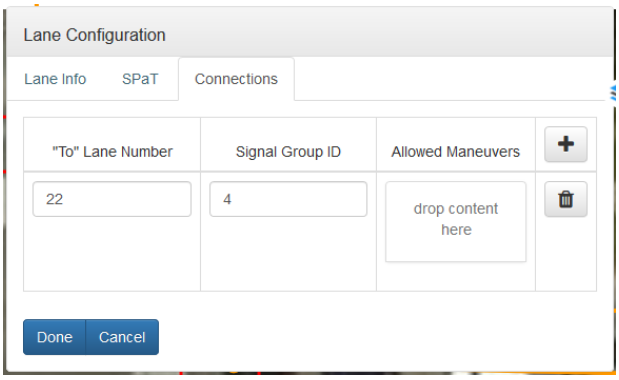
38. Left click on the **Builder Menu** to open the **Lane** tab.



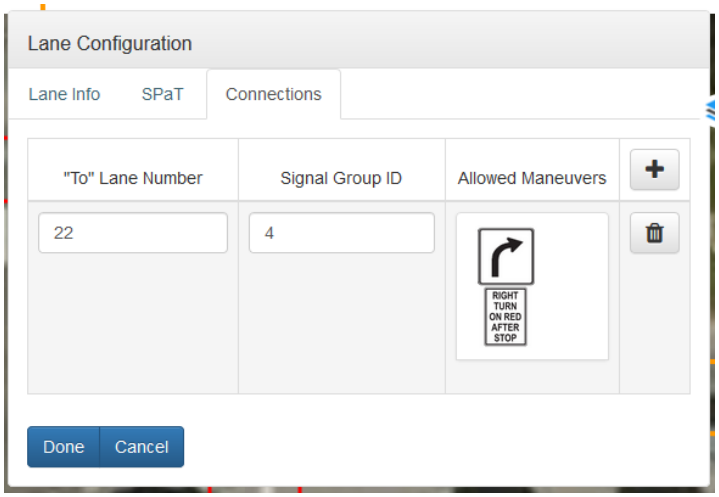
39. You should have a diagram of the intersection provided by a traffic engineer. Open the file of the intersection diagram. An example diagram is shown below.



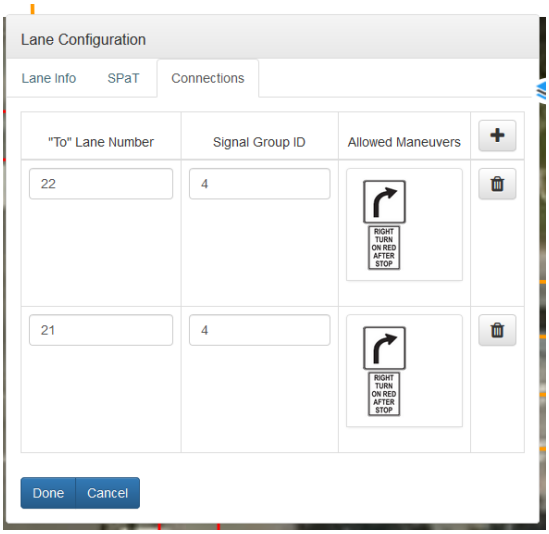
40. Using the intersection diagram as a reference, enter the destination lane number in the **"To" Lane Number** field and the phase number associated with the movement in the **Signal Group ID** field.



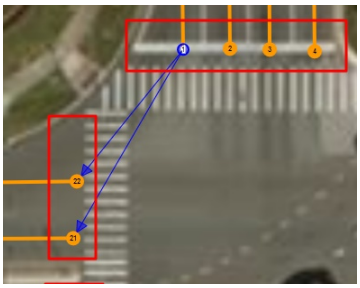
41. Drag and drop the **allowed maneuvers** for the given phase and lane number from the Lane tab of the Builder menu to the **Allowed Maneuvers** Box in the **Connections** tab window.



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

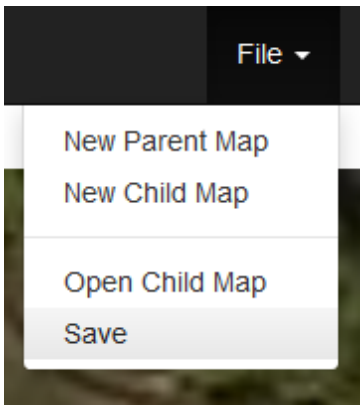


43. Click again on **node 1**. Blue arrows will be visible to show established connections.

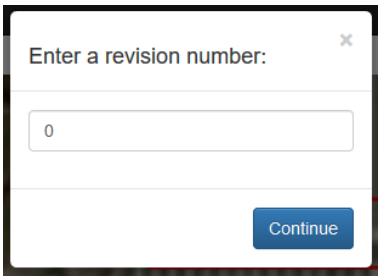


44. Repeat this process for every **Ingress** lane in the intersection.
Note: Egress lanes do not need connections.

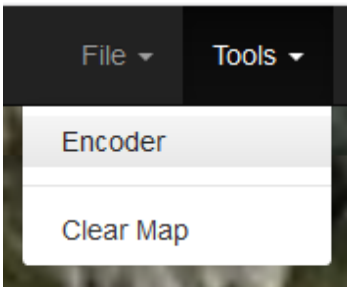
45. Click **File > Save** to save the Child Map.



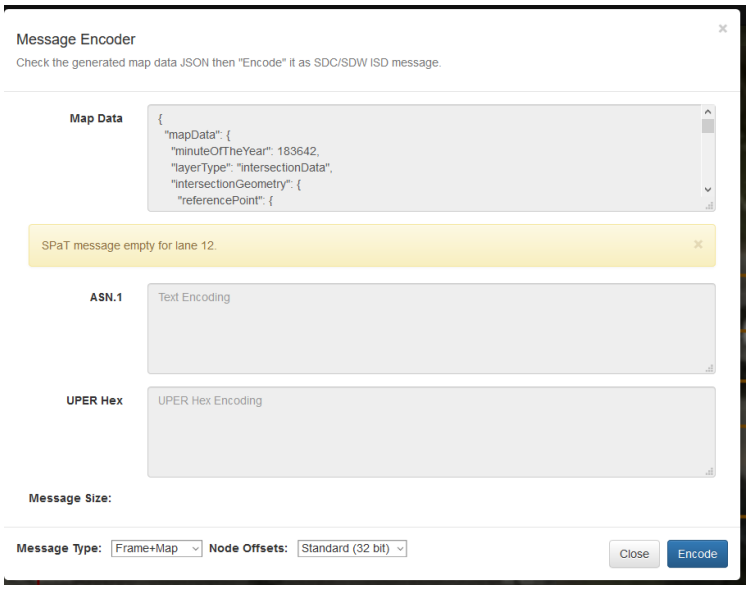
46. When prompted, enter the revision number starting with **0**. Then click **Continue**.
    Note: Do NOT press **Enter**—make sure you click **Continue**.



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.

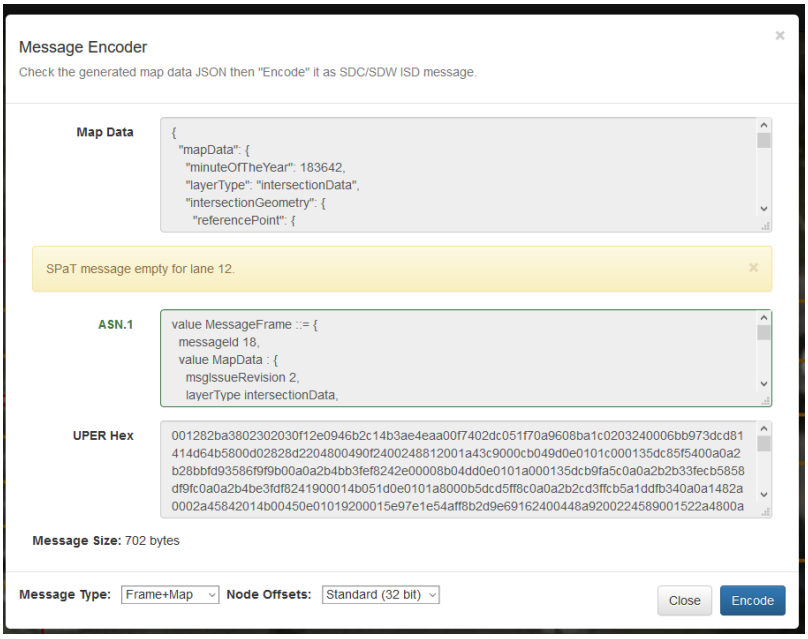


49. For Message Type, select Frame+Map and, for Node Offsets, select Standard (32 bit)



.

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.



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.

10. Appendix – How to Change the Default Login Password

How to Change the Default Login

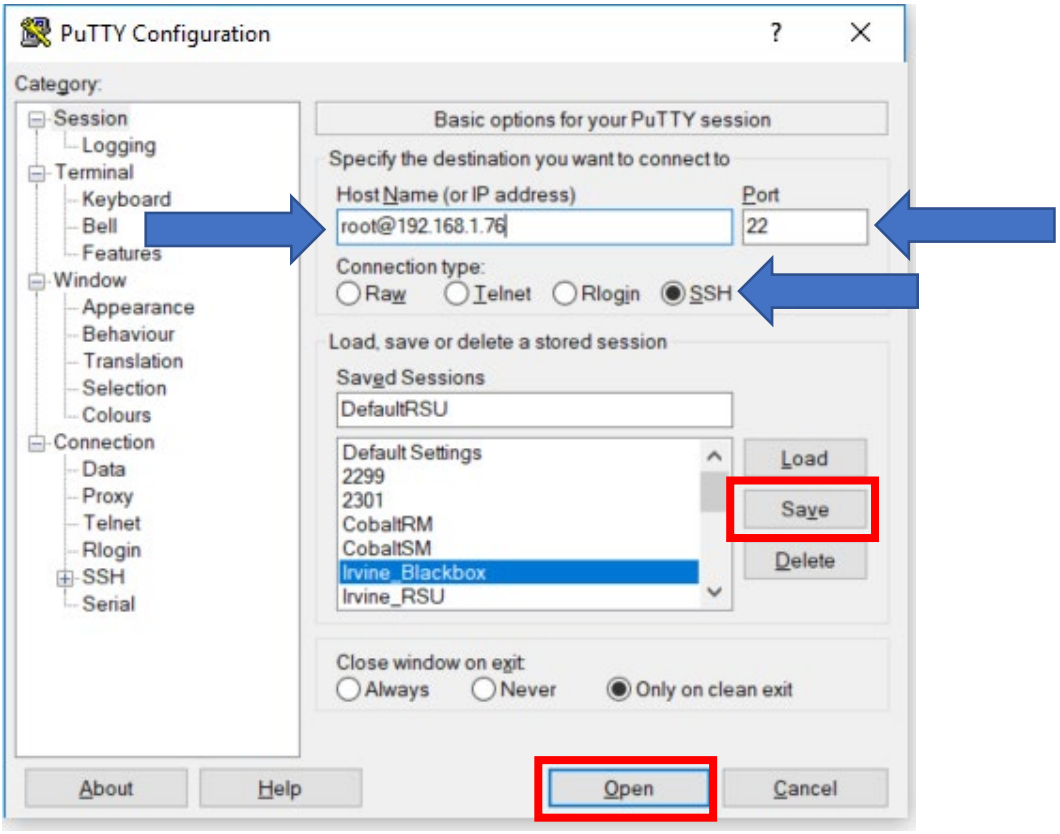
The BlueTOAD Spectra RSU firmware enables “root” password protection. You are not able to log into the RSU without the password. The default password may be changed by an end user. However, be advised that once you change the default password, you may not be able to log back into the unit if you lose the password.

Use an SSH Client terminal program for Microsoft Windows to log into the BlueTOAD Spectra RSU and change its default login Password. PuTTY is a software program that uses the Secure Shell protocol to connect to a remote computer, in this case the BlueTOAD Spectra RSU.

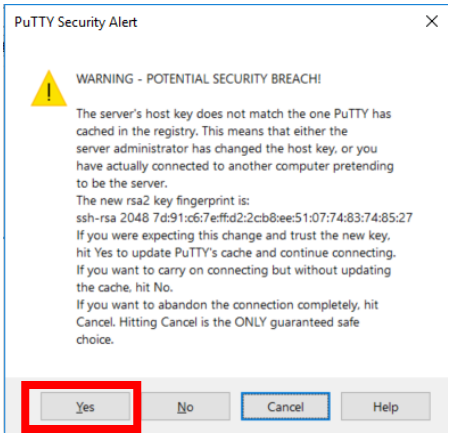
The RSU will fail the login attempt if you enter the password incorrectly three consecutive times. If a user attempts to use the password utility to create a new user, be advised that the new user may only be able to log into the RSU but may not have other “root” privileges available. Therefore, it is not recommended that a new username is created.

Changing the “Root” User Password

1. Open PuTTY to start an SSH session into the RSU. Set the Host Name to **root@192.168.1.76 (or use the assigned IP Address for that specific RSU)**, Port to **22**, Connection Type to **SSH**, and save the session as “**DefaultRSU**” (or name to a “location-based” name, which can be accessed later) for future use.

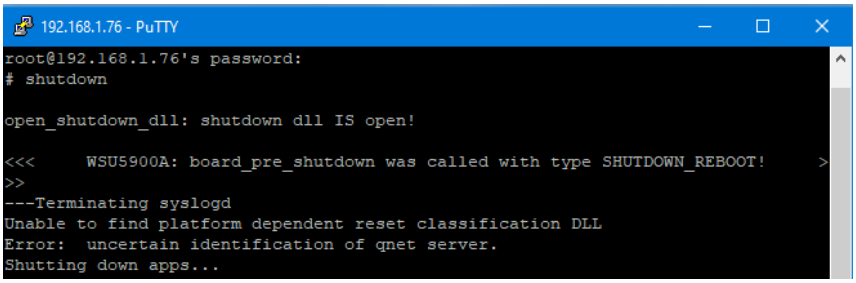


2. If prompted to accept the RSA key of the RSU click **Yes**.
3. Login with current default credentials



   a. Username: **root**

   b. Password: **6efre#ESpe**



4. Enter following command to change password.

   a. Passwd

5. Enter a **New Password (ex: temp123)**. You will be prompted to confirm the Password change.
6. Confirm the New Password (ex: temp123).
7. Once the BASH shell is available, use the command **"shutdown"** to **Restart** and **Apply** the configuration changes to the RSU.

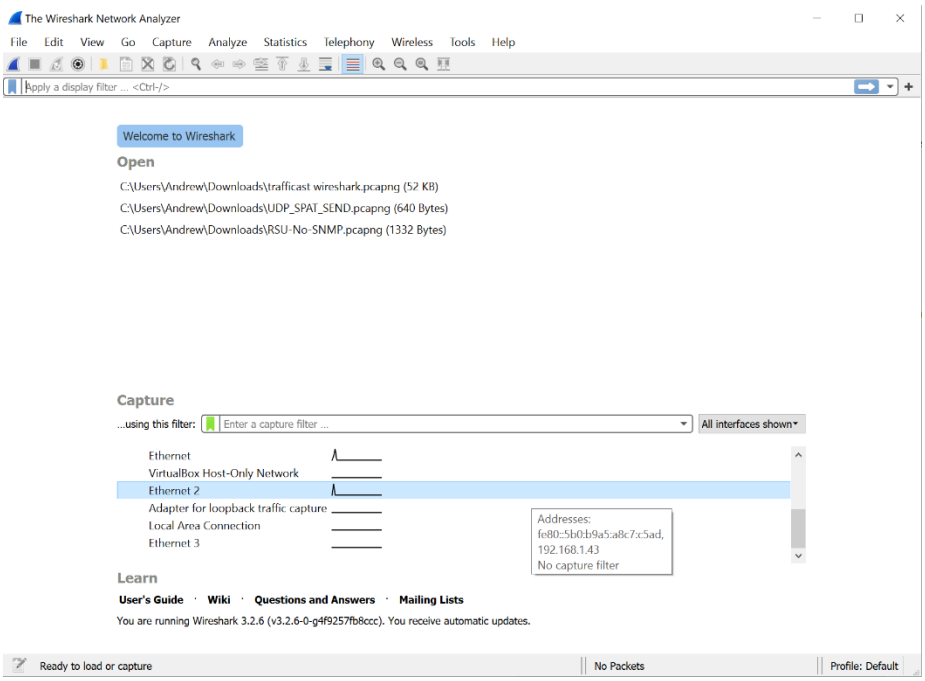
Note: If the Password has been changed from the factory default, use the new Password to access the login website.
Please save the New Password, retrieving a forgotten Password will involve a factory reset of the device by return to the Iteris support facilities.

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

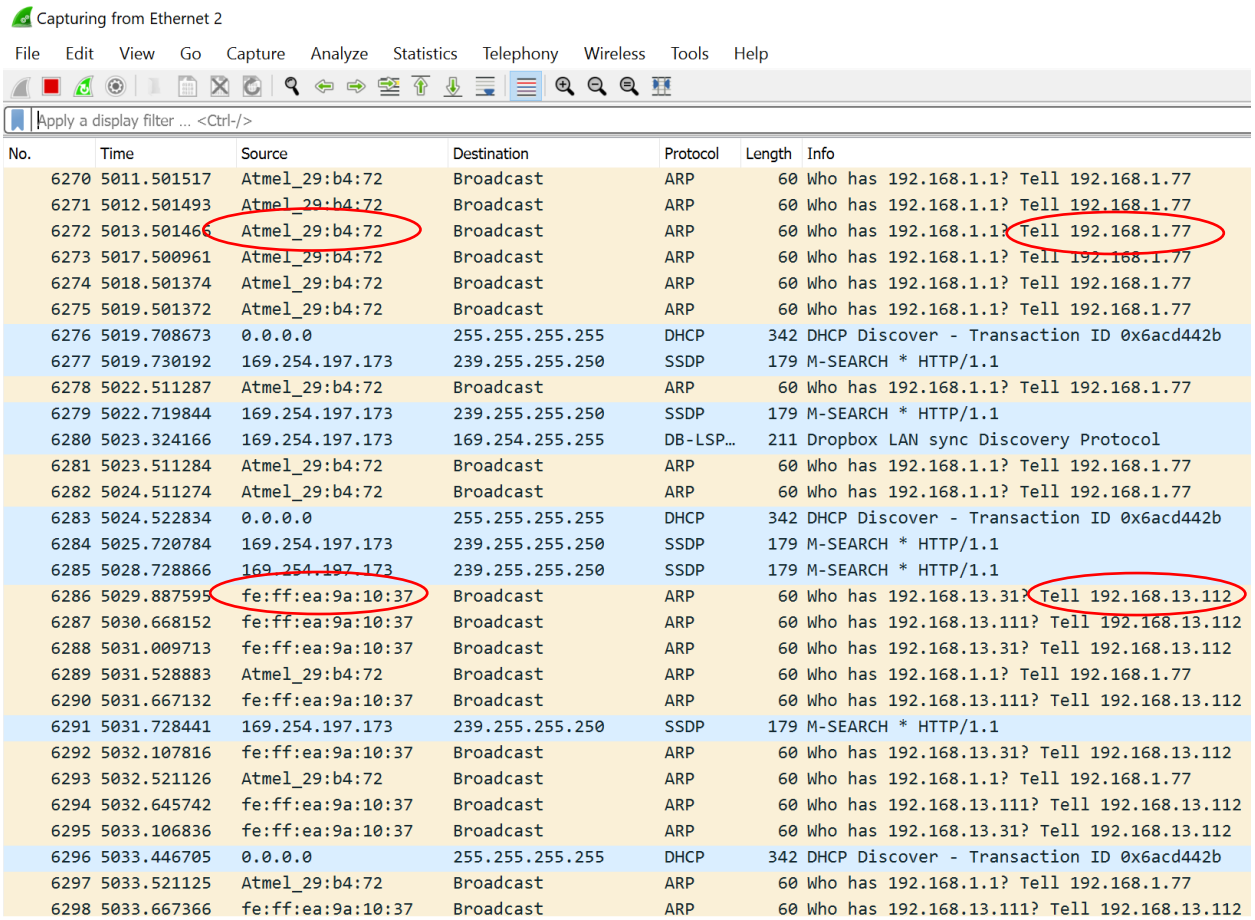
Use the Wireshark utility to capture packet data in detail to ascertain the IP Addresses used by the BlueTOAD Spectra RSU. Wireshark is a free opensource application that serves as a network packet analyzer, which displays packets with detailed protocol information. The Wireshark utility can be obtained 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.
5. 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.



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.

12. Appendix – Basic Safety Message (BSM) REST API

BSM API Overview

Iteris uses a REST or RESTful API design (Representational State Transfer) intended to enable HTTP applications used in combination with Iteris' BlueARGUS travel time system's Web API. The Iteris REST API architecture uses the JSON format to present vehicle Basic Safety Message data to a BlueARGUS User's specified client.

The Iteris API enables a client to "Pull" data from the BlueARGUS "Cloud" reporting system to an authorized agency stakeholder software system (or internal database). The following outlines parameters for implementing a RESTful API defining specific URL endpoints.

Iteris REST Service Endpoints

The Iteris REST Service Endpoint is an endpoint which services a set of REST resources available for authorized users. As outlined below, all the resources are handled by one server, utilizing a base URL for the REST Service Endpoint. To retrieve BSM data for a DSRC/C-V2X location/device there are three different endpoints which can be used. Each endpoint returns a different type of BSM data stream:

1. The GET location endpoint returns a list of all the BSM data currently at that location. This is the "real-time" endpoint, although note that the data might be delayed by up to one minute.
2. The POST location BSM Data endpoint returns a paginated list (see section, "How to Use Pagination" below) of all the BSM data seen for a specific location.
3. The POST BSM Report endpoint returns two types of reports summarizing the BSM data for a location: Speed Reports and BSM and Vehicle Count reports.

Authentication and API Basics

To use the API, you should authenticate your request by including your API key as a bearer token value:

- Authorization: Bearer API_KEY_HERE
- Be sure to use application/json content type as detailed below…
    - Content-Type: application/json
- To obtain an API token, please email bluetoad-help@trafficcast.com to receive exclusive API token

Fetch a List of All Locations

The first step in getting BSM data is to retrieve a list of all the Locations/Devices associated with the Agency/User (Group) account. This list will include the **"nid"** values for each location. The **"nid"** attribute for a location is the primary identifier which is used by the Iteris API to track a specific location. This value is needed for the other subsequent BSM-related API calls.

To retrieve a list of all Iteris RSU locations, send an authenticated GET request to:
https://blueargus.trafficcast.com/api/locations

This will return a list of all the available Iteris RSU locations. As noted, the **"nid"** attribute for each location is needed for the subsequent API endpoints listed below.

Retrieve Current BSM Data for a Location

The real-time BSM data for a single Iteris RSU location can be retrieved via a GET request to the URL **https://blueargus.trafficcast.com/api/locations/${location.nid}** where "location.nid" represents the "nid" attribute for the desired location (as determined by the prior endpoint).

The data which is returned from this endpoint will contain BSM data in the following location: "dsrcLocation.bsmData". The "bsmData" array will contain a list of individual BSM datapoints. Each data point represents a single vehicle that is currently within range of the Iteris RSU location. The data is limited to one data point per vehicle. As a result, this data is not a true real-time feed of all the BSM messages. Instead it should be treated as a summary of all the vehicles currently present within range of a specific location.

The data composition is as follows:

'id' => This is an internal ID used by our system,
'bsm_id' => The BSM ID provided by the vehicle,
'dsrc_location_db_key' => Another internal ID used by our system,
'created_at' => When the vehicle first appeared at the location,
'updated_at' => When the vehicle was last observed at the location,
'lat' => Latitude of the vehicle,
'lon' => Longitude of the vehicle,
'speed_in_mps' => Speed of the vehicle in meters per second,
'speed_per_unit' => Speed of the vehicle in either mph or kph,
'speed_unit' => Either mph or kph (as determined by the group configuration),
'json' => Raw JSON BSM data of the most recent message,
'vehicle_length' => Vehicle length in centimeters,
'vehicle_width' => Vehicle width in centimeters,

Retrieve Archived BSM Data for a Location

The historical BSM data for a single Iteris RSU location can be retrieved via a POST request to the URL **https://blueargus.trafficcast.com/api/locations/${locationn.nid}/bsm?page=1** where "location.nid" represents the "nid" attribute for the desired location (as determined by the prior endpoint).

The following two parameters are supported by this endpoint and should be passed in the POST data:

- **startDate** -- This should be an ISO 8601 formatted timestamp. This denotes the start date for which you want to fetch BSM data for this location.
- **endDate** -- This should be an ISO 8601 formatted timestamp. This denotes the end date for which you want to fetch BSM data for this location.

The data which is returned from this endpoint will contain BSM data in the "bsmData" array. Each data point in this array, which is sorted by date, represents a single BSM message for a vehicle. However, the data is limited to one data point per vehicle per X seconds, where X is determined by a dynamic formula. In other words, this endpoint cannot be used to retrieve EVERY BSM message sent by a vehicle, since this behavior could result in thousands of messages needing to be saved per vehicle. Instead the messages are throttled/deduplicated and only a sampling of them is saved and available for retrieval.

The data composition is as follows:

- 'id' => This is an internal ID used by our system that is useful for de-duplication,
- 'bsm_id' => The BSM ID provided by the vehicle,
- 'dsrc_location_db_key' => Another internal ID used by our system,
- 'detected_at' => When the BSM message was detected,
- 'lat' => Latitude of the vehicle,
- 'lon' => Longitude of the vehicle,
- 'speed_in_mps' => Speed of the vehicle in meters per second,
- 'speed_per_unit' => Speed of the vehicle in either mph or kph,
- 'speed_unit' => Either mph or kph (as determined by the group configuration),
- 'json' => Raw JSON BSM data of the most recent message,
- 'vehicle_length' => Vehicle length in centimeters,
- 'vehicle_width' => Vehicle width in centimeters,

How to Use Pagination

Here are a few notes about how pagination works with this endpoint:

- By incrementing the "page=1" GET parameter on the endpoint, the end user can fetch additional result sets
- All pagination metadata around how many individual BSM messages exist for the passed **startDate** and **endDate** and how many pages this is (including how many results per page) can be viewed within the "metadata.pagination" attribute in each response.
- New data from recently observed BSM messages could be added to the database while a multi-page response is being retrieved. This might result in the paginated data shifting and changing as you are retrieving it. The specific effect of this behavior is that individual BSM data might be returned twice (once at the end of a page and then again at the beginning of the next page). There are two approaches to dealing with this phenomenom:
    - Post-process the data after it has been fully retrieved to remove all the duplicates. This can be done with the "bsmData.id" field. A given "id" should only ever appear once in the data set.
    - Set the **startDate** to a value that is at least one hour AFTER the current timestamp. This should ensure no new data is coming in and altering the page counts

BSM Report Data

BSM reporting data for a single DSRC/C-V2X location, or all locations combined, can be retrieved via a POST request to the URL **https://blueargus.trafficcast.com/api/report/bsm.** The following POST parameters are supported and should be supplied:

- 'reportType' => Either 'location_bsm' or 'location_speed',
- 'timeInterval' => Either 1, 5, 15, 30 or 60,
- 'nid' => The "nid" of the desired location,
- 'startDate' => This should be an ISO 8601 formatted timestamp. This denotes the start date of the reporting data,
- 'endDate' => This should be an ISO 8601 formatted timestamp. This denotes the end date of the reporting data,
- The "timeInterval" value determines the windowing which will be applied to the data, specifically whether the timestamps in the returned data increment by 1, 5, 15, 30 or 60 minutes.

The "reportType" value is used to specify what type of report to run:

- **location_bsm** indicates a Vehicle and BSM Data report. This describes how many BSM messages and how many unique vehicles were detected in the given period
- **location_speed** indicates a Speed Report. This tracks the average, median and maximum speeds, as determined by the observed BSM Data

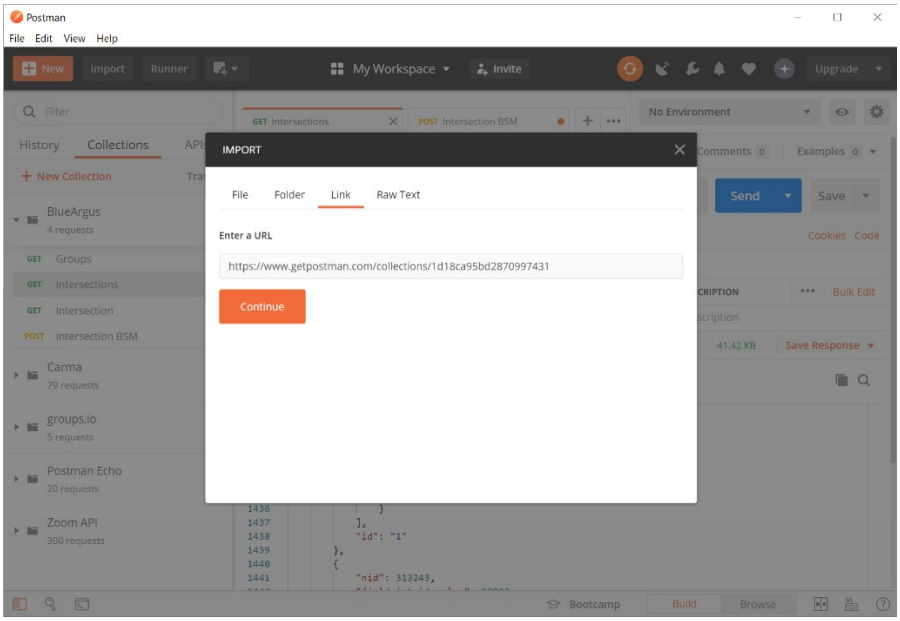
The format of the returned data will be determined by which type of report is being run. Specifically, the data formats are as follows:

- **location_bsm** report returns a list of arrays where each value in the array is defined as follows (as determined by array index)
  - 0: timestamp of the reporting window (in UTC)
  - 1: count of all BSM messages observed in that window
  - 2: count of all unique vehicles observed in that window
- **location_speed** report returns a list of arrays where each value in the array is defined as follows (as determined by array index)
  - 0: timestamp of the reporting window (in UTC)
  - 1: average speed for all vehicles in that window
  - 2: median speed for all vehicles in that window
  - 3: maximum observed speed for all vehicles in that window

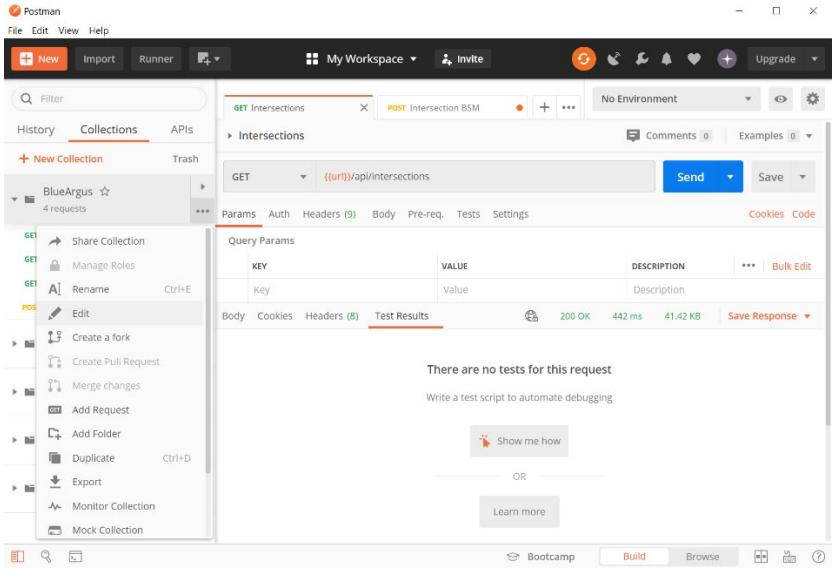
Note: the values returned for the **location_speed** report will be in either mph or kph, as determined by the setting defined for the Agency's Group which is linked to the DSRC/C-V2X location being reported on.

Using Postman User Interface for Interacting with Iteris API

We recommend using Postman UI for REST API testing and evaluation. We have published a Postman collection that can be imported using this URL:
https://www.getpostman.com/collections/1d18ca95bd2870997431



1. Once you have imported the collection, you need to add your authorization token. To edit the collection, click the **"…"** button on the BlueArgus collection and then select **"Edit"**.

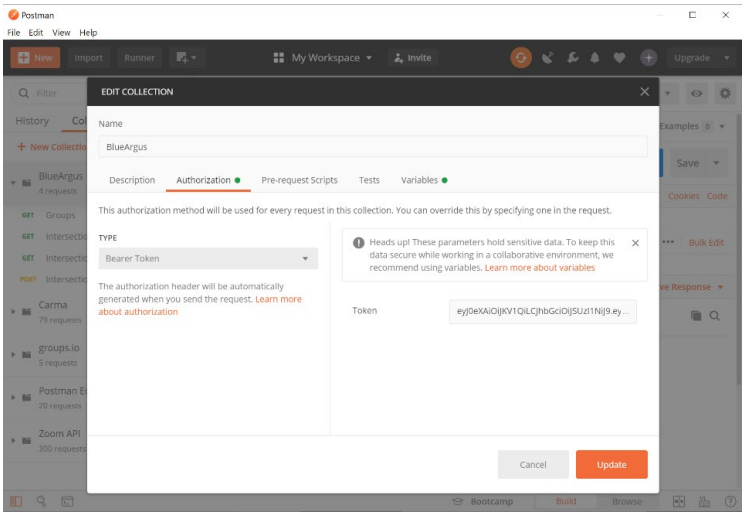


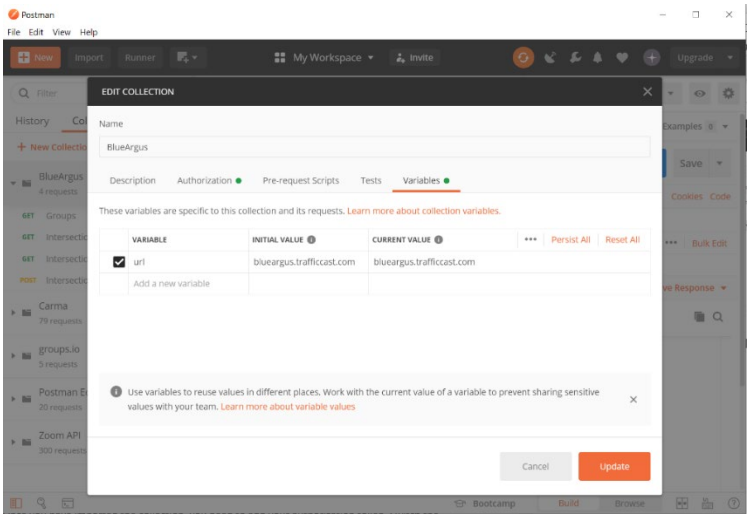
2. Next, switch the Authorization Type from **None** to "**Bearer Token**" and paste in the token you have received from Iteris.

3. You will also need to add a **"url"** variable to the collection and set the value to **"blueargus.trafficcast.com"**

–

4. You can now make API calls and see the input and response data via Postman.





13. Appendix – BlueTOAD Spectra RSU System Requirements and Validation Process

System Evaluation Overview

This Evaluation Procedure is to address the requirement for minimum required evaluation and operations tests for the Iteris BlueTOAD Spectra RSU.

It is assumed that the BlueTOAD Spectra RSU under test has already gone through factory acceptance inspections and demonstrated full compliance with all project requirements and works “out of the box”, by visual inspection, setup and operation "on the bench", functional testing of the component including manufacturer’s recommended startup diagnostics and testing prior to any field installation of equipment or material.

This Evaluation Procedure will focus on SPaT, MAP, TIM and BSM Data Broadcasting verification which were not covered in initial product configuration and inspections. This Evaluation Procedure will confirm that the BlueTOAD Spectra RSU complies with USDOT Dedicated Short Range Communications (DSRC) standards, based on Society of Automotive Engineers SAE J2735 March 2016 standards-based message exchange between Roadside Units (RSU) and vehicle Onboard Units (OBU).

For your convenience, we added an Evaluation Sign-Off Checklist form to this document for use as a guide for the evaluation procedure – see “Evaluation Sign-Off Checklist” section of this document.

Supporting Equipment

- Windows PC and Ethernet Cables
- BlueTOAD Spectra RSU Configuration Utility (Microsoft Windows 10 App)
- WinSCP or equivalent File Transfer Application
- PuTTY or equivalent SSH Client
- Iteris BlueTOAD Spectra RSU
- Traffic Controller with Power Cable or Similar ATC Controller

  Iteris recommends any of the following Traffic Controllers as they are compatible with BlueTOAD Spectra RSU:

  - Econolite
  - Intelight
  - McCain
  - Siemens
  - Trafficware
- 7-Zip Archiving Utility
- Advanced IP Scanner (Optional)
- PoE Injector + Power Supply
- Shielded CAT-5 or CAT-6 Cable
- Mounting Bracket + Fasteners
- Cable Band
- Access to BlueARGUS Software

Visual Inspection

Verifying the BlueTOAD Spectra RSU is in good shape and not physically damaged.

Check for damage to the:

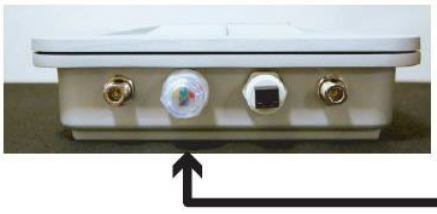
- Antenna
- Ports
- LEDS
- Enclosure

BlueTOAD Spectra RSU Power Up

Before the RSU installation, confirm the following:

1. The network settings (for example, IP address, gateway, subnet mask, and DNS) are correctly set and that all ports (123, 8010, 10001) are open and set for outbound data traffic. Confirm all necessary inbound/outbound network ports have been set up.
    a. IP Configuration Requirements
        i. BlueTOAD Module assigned: IP Address, Subnet Mask and Gateway
        ii. DSRC/C-V2X Module assigned: IP Address, Subnet Mask and Gateway
        iii. In-Cabinet Processor assigned: IP Address, Subnet Mask and Gateway
    b. Network Port Configuration:
        i. Port 10001 needs to be open to 52.39.79.127 (Connected Vehicle specific data)
        ii. Port 8010 needs to be open to btserver.trafficcast.com
        iii. Port 123 needs to be open, only if using an external NTP server.
    c. Required DNS entries for btserver.trafficcast.com:
        i. 18.220.189.165
        ii. 3.18.180.164
        iii. 3.18.166.19
2. The IP addresses assigned to the Traffic Controller and to the RSU should be known. (**Note**: If there is a Processor (optional), it also has an IP address.).
3. Power ON (Connect Ethernet cable from RSU to PoE Injector) the RSU and confirm all LEDs are normal after the unit initializes:

Iteris RSU (Bottom View)



LED Indicators
Green – Device operational
Amber – Device ON
Red - Fault

How to Set Up the Traffic Controller

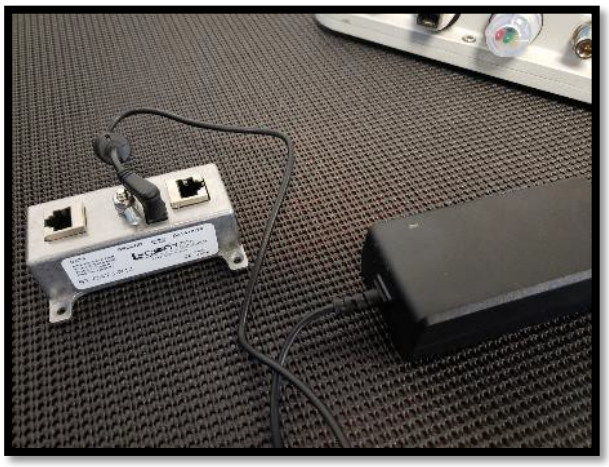
This example uses an Econolite **traffic controller**, model Cobalt Advanced Traffic Controller (ATC). However, you can use ATC controllers (preferred) from other manufacturers that have Ethernet and IP interfaces. Refer to the table on Page 1-2 for Compatible Traffic Controllers. Also, you can consult Iteris Support for models of traffic controllers supported; these include McCain (software Version 1.10.2.6705-2018-03-23), Siemens (software Version 3.59+), Trafficware (software Version 76.15N+) and Intelight (Maxtime CV).

1. Attach the Traffic Controller "**A**" power cable to the "**A**" connector of the controller.

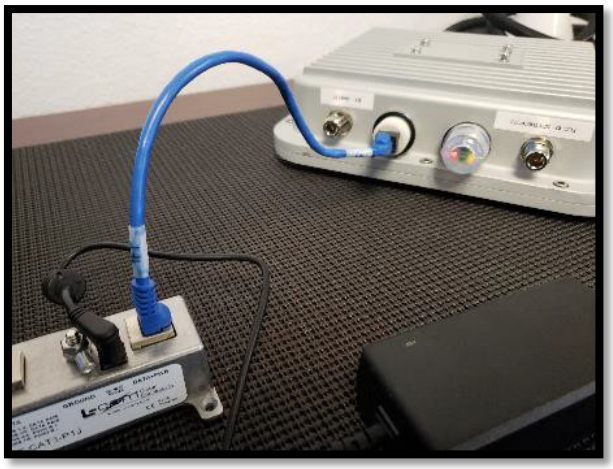
2. Plug the "A" power cable into an AC power source. The controller should power ON.
3. Using the assigned IP address of the BlueTOAD Spectra RSU, navigate to the Ethernet communications page of the controller.
4. Verify the controller IP address and Netmask. Set the Ping Server to the IP address of the RSU.

5. Plug the AC power cable of the POE injector AC adapter to an AC power source.

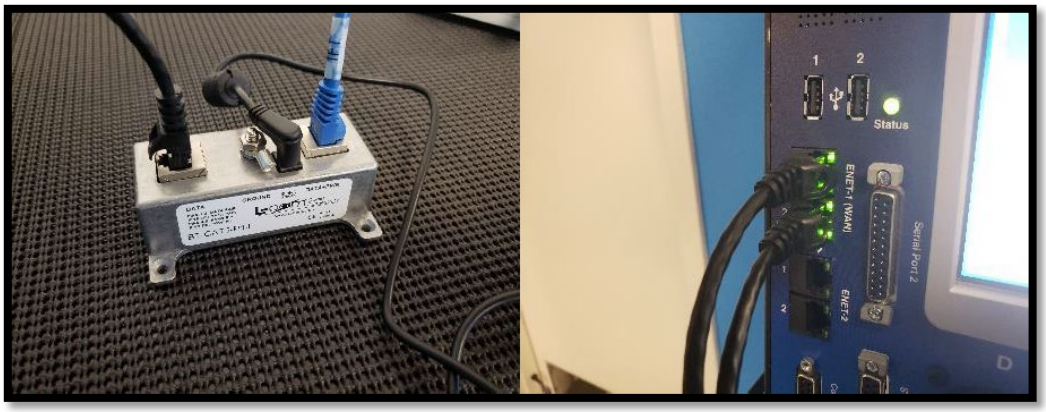
6. Plug the AC adapter output power cable into the POE injector. The AC adapter LED indicator should light up with power.



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.



–

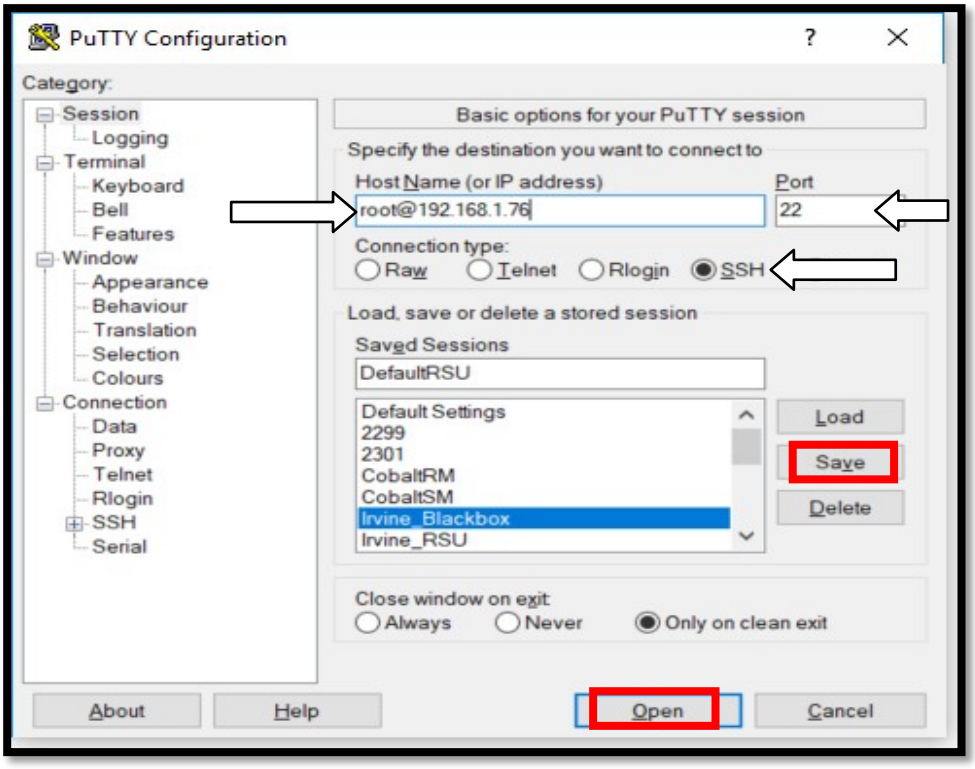
9. Connect the computer to Port 2 of ENET-1 (WAN) of the controller with an Ethernetcable.
10. Set the computer IP address to match the subnet of the RSU and controller.

System Evaluation Procedure

SPaT, MAP and BSM Data Broadcasting Verification

It is assumed that the BlueTOAD Spectra RSU under test has been installed in the field and already setup and configured. For Iteris' Recommended Network Configuration Implementation and setup procedure refer to system documentation provided by Iteris.

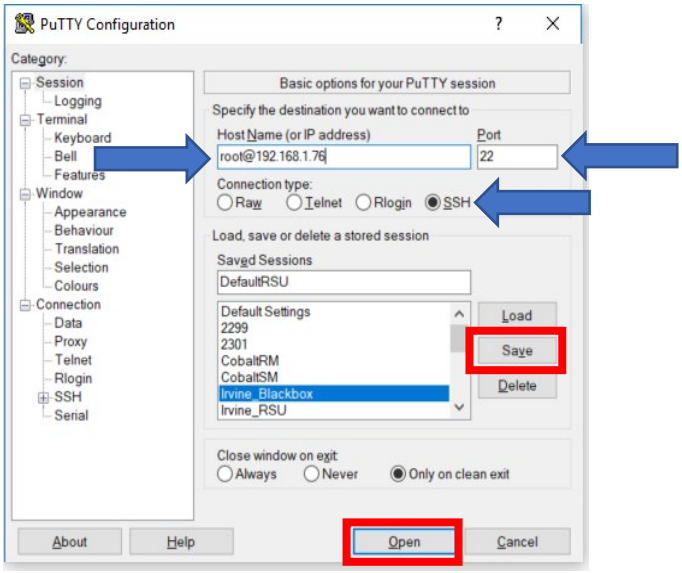
1. Open PuTTY to start an SSH session into the RSU. Set the Host Name to root@192.168.1.76, Port to 22, Connection Type to SSH, and save the session as "DefaultRSU" for future use.

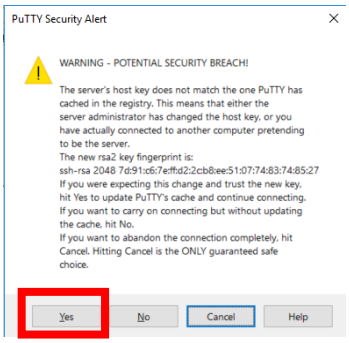


2. If prompted to accept the RSA key of the RSU click **Yes**.

How to Access RSU Using CLI Commands

6. Open PuTTY to start an SSH session into the RSU. Set the Host Name to **root@192.168.1.76**, Port to **22**, Connection Type to **SSH**, and save the session as "**DefaultRSU**" for future use.





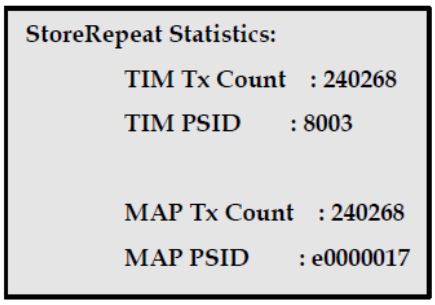
7. If prompted to accept the RSA key of the RSU click Yes.
8. When prompted, enter Default Password: **6efre#ESpe**
9. Once the BASH shell is available, you can begin retrieving RSU information.

Store and Repeat Messages

The following parameters get displayed in the Store and Repeat application status command:

/ # rsu_stats -s

Sample output as shown gets displayed. This example displays the Store and Repeat application in 'Running' state for 1 Active Message List.

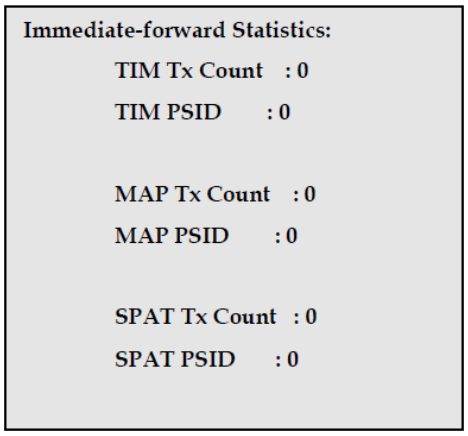


Immediate Forward Message

Execute the following commands to display the parameters and counters in the Immediate Forward status

/ # rsu_stats -i

Sample output as shown below gets displayed.

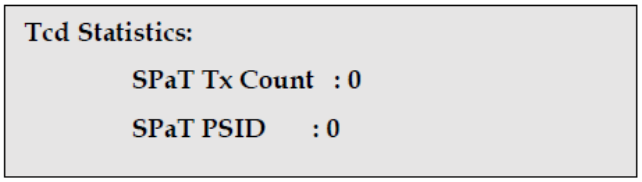


Traffic Controller Data (TCD)

Execute the following command to display the TCD app status parameters:

/ # rsu_stats -t

Sample output as shown gets displayed.



V2X Message Forward

10. Execute the following command to fetch statistics at the Network Proxy Forwarding layer

    /# savapp_us -p

    Sample output as shown is displayed.

11. Execute the following command to reset statistics at the Network Proxy Forwarding layer

    /# savapp_us -z

    Sample output:

```
CV2X Network Proxy reset successfully
```

```
NETWORK PROXY STATISTICS
**********Service 1 **********:
    Service ID              : 0x8002
    Service Direction       : TRX
    Transmit Count          : 0
    Receive Count           : 0
    Signing Failure Count   : 0
    Verification Failure Count : 0
**********Service 2 **********:
    Service ID              : 0x2
    Service Direction       : TRX
    Transmit Count          : 0
    Receive Count           : 0
    Signing Failure Count   : 0
    Verification Failure Count : 0
**********Service 3 **********:
    Service ID              : 0x8003
    Service Direction       : TRX
    Transmit Count          : 240362
    Receive Count           : 0
    Signing Failure Count   : 0
    Verification Failure Count : 0
**********Service 4 **********:
    Service ID              : 0x4
    Service Direction       : TRX
    Transmit Count          : 0
    Receive Count           : 0
    Signing Failure Count   : 0
    Verification Failure Count : 0
**********Service 5 **********:
    Service ID              : 0xe0000017
    Service Direction       : TRX
```

How to Use OBU for Connected Vehicle Message Verification Instructions

Objective

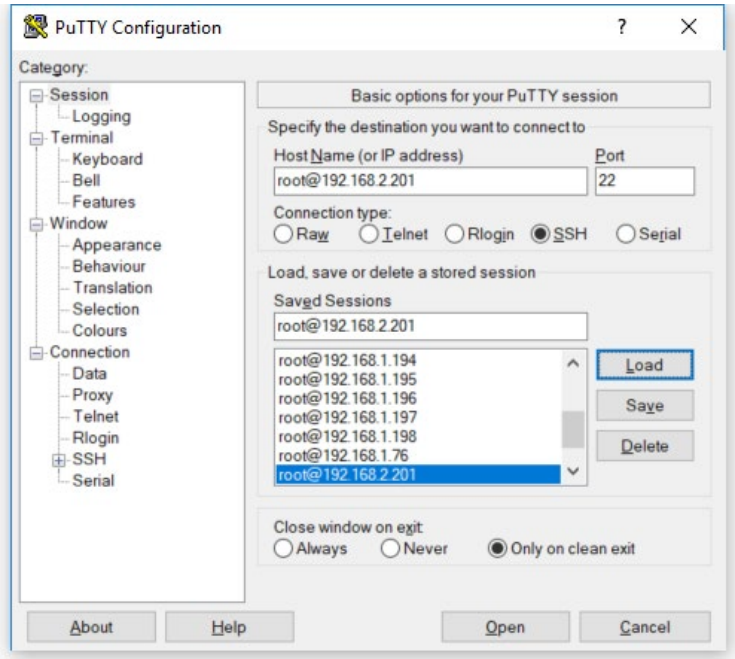
This procedure outlines the steps taken to capture WSMs received by the Onboard Unit (OBU) for packet analysis. J2735 messages are encoded using unaligned packed encoding (UPER) rules when transmitted from the roadside unit based on the 2016 standard's requirements. Due to this encoding scheme, any messages received must be decoded using the USDOT Connected Vehicles Tools Message Validator utility. This procedure assumes user familiarity with the OBU and Roadside Unit (RSU) as well as the WAVE short message protocol (WSMP).

Material Requirements

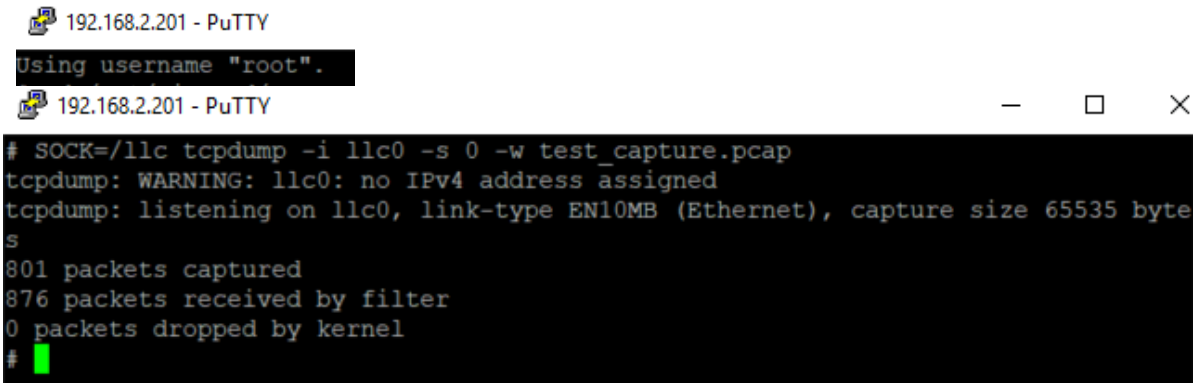
1. Windows laptop with PuTTY, WinSCP, Wireshark and web browser (Chrome or Firefox)
2. ITERIS On Board Unit (OBU)
3. Preconfigured Iteris Roadside Unit (RSU)

Message Capture and Validation

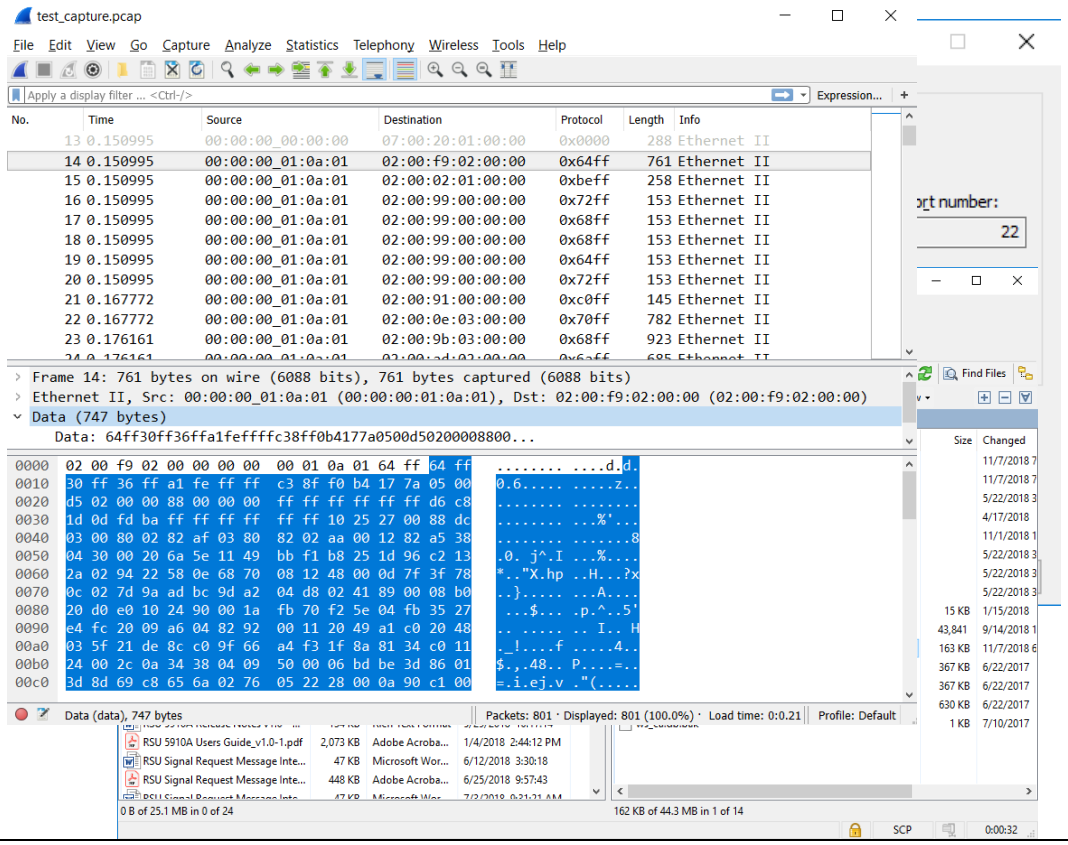
1. Power up and connect the RSU.
2. Power up and connect the OBU.
3. Connect the laptop to the OBU Wi-Fi network, denoted with the **#OBU** SSID.
4. Open PuTTY and connect to the OBU at the default OBU IP address **192.168.2.201 (or Default)**.



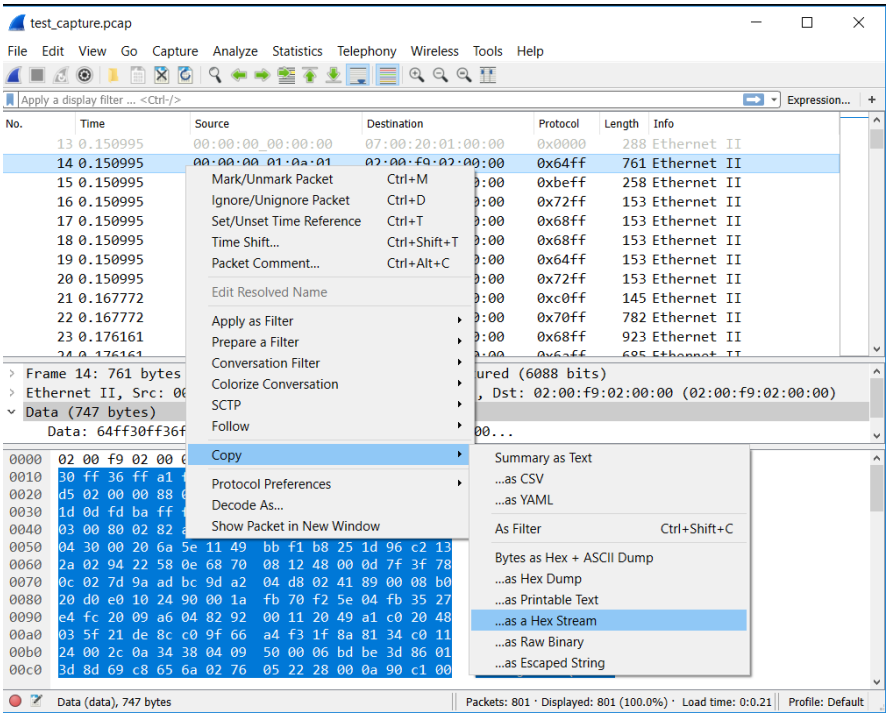
5. Change the working directory to that of the MicroSD card with "**cd /mnt/microsd/**".



6. Enter the following command to start the packet capture "**SOCK=/llc tcpdump -i llc0 -s 0 -w filename.pcap**" (note, earlier OBU software builds use "llc0" instead of "cw-llc00"), replacing "filename" with any preferred name. Press **Ctrl-C** to stop capturing data when finished.
7. Open WinSCP and connect to the OBU.
8. Navigate to the MicroSD card's directory in WinSCP.
9. **Left click** and drag the PCAP file with captured data onto the local directory.
10. Open Wireshark and open the PCAP file.
11. Search through the PCAP and select a packet to be decoded.

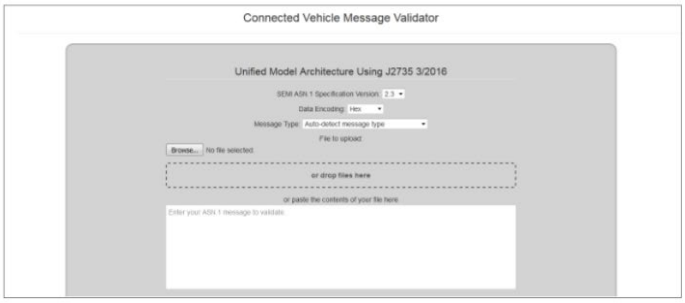


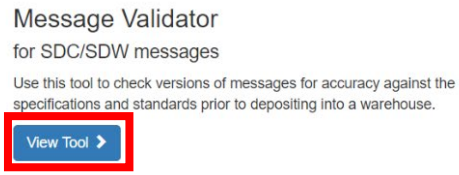
12. **Right-click** and select **Copy …As a Hex Stream** to copy the packet hex data.



13. Open the USDOT Connected Vehicles Tools website: https://webapp.connectedvcs.com/

14. Click on **View Tool** to open the Message Validator.

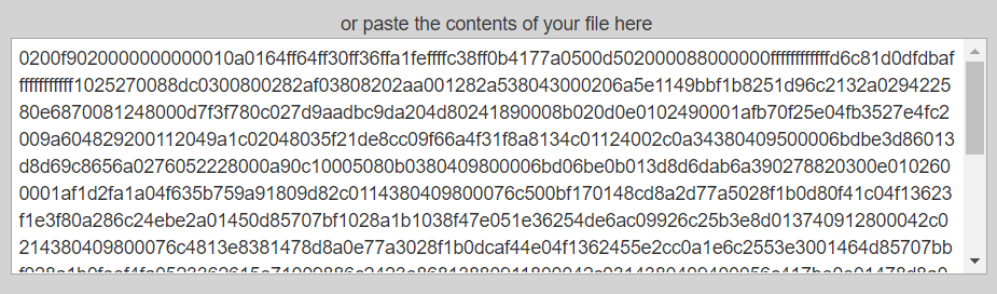




15. Set the Message Type to **Message Frame**.

16. Paste the copied hex data from Wireshark onto the blank entry field.

You typically only need a few minutes' worth of capture data to find everything provided you're



recording within range of the RSU from your OBU. There is a recognizable pattern for finding the legitimate data because the ones you want seem to always have the same pattern. You need to find the following byte patterns in the data:

SPAT: 00 13

MAP: 00 12

TIM: 00 1f

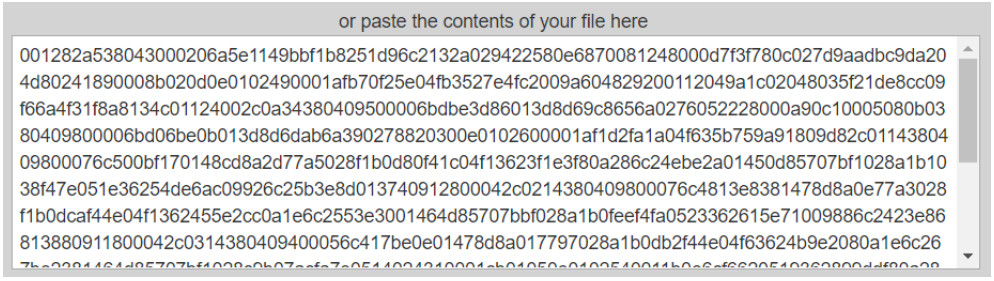
BSM: 00 14

To find these specific patterns from within the pcap you created, do a Find <ctrl-f>, set the display filter for "Hex value" and click on "Find" the exact pattern you want and that's the message you're looking for. **NOTE: all above have space between the 1st and 2nd couplets.**

When you copy the hex data for translation you need to delete everything in the packet before the pattern (without spaces between the couplets) begins. That means in the hex string delete everything else (header information), but keep (copy) only what is highlighted in Red:

0200990000000000010a019cff96ff30ff36ff55feffffa525e729a889050075000000880000000ffffffffffff9a09d7494549ffffffffffff50f6220088dc030080025003804d**00134a4329350082e1ce5000036fd0700104342cbeada9801023215f15607c00c10d0afdab08e0080868585159cd00504342cbeada9803023215f15607c01c10d0afdab08e0100868585159cd08129d172**

17. The packet includes WSMP header information. Delete the header (as noted above in Step 16) from the pasted hex data, typically the first 72 to 75 bytes.



18. Click on Validate to decode the hex data. Green filled area text indicates the message meets the latest USDOT standard message format. If an error appears, re-evaluate the hex data based on the error. Observe…

BlueTOAD Spectra 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

This form must be printed for each RSU along with the BlueTOAD Spectra RSU Site Requirements form.

Date:

RSU Serial Number:

RSU IP Address:

BlueTOAD IP Address:

Category		Items tested	Date & Time	Pass	Signature of Evaluator
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.	Configure IP Address settings for RSU and BlueTOAD modules.			
	2.	Configure IP Address settings for traffic controller and In-Cabinet Processor (if applicable)			
	3.	Confirm ports 123, 8010 and 10001 are open and set for outbound RSU data traffic.			
Confirm Iteris System Data Collection	1.	RSU SPaT Data collection and display in BlueARGUS Travel Time system. (Signalized Intersection Locations ONLY)			
	2.	Bluetooth Data collection and display in BlueARGUS Travel Time system. (BlueTOAD Spectra RSU ONLY)			
Confirm Operation	1.	GPS Functionality Verified			
	2.	SPaT and MAP Broadcasting Verification (generated by RSU): Verified 11 messages per second - 10 SPaT messages - 1 MAP message			
	3.	SPaT, MAP, TIM and BSM Data DSRC/C-V2X Message Verification and validation USDOT / SAE J2735 (March2016)			
	4.	SCMS Certificate usage and validation			