CAVe-in-a-Box

Instruction Set

Table of Contents

List of Figures

CAVe-in-a-box

Acceptance Checklist

☐ All the **antennas** and **devices** firmly fastened to the box

☐ RSU ☐ OBU ☐ Wired Network Switch

☐ Wi-Fi Switch ☐ Traffic Signal Controller
☐ V2X Hub ☐ Tablet PC

☐ RSU antenna ☐ OBU antenna

☐ Able to **power ON all components** with one switch

☐ **LED/Light** turns to the color indicating operating mode depending on the vendors

☐ RSU LED ☐ OBU LED ☐ Wired Network Switch LED flickering green

☐ Wi-Fi Switch LED green ☐ Traffic Signal Controller LCD screen

☐ V2X Hub ☐ Tablet PC

Network scan test [cave-in-a-box.sh from *https://github.com/usdot-fhwa-stol/cav-education*]

☐ Do all the devices have correct IP/Port combination? If No,

Which devices have incorrect networking?

☐ RSU ☐ OBU ☐ Wired Network Switch ☐ Wi-Fi Switch

☐ Traffic Signal Controller ☐ V2X Hub ☐ Tablet PC

V2X Hub admin portal using the tablet

☐ Enable SPaT Application

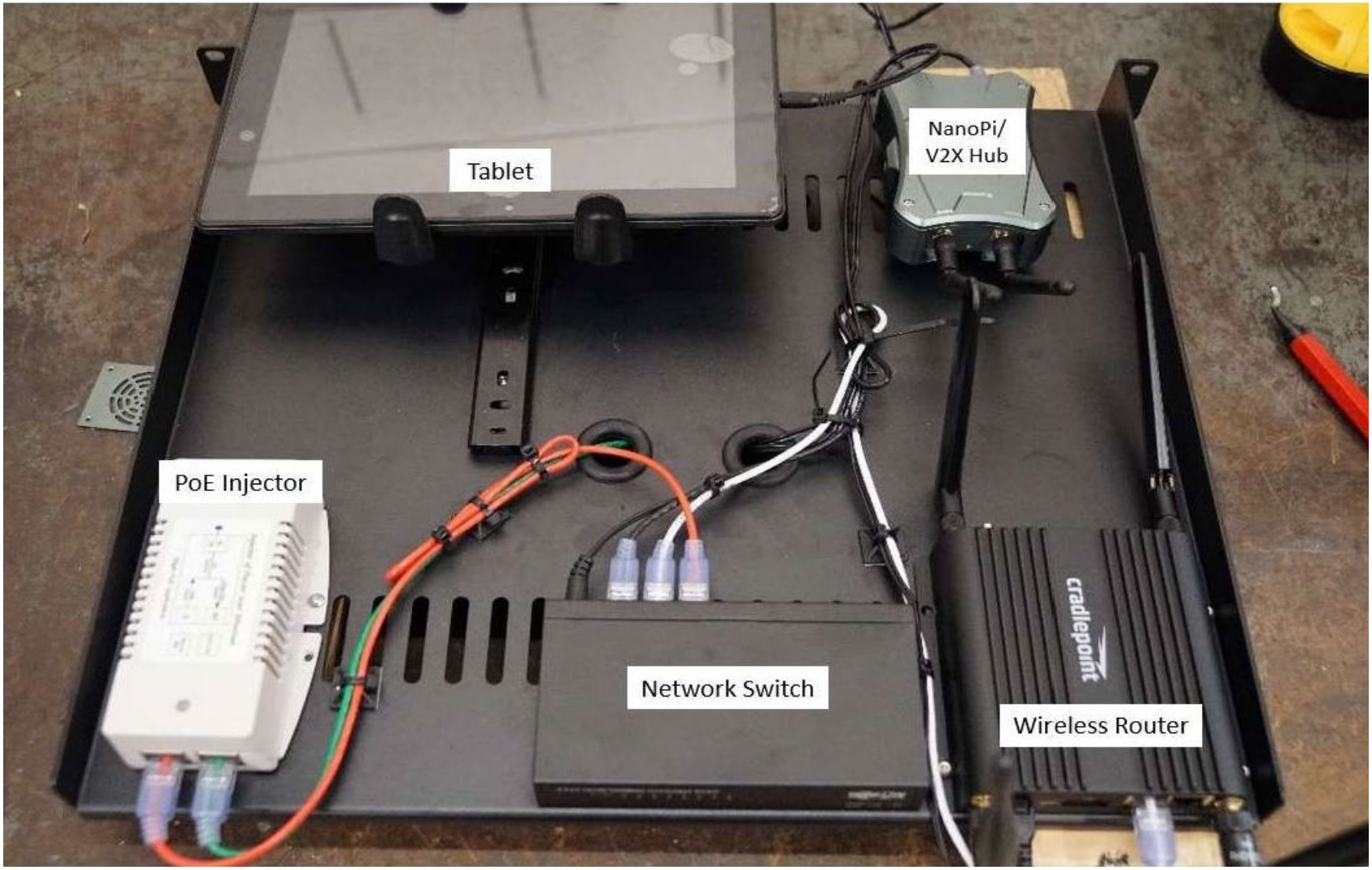
☐ Confirm SPaT message count is incremental and frequency is correct (around 100 which means 100 milliseconds between each SPaT message)

BSM receiving

- ☐ Able to login to the OBU using the tablet (If applicable)
- ☐ Run vendor specific commands to enable BSM broadcast
- ☐ Re-connect with the V2X Hub admin portal and enable MessageReceiver plugin
    - ☐ Confirm BSM count is incremental, and frequency is correct (around 100 which means 100 milliseconds between each SPaT message)

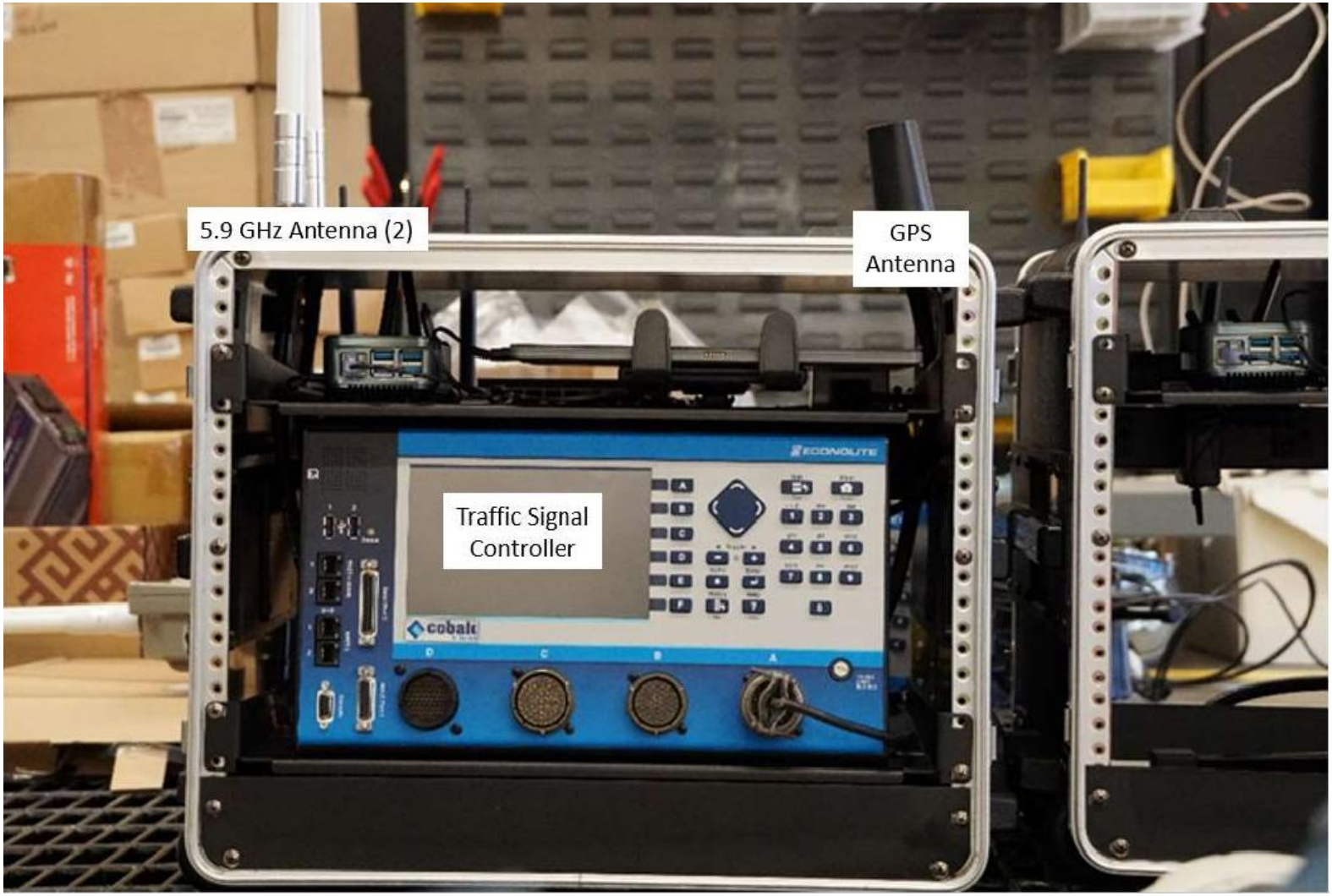
CAVe Test Tool application - optional

- ☐ Confirm the application is running by going to the http://localhost:8000
- ☐ Confirm BSM displayed as they are received from the OBU



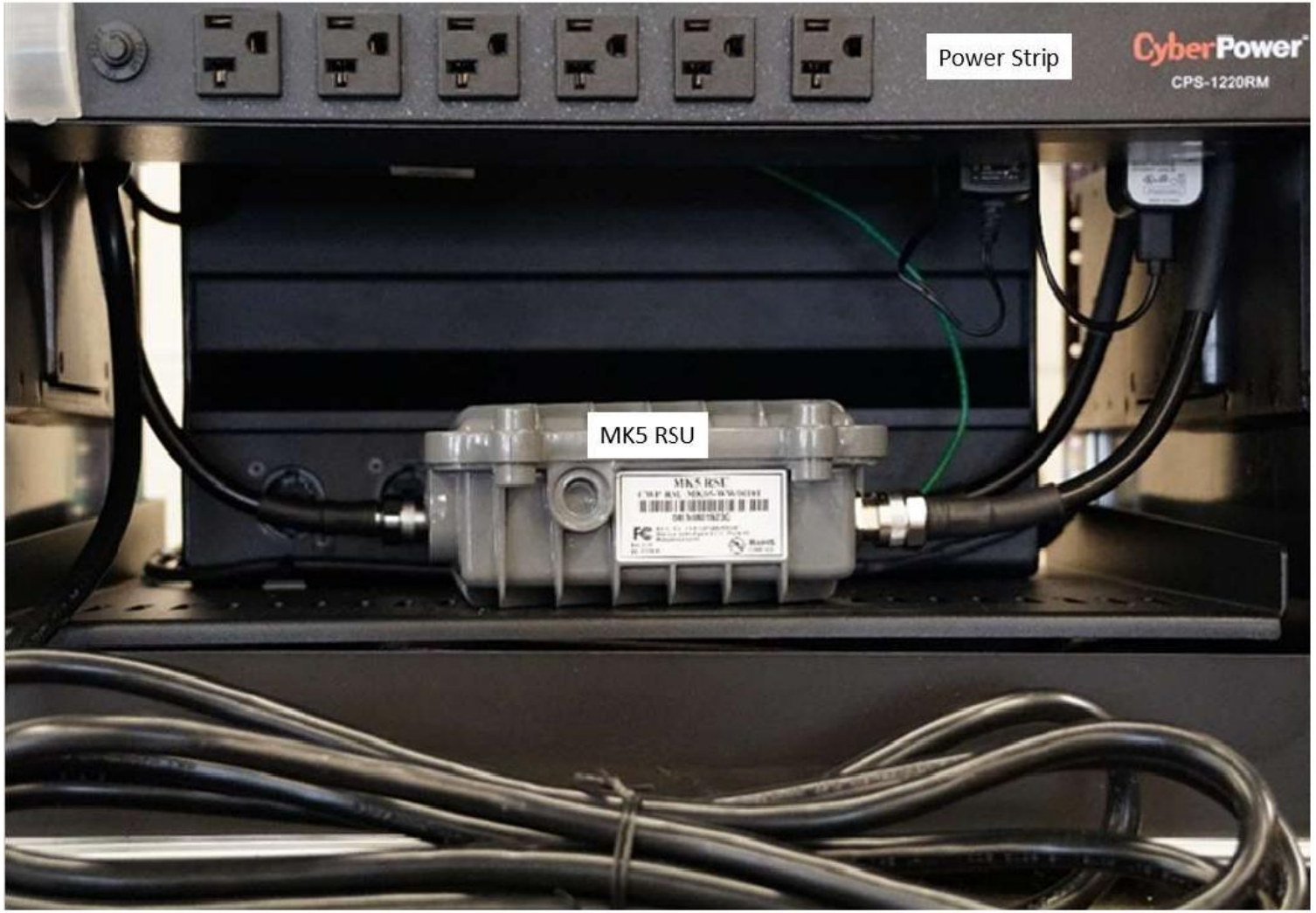
Source: FHWA.

Figure 1. Image. CAVe-in-a-box shelf.



Source: FHWA.

Figure 2. Image. Front view of infrastructure kit.



Source: FHWA.

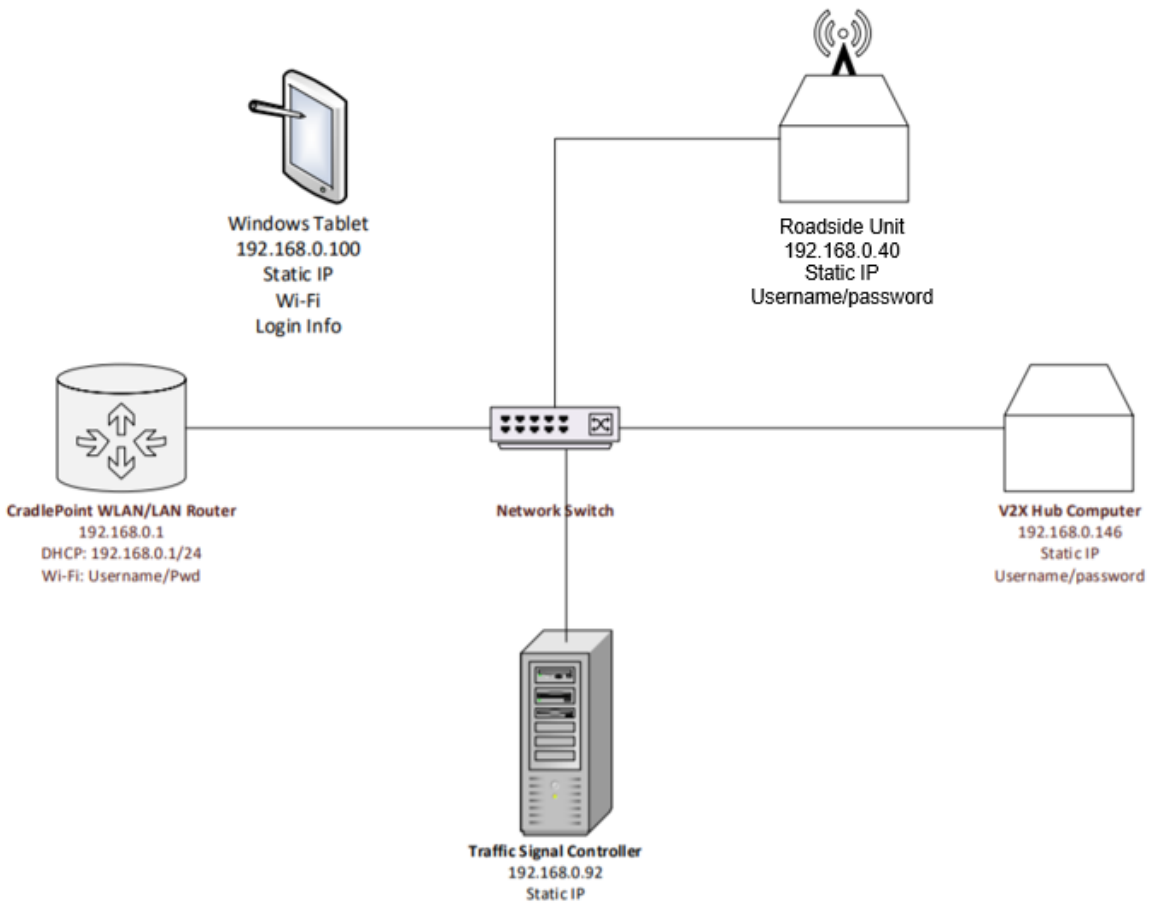
Figure 3. Image. Roadside unit (RSU) in infrastructure kit.

List of Abbreviations

API	application programming interface
ASN.1	Abstract Syntax Notation One
BSM	basic safety message
C-V2X	cellular vehicle-to-everything
CAN	Controller Area Network
CAV	connected and automated vehicle
CAVe	Connected and Automated Vehicle education
CV	connected vehicle
DHCP	Dynamic Host Configuration Protocol
DMS	dynamic message sign
DSRC	dedicated short-range communications
FHWA	Federal Highway Administration
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GUI	graphical user interface
HDMI	High-Definition Multimedia Interface
HIL	hardware-in-the-loop
IP	Internet Protocol
ITIS	International Traveler Information System
ITS	intelligent transportation system
ITS JPO	Intelligent Transportation Systems-Joint Program Office

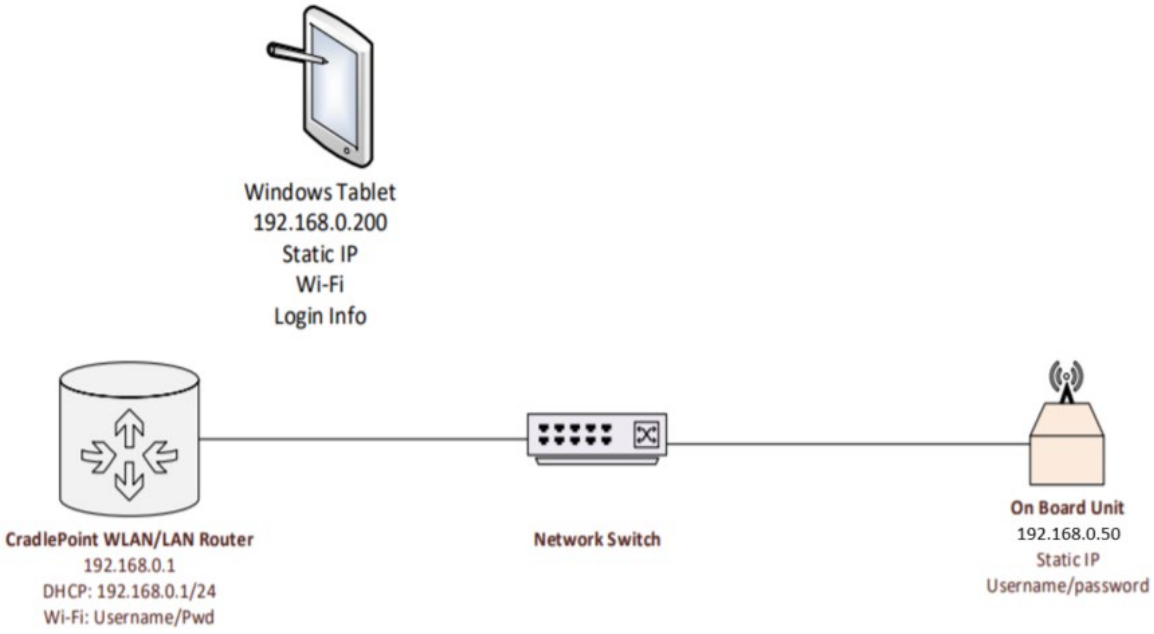
JSON	Java Script Object Notation
LiDAR	Light Detection and Ranging
LTE	Long-Term Evolution
MUTCD	Manual on Uniform Traffic Control Devices
NTCIP	National Transportation Communications for ITS Protocol
OBD	Onboard Diagnostics
OBU	onboard unit
PoE	Power over Ethernet
PSID	Provider Service Identifier
PSM	personal safety message
RSU	roadside unit
SAE	Society of Automotive Engineers
SDX	Situation Data Exchange
SNMP	Simple Network Management Protocol
SPaT	Signal Phase and Timing
SRM	Signal Request Message
SSH	Secure Shell
STOL	Saxton Transportation Operations Laboratory
TCP/IPv4	Internet Protocol version 4
TFHRC	Turner-Fairbank Highway Research Center
TIM	traveler information message
TMC	traffic management center

TSC	traffic signal controller
UDP	User Datagram Protocol
UPER	unaligned packet encoding rules
USDOT	United States Department of Transportation
V2I	vehicle-to-infrastructure
V2X	vehicle-to-everything
WAVE	Wireless Access in Vehicular Environments
WSA	WAVE Service Advertisement
WZDx	Work Zone Data Exchange



Source: FHWA.

Figure 4. Diagram. CAVe-in-a-box network configuration.



Source: FHWA.

Figure 5. Diagram. Mobile kit network configuration.

CradlePoint Router Wireless Connection

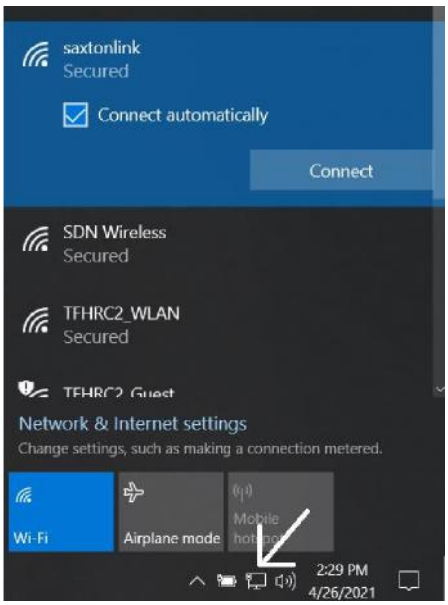
Items Needed

- CradlePoint Router.
- Computer/Tablet.

Setup

The following connection instructions are for setting up a wireless connection to the CAVe-in-a-Box *local* network. The routers do not contain active SIM cards for internet access. No internet access is required to connect to the kit. This section is optional. A direct connection via ethernet may be established instead.

1. Open the network connections icon at the bottom right of the taskbar. Refer to figure 6.



Source: FHWA.

Figure 6. Screenshot. Open Network Connections.

2. Select the router's Wi-Fi SSID and enter the password. It may be one of the following two routers:
    a. IBR600C-ca2
        i. WA202500327110
    b. IBR600C-f30
        i. WA202500327328
    c. If not listed above, the SSID and password will be noted on the router itself.
3. The computer should now be within the CAVe-in-a-Box network.

NanoPi V2X Hub Setup

These NanoPi V2X Hub instructions only apply to users who are building their own CAVe-in-a-Box and using a NanoPi. Any other single-board computer may be used. If using another computer, please use the recommended operating system provided by the vendor.

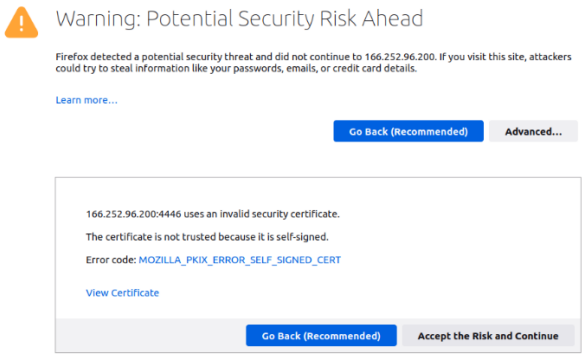
Installing OS

1. Download appropriate image file for NanoPi on your PC.
    a. Download link provided:
        i. https://drive.google.com/file/d/1-MVs9aIsdL_S-eH1LzXAEOBevWtOL_OY/view?usp=sharing.
    b. Un-zip downloaded package.
2. Using an image installer, install the image on your SD card.
    a. If loaned from Saxton Lab, an SD card is provided.
    b. A few image installers:
        i. Windows – Rufus.
        ii. MacOS – Etcher.
        iii. Linux – Etcher.
3. Eject SD Card from PC when finished
    a. Insert in NanoPi.
    b. Connect NanoPi to a monitor via HDMI.
    c. Power NanoPi.

Installing V2X-Hub

1. Establish an internet connection.
2. Open a Terminal (Terminator) and run:
    a. `sudo apt-get install git`
3. Open a web browser and go to:
    a. https://github.com/usdot-fhwa-OPS/V2X-Hub.
4. Copy link for cloning:
    a. https://github.com/usdot-fhwa-OPS/V2X-Hub.git.
5. In Terminal, enter:
    a. `git clone https://github.com/usdot-fhwa-OPS/V2X-Hub.git`
6. Following the ARM-specific instructions in the Docker_Instructions.md folder on GitHub:
    a. `cd V2X-Hub/configuration/arm64/`
    b. `chmod +x initialization.sh`
    c. `sudo ./initialization.sh`
7. When prompted for a login:
    a. `Login: v2xadmin`
    b. `Password: V2xHub#321`
    c. This will be your V2X-Hub administrator login information
8. Installation will automatically begin. Skip to section 11 if no errors occur
    a. If confronted with error “No module named setuptools_rust,” enter:
        i. `python3 -m pip install setuptools`
        ii. `python3 -m pip install setuptools-rust`
    b. Copy and paste “sudo…cargo” under Debian/Ubuntu from website to Terminal:
        i. https://cryptography.io/en/latest/installation.html#debian-ubuntu
        ii. When prompted, select <Yes>
    c. `python3 -m pip install cryptography`
        i. If cryptography install fails, run:
            1. `sudo apt-get update`
            2. Repeat steps 8d-8e
9. Once cryptography is successfully installed, run the previously failed setup using:
    a. `sudo pip3 install docker-compose`

10. Repeat steps 6(c)-7.
11. Installation is complete.
    a. In a browser, go to: https://127.0.0.1:19760.
    b. Accept/save the credentials on the screen.
        i. Refer to figure 7.
    c. Open a new tab and go to http://127.0.0.1.
    d. Login to V2X-Hub using login information above.



Source: FHWA.

Figure 7. Screenshot. Accept Security Credentials.

CAVe-in-a-Box Setup and Test

Items Needed

- CAVe-in-a-Box.
- Optional: External Monitor.
- Optional: Keyboard + Mouse.
- Optional: External Computer.

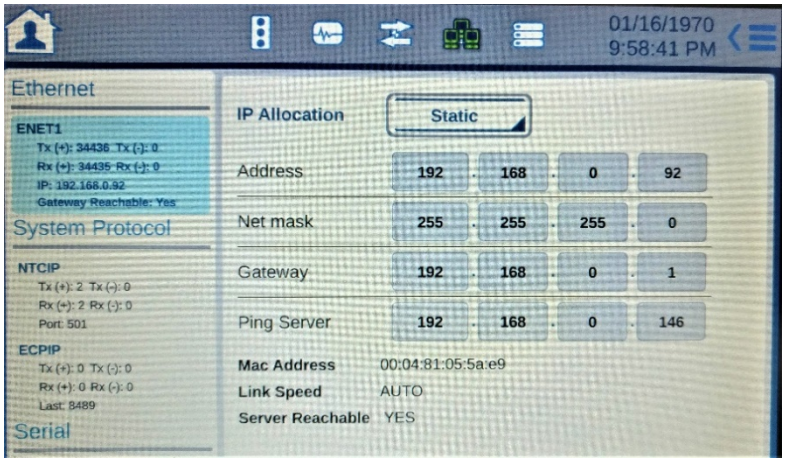
Basic Setup

1. Using the acceptance checklist, make sure all antennas and devices are firmly fastened to the box.
    a. Mark off each unit on the checklist.
2. Connect **CAVe-in-a-box** surge protector to AC power source.
3. On the back of the CAVe-in-a-box, turn on the **surge protector.**
    a. All units within the CAVe-in-a-box will power on.
    b. Component images and names are in the **Component Names** document.
    c. Mark results in checklist.
4. Connect **Mobile Kit** to respective power source.
    a. All units within Mobile Kit will power on.
    b. Mark results in checklist.
    c. After a few seconds, all unit LEDs will be powered on.
    d. Check each unit and mark results on checklist.
5. For the other sections, either an external monitor and keyboard + mouse can be plugged into the NanoPi/V2X-Hub computer or an external computer can be connected to the network switch.
6. The NanoPi has an Operating System and the V2X-Hub pre-installed.
    a. If desired, the instructions for setting both up can be found in the NanoPi V2X-Hub Setup document.
    b. Pre-configured NanoPi Login Information:
        i. Username: `pi`
        ii. Password: `pi`

Traffic Signal Controller

The following steps show which Traffic Signal Controller settings must be changed at a minimum. Every intersection has a different setup. Therefore, some settings are only examples.

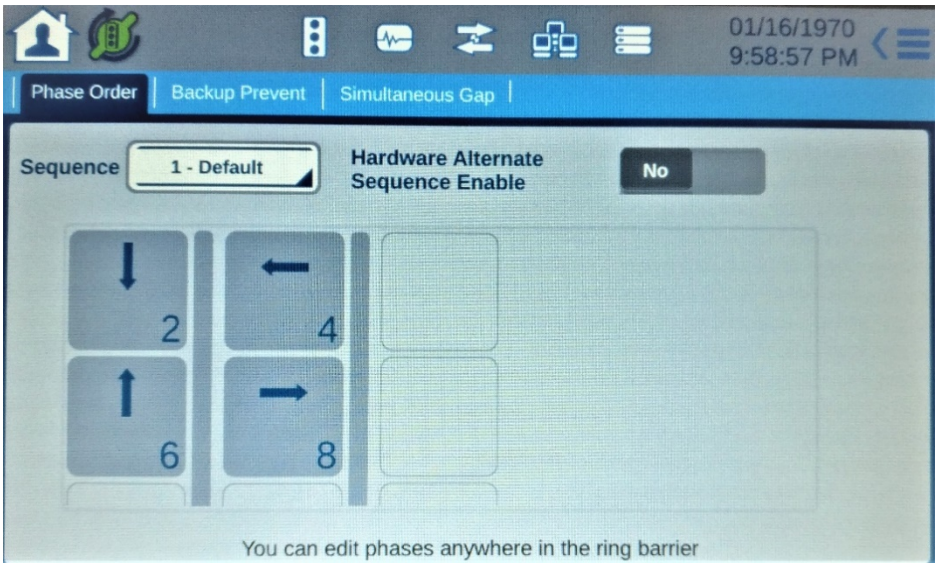
1. The **network configuration settings** must be changed to communicate with the V2X Hub
    a. Address: 192.168.0.92
    b. Net Mask: 255.255.255.0
    c. Gateway: 192.168.0.1
    d. Ping Server: 192.168.0.146
    e. Refer to figure 8.



Source: FHWA.

Figure 8. Screenshot. TSC Network Configuration.

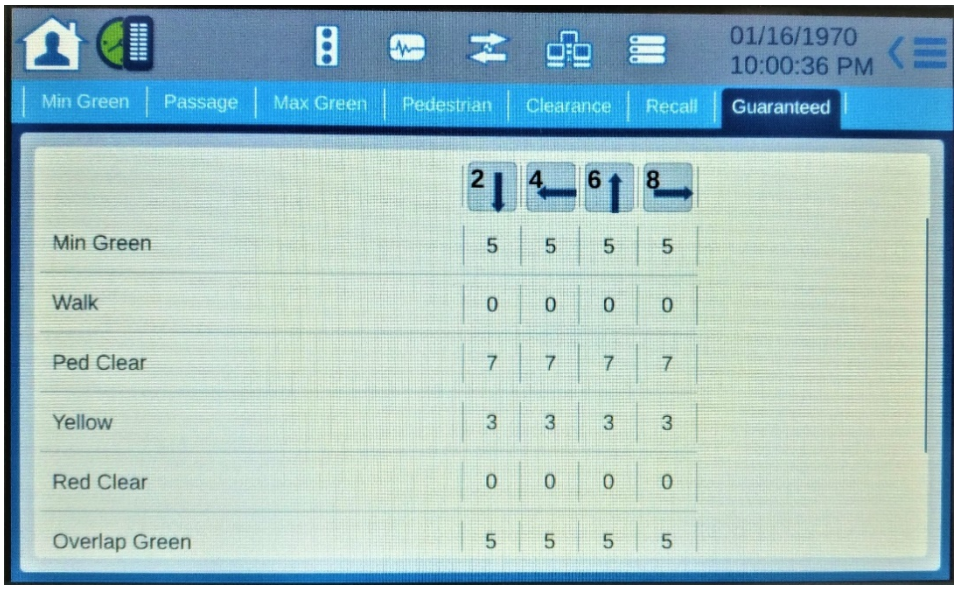
2. The **Phase Order** settings can be found on the home page. Select the symbol and adjust to match your intersection's phase order.
    a. Barriers separate active phases.
    b. Tap on a phase symbol or empty box to view edit menu.
    c. Refer to example in figure 9.



Source: FHWA.

Figure 9. Screenshot. Example phase order settings.

3. In the **Timing Plans** settings, all the separate tabs, seen in figure 9, can be changed to match your desired signal timing.



Source: FHWA.

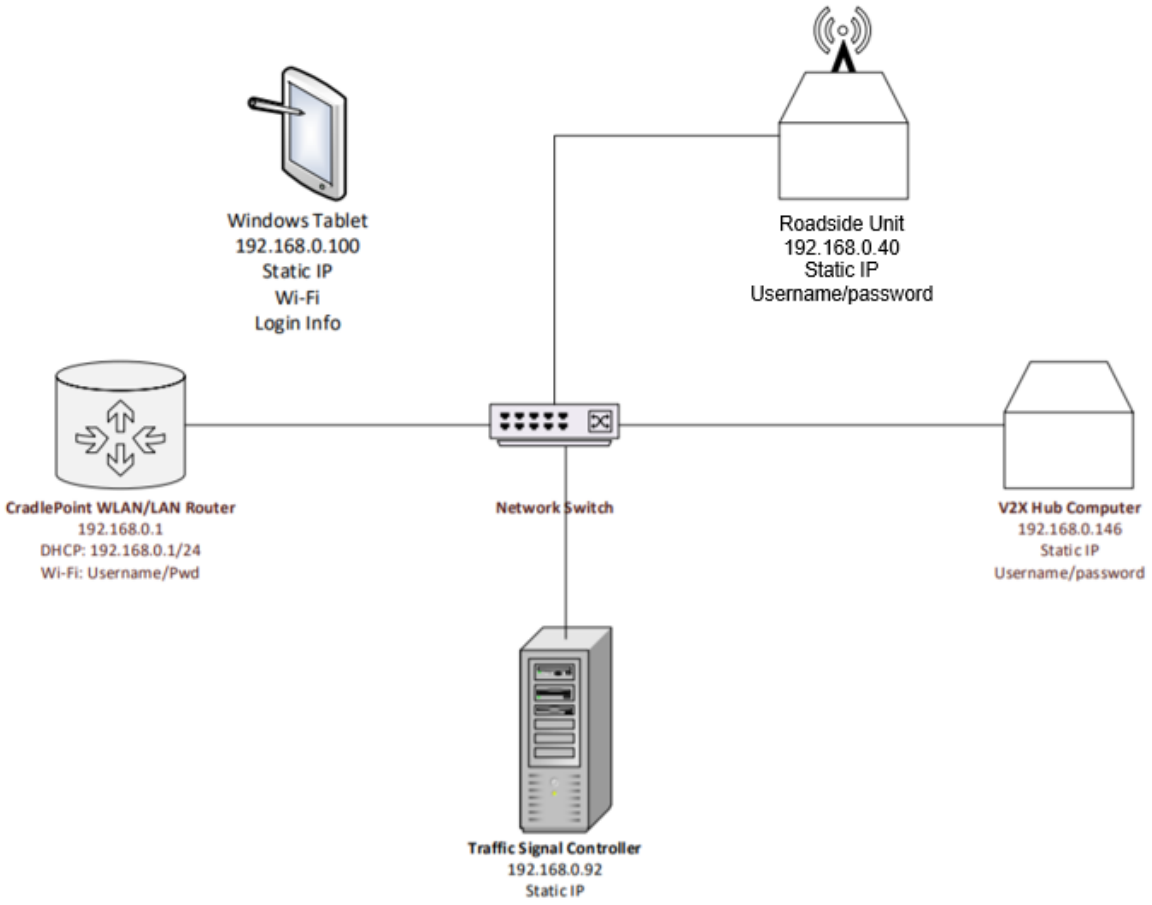
Figure 10. Screenshot. Timing settings.

4. There are many other settings available to be changed. Not all need to be adjusted but can be to reflect your desired SPaT messages.

Network Setup

Users connected to the **Wireless Router** or the LAN **Network Switch** with an external PC/tablet can ping other devices within the network.

1. Attempt to `ping` each device within the CAVe-in-a-box. Refer to figure 11.
    a. Example: `ping 192.168.0.1`.
    b. To stop ping process: <Ctrl>C.



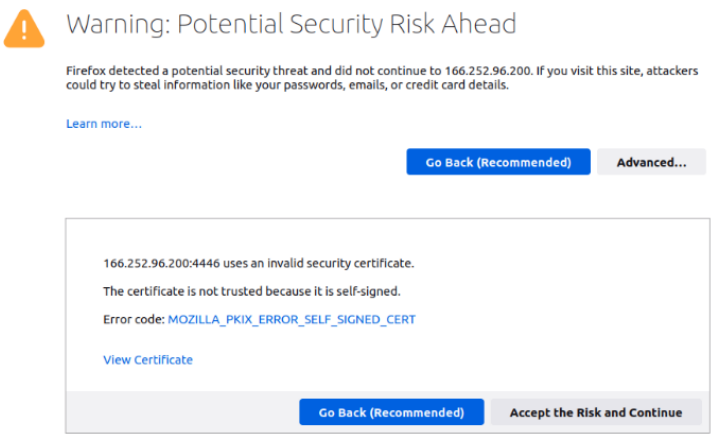
Source: FHWA.

Figure 71. Diagram. CAVe-in-a-box network configuration.

2. External Kit IP addresses are checked later in the process.
3. Check off the box indicating correct IP/Port combinations.

V2X Hub + SPAT Plugin

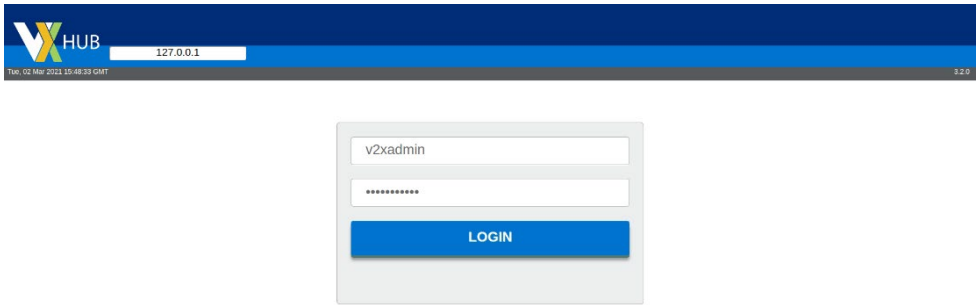
1. Using the CAVe-in-a-box tablet, open an internet browser and go to:
    a. https://192.168.0.146:19760/
    b. Accept the credentials on the page. Refer to figure 12.



Source: FHWA.

Figure 82. Screenshot. Accept Security Credentials.

2. Open a new tab and go to:
    a. 192.168.0.146
    b. If using an external computer, you will have to change the IP address in the text box to:
        i. 192.168.0.146
        ii. Default is 127.0.0.1 if logging in from the Nano Pi.
        iii. Refer to figure 13 for the text box.
3. Login using:
    a. Username: v2xadmin
    b. Password: V2xHub#1234
    c. Refer to figure 13.

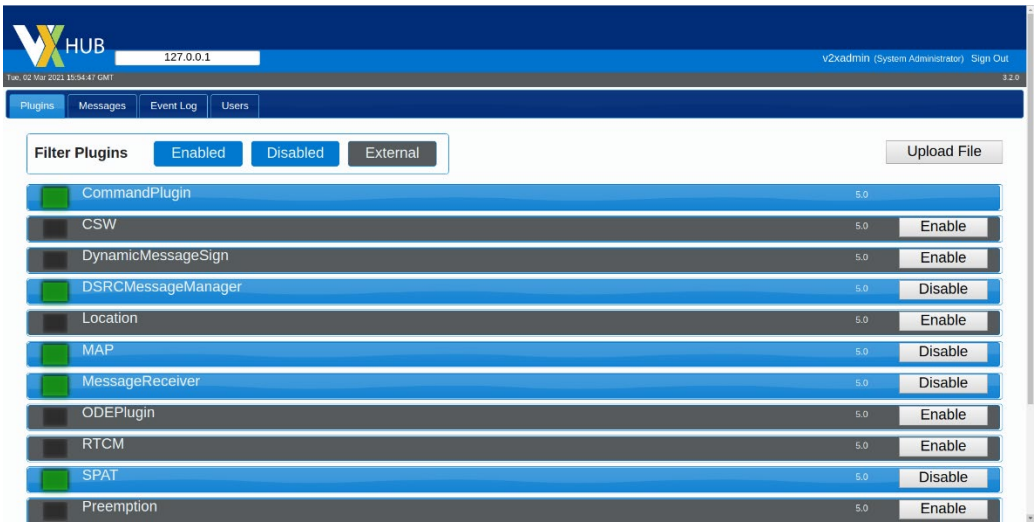


Source: FHWA.

Figure 93. Screenshot. V2X Hub login screen.

4. Once logged in, **Enable** the **SPaT** plugin if it is not already enabled. Refer to Figure 14.

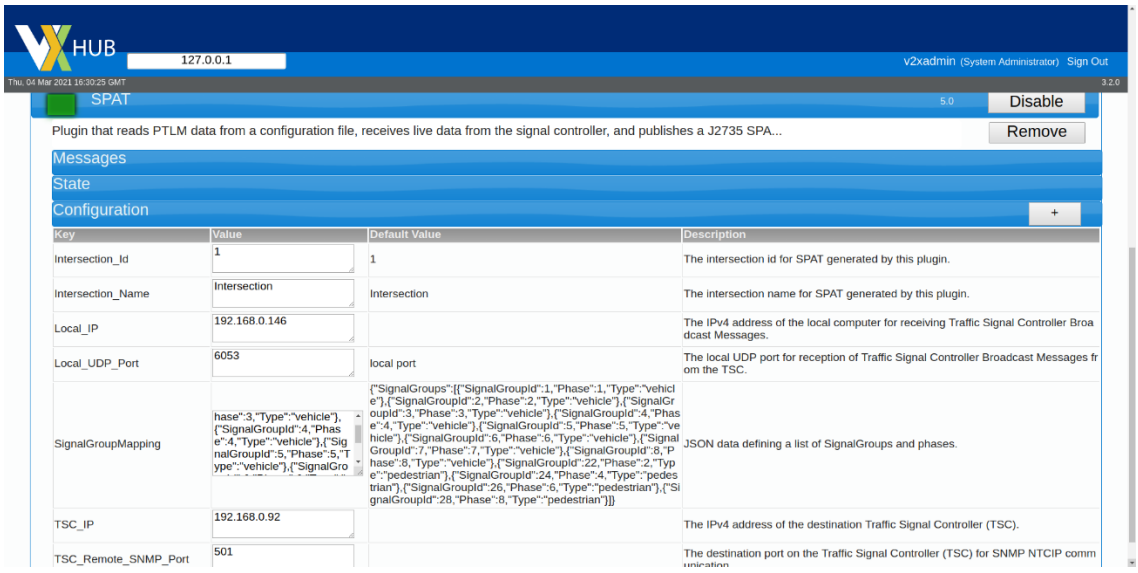
a. If SPaT is not listed as below, the Enabled, Disabled, and External filters may be toggled on or off to show/hide plugins
b. Check “Enable SPaT Application” in acceptance checklist.



Source: FHWA.

Figure 104. Screenshot. Plugins with enabled and disabled filters ON.

5. Click on the **SPaT** row to expand it:
   a. Expand the **Configuration** row and ensure the values match figure 15.
   b. The **SignalGroupMapping** section is valid for any standard 4-way intersection.
      i. It must otherwise be changed to match your intersection’s SPaT settings.

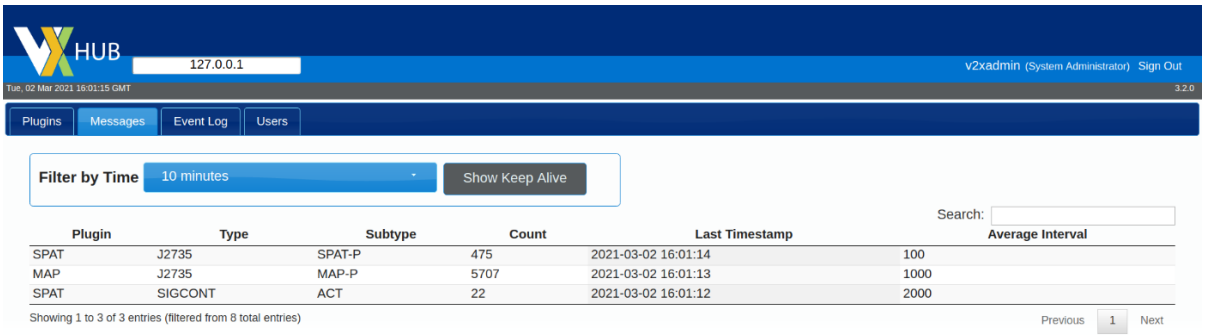


Source: FHWA.

Figure 115. Screenshot. SPaT plugin settings.

6. Select the **Messages** tab at the top to view the messages being received.

a. The **SPaT-P** Subtype will eventually reach a 100 Average Interval.
b. Check off results in acceptable checklist.
c. Refer to figure 16.



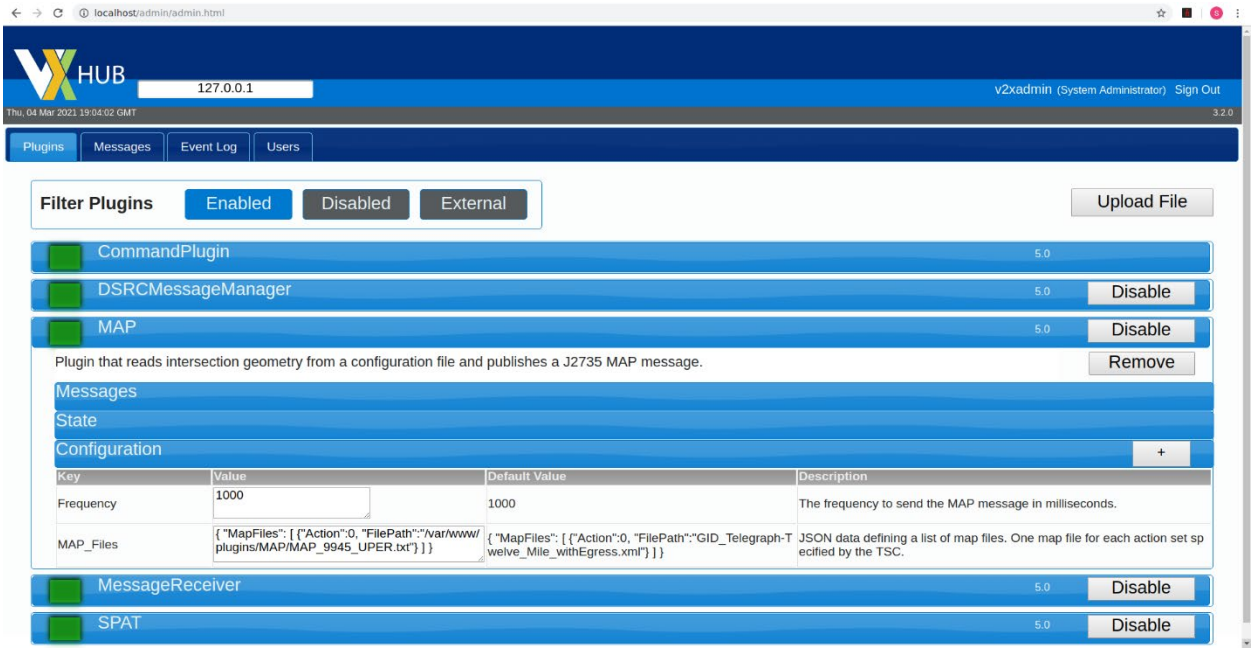
Source: FHWA.

Figure 126. Screenshot. Messages received.

MAP Plugin

To use the MAP plugin in V2X Hub, a map file must be saved in the V2X Hub file path. The map file is an UPER string saved as a .txt file. An example map file is provided in the MAP folder. If desired, a new map file for an intersection may be created following the ISD MAP Tool instructions. An internet connection is required for creating a MAP. **Skip to step 5 if using the provided MAP.**

1. Following the **ISD Message Creator** tool instructions, move your file into the V2X Hub computer.
2. Via USB flash drive:
    a. Insert your USB containing the folder into the computer.
    b. Move the file to one of the locations provided in steps 3 and 4
3. Via Ethernet:
    a. Connect external computer to kit's network switch.
    b. Change external computer's wired settings to be within the CAVe network.
    c. Open a terminal in your external computer.
    d. `cd <directoryContainingFile>`
    e. `sudo scp file_name pi@192.168.0.146:/home/pi/V2X-Hub/configuration/arm64/MAP/`
    f. If prompted: *Yes*
        i. *Note:* If an error appears, simply copy and run the recommended command
    g. Password: pi
4. If your kit **does not** contain a single-board computer (NanoPi, RaspberryPi, etc.) follow for amd64:
    a. `cd <directoryContainingFile>`
    b. `sudo scp file_name <username>@192.168.0.146:/home/<username>/V2X-Hub/configuration/amd64/MAP/`
    c. If prompted: *Yes*
    d. Password: <*password*>
    e. Username and Password are **noted within the box**, due to various computers being used
5. Return to the Plugins tab in V2X Hub and ENABLE the MAP plugin if it is not already enabled.
6. Check "Enable MAP Application" in acceptance checklist.
7. Click on the MAP row to expand it.
8. Expand the Configuration row and ensure the values match figure 17.
9. Change the file name in the *Value* section to match your .txt file.



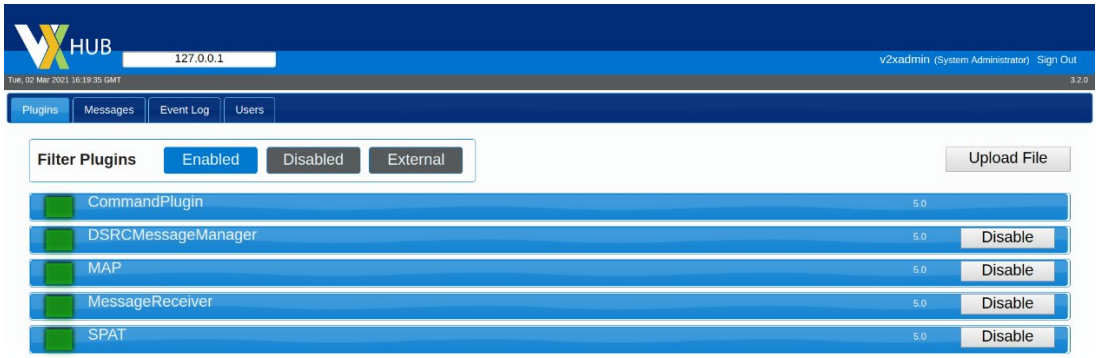
Source: FHWA.

Figure 137. Screenshot. MAP plugin settings.

10. Select the Messages tab at the top to view the messages being received.
11. The MAP-P Subtype will eventually reach a 1000 Average Interval.
    a. Refer to figure 16 from the previous section.
12. Check off results in acceptable checklist.

DSRC Message Manager

1. ENABLE the DSRCMessageManager plugin if it is not already enabled. Refer to figure 18.
    a. Check “Enable DSRCMessageManager Application” in acceptance checklist.



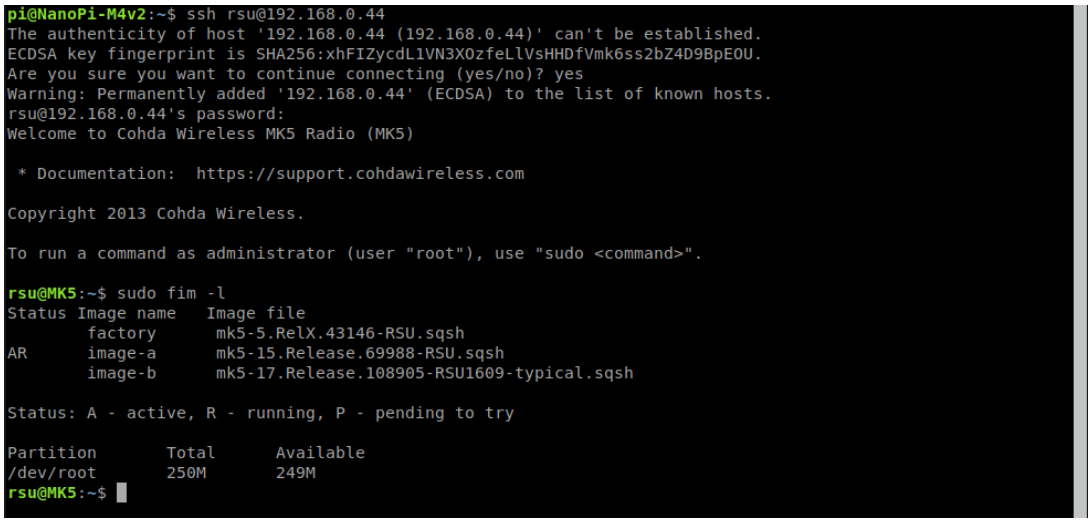
Source: FHWA.

Figure 14. Screenshot. DSRCMessageManager plugin enabled.

2. Open a Terminal and enter:
    a. `ssh rsu@192.168.0.40`

b. If prompted to continue connecting, enter: `yes`
c. Password: `rsuadmin`
d. Refer to figure 19.

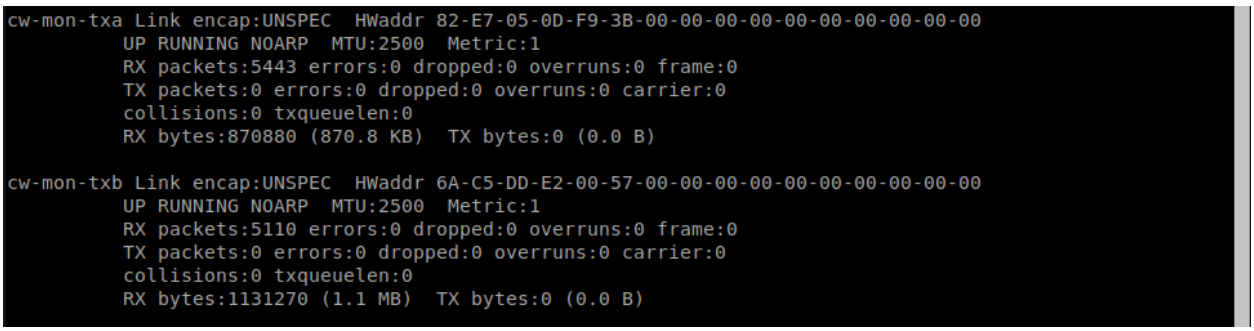
3. The Terminal is now logged into the MK5 RSU. Type:
   a. `sudo fim -l`
   b. Refer to figure 19 for an example output.



Source: FHWA.

Figure 15. Screenshot. Checking MK5 RSU firmware.

4. The firmware should point with “AR” to mk5-15.Release.69988-RSU.sqsh. or a later release
   a. Refer to figure 19 above.
5. To ensure GPS is running, enter:
   a. `date`
   b. The output should be the current date and time.
   c. If date is not correct, move box to a location with better signal.
6. To ensure Map and SPaT messages are being transmitted from the RSU, enter:
   a. `ifconfig`
   b. From the output, interfaces cw-mon-txb will be seen in the list.
   c. Refer to figure 20.



Source: FHWA.

Figure 16. Screenshot. Network interfaces output.

d. Run: `tcpdump –i cw-mon-txb –xx | grep "00 13"`
e. Stop the process with <Ctrl>c.
f. Refer to figure 21 for output.

```
root@MK5:/opt/cohda/application/rsu1609# tcpdump -i cw-mon-txb -xx | grep "00 13"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on cw-mon-txb, link-type IEEE802_11_RADIO (802.11 plus radiotap header), capture size 262144 by
tes
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x01d0:  0500 0040 0000 13e1 74d0 1414 9916 5540
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x01d0:  0500 0040 0000 13e1 74d0 1414 9916 5540
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
```

Source: FHWA.

Figure 17. Screenshot. Observing SPaT message transmission.

g. Run: `tcpdump –i cw-mon-txb –xx | grep "0012"`
h. Stop the process with <Ctrl>c.
i. Refer to figure 22 for output.

```
root@MK5:/opt/cohda/application/rsu1609# tcpdump -i cw-mon-txb -xx | grep "0012"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on cw-mon-txb, link-type IEEE802_11_RADIO (802.11 plus radiotap header), capture size 262144 by
tes
        0x0050:  0401 9400 8002 81ad 0012 81a9 3803 3020
        0x0050:  0401 9400 8002 81ad 0012 81a9 3803 3020
        0x0050:  0401 9400 8002 81ad 0012 81a9 3803 3020
```

Source: FHWA.

Figure 18. Observing MAP message transmission.

7. If neither command runs the correct output, refer to RSU document for troubleshooting.

8. Verify forwarding BSM and Mobility messages are set:
    a. The RSU forwards BSMs - received from the OBU - over to V2X Hub, using port 26789.
    b. `tcpdump port 26789`
    c. Refer to figure 23 for output.

```
root@MK5:~# tcpdump port 26789
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:23:59.503400 IP 192.168.0.40.44163 > 192.168.0.146.26789: UDP, length 60
16:23:59.604349 IP 192.168.0.40.50627 > 192.168.0.146.26789: UDP, length 60
16:23:59.704378 IP 192.168.0.40.50132 > 192.168.0.146.26789: UDP, length 60
16:23:59.804597 IP 192.168.0.40.36665 > 192.168.0.146.26789: UDP, length 60
16:23:59.904724 IP 192.168.0.40.35756 > 192.168.0.146.26789: UDP, length 60
```

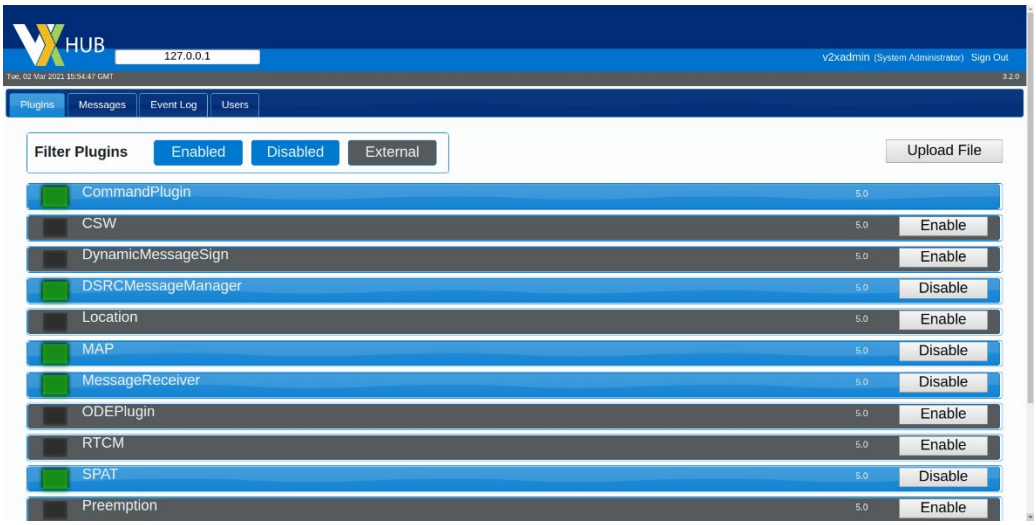
Source: FHWA.

Figure 19. Screenshot. RSU forwarding BSM.

Message Receiver

To ensure BSMs are being received by V2X Hub, transmission from the OBU is first tested.

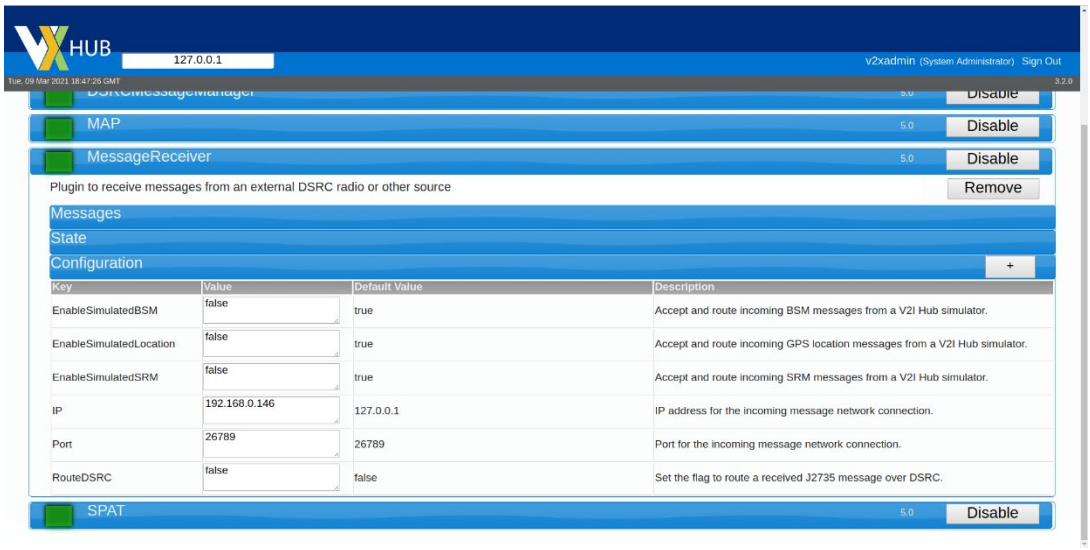
1. Using the tablet or an external computer, connect to the CradlePoint router using the information provided inside the external kit.
2. Follow the separate instructions provided to test the BSM transmission from the OBU.
3. Once BSM transmission is verified, open V2X Hub on the NanoPi.
4. Enable the MessageReceiver plugin if it is not already enabled.
    a. Refer to figure 24.



Source: FHWA.

Figure 20. Screenshot. Enabled MessageReceiver plugin.

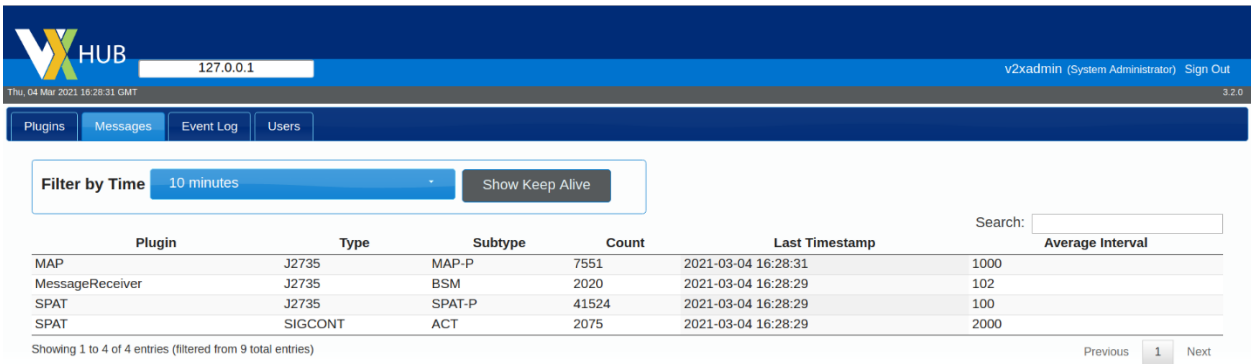
5. Click on the MessageReceiver plugin to expand it.
    a. Expand the Configuration row and ensure the values match figure 25.



Source: FHWA.

Figure 21. Screenshot. MessageReceiver configuration.

6. Navigate to the Messages Tab and verify that BSMs are being received.
    a. The BSM subtype will eventually reach 100 average interval.
    b. Refer to figure 26.



Source: FHWA.

Figure 22. Screenshot. BSMs received.

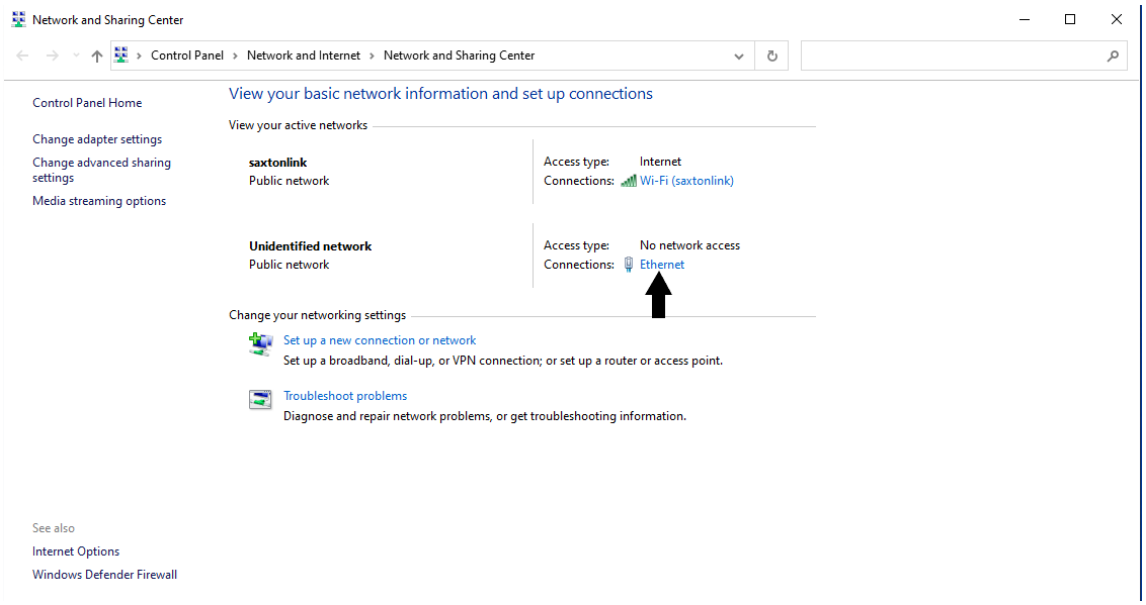
Cohda MK5 Onboard Unit– Functional Test

Items Needed

- MK5 OBU Unit.
- 12V DC Adapter.
- Lab Mobile DSRC antenna.
- Test PC.
- Ethernet Cable.

Basic Setup

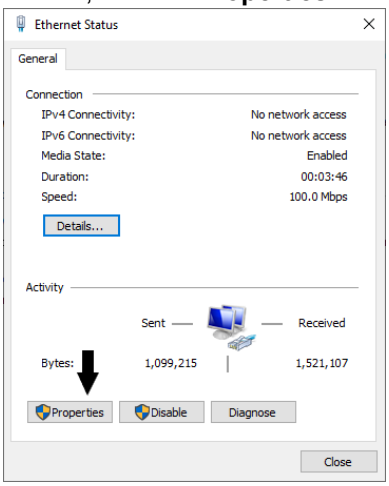
1. Using the tablet or an external computer, connect to the CradlePoint router using the WiFi SSID Info document.
2. If your mobile kit does not have a router, you may connect to the OBU via Ethernet. Otherwise, continue to step 7.
    a. Check your IP Address by opening **Network and Sharing Center** in Windows.
    b. Within that window, click on **Ethernet.**
    c. Refer to figure 27.



Source: FHWA.

Figure 23. Screenshot. Network and Sharing Center.

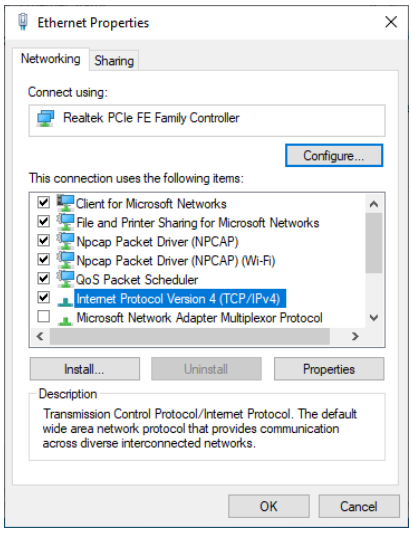
3. A new window will open. In that window, click on **Properties**. Refer to figure 28.



Source: FHWA.

Figure 24. Screenshot. Ethernet status.

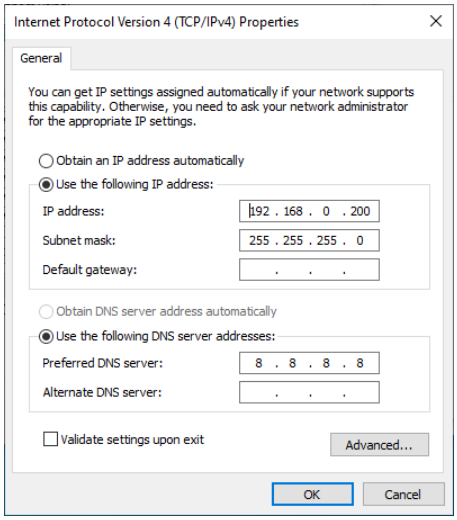
4. Within the Ethernet Properties window, double-click/open **Internet Protocol Version 4 (TCP/IPv4).**
    a. Refer to figure 29.



Source: FHWA.

Figure 25. Screenshot. Ethernet properties.

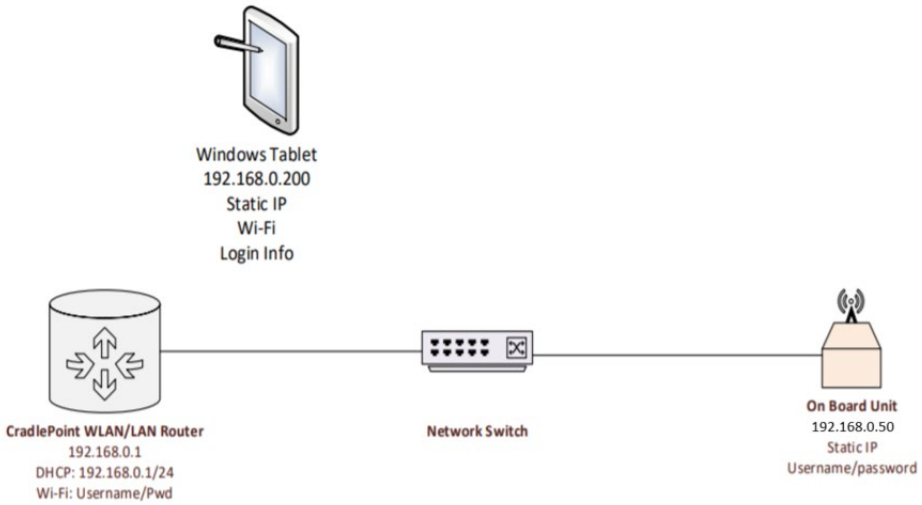
5. Ensure that **Use the following IP address** is selected. Input the same configurations as figure 30.



Source: FHWA.

Figure 26. Screenshot. IPv4 settings.

6. Click **OK** at the bottom of the window, then close all previous Windows.
7. Open a Terminal/Command Prompt.
    a. If using a tablet, you may not have access to a terminal. Skip to Step 9.
8. Attempt to ping each device within the Mobile Kit. Refer to figures 31 and 32.
    a. ping 192.168.0.50
    b. To stop ping process: <Ctrl>C.



Source: FHWA.

Figure 27. Diagram. Mobile kit network configuration.

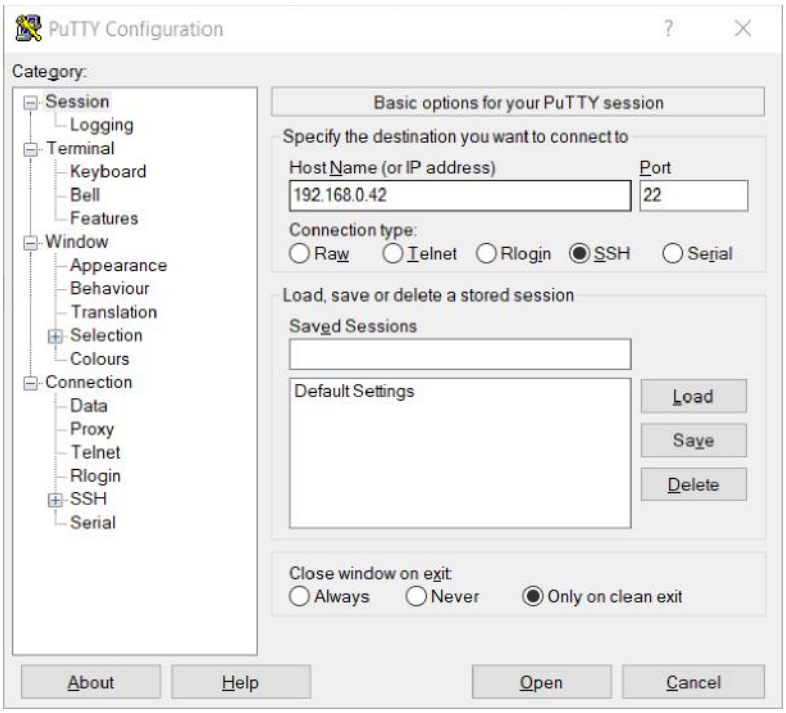
```
v2x@v2x-Lenovo-ideapad-510-15IKB:~$ ping 192.168.0.42
PING 192.168.0.42 (192.168.0.42) 56(84) bytes of data.
64 bytes from 192.168.0.42: icmp_seq=1 ttl=64 time=0.789 ms
64 bytes from 192.168.0.42: icmp_seq=2 ttl=64 time=0.574 ms
^C
--- 192.168.0.42 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.574/0.681/0.789/0.110 ms
v2x@v2x-Lenovo-ideapad-510-15IKB:~$
```

Source: FHWA.

Figure 28. Screenshot. Example positive ping output.

9. Using the acceptance checklist, mark off the box indicating correct IP/Port combinations.

10. If using a tablet, open PuTTY. Copy the settings in figure 33 and click on **Open**.
    a. Use the password in step 11 to login to the OBU.



Source: FHWA.

Figure 29. Screenshot. PuTTY settings.

11. To connect to OBU use:

    a. ssh user@192.168.0.50
    b. If prompted to continue connecting, enter: yes
    c. Password: user
    d. Refer to figure 34 for an example login output.

```
v2x@v2x-Lenovo-ideapad-510-15IKB:~$ ssh user@192.168.0.42
user@192.168.0.42's password:
Welcome to Cohda Wireless MK5 Radio (MK5)

 * Documentation:  https://support.cohdawireless.com
Last login: Mon Mar  8 14:44:33 2021 from 192.168.0.1
root@MK5:~#
```

Source: FHWA.

Figure 30. Screenshot. OBU login example.

Testing GNSS Operation

1. Connect the antenna to the OBU.
    a. Make sure the GPS is connected to the blue fakra connection labelled as GNSS in figure 35. The Lab Mobile DSRC antenna GPS connector is also blue.
    b. The other two can be connected in any order to Ant 1 and Ant 2.

Source: FHWA.

Figure 31. Photo. MK5 OBU hardware setup.

2. To send BSMs, GPS must first be established.
    a. To check for proper GPS signal, use:
        i. `date`
        ii. The output will be the current date. Refer to figure 36 for example output.
        iii. If date is not correct, move antenna to an area with better reception.

```
root@MK5:~# date
Mon Mar  8 19:39:33 UTC 2021
root@MK5:~#
```

Source: FHWA.

Figure 32. Screenshot. GPS date output.

Testing BSM Transmission

1. To check for BSM transmissions, enter:
    a. `ifconfig`
    b. A list of network interfaces will appear. If you do not see “cw-mon-txb”:
        i. `cd /opt/cohda/application/example1609`
        ii. `./rc.example1609 start obu`
        iii. Repeat step 1a
        iv. If process does not begin, a GPS signal is not available
    c. Otherwise, continue to step 2
2. A further check after cw-mon-txb is available:
    a. `tcpdump -i cw-mon-txb -xx`
    b. The BSM message ID is 14 in Hexadecimal. The ID can be seen below

c. A search for the ID can be run by adding:
    i. `| grep "00 *14"`
d. Refer to figure 37 for output.

Source: FHWA.

Figure 33. Screenshot. BSM transmitting output.

Testing DSRC Message Receiving

1. The interface for receiving messages is cw-mon-rxb. Check messages received:
    a. `tcpdump -i cw-mon-rxb -xx`
    b. The MAP message ID is 12 in Hexadecimal.
        i. A search for the ID can be run by adding either:
            1. `| grep "00 *12"`
    c. The SPAT message ID is 13.
        i. A search for the ID can be run by adding either:
            1. `| grep "00 *13"`
    d. Outputs will be similar to figure 37.

Changing Radio Settings

The radio settings may be changed in the obu.conf file. This file is located in the /mnt/rw/example1609/ directory. Before changes are made, rc.example1609 must be stopped.

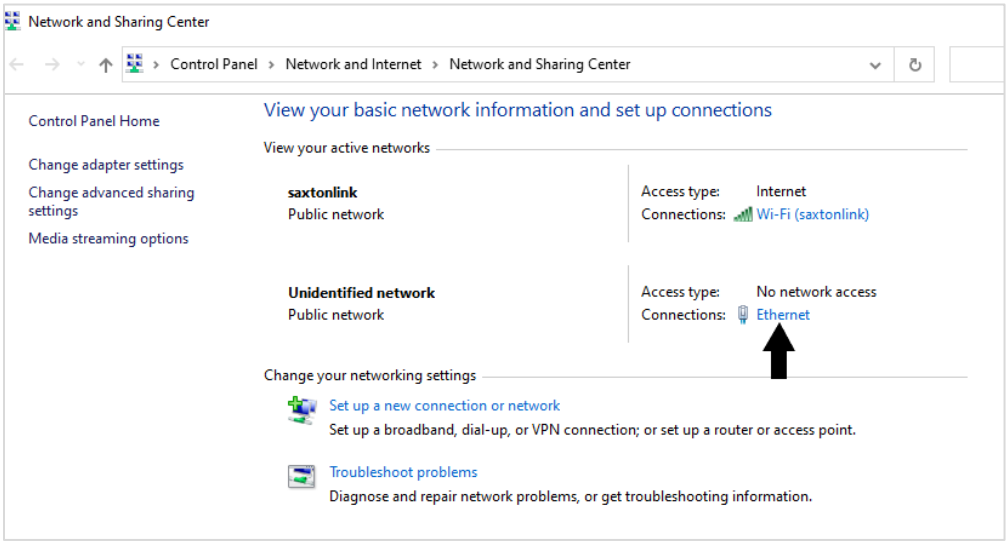
1. Stop example1609:
    a. `/opt/cohda/application/example1609/rc.example1609 stop`
2. Open the obu.conf file:
    a. `cd /mnt/rw/example1609/`
    b. `vi obu.conf`
3. Make changes to the file:
    a. Type `i` to insert characters.
    b. To cancel inserting, hit <Esc>.
    c. To exit file without saving:
        i. :q!
    d. To write and exit:
        i. :wq

Items Needed

- Savari MW1000 OBU.
- 12V DC Adapter.
- Lab Mobile DSCR/CV2X antenna.
- Tablet/Test PC.
- Ethernet Cable.

Basic Setup

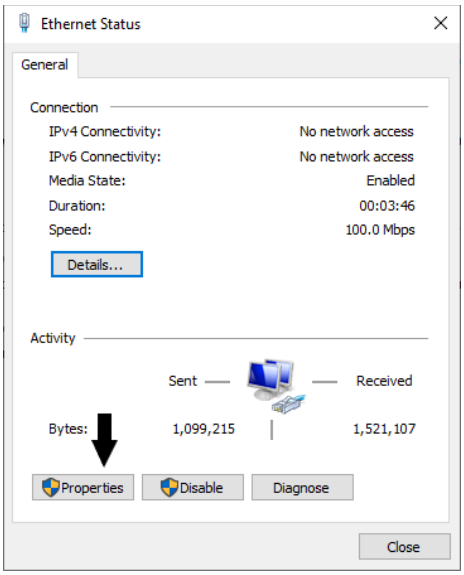
1. Using the tablet or an external computer, connect to the CradlePoint router using the WiFi SSID Info document.
2. If your mobile kit does not have a router, you may connect to the OBU via Ethernet. Otherwise, continue to step 7.
    a. Check your IP Address by opening **Network and Sharing Center** in Windows.
    b. Within that window, click on **Ethernet.**
    c. Refer to figure 38.



Source: FHWA.

Figure 34. Screenshot. Network and sharing center.

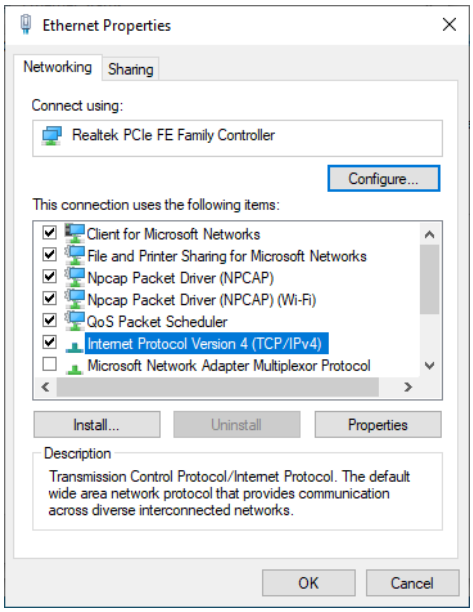
3. A new window will open. In that window, click on **Properties**. Refer to figure 39.



Source: FHWA.

Figure 35. Screenshot. Ethernet status.

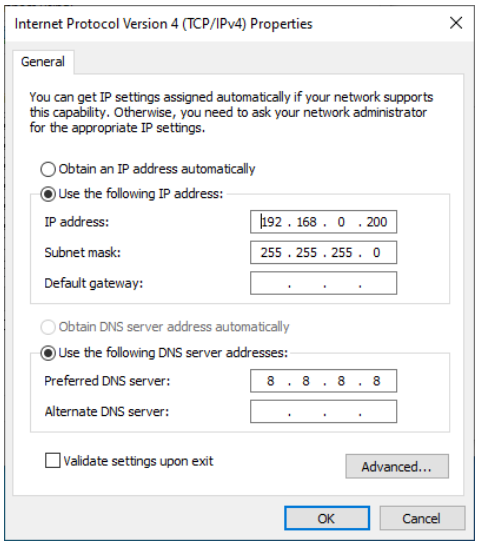
4. Within the Ethernet Properties window, double-click/open **Internet Protocol Version 4 (TCP/IPv4).**
    a. Refer to figure 40.



Source: FHWA.

Figure 36. Screenshot. Ethernet properties.

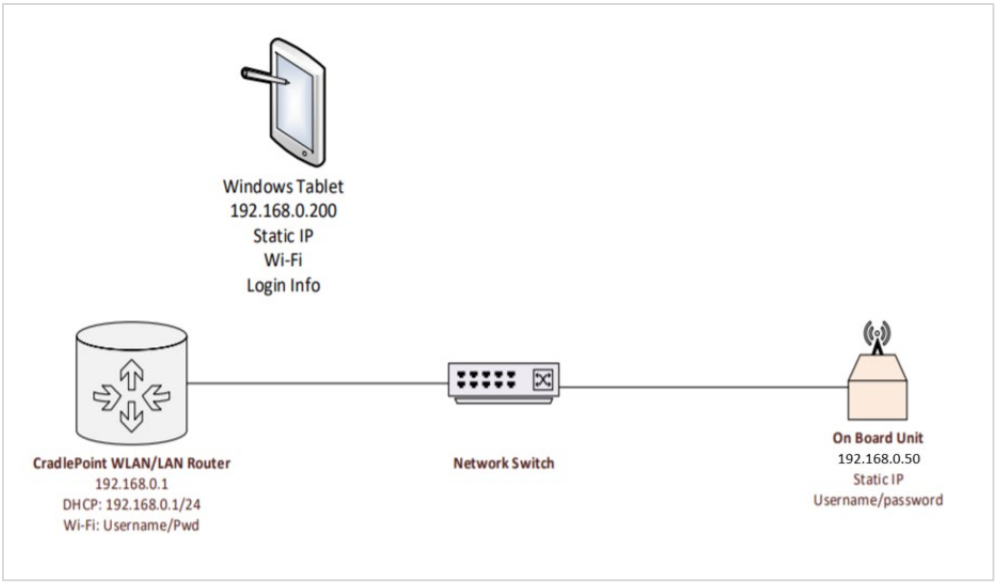
5. Ensure that **Use the following IP address** is selected. Input the same configurations as figure 41.



Source: FHWA.

Figure 37. Screenshot. IPv4 settings.

6. Click **OK** at the bottom of the window, then close all previous Windows.
7. Open a Terminal/Command Prompt.
    a. If using a tablet, you may not have access to a terminal. Skip to Step 9.
8. Attempt to `ping` each device within the Mobile Kit. Refer to figures 42 and 43.
    a. `ping 192.168.0.50`
    b. To stop ping process: <Ctrl>C.



Source: FHWA.

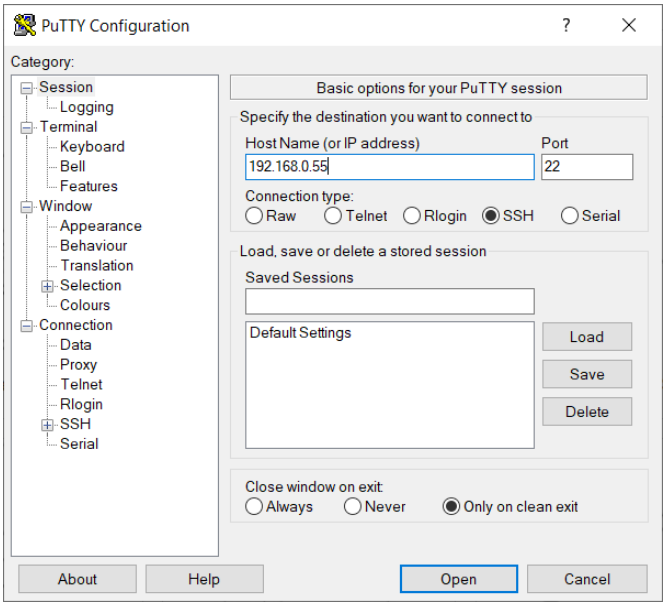
Figure 38. Diagram. Mobile kit network configuration.

```
pi@NanoPi-M4v2:~$ ping 192.168.0.55
PING 192.168.0.55 (192.168.0.55) 56(84) bytes of data.
64 bytes from 192.168.0.55: icmp_seq=1 ttl=64 time=21.9 ms
64 bytes from 192.168.0.55: icmp_seq=2 ttl=64 time=34.0 ms
64 bytes from 192.168.0.55: icmp_seq=3 ttl=64 time=12.8 ms
64 bytes from 192.168.0.55: icmp_seq=4 ttl=64 time=14.7 ms
^C
--- 192.168.0.55 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 12.870/20.901/34.069/8.328 ms
pi@NanoPi-M4v2:~$
```

Source: FHWA.

Figure 39. Screenshot. OBU ping output.

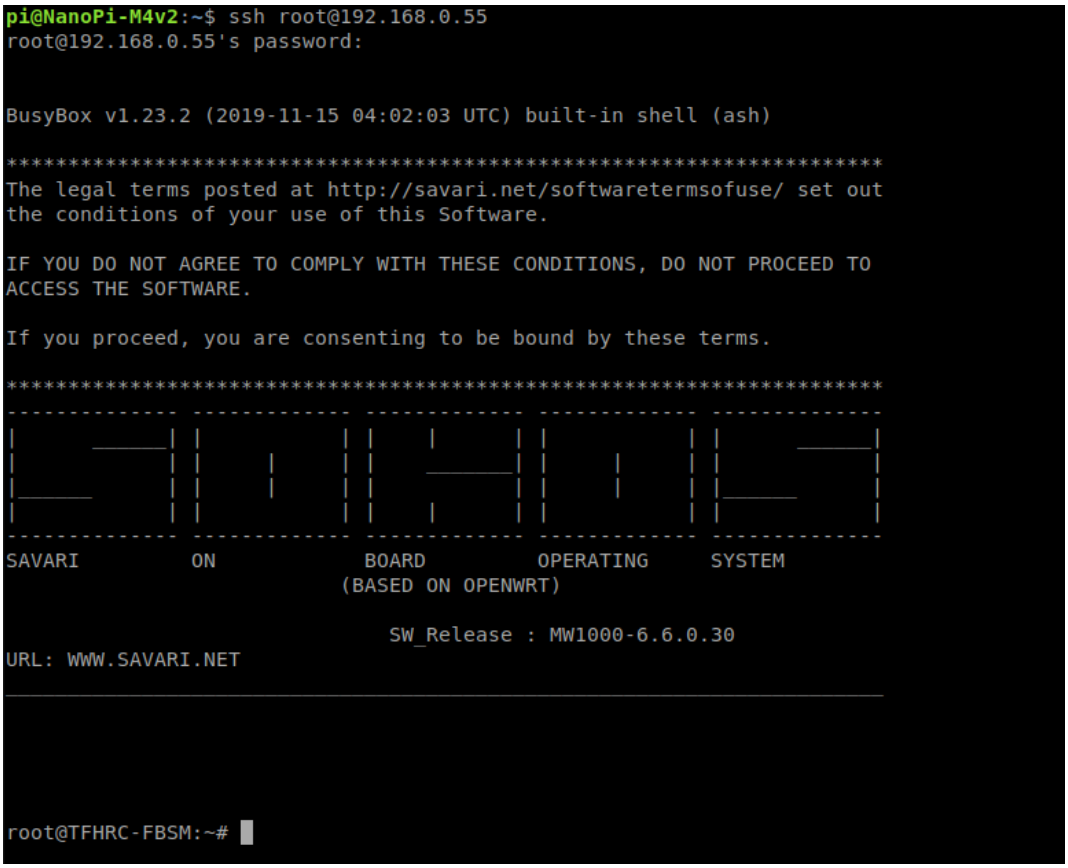
9. Using the acceptance checklist, mark off the box indicating correct IP/Port combinations.
10. If using a tablet, open **PuTTY**. Enter settings in the fields shown in figure 44 and click on **Open.**
    a. Use the password in step 11 to login to the OBU.
    b. **Note:** Please use 192.168.0.50 and 22



Source: FHWA.

Figure 40. Screenshot. PuTTY example settings.

11. To connect to OBU via terminal use:
    a. `ssh root@192.168.0.50`
    b. If prompted to continue connecting, enter: `yes`
    c. Password: `5@G3p9axINJA`
    d. Refer to figure 45 for example output.



Source: FHWA.

Figure 41. OBU SSH login example.

Testing GNSS Operation

1. Connect the antenna to the OBU.
    a. Make sure the GPS is connected to the blue fakra connection labelled as GPS in figure 46. The Lab Mobile antenna GPS connector is also blue.
    b. The other two can be connected in any order to DSRC1-1 and DSRC 1-2

Source: FHWA.

Figure 42. Photo. Savari OBU hardware setup.

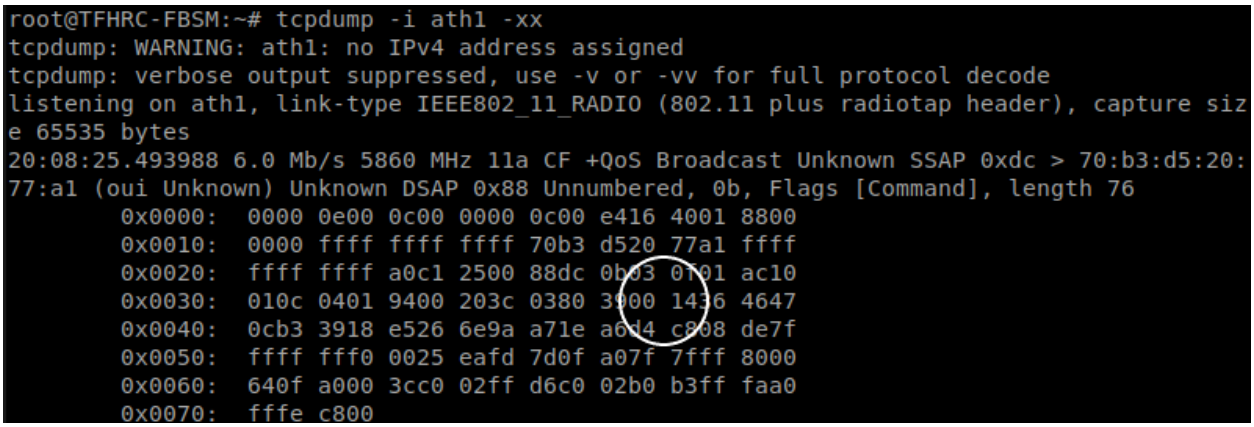
2. In order to send BSMs, GPS must first be established:
    a. To check for proper GPS signal, use:
        i. `date`
        ii. The output will be the current date. Refer to figure 47 for example output.
        iii. If date is not correct, move box to an area with better reception.

Source: FHWA.

Figure 43. Screenshot. GPS date output.

Testing BSM Transmission

1. To check for BSM transmissions, enter:
    a. `tcpdump – i ath1 –xx | grep "00 *14"`
    b. The BSM transmission ID is 0014 in Hexadecimal. The ID can be seen below.
    c. Refer to figure 48 for output.



Source: FHWA.

Figure 44. Screenshot. BSM transmitting output.

Items Needed

- CAVe-in-a-box w/ MK5 RSU.
- 5.9GHz antenna (2).
- GPS Antenna.
- Ethernet Cable.
- POE Injector.
- External PC.

Basic Setup

1. Attach all antennas per figure 49.
    a. Antennas are connected to the RSU via extension cables in the box.

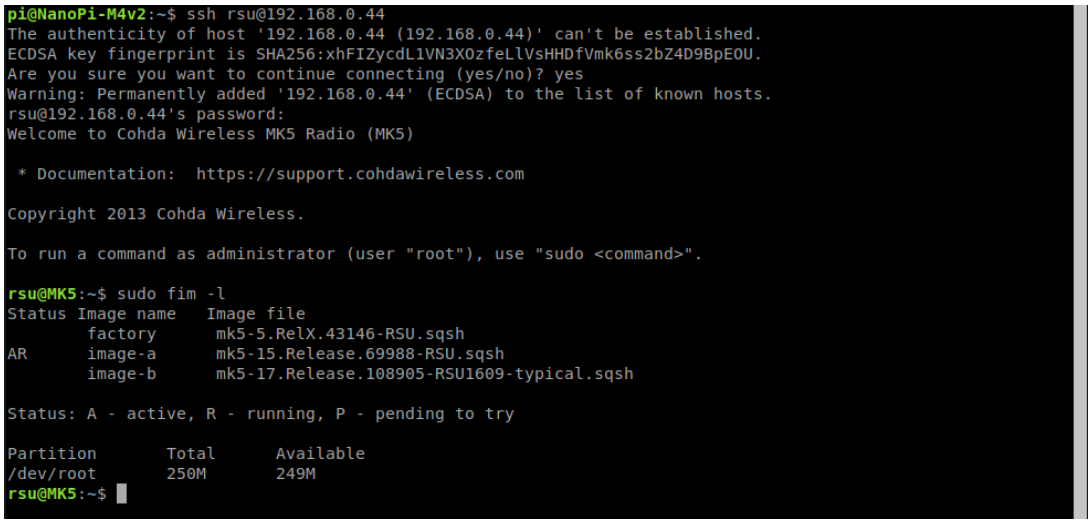
Source: FHWA.

Figure 45. Photo. External RSU setup.

2. Connect RSU to POE Injector via appropriate Ethernet cable.
    a. Connect POE Injector data output to Network Switch.
3. Connect PC to Network switch or Wireless Router.
4. Set the PC Ethernet/Wireless IPv4 configuration to:
    a. IP Address: 192.168.0.100
    b. Subnet Mask: 255.255.255.0
    c. Gateway: 192.168.0.1

Testing Operation

1. Open a Terminal and enter:
    a. `ssh rsu@192.168.0.40`
    b. If prompted to continue connecting, enter: `yes`
    c. Password: `rsuadmin`
    d. Refer to figure 48.
2. The Terminal is now logged into the MK5 RSU. Type:
    a. `sudo fim -l`
    b. Refer to figure 50 for the output.



Source: FHWA.

Figure 46. Screenshot. Checking MK5 RSU firmware.

3. The firmware should point with “AR” to mk5-15.Release.69988-RSU.sqsh or later
    a. Refer to figure 50 above.
4. To ensure GPS is running, enter:
    a. `date`
    b. The output should be the current date and time
    c. If date is not correct, move box to a location with better signal
5. To ensure Map and SPaT messages are being transmitted from the RSU, enter:
    a. `ifconfig`
    b. From the output, interfaces cw-mon-txa and cw-mon-txb will be seen.
    Note: MAP and SPAT must be forwarded to the RSU for it to transmit these messages.
    c. Refer to figure 51.

```
cw-mon-txa Link encap:UNSPEC  HWaddr 82-E7-05-0D-F9-3B-00-00-00-00-00-00-00-00-00-00
          UP RUNNING NOARP  MTU:2500  Metric:1
          RX packets:5443 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:870880 (870.8 KB)  TX bytes:0 (0.0 B)

cw-mon-txb Link encap:UNSPEC  HWaddr 6A-C5-DD-E2-00-57-00-00-00-00-00-00-00-00-00-00
          UP RUNNING NOARP  MTU:2500  Metric:1
          RX packets:5110 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1131270 (1.1 MB)  TX bytes:0 (0.0 B)
```

Source: FHWA.

Figure 47. Screenshot. Network interfaces output.

d. Run: `tcpdump –i cw-mon-txb –xx | grep "00 *13"`
e. Stop the process with <Ctrl>c.
f. Refer to figure 52 for output.

```
root@MK5:/opt/cohda/application/rsu1609# tcpdump -i cw-mon-txb -xx | grep "00 13"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on cw-mon-txb, link-type IEEE802_11_RADIO (802.11 plus radiotap header), capture size 262144 by
tes
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x01d0:  0500 0040 0000 13e1 74d0 1414 9916 5540
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x01d0:  0500 0040 0000 13e1 74d0 1414 9916 5540
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
        0x0050:  0401 9400 8002 6200 135f 0038 1b1e 1ed9
```

Source: FHWA.

Figure 48. Screenshot. Observing SPaT message transmission.

g. Run: `tcpdump –i cw-mon-txb –xx | grep "00 *12"`
h. Stop the process with <Ctrl>c
i. Refer to figure 53 for output.

```
root@MK5:/opt/cohda/application/rsu1609# tcpdump -i cw-mon-txb -xx | grep "0012"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on cw-mon-txb, link-type IEEE802_11_RADIO (802.11 plus radiotap header), capture size 262144 by
tes
        0x0050:  0401 9400 8002 81ad 0012 81a9 3803 3020
        0x0050:  0401 9400 8002 81ad 0012 81a9 3803 3020
        0x0050:  0401 9400 8002 81ad 0012 81a9 3803 3020
```

Source: FHWA.

Figure 49. Screenshot. Observing MAP message transmission.

Before continuing to the BSM section, BSM forwarding on the RSU must be set up. This is called WSM Forwarding and is generally set up automatically with a script. Settings may be checked:

```
cd /mnt/rw/rsu1609/conf
cat user.conf
```

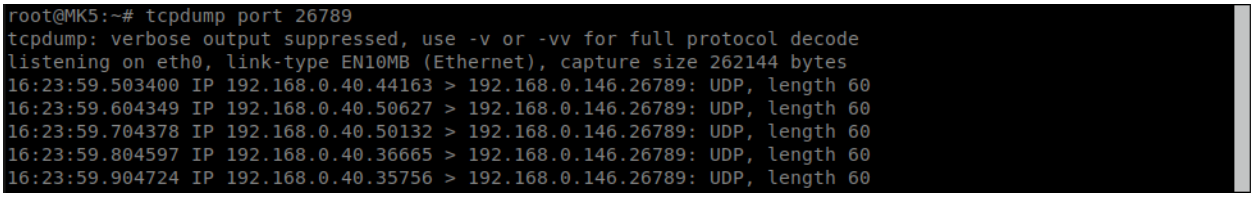
Additional radio setting may be checked:

```
cd /mnt/rw/rsu1609/conf
cat stack.conf
```

Verify forwarding BSM and Mobility messages are forwarded:

```
tcpdump port 26789
```

Refer to figure 54 for output.



Source: FHWA.

Figure 50. Screenshot. RSU forwarding BSM.

USDOT's ISD Message Creation Tool

Using the Intersection Situation Data (ISD) Message Creation Tool requires internet access. It is recommended to use the tool on an external computer. Created MAP files will need to be transferred to the V2X Hub computer. Either a USB, ethernet connection, or wireless connection to kit's router may be used to transfer file.

1. Navigate to the address where the ISD message would be created (refer to figure 55).

Source: USDOT.

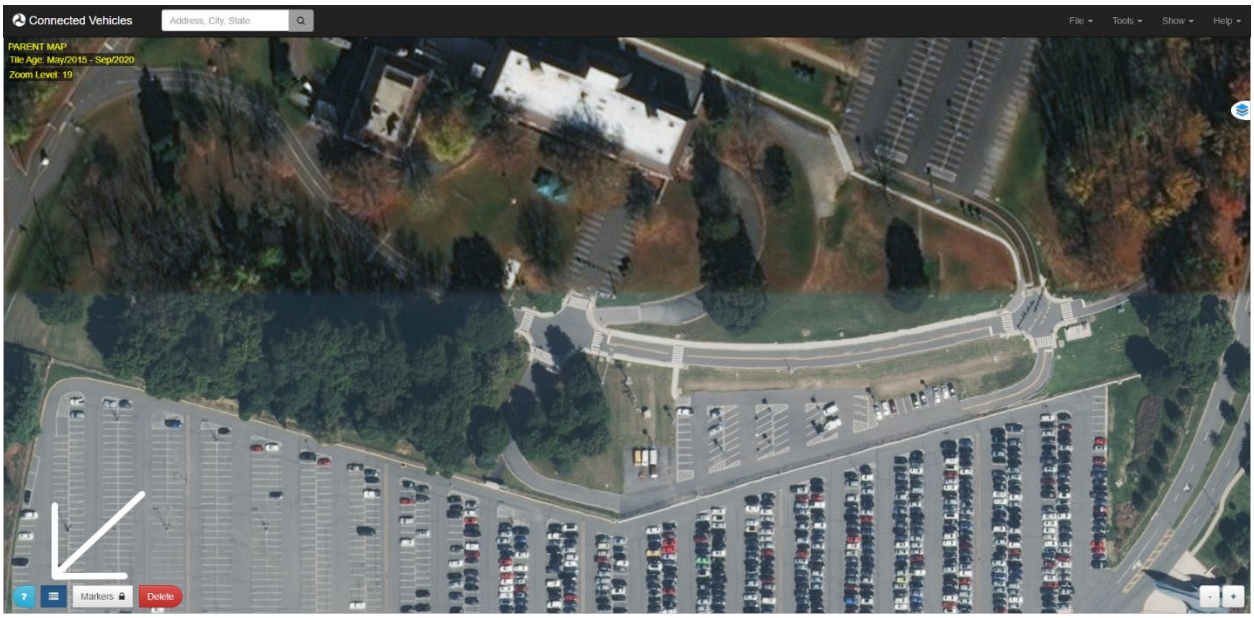
Figure 51. Screenshot. Address Navigation

2. From the top navbar, go to **New Parent Map** to enter parent map editing mode (refer to figure 56).

Source: USDOT.

Figure 52. Screenshot. New Parent Map

3. Select the **Builder** icon to bring up the builder menu (refer to figure 57). In the **Intersection** tab, you should see the two intersection options, including the **Reference Point Marker** (refer to figure 58).



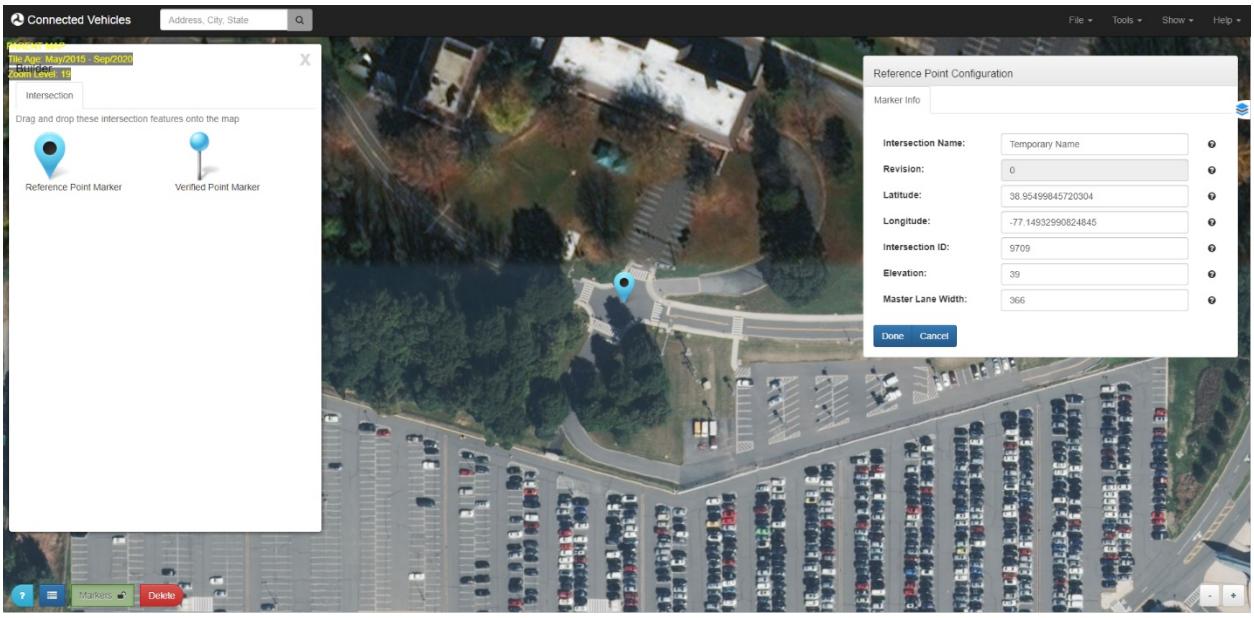
Source: USDOT.

Figure 53. Screenshot. Builder icon.

Source: USDOT.

Figure 54. Screenshot. Reference point marker.

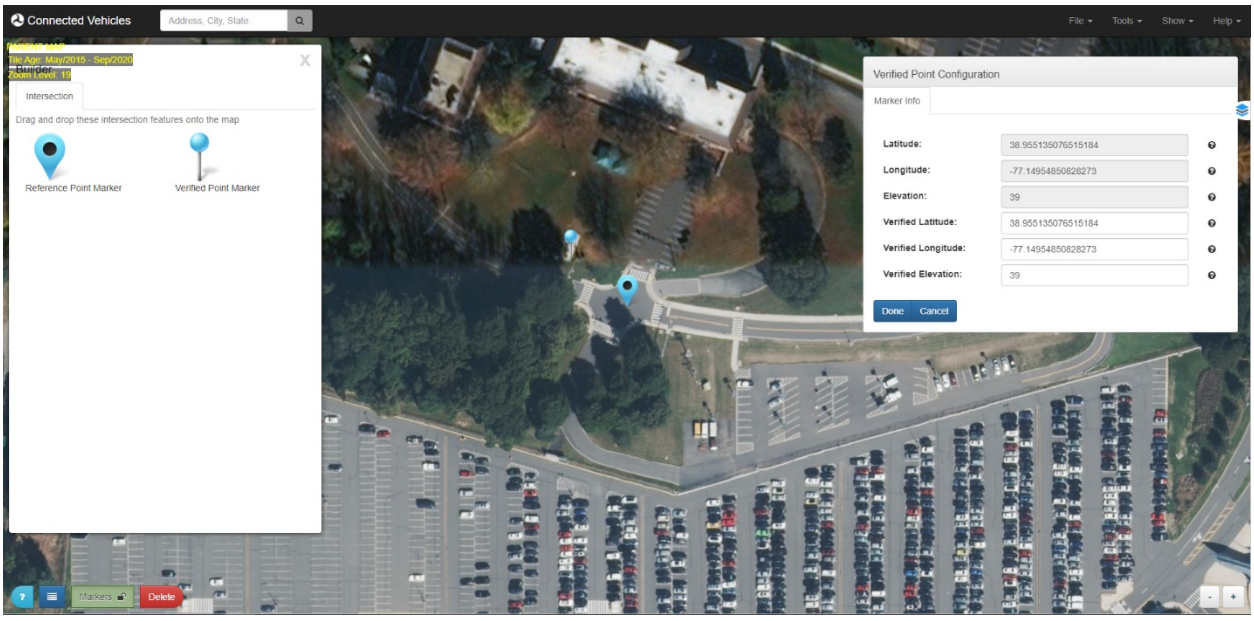
4. Click and drag a reference point marker to the **center of your intersection**. You can only place one reference point per message.
    - Note that the **Markers** Control becomes enabled once the marker is placed (refer to figure 59).
    - You may drag around the marker after being placed to tweak its location.
    - Click on the marker to open and close the **Configuration** dialog. From here you can view its Latitude, Longitude, Elevation, and other variables.
    - You may toggle the control back off or click **Done** once you are finished tweaking the location of the marker to lock it place.



Source: USDOT.

Figure 55. Screenshot. Marker configuration dialog.

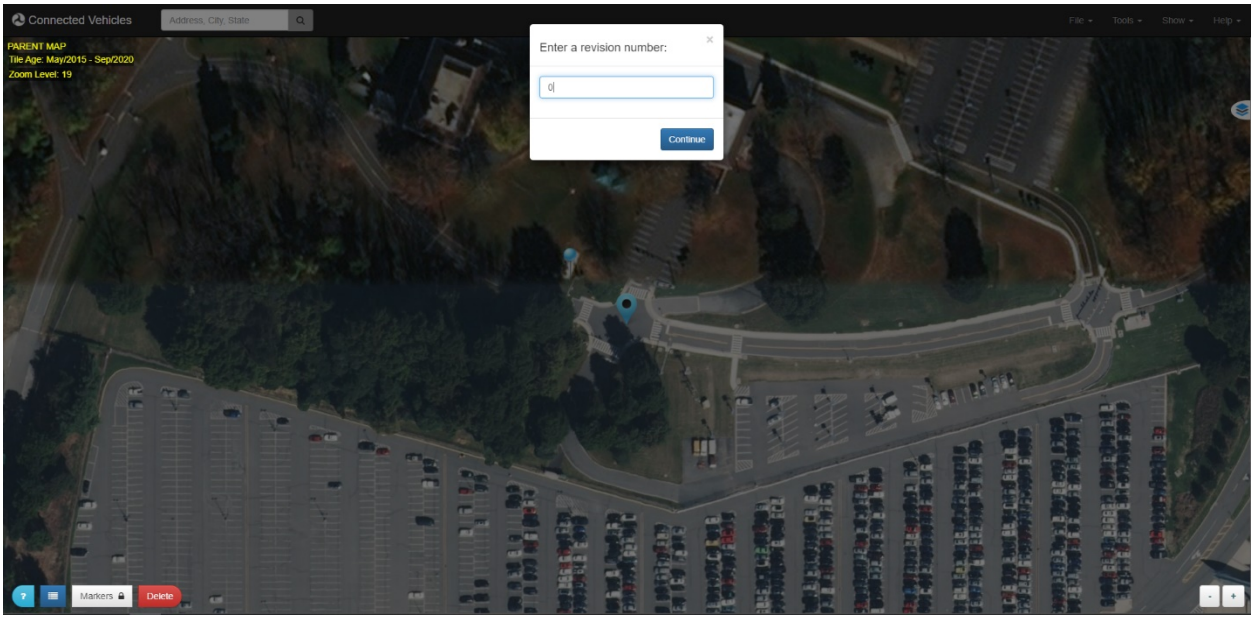
5. Click and drag the **Verified Point Marker** to a known, surveyed location on the map.
   - Click on the marker to open up the **Configuration** dialog (refer to figure 60). You can view the location of the marker on the map, as well as view and modify the verified location of the marker.
   - Check the verified marker information and edit as necessary. Click **Done** when finished.



Source: USDOT.

Figure 56. Screenshot. Verified point configuration.

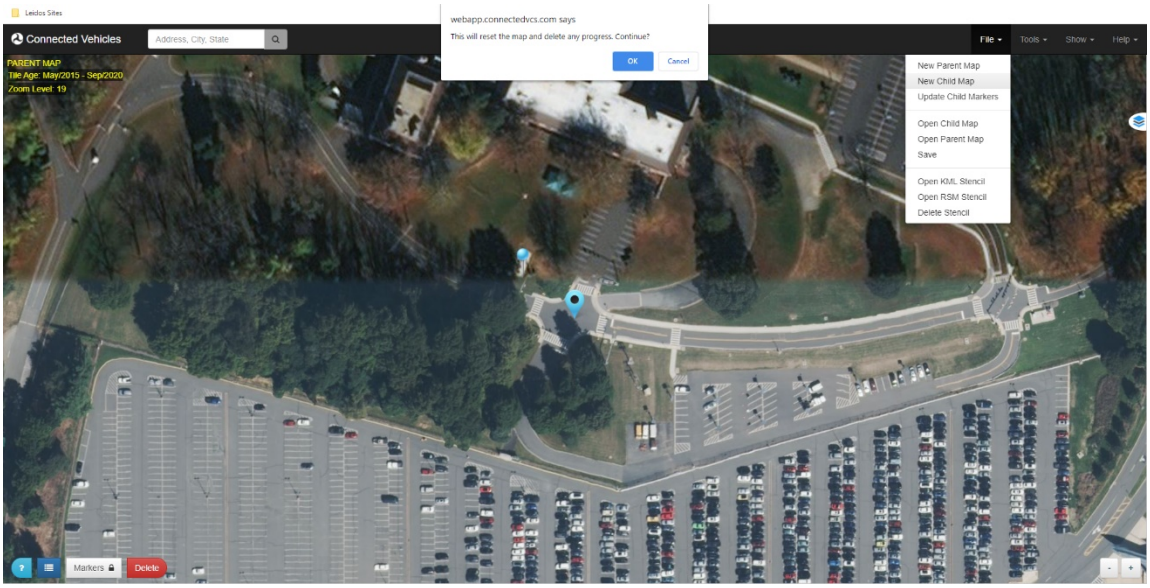
6. Close the **Builder** once you are finished placing the two markers.
7. Go to **File** then **Save** and enter your revision number (refer to figure 61).



Source: USDOT.

Figure 57. Screenshot. Setting revision number.

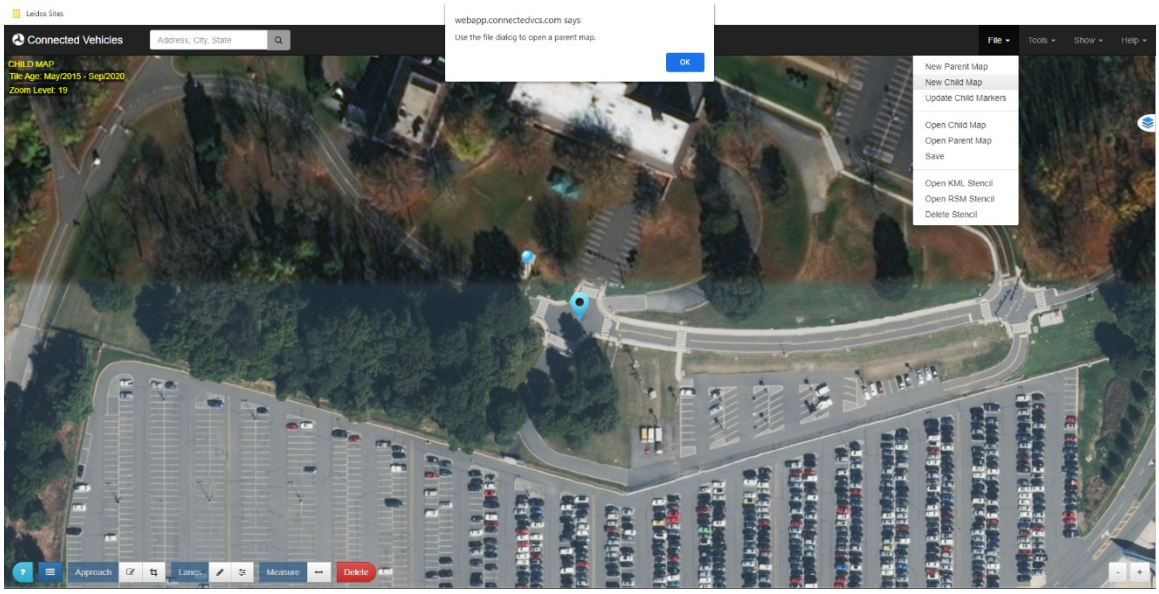
8. Save file and continue to create a **New Child Map** in the file menu. Selecting new child map will bring up a dialog box. Click **OK** if your parent map has been saved (refer to figure 62).



Source: USDOT.

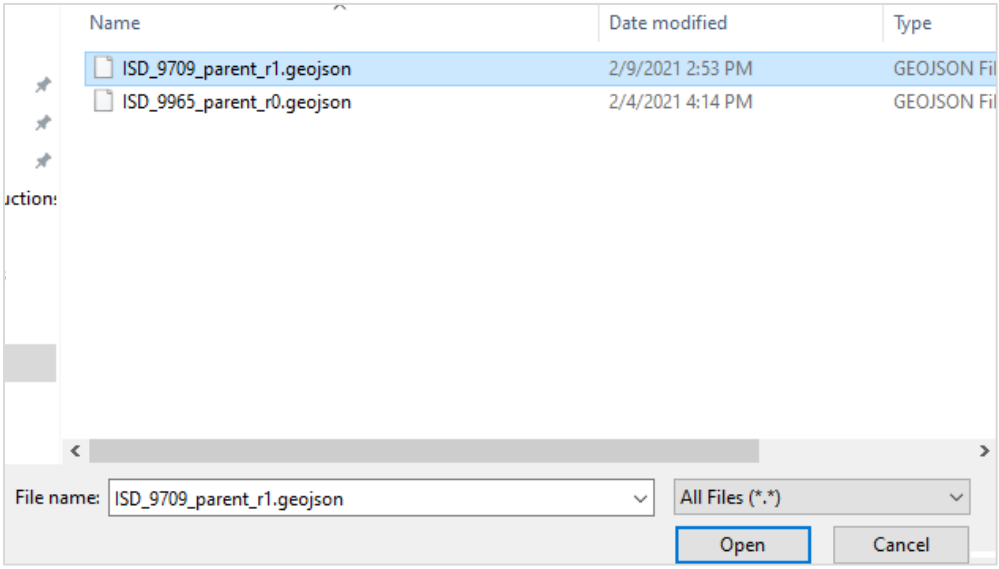
Figure 58. Screenshot. New child map.

A second dialog box will direct to opening a parent map, which is used to build the child map (refer to figure 63). Select the saved parent map and open (refer to figure 64).



Source: USDOT.

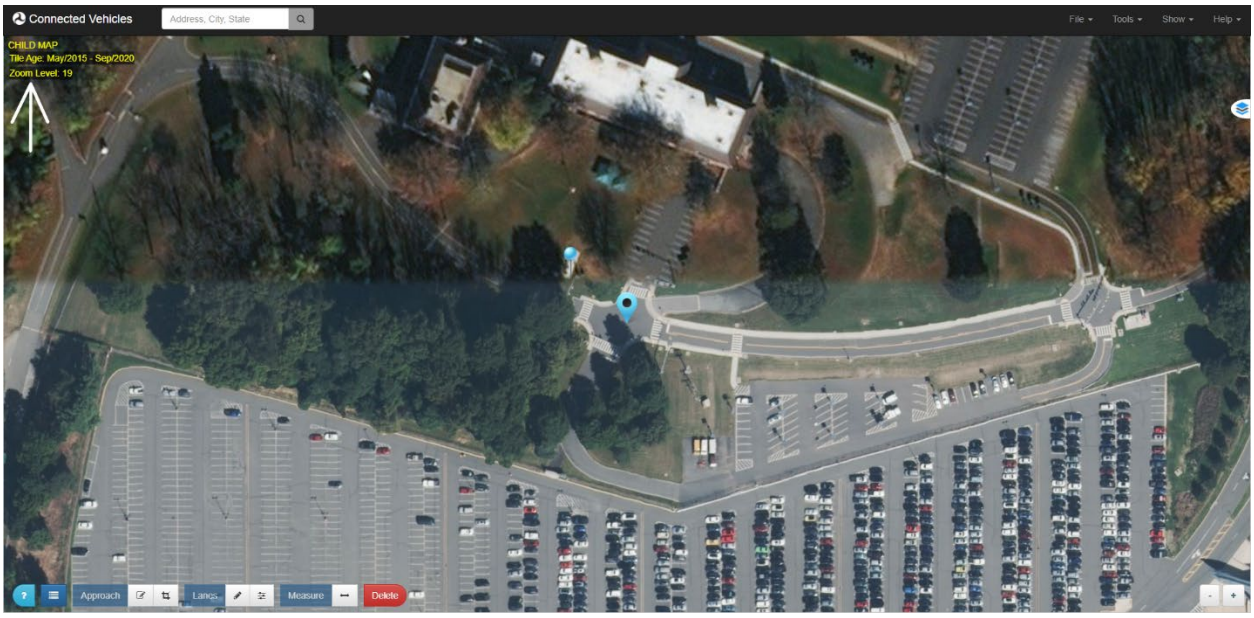
Figure 59. Screenshot. New child map.



Source: USDOT.

Figure 60. Screenshot. Selecting parent map.

9. Once opened, the information from the parent map will be imported to the new child map (refer to figure 65).



Source: USDOT.

Figure 61. Screenshot. New child map.

Defining the Region

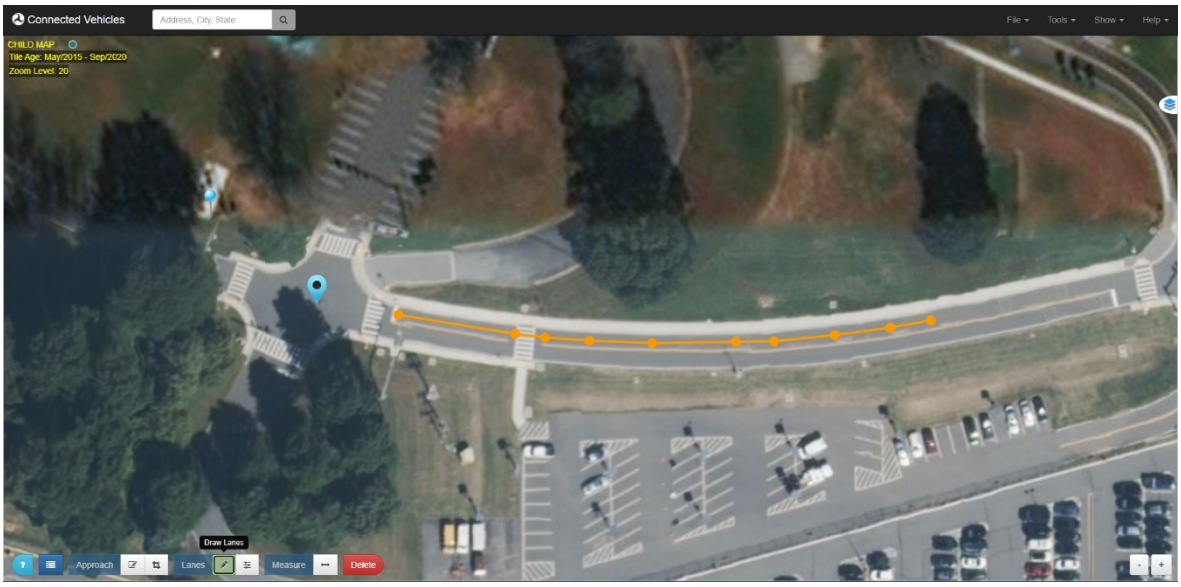
1. Toggle ON the **Draw Lane** control from the bottom Control Panel. A lane region is started from the STOP bar, down the center of the lane, until about 1000 feet away from the intersection. Single click to drop points, double click to stop drawing. (refer to figures 66, 67, 68).

Source: USDOT.

Figure 62. Screenshot. Draw Lane

Source: USDOT.

Figure 63. Screenshot. Draw lane in progress.



Source: USDOT.

Figure 64. Screenshot. Completed lane.

2. Ingress lanes are marked from the beginning of the STOP bar and egress lanes are marked from the beginning of the CROSSWALK (refer to figure 69).

Source: USDOT.

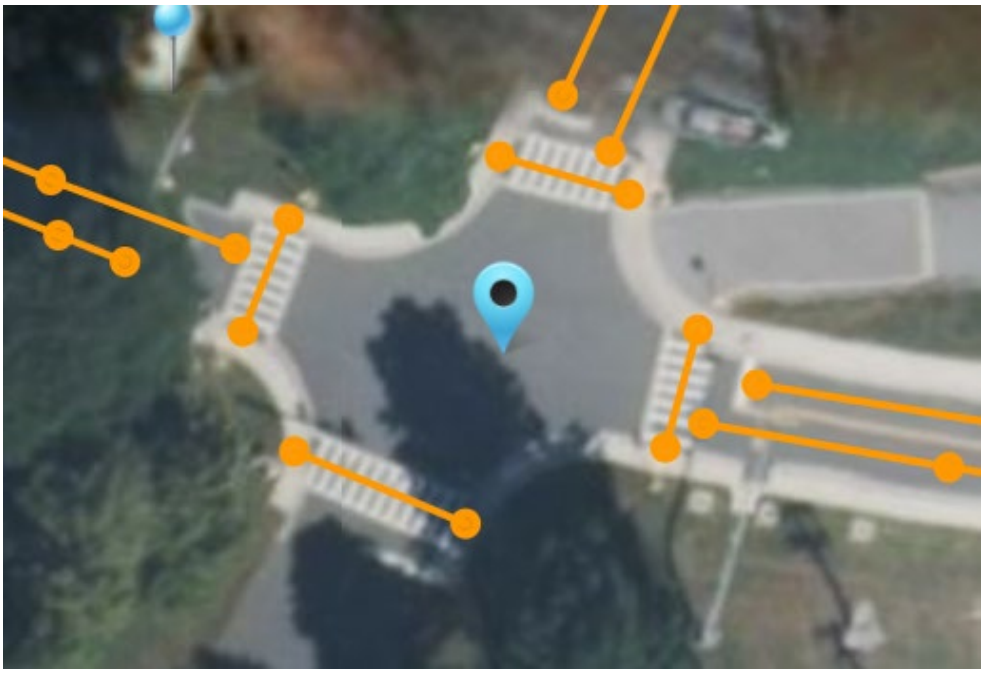
Figure 65. Screenshot. Ingress and egress lanes.

3. Lanes can be edited using the **Edit Lanes** button at the bottom of the screen. Selected lane will show markers, which can be moved (refer to figure 70).

Source: USDOT.

Figure 66. Screenshot. Edit lanes.

4. Crosswalks are marked using the same **Draw Lanes** tool (refer to figure 71).



Source: USDOT.

Figure 67. Screenshot. Drawing crosswalks.

5. An approach is drawn by selecting the **Draw Approaches** tool at the bottom of the screen. Click and drag across a region to draw (refer to figure 72).

Source: USDOT.

Figure 68. Screenshot. Drawing an approach.

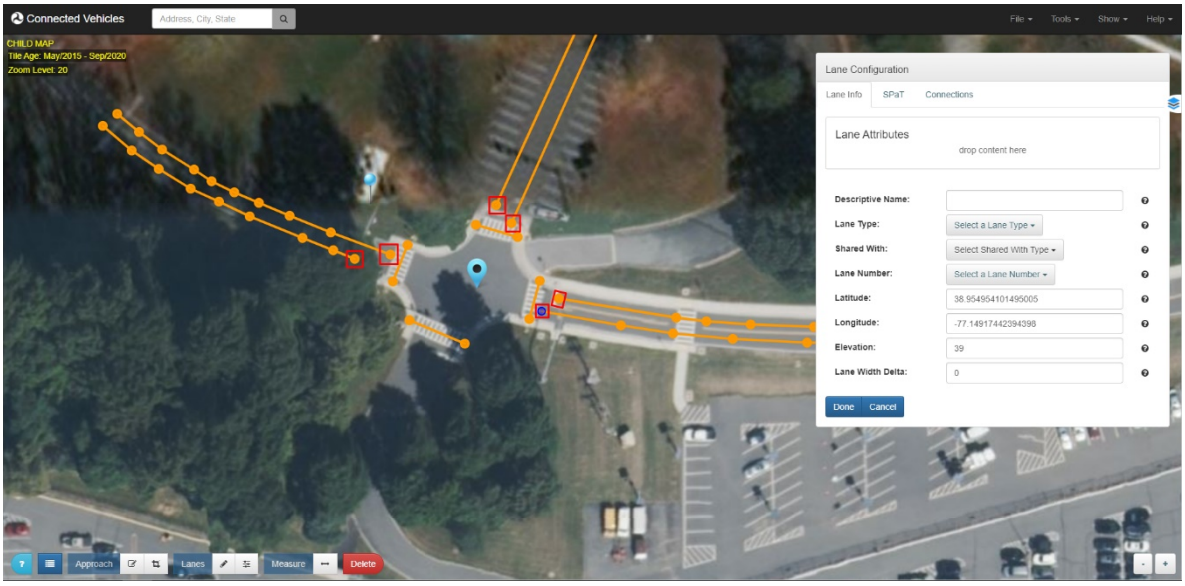
6. Approaches can be edited by selecting the **Edit Approaches** tool at the bottom of the screen. Clicking on an approach will allow you to move and adjust the approach (refer to figure 73).

Source: USDOT.

Figure 69. Screenshot. Editing an approach.

7. Feel free to save the maps at any time. This way, previous revisions can be accessed if desired.

8. Lane configurations can be updated by clicking on the **first node** drawn at each lane (refer to figure 74).



Source: USDOT.

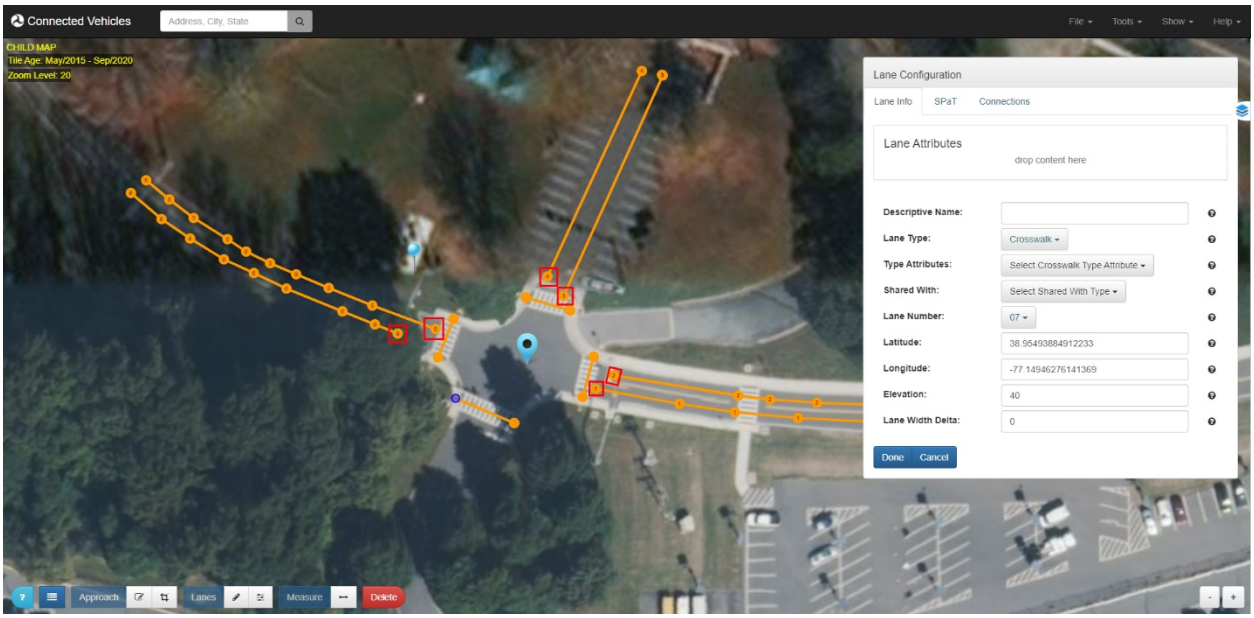
Figure 70. Screenshot. Lane configuration.

9. Set the **Lane Type** and **Lane Number** for each node in the intersection (refer to figure 75).

Source: USDOT.

Figure 71. Screenshot. Lane configuration.

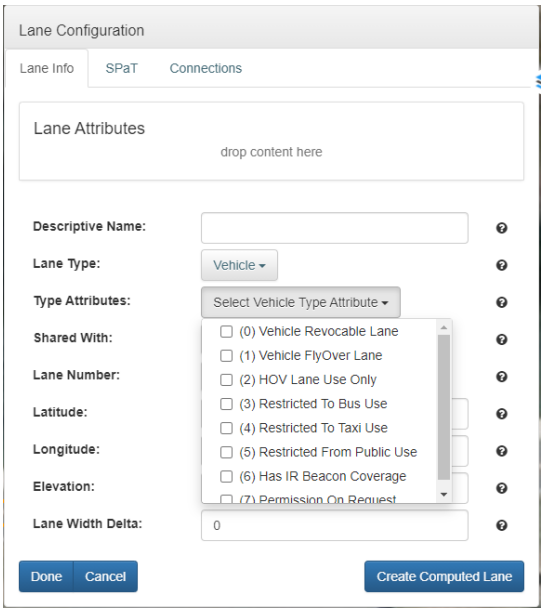
10. Crosswalks can be set and numbered as well (refer to figure 76).



Source: USDOT.

Figure 72. Screenshot. Crosswalk configuration.

11. **Type Attributes** and **Shared With** can be selected if needed for a specific lane in the lists (refer to figure 77).



Source: USDOT.

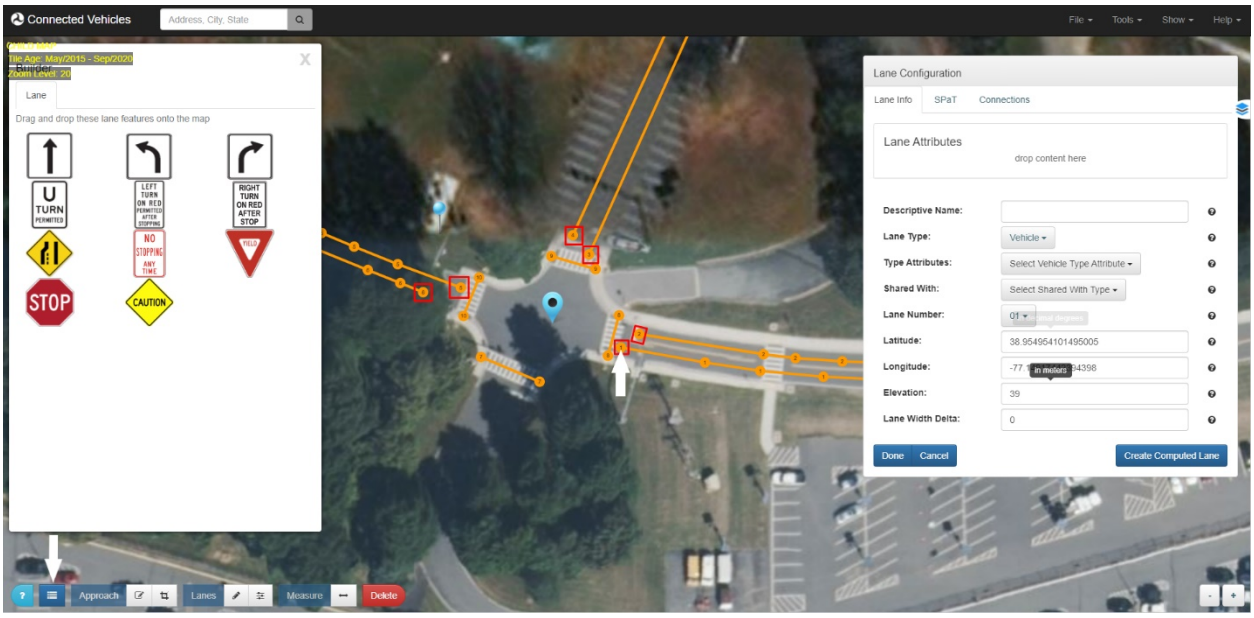
Figure 73. Screenshot. Additional lane configurations.

12. **Approach Configurations** are added by clicking on each approach border (refer to figure 78). This allows the user to set the approach as either an Ingress, Egress, Both, or None.

Source: USDOT.

Figure 74. Screenshot. Approach configurations.

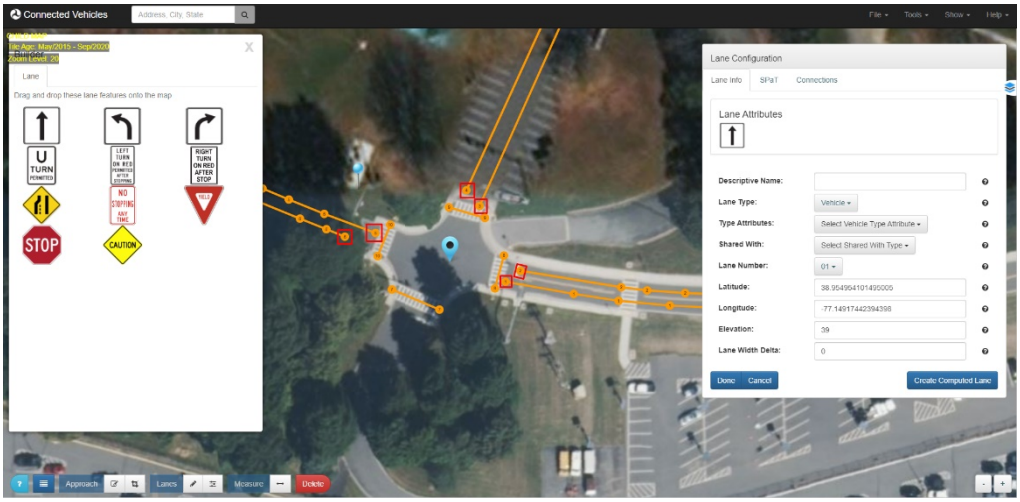
13. In order to define how the lanes and crosswalks interact, the **Lane Attributes** must be edited. Select a lane node to open the **Lane Configuration** window, then open the **Builder** tool (refer to figure 79).



Source: USDOT.

Figure 75. Screenshot. Lane attributes.

14. When both windows are open, a **Lane Feature** can be drag-and-dropped to the **Lane Attributes** section in the Lane Configuration window (refer to figure 80).

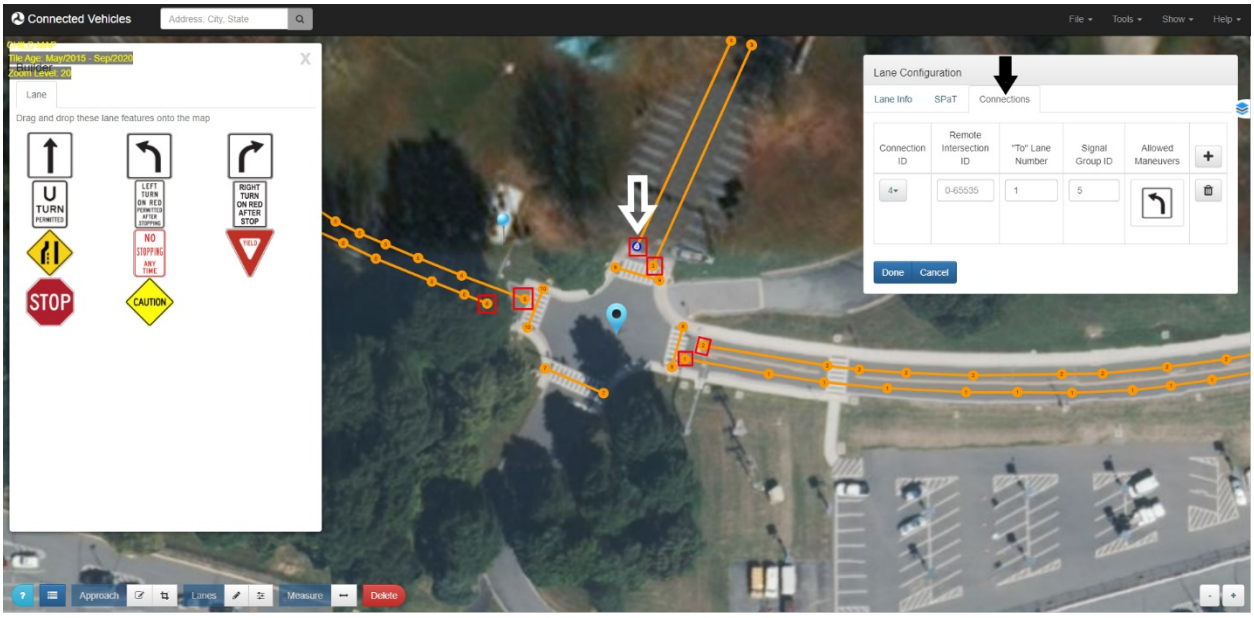


Source: USDOT.

Figure 76. Screenshot. Lane attributes.

15. Another method for assigning lane attributes can be done using the **Connections** tab. Here, a lane-to-lane connection through the intersection can be specified. The IDs in this tab are specified by the particular intersection's traffic signal controller configurations.

    A left turn connection example from **Lane 4 to Lane 1** is shown (refer to figure 81).



Source: USDOT.

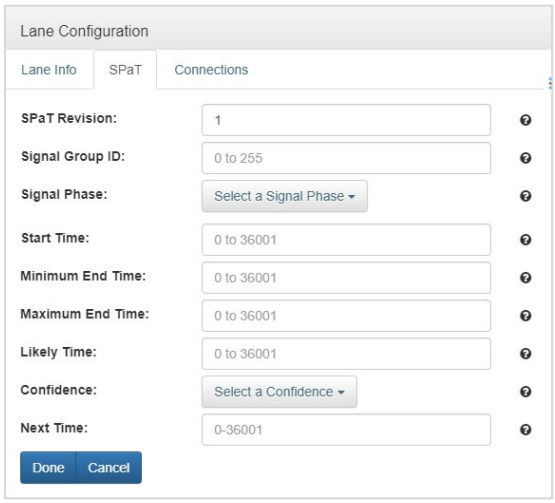
Figure 77. Screenshot. Left turn attribute.

16. Once the connection is made and **Done** is selected, a connection on the map can be seen when the approach is selected (refer to figure 82).
    a. All lanes are configured individually.

Source: USDOT.

Figure 78. Screenshot. Added left turn attribute.

17. The final lane configuration is the SPaT tab. Here, you can input all the SPaT information for each lane (refer to figure 83). This is optional, however, and not covered in this MAP-specific tutorial.



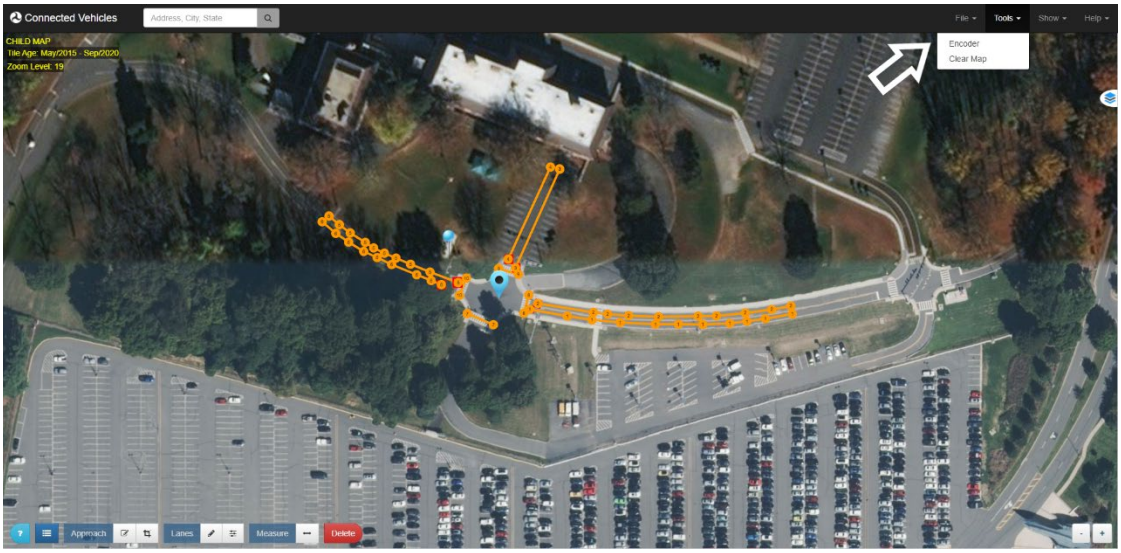
Source: USDOT.

Figure 79. Screenshot. SPaT configurations.

Finish and Encode or Deposit

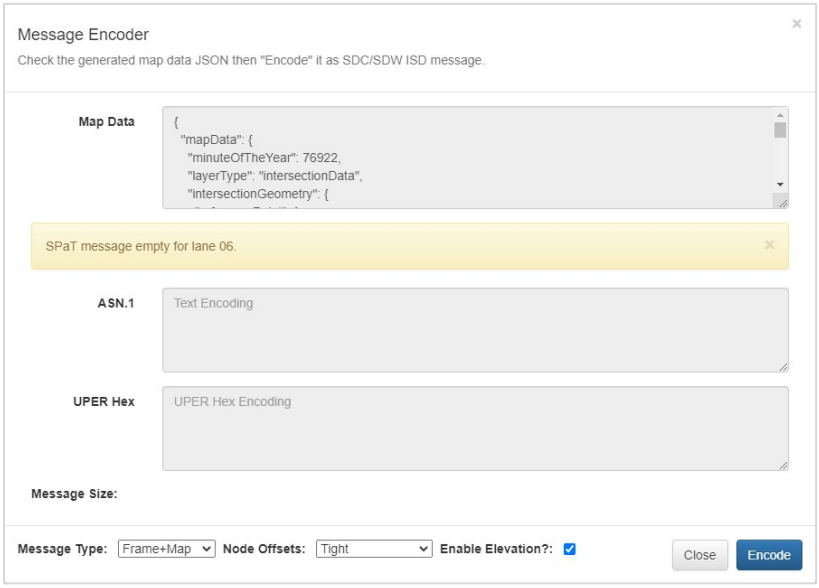
Encode your ISD message to the intersection once you are finished building it.

1. Open Encode/Deposit dialog
   a. Click on **Tools Encode** to load the deposit window (refer to figure 84). Unless there are errors, a JSON message should already be generated from the map data. Its contents will appear in the **Message** text box (refer to figure 85).
   b. Verify the contents of the message.



Source: USDOT.

Figure 80. Screenshot. Open Encode/Deposit window



Source: USDOT.

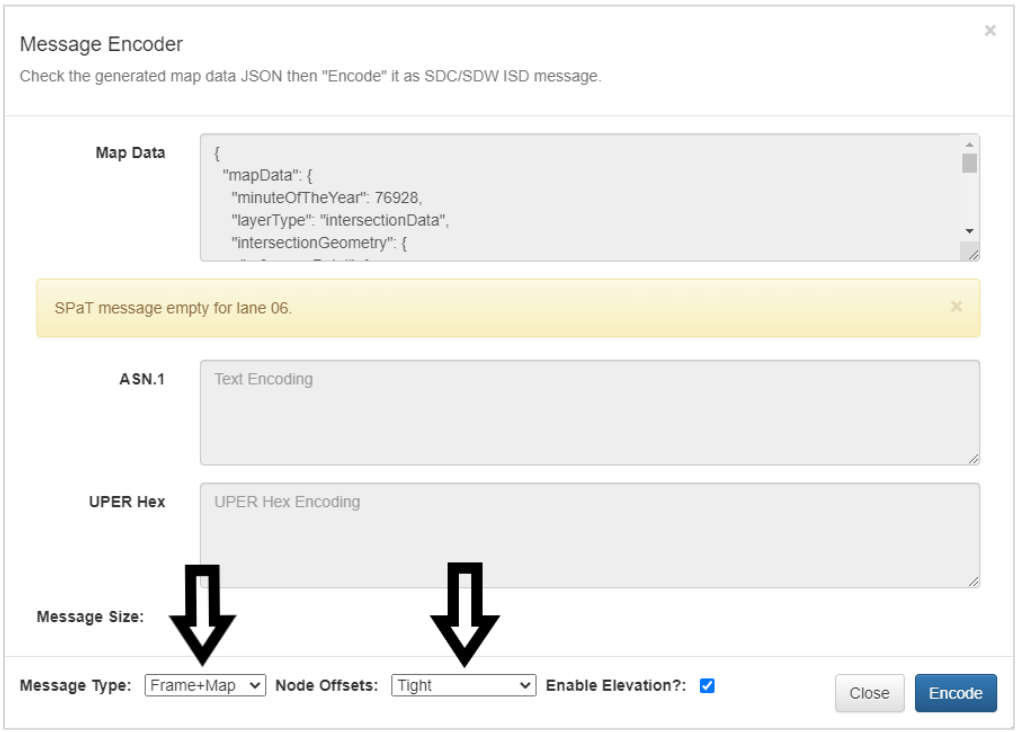
Figure 81. Screenshot. Message Deposit Window.

2. Select desired Message Type (refer to figure 86)

    a. **ISD** – ISD Safety Message
    b. **Map** – Raw map contents
    c. **Frame+Map** – SAE J2735 Message Frame message with MAP contents
    d. **SPaT** – If SPaT sample data is included in the map message
    e. **Frame+SPaT** – SAE J2735 Message Frame message with SPaT contents
    f. **SPaTRecord** – SPaT Record portion of ISD message

3. Select desired nodes offsets encoding (in the descending order of the message size)

    a. **Tight** - uses the absolute minimal SAE J2735 Node-XY-?? offset value encoding for each node (refer to figure 86)



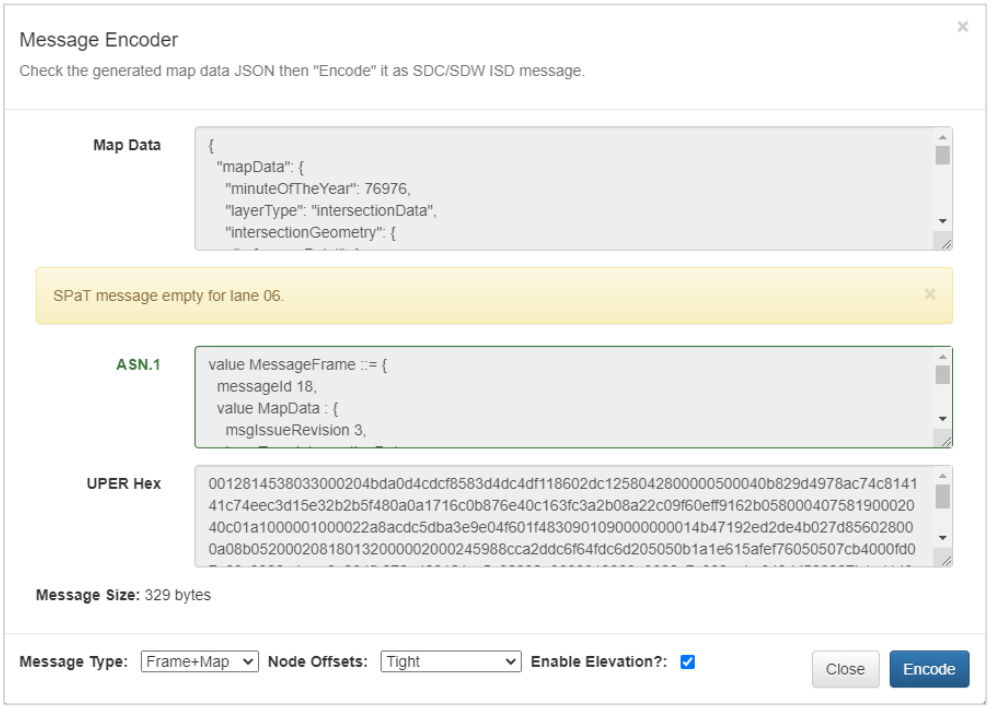
Source: USDOT.

Figure 82. Screenshot. Message type and node offsets.

4. Encode the MessagePress the **Encode** button to generate the UPER encoding (refer to figure 87)

    b. The **Hex** text area box will display the hex encoded message if successful, or an error message if unsuccessful.
    c. The **ASN.1** text area box will display the ASN.1 encoded message if successful, or an error message if unsuccessful.
    d. Note that although the cursor in all text areas is the prohibition sign, because the text areas are read-only, you can select the content of any text area and copy it via standard shortcut keys or a

context menu available on the right-click. The easiest way to copy all content from a text area is to click in the text area and then type Ctrl-A to select all lanes and Ctrl-C to copy to clipboard.



Source: USDOT.

Figure 83. Screenshot. Frame+Map encoded message.

5. When encoding as Frame+Map or Map, the Hex text area will output the UPER encoded SAE J2735 payload for broadcast. This payload must be copied an edited to be used with V2X Hub.
6. Copy and paste the payload into a text editor and **delete** the first 4 octets (8 characters).
   a. Example: 00128145
7. Save the file with a name for your intersection.
   a. Example: MAP_9709_UPER.txt

References

United States Department of Transportation. 2019. *ISD Builder Tool for J2735 3/2016* (software). Version 2.3.1. https://webapp.connectedvcs.com/isd/