CohdaWireless™

www.cohdawireless.com

User Manual

ISO12207

Roadside Unit 1609

Issue Date:	9 February 2018
Version:	10.9.0
Document No:	CWD-P0162-RSU-USRM-WW01-518
Prepared for:	Cohda Wireless Pty Ltd.
Prepared by:	Troy Tobin / Senior Software Engineer Clark Li / Software Engineer
Authorised By:	Max Tykesson / Senior Project Manager
Distribution:	External
Template Version No:	1.0.0
Template Issue Date:	02/03/14

This document is offered in confidence and may not be used for any purpose other than that for which it is supplied.

ABN 84 107 936 309

Cohda Wireless Pty Ltd
82-84 Melbourne Street
North Adelaide, SA 5006 Australia

P +61 8 8364 4719
F +61 8 8364 4597

www.cohdawireless.com

Table of Contents

1 Scope

1.1 Identification

This Software User Manual (SUM) applies to the "***Roadside Unit (RSU) 1609***" software which is developed and is maintained at Cohda Wireless Pty Ltd. located in Adelaide, South Australia.

The software is aimed at supporting the US DOT DSRC Roadside Unit Specification. The US DOT DSRC Roadside Unit Specification has recently undergone an update from version 4.0 [2] to version 4.1 [1]. The current RSU 1609 software package is largely based on version 4.0 of the specification with select updates to the version 4.1 of the specification. In particular, these updates include Active Message SNMP support and IEEE1609 2016 standard WSA support.

The software is packaged as a single image that contains the full MK5 filesystem including the RSU application software. It is named by the following convention.

mk5-5.<release-base>.<version>-<configuration>-RSU.img

1.2 System Overview

The Roadside Unit (RSU) software is an application that runs on MK5 Cohda Wireless DSRC radios. The software is used to:

- Broadcast SAE J2735 messages over the DSRC radio
- Receive Wave Short Messages (WSM)
- Route and forward IPv6 traffic for connected mobile units
- Provide SNMP device management

1.3 Document Overview

This document provides a brief step-by-step guide to the Roadside Unit software. It details the applications' installation and execution.

The remainder of this document is organized into the following sections:

Section 2 (Referenced documents) – This section provides identification of all documents referenced by this document.

Section 3 (Software summary) – This section provides a brief description of the intended uses of the software.

Section 4 (Access to the software) - This section contains step-by-step procedures oriented to the first time/occasional user.

Section 5 (Processing reference guide) – This section provides the user with procedures for using the software.

Section 6 (Notes) - This section contains any general information that aids in understanding this document.

2 Referenced Documents

[1] US DOT Federal Highway Administration, *DSRC Roadside Unit (RSU) Specifications Document v4.1*, US DOT Federal Highway Administration, 2016.

[2] US DOT Federal Highway Administration, *DSRC Roadside Unit (RSU) Specifications Document v4.0*, US DOT Federal Highway Administration, 2014.

[3] “Net SNMP,” [Online]. Available: http://www.net-snmp.org/. [Accessed 13 January 2016].

[4] “UncomplicatedFirewall,” [Online]. Available: https://wiki.ubuntu.com/UncomplicatedFirewall. [Accessed 13 January 2016].

[5] Cohda Wireless, “Roadside Unit (US DOT V4.0) Quick Start Guide,” 2016.

3 Software Summary

3.1 Software Application

The Roadside Unit software is an application that runs on the MK5 Cohda Wireless DSRC radio. The software is aimed at supporting the US DOT DSRC Roadside Unit Specification.

3.2 Software Inventory

The software is packaged as a full MK5 filesystem that includes the RSU application software. The core RSU file inventory is as follows:

```
/opt/cohda/application/
├── rc.local
└── rsu1609
    ├── ieeeAcfGenerator
    ├── acfInfo
    ├── aerolink
    │   ├── certificates
    │   │   ├── ieee-v3-demo-pca.cert
    │   │   ├── ieee-v3-demo-pca.signKey
    │   │   ├── ieee-v3-demo-root.cert
    │   │   ├── ieee-v3-demo-root.signKey
    │   │   ├── RSU-20170614.acf
    │   │   └── WSA-20170614.acf
    │   ├── etc
    │   │   └── aerolink
    │   │       ├── aerolink.conf
    │   │       └── security-profile
    │   │           ├── crl.prof
    │   │           ├── map.prof
    │   │           ├── spat.prof
    │   │           ├── tim.prof
    │   │           └── wsa.prof
    │   ├── revoked_certs
    │   │   └── revoked_certs.db
    │   ├── security-context
    │   │   └── rsu.wsc
    │   └── wscs
    │       └── ws_ca.db
    ├── certadm
    ├── conf -> conf.typical
    ├── conf.typical
    │   ├── rsu.cfg
    │   ├── stack.conf
    │   └── user.conf
    ├── example
    │   ├── MAP.txt
    │   ├── SPAT.txt
    │   └── TIM.txt
    ├── ieee-v3-demo-pca.cert
    ├── ieee-v3-demo-pca.signKey
    ├── ieee-v3-demo-root.cert
    ├── ieee-v3-demo-root.signKey
    ├── lib1609fac.so
    ├── libc2x.so.1
    ├── libclv.so
    ├── libext.so
    ├── libJ2735.so
    ├── libLLC.so
    ├── libNxDispatcher.so
    ├── libNxDispatcher.so.0
    ├── libNxDispatcher.so.0.1
    ├── libNxDispatcher.so.0.1.0
    ├── libNxDispatcher.so.0.3
    ├── libNxDispatcher.so.0.3.0
    ├── libNxDispatcher.so.0.5
    ├── libNxDispatcher.so.0.5.5
    ├── libplat.so
    ├── libpos.so
    ├── libSync.so
    ├── libubx.so
    ├── libviicsec.so.1
    ├── msg
    ├── ndppd_watch
    ├── rc.aerolink
    ├── rc.rsu
    ├── rsu1609
    ├── rsu-monitor
    └── version
```

3.3 Software Environment

The software environment is a Linux-based operating system. On MK5 DSRC units the environment is based on kernel 3.10.17.

3.3.1 Ethernet Interface

The RSU utilises the Ethernet for the following functions:

- Log in to the RSU for application management
    a. Start/Stop
    b. Initial configuration
- SNMP Management
    a. RSU status
    b. RSU configuration
    c. Active message addition, deletion and modification
- Accepting SAE J2735 messages for immediate forwarding on the DSRC radio interface
- Forwarding GPS GGA NMEA sentences to a connected host
- Forwarding WSM messages received on the DSRC radio to an external host
- Off-loading log files for inspection
- IPv6 network connectivity

3.3.2 DSRC Radio Interface

The RSU utilises the DSRC Radio interface to:

- Broadcast SAE J2735 messages
- Transmit Wave Service Announcements (WSA)
- Receive WSM messages
- Provide IPv6 connectivity to On-board Units (OBU)

3.4 Software Organization and overview of Operation

The RSU software runs on Cohda Wireless MK5 DSRC radio units. It broadly performs the following functions:

- Broadcasts SAE J2735 messages on the DSRC radio interface

- Monitors for forwarded SAE J2735 messages on its Ethernet Interface to broadcast on DSRC radio interface
- Receives Wave Short Messages (WSM)
- Transmits Wave Service Announcements (WSA)
- Routes IPv6 traffic for connected mobile units
- IEEE 1609.2 message signing and verification
- Logs transmitted and received message on DSRC radio interface
- Logs system status messages

3.4.1 Software Modules

When running, the software utilises the following modules:

Module	Description
rsu	Main RSU application encapsulating the RSU application requirements and the 1609 standard requirements: • IEEE 1609.4 functionality • IEEE 1609.3 functionality • IEEE 1609.2 functionality • Broadcasting/Forwarding SAE J2735 messages • IPv6 connectivity

Figure 1 shows a block diagram for the RSU software architecture. It is important to note that the RSU application encompasses the,

- RSU application layer specific modules (highlighted in **ORANGE**)
- Facilities and Network Layers Stack related functionality (highlighted in **BLUE**)
- Standard Linux components (highlighted in **RED**).

This distinction is important when considering the RSU configuration.

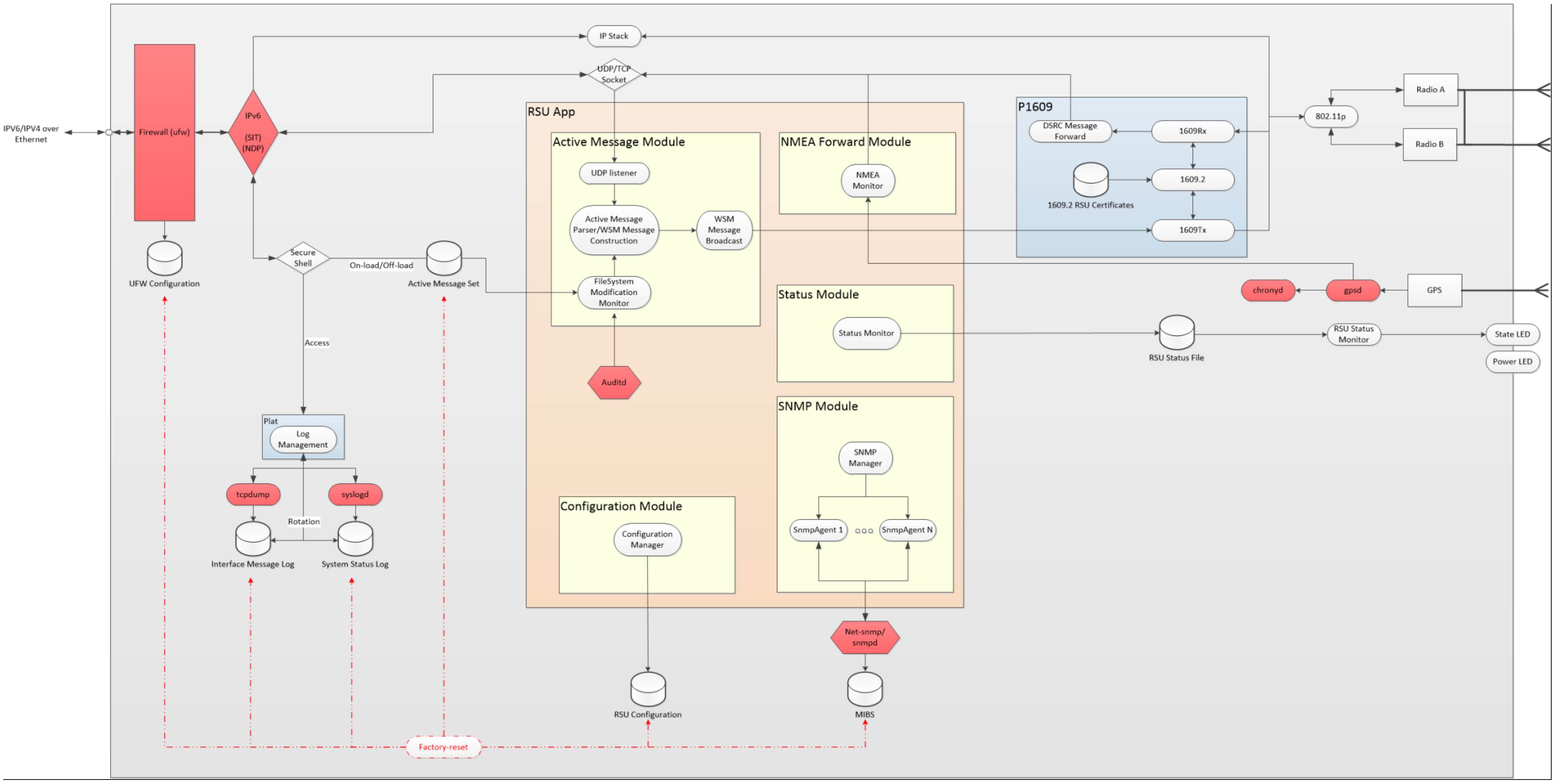

Figure 1: RSU software block diagram

3.5 Contingencies and alternate states and modes of operation

This paragraph is not used and has been tailored out in line with ISO 12207 guidelines.

3.6 Security and privacy

3.6.1 Message Signing and Verification

The RSU operates by default with message signing and verification enabled. However to operate successfully, the RSU requires access to 1609.2 certificates. The current RSU release includes a root certificate and signing keys to generate its own 1609.2 certificates. When the RSU transitions to the OPERATE state, it will re-generate certificates for MAP, SPAT, TIM and WSA message signing that are valid for 60 days.

3.6.1.1 Installing Certificates

In future releases, the RSU will utilise certificates provided by the system administrator that are loaded to directory */mnt/ubi/1609Certificates*. An example directory listing showing these certificates is shown in Figure 2. In this example certificates are present for signing MAP, SPAT, TIM and WSA messages. The root CA certificate is also present – this is required to correctly sign and verify messages.

```
/mnt/src/1609Certificates
          ├── MAP20140528.crt
          ├── root_ca.cert
          ├── SPAT20140528.crt
          ├── TIM20140528.crt
          └── WSA20140528.crt
```

Figure 2: Example listing of Certificates required for signing WSAs, MAP, SPAT and TIM messages

3.7 Assistance and problem reporting

Please contact Cohda Wireless Pty Ltd. for questions relating to the installation process.

Contact details are as follows:

Phone: +61 8 7099 5500 (9AM to 5PM ACST)
Fax: +61 8 8364 4597
Email: support@cohdawireless.com

4 Access to the software

4.1 First-time user of the Software (Hardware)

4.1.1 Equipment familiarization

4.1.1.1 RSU Interface location

The location of the system interfaces provided by the RSU is shown in Figure 3.

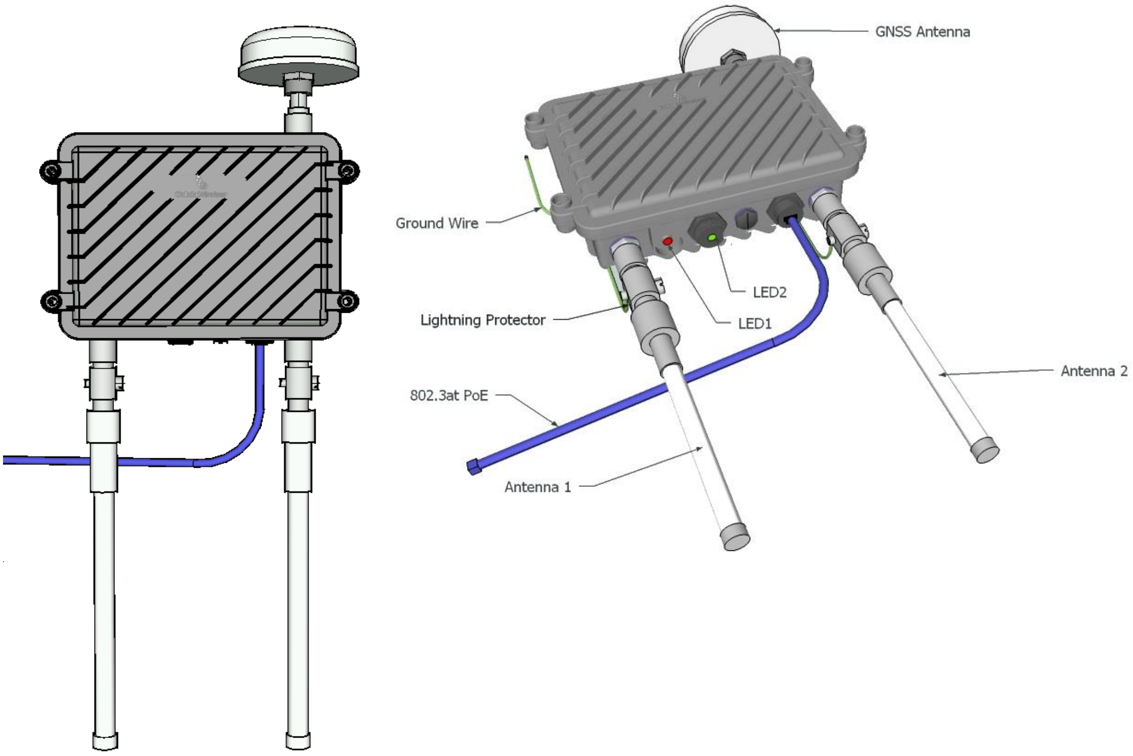

Figure 3 Location of RSU interfaces

A brief description of these interfaces is provided in Table 1.

Interface	Description
Antenna 1 / 2	5.9 GHz N-Type Male for DSRC radio
LED1	Multi-colour Light Emitting Diode (LED). This LED is utilised to indicate the RSU state. • Off: No Power • Blinking Green: RSU is starting • Solid Green: RSU is Operational/Running • Amber: Firmware upgrade is occurring • Red: Fault
LED2	Multi-colour Light Emitting Diode (LED). This LED is utilised to indicate the RSU Power, • Off: No Power • Solid Green: Powered On
Ethernet	Ethernet socket with Power over Ethernet
GNSS Antenna	Global Navigation Satellite antenna connector (N-Type Male connector)

Table 1 RSU Interface descriptions

4.1.1.1.1 Ethernet Interface

The Ethernet socket takes a RJ45 plug and connects to an internal PoE Splitter providing separate power and Ethernet to the MKx board. The internal PoE splitter is configured to support 802.3at Mode A/B.

4.1.1.1.2 DSRC ANT1 and ANT2 Interfaces

The RSU provides a single DSRC radio set, denoted by interfaces ANT1 and ANT2.

WARNING!* *Both antennae must be attached whenever the RSU is powered or permanent system damage could occur.

4.1.1.1.3 GNSS Interface

The RSU provides a GNSS interface to receive global positioning data transmitted by satellites.

4.1.2 Access control

The MKx RSU can be accessed via a secure shell (e.g. SSH or Putty) session using the following default credentials:

- **Username**: rsu
- **Password**: rsuadmin

The RSU supports rules for IP access control defined as firewall rules as discussed in section 5.1.6.

CAUTION:* *The RSU is provided with default credentials and should be updated by an authorised person to meet organisational policies related to computer security.

```
rsu@ MK5:/mnt/ubi $ passwd rsu
```

The root user is required to perform software installation in addition to running the RSU application. To transition to the root user, use the following *sudo* command:

```
rsu@ MK5:/mnt/ubi $ sudo -i
```

4.1.3 Installation and setup

4.1.3.1 Powering the RSU

The PoE splitter, internal to the RSU, is configured to connect to a PoE (802.3at) Mode A/B Power Supply Equipment (PSE), supplying 48V DC over the Ethernet interface. If the installation site does not support 802.3at, then an additional PoE Injector taking DC input and supplying 48V DC 802.3at Mode A/B output will be required to power the unit. The maximum distance between the PSE and the Powered Device (PD), and the RSU, is 100 metres. Providing power beyond 100 metres requires an additional PoE extender

4.1.3.2 RSU Antenna Connections

The RSU requires an Omni-directional antenna connected to each DSRC radio (interface ANT1 and ANT 2), and a Global Positioning System (GPS) Antenna connected to the GNSS interface.
It is extremely important to weather proof all Radio Frequency (RF) connectors and lightning surge arresters with self-fusing rubber tape.

4.1.3.2.1 Lightning Surge Arresters (optional item)

The DSRC radios and GNSS receiver on the RSU can be protected by attaching optional Lighting Surge Arresters. If lightning surge arresters are to be fitted, they must be connected directly to the RSU ANT1, ANT2 and GNSS interfaces. It is extremely important, all lightning surge arresters are connected to a good common earthing point.

4.1.3.2.2 Omni-directional Antenna

An optional Lightning Surge Arrester can be connected in-line with each DSRC radio shown in Figure 3. An earth grounding wire must be attached to the body of each lighting surge arrester. The earth grounding wires are connected to same common earth ground point used by the RSU.

4.1.3.2.3 GPS Antenna

The GPS antenna is attached to the RSU GNSS interface, illustrated in Figure 6.

Note: ***The positioning of the final RSU assembly should provide a clear-sky view to provide best overall acquisition of GPS satellites.***

4.1.3.3 Pole Mounting

The RSU has a flat surface, with four equally spaced mounting holes and is capable of accepting an optional mounting bracket. Size and location of these mounting holes is illustrated in Figure 4.

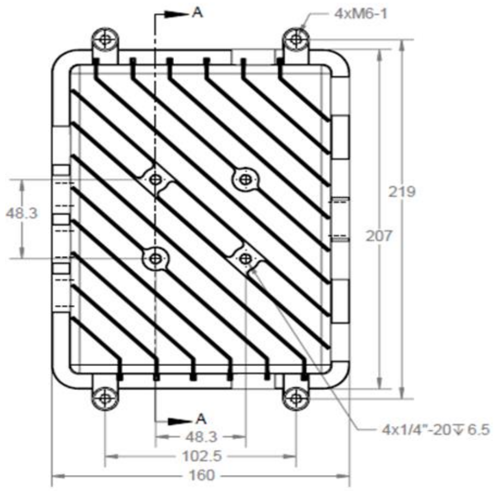

Figure 4 Pole mounting holes

The mounting bracket can be attached to facilitate mounting to a vertical or horizontal pole, as shown in Figure 5.

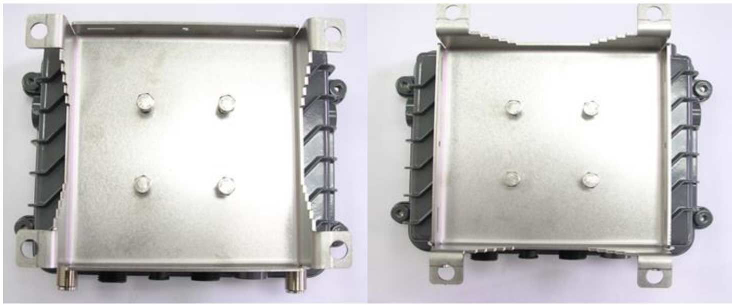

Figure 5 Mounting bracket attached to RSU for horizontal (left) and vertical (right) mounting

Adjustable stainless steel straps can be threaded through slots in the mounting bracket to fasten the mounting bracket to the pole. An illustration on mounting a RSU to a horizontal pole is shown in Figure 6.

Note: Optional lightning surge arresters are not fitted in this illustration.

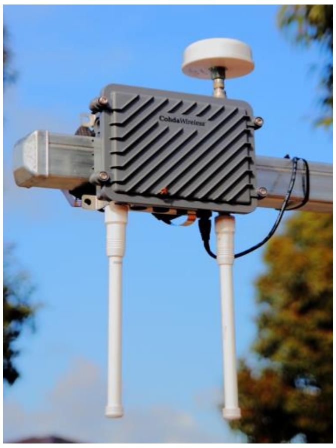

Figure 6 RSU attached to a horizontal square-tube pole.

4.1.3.4 RSU Infrastructure Mounting Options

4.1.3.4.1 Pole Mount

An RSU attached to a horizontal pole, see Figure 7. The minimum recommended separation between the pole and the Antenna closest to the pole is 2 metres.

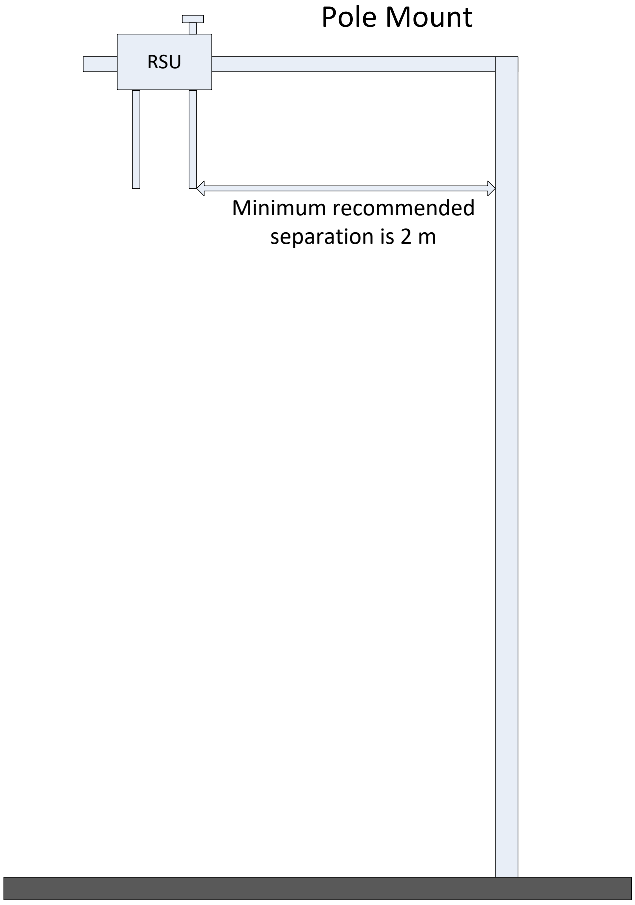

Figure 7 RSU attached to Pole.

4.1.3.4.2 Gantry Mount

Multiple RSUs attached to a gantry structure, see Figure 8. The gantry attachment to the building could be replaced with another pole to provide support for the gantry. **Note**: The distance from the RSU to the antennas is not to exceed 10 metres (based on standard LMR-400 cable). When mounting multiple RSUs, it is recommended each RSU is assigned a different Service Channel Number (see section **Error! Reference source not found.** for details on configuration).

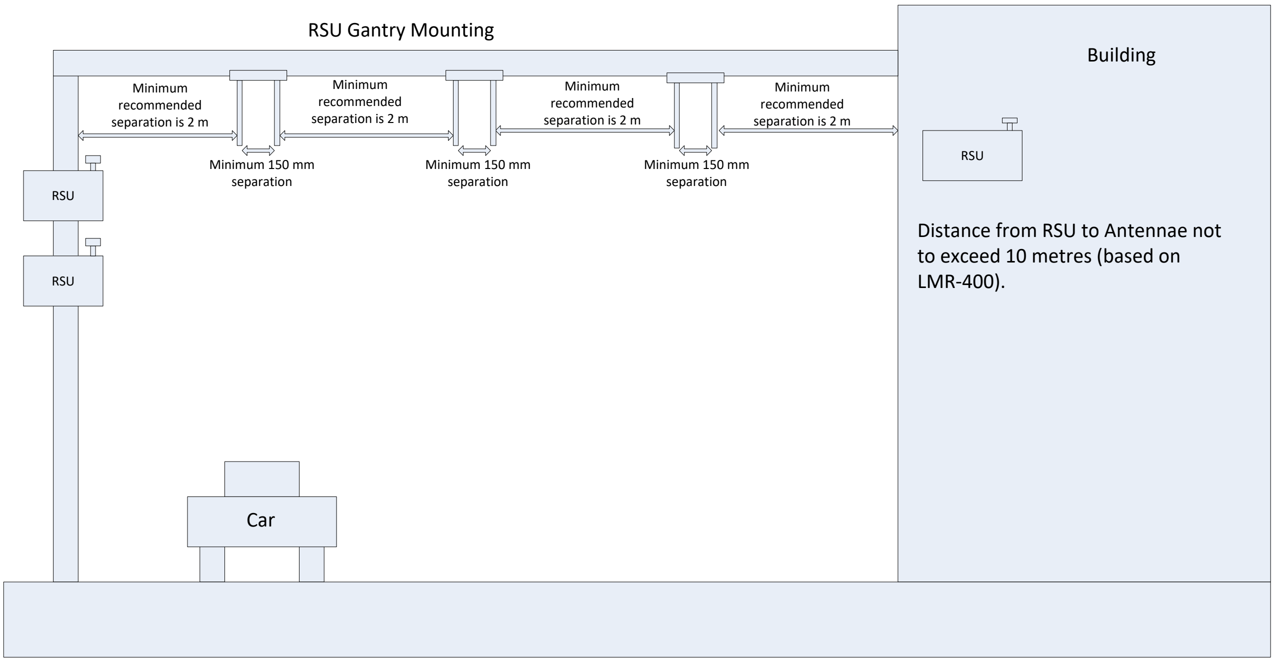
RSU Gantry Mounting
Building
Minimum recommended separation is 2 m
Minimum recommended separation is 2 m
Minimum recommended separation is 2 m
Minimum recommended separation is 2 m
Minimum 150 mm separation
Minimum 150 mm separation
Minimum 150 mm separation
RSU
RSU
RSU
Distance from RSU to Antennae not to exceed 10 metres (based on LMR-400).
Car

Figure 8 RSU Gantry Mounting

4.2 First-time user of the Software

4.2.1 Installing RSU Software

The RSU is provided with the most recent update of the RSU application software - however, this image may be upgraded. To install the RSU software, the package should be transferred to the MK5 device at location ***/mnt/ubi***.

To do this, the MK5 unit may be accessed via its Ethernet Interface using secure copy (e.g. the scp linux command line program, or the WinSCP Windows GUI). See section 4.1.2 for details of credentials used to access the MK5 device.

Once the software package is transferred, log in to the device and access the root user account. See section 4.1.2 for credential and root user account details. Change to the ***/mnt/ubi/*** directory, and run the firmware upgrade command (***fim***),

```
rsu@ MK5:/ $ sudo -i
root@ MK5:/ $ cd /mnt/ubi
root@ MK5:/mnt/ubi $ fim -u mk5-5.RSU_4_1.56829-typical-RSU.img
```

The firmware upgrade will update the complete root file-system. On completion, the RSU device must be rebooted for the upgrade to take effect,

```
root@ MK5:/mnt/ubi $ sync
root@ MK5:/mnt/ubi $ reboot
```

Note: To confirm the RSU has been upgraded, log into the device after the reboot and list the installed image using the fim utility. It will list the active (A) and running (R) image, whose version number should match that of the image utilised in the upgrade process.

```
root@/mnt/ubi $ fim -l
Status Image name   Image file
       factory      mk5-5.11.31102.sqsh
       image-a      mk5-5.RSU_4_1.56764-RSU.sqsh
AR     image-b      mk5-5.RSU_4_1.56829-RSU.sqsh
```

4.2.2 Starting the RSU application

The RSU application will start automatically on boot, however if required it can also be started manually (***if in the stopped state)*** as the root user by issuing a ***start*** command to the ***rc.local*** script located at ***/opt/cohda/application/***.

```
root@ MK5:/ $ /opt/cohda/application/rc.local start
```

4.2.3 Stopping the RSU application

The RSU application can also be stopped manually as the root user by issuing a ***stop*** command to the ***rc.local*** script located at ***/opt/cohda/application/***.

```
root@ MK5:/ $ /opt/cohda/application/rc.local stop
```

4.3 Initiating a session

WARNING! Both antennae must be attached whenever the RSU is powered or permanent system damage could occur.

Over the lifetime of the RSU device, it is capable of transitioning between several states as indicated by Figure 9.

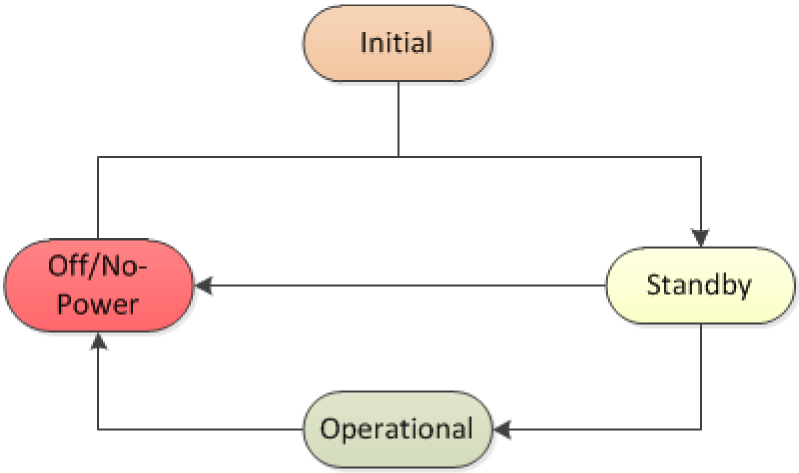

Figure 9: RSU application state diagram

When the RSU is first installed it is in the Initial (Factory) State. In this state the persistent partition of the RSU (/mnt/ubi) is cleared of all RSU files and the root RSU filesystem is installed. On first boot the RSU persists a number of critical files to the /mnt/ubi partition as it transitions from the Initial State to the Standby State

Following this, all subsequent booting sequences of the RSU device will begin from the Standby State.

The RSU will proceed through its boot sequence to Standby and then to Operational state automatically when power is applied to the device. The state of the RSU is indicated by the two LEDs located on the devices enclosure - see Figure 3 and Table 1 for more information.

4.3.1 Manually starting the RSU application

WARNING!* *Both antennae must be attached whenever the RSU is powered or permanent system damage could occur.

The RSU application will start automatically on boot, however if required, the RSU application can be started manually using the ***rc.local*** script located at ***/opt/cohda/application/***. As the root user, the start command can be specified as follows:

```
root@ MK5:/ $ /opt/cohda/application/rc.local start
```

To inspect if the RSU application is running already, use the ***ps -eo pid,etime,comm | grep -i rsu1609*** command to list processes currently running on the MKx unit. If running, the RSU application will be present in the list of running processes.

Example with sample output:

```
root@ MK5:/ $ ps -eo pid,etime,comm | grep -i rsu1609
3369 1245:08 rsu1609
```

4.3.2 Manually stopping the RSU application

The RSU application can be stopped manually using the ***rc.local*** script located at ***/opt/cohda/application/***. As the root user, the stop command can be specified as follows:

```
root@ MK5:/ $ /opt/cohda/application/rc.local stop
```

To inspect if the RSU application has stopped, use the ***ps -eo pid,etime,comm | grep -i rsu1609*** command to list processes currently running on the MKx unit. If stopped, the RSU application will not be present in the list of running processes.

4.3.3 Restarting the RSU application

The RSU application can be restarted using the ***rc.local*** script located at ***/opt/cohda/application/***. As the root user, the restart command can be specified as follows:

```
root@ MK5:/ $ /opt/cohda/application/rc.local restart
```

Alternatively, the device may be power-cycled to restart the application

4.3.4 Transition the RSU application to Standby Mode

The RSU application can be transitioned to standby mode (from operating) using the ***rc.local*** script located at ***/opt/cohda/application/***. As the root user, the standby command can be specified as follows:

```
root@ MK5:/ $ /opt/cohda/application/rc.local standby
```

Alternatively, SNMP may be used to remotely transition the RSU to standby mode using the rsuMode OID described in section 5.1.1.1.3.

```
snmpset -v 3 -l authPriv -u $USERNAME -A $PASSWORD -X $PASSWORD -a SHA -x AES $RSU_IP_ADDR 1.0.15628.4.1.99.1.0 i 2
```

4.3.5 Transition the RSU application to Operate Mode

The RSU application can be transitioned to operate mode (from standby) using the ***rc.local*** script located at ***/opt/cohda/application/***. As the root user, the operate command can be specified as follows:

```
root@ MK5:/ $ /opt/cohda/application/rc.local operate
```

Alternatively, SNMP may be used to remotely transition the RSU to operate mode using the rsuMode OID described in section 5.1.1.1.3.

```
snmpset -v 3 -l authPriv -u $USERNAME -A $PASSWORD -X $PASSWORD -a SHA -x AES $RSU_IP_ADDR 1.0.15628.4.1.99.1.0 i 4
```

4.4 Software Configuration

The RSU application is configured by three configuration files located at */mnt/ubi/rsu1609/conf.*

- rsu.cfg: Application specific configuration file
- stack.conf: Initial overrides for the Facilities and Network Layers Stack configuration
- user.conf: SNMP overrides for the Facilities and Network Layers Stack configuration

4.4.1 RSU Application Configuration

The RSU application layer is configured via a single hierarchical file – ***rsu.cfg***. This file is used to configure the following RSU modules,

- Active messages: Configures the Active message location and how often to attach 1609.2 credentials.
- NMEA Forwarding: Configures the GGA NMEA sentence forwarding
- Status: Configures how often the RSU will notify of successful status.
- RSATx: Configures a single hard-coded Road-side Alert broadcast.
- RawTx: Configures a single hard-coded Raw data broadcast.
- XtSysRq: Configures the remote SysReq capability to reboot the RSU over the network with special packet.
- IPV6SITTunnel: Configures the IPv6 SIT capability.
- IPV6NDPBridge: Configures the IPv6 NDP capability.
- IPV6Static: Configures the IPv6 static addresses.

4.4.1.1 RSU application layer configuration parameter description

The application configuration file is constructed in a hierarchical structure, and will be represented here in the following description using a dot notation. For example the configuration option *Application.ParameterBlock.Parameter* will be used to denote the hierarchical structure of **Error! Reference source not found.**

```
Application = {
          ParameterBlock = {
                    Parameter=”value”;
          }
}
```

Figure 10: Heirarchal configturation file format

RSU.APP	
Setting	**Description**
NMEAFwd	The NMEAFwd option specifies if the GGA NMEA forwarding module is enabled or disabled. Valid values are: • true – indicates the module is enabled • false – indicates the module is disabled Default value: true – indicating the module is enabled
Status	The Status option specifies if the RSU status monitor module is enabled or disabled. Valid values are: • true – indicates the module is enabled • false – indicates the module is disabled Default value: true – indicating the module is enabled
XtSysRq	The XtSysRq option specifies if the remote XtSysReq control module is enabled or disabled. Valid values are: • true – indicates the module is enabled • false – indicates the module is disabled Default value: false – indicating the module is disabled
IPV6SITTunnel	The IPV6SITTunnel option specifies if the SIT (IPv6 in IPv4) tunnel module is enabled or disabled. Valid values are: • true – indicates the module is enabled • false – indicates the module is disabled Default value: false – indicating the module is disabled **Note:** Only one of IPV6SITTunnel, IPV6NDPBridge or IPV6Static can be enabled at one time.
IPV6NDPBridge	The IPV6NDPBridge option specifies if the NDP proxy capability for IPv6 connectivity and routing on the DSRC interface is enabled or disabled. Valid values are: • true – indicates the module is enabled • false – indicates the module is disabled Default value: false – indicates the module is disabled **Note:** Only one of IPV6SITTunnel, -IPV6NDPBridge or IPV6Static can be enabled at one time.

IPV6Static	The IPV6Static option specifies if static IPv6 addresses should be configured for the ethernet and DSRC interface. Valid values are: • true – indicates the module is enabled • false – indicates the module is disabled Default value: false – indicates the module is disabled **Note:** Only one of IPV6SITTunnel, -IPV6NDPBridge or IPV6Static can be enabled at one time.

RSU.ActiveSrvs	
Setting	**Description**
Path	The Path option specifies the location of local Active Messages for broadcasting by the RSU. Valid values for this option are any valid directory path Default value: /mnt/ubi/rsu1609/msg
Port	The Port option specifies the UDP port listening for Active Messages delivered over the network for immediate forwarding by the RSU. Valid values are any valid port number. Default value: 1516
CertAttachInterval	The CertAttachInterval option specifes the message period for attaching 1609.2 security credentials to a transmitted WSM message. Valid values are in the range [1 – 100], • 1 – inidicates attach the security credentials to every WSM • 100 – indicates attach the security credentials to every 100 WSMs **SNMP OID:** 1.0.15628.4.1. 11 **SNMP Format:** 1 byte

RSU.NMEAFwd	
Setting	**Description**
Host	The Host option specifies the IP host endpoint to forward the RSU's GGA NMEA sentences retrieved from the on-board GPS unit. The GGA NMEA sentences are sent in the form, **$GNGGA,050351.00,3454.37667,S,13836.48163,E,2,12,0.74,38.6,M,-3.5,M,,0000*7A** Valid values are any valid IP address. The setting is 16 bytes, which can contain either an IPv6 or IPv4 destination address, as follows: **For IPv6 destination address:** Fill out all 16 bytes with the full 128-bit IPv6 destination address. e.g. for IPv6 destination address **fe80::aabbcc** set it to: 0xfe800000000000000000000000aabbcc **For IPv4 destination address:** Zero the first 12 bytes, and set the last 4 bytes to the full 32-bit IPv4 address. e.g. for IPv4 destination address **192.168.0.1** set it to 0x000000000000000000000000c0a80001 **SNMP OID:** 1.0.15628.4.1.8.2.0 **SNMP Format:** 16 bytes
Port	The Port option specifies the UDP port endpoint to forward the RSU's GGA NMEA sentences. Valid values are any valid port number. **SNMP OID:** 1.0.15628.4.1.8.1.0 **SNMP Format:** 2 bytes
InterfaceName	The InterfaceName option specifes the local RSU network interface to bind the transmission socket to. In the standard RSU configuration, networking is enabled on ***eth0*** and so this is the default value. Under normal operation, this value should not be changed. **SNMP OID:** 1.0.15628.4.1.8.3.0 **SNMP Format:** up to 15 byte string
SampleRate	The SampleRate option specifies the how often to sample the GPS NMEA stream. Valid values are in the range: 1 – 18000 (seconds) Default value: 1 (second) **SNMP OID:** 1.0.15628.4.1.8.1.4.0 **SNMP Format:** 4 bytes

RSU.Status	
Setting	**Description**
Interval	The Interval option specifies how often to determine and report on the state of the RSU software. **Note:** The reporting is not external, but is provided to the module driving the LED indicators. Therefore this value will determine the delay in changes to the State LED indicator. Valid values are: Any 32-bit unsigned integer (milli-seconds) Default value: 1000 (milli-scond)

RSU.XtSysRq	
Setting	**Description**
Password	The Password option specifies the password for the remote SysRq communication. This password should be unique across devices. If set, the SysRq service is enabled. If not set, the SysRq service is disabled Valid values are: • Any valid ascii string Default value: Not set (“”), indicating the SysRq service is disabled
Port	The Port option specifies the port the SysRq service should receive magic packets on. Valid values are any valid port number Default value: 9
SourceIP	The SourceIP option specifies the IP Address (IPv4 or IPv6) to allow SysRq packets from. If not set, the SysRq service will match any IP address Valid values are any valid IPv4 or IPv6 address Default value: Not set (“”), indicating the SysRq service will match any IP address
SourceMAC	The SourceMAC option specifies the MAC address to allow SysRq packets from. If not set, the SysRq service will match any MAC address Valid values are any valid MAC address Default value: Not set (“”), indicating the SysRq service will match any MAC address

RSU.IPV6SITTunnel	
Setting	**Description**
Name	The Name option specifies the name of the created SIT tunnel. This interface will be present when interrogated via the Linux ***ifconfig*** command. Valid values are any valid string up to 15 characters Default value: sit1

RSU.IPV6SITTunnel	
Setting	**Description**
RemoteAddress	The RemoteAddress option specifies the IPv4 address SIT tunnel endpoint at the remote host. If not set the SIT tunnel is disabled Valid values are any valid IPv4 address Default value: Not set (“”)
Routes	The Routes option specifies any custom IPv6 routes to add via the SIT tunnel interface. Valid values are: • any set of valid IPv6 address – indicates specific IPv6 routes • “default” – indicates to route all IPv6 traffic via the SIT tunnel Default value: default (sets the default IPv6 routing via the SIT tunnel)
TunnelAddresses	The TunnelAddress option specifies the IPv6 address/es to assign to the SIT tunnel. If not set, the SIT tunnel is disabled. Valid values are any set of valid IPv6 address with the prifix length specified. For example, cafe:beef::1/64 Default value: Not set (“”)
WaveDataAddress	The WaveData option specifies the IPv6 address to assign to the DSRC interface. If not set, the SIT tunnel is disabled Valid values are any valid IPv6 address with the prefix length specified. For example, cafe:beef::2/64 Default value: Not set (“”)

RSU.IPV6Static	
Setting	**Description**
EthernetAddress	Static IPv6 address for the ethernet interface. Valid values are any set of valid IPv6 address with the prifix length specified. For example, fd4e:20ec:7fb0:0000::1/64 Default value: empty
WaveDataAddress	Static IPv6 address for the DSRC interface. Valid values are any set of valid IPv6 address with the prifix length specified. For example, fd4e:20ec:7fb0:0001::1/64 Default value: empty

RSU.IPV6Static	
Setting	**Description**
GatewayAddress	Gateway router IPv6 address. For example, fd4e:20ec:7fb0:ffff Default value: empty
Subnet	Subnet that is routed to via Gateway. For example, fd4e:20ec:7fb0:0000::1/64 Default value: Not set (“”)

4.4.2 Active Message (Store and Repeat) Configuration

Active (Store and Repeat) Messages are installed, modified, viewed and deleted via an SNMP table located at MIB OID 1.0.15628.4.1.4. These elements of this table are marked as read-create, meaning that table rows may be added and deleted using the *RowStatus* element (1.0.15628.4.1.4.1.11.X).

Note: Active messages may be present in the system (i.e. listed in the Active Message table) but are only transmitted if all required information is set in the MIB and the message is also enabled with the *Enable* parameter (1.0.15628.4.1.4.1.10).

Active Message	
Setting	**Description**
storeAndRepeatPsid	The storeAndRepeatPsid option indicates the PSID of the Xth Active Message currently being broadcast. **SNMP OID:** 1.0.15628.4.1.4.1.2.X **SNMP Format:** 2-byte OCTET STRING
storeAndRepeatDsrcMsgId	The storeAndRepeatDsrcMsgId option indicates the DSRC Message ID of the Xth Active Message currently being broadcast. **SNMP OID:** 1.0.15628.4.1.4.1.3.X **SNMP Format:** INTEGER
storeAndRepeatTxMode	The storeAndRepeatTxMode option indicates the mode (continuous or alternating) of the Xth Active Message currently being broadcast. **SNMP OID:** 1.0.15628.4.1.4.1.4.X **SNMP Format:** INTEGER 0 – Continuous 1 – Alternating
storeAndRepeatTxChannel	The storeAndRepeatTxChannel option indicates the channel number of the Xth Active Message currently being broadcast. **SNMP OID:** 1.0.15628.4.1.4.1.5.X **SNMP Format:** INTEGER

Active Message	
Setting	**Description**
storeAndRepeatTxInterval	The storeAndRepeatTxInterval option indicates the transmission interval (milli-seconds) of the Xth Active Message currently being broadcast. **SNMP OID:** 1.0.15628.4.1.4.1.6.X **SNMP Format:** INTEGER
storeAndRepeatDeliveryStart	The storeAndRepeatDeliveryStart option indicates the time of the Xth Active Message started being broadcast. **SNMP OID:** 1.0.15628.4.1.4.1.7.X **SNMP Format:** 6-Byte OCTET STRING YYMDHm YY – Year M – Month D – Day H – Hour m - Minute
storeAndRepeatDeliveryEnd	The storeAndRepeatDeliveryEnd option indicates the time the Xth Active Message broadcast will end. **SNMP OID:** 1.0.15628.4.1.4.1.8.X **SNMP Format:** 6-Byte OCTET STRING YYMDHm YY – Year M – Month D – Day H – Hour m - Minute
storeAndRepeatPayload	The storeAndRepeatPayload option indicates the payload of the Xth Active Message broadcast. **SNMP OID:** 1.0.15628.4.1.4.1.9.X **SNMP Format:** 2302-byte (MAX) OCTET STRING

Active Message	
Setting	**Description**
storeAndRepeatEnable	The storeAndRepeatEnable option indicates whether the Xth Active Message broadcast is enabled or disabled. **SNMP OID:** 1.0.15628.4.1.4.1.10.X **SNMP Format:** INTEGER 0 – Disabled 1 – Enabled
storeAndRepeatStatus	The storeAndRepeatStatus option is used to manage the Xth Active Message MIB table row. **SNMP OID:** 1.0.15628.4.1.4.1.11.X **SNMP Format:** INTEGER 4 – CreateAndGo (Need to provide all active message MIB OID data in the one PDU) 5 – CreateAndWait (Create a new Active Message MIB Row. All active message MIB OID data provided in following PDU) 6 – Destroy (Delete the Active Message MIB Row)

4.4.3 RSU Stack Configuration

The RSU stack layer is configured via two separate, but related configuration files – ***stack.conf*** and ***user.conf***. These files are used to configure the following functionality,

- DSRC channel numbers
- 1609.2 security configuration
- Wave Short Message (WSM) forwarding
- Wave Service Announcement (WSA) content configuration
- Wave Routing Advertisement (WRA) content configuration
- Interface log configuration
- System log configuration
- Debug log configuration

CAUTION: **user.conf** ***is an auto-generated file that is used to override a subset of the configurations stored in stack.conf. This file is utilised by the SNMP configuration management module and as such the end-user should not modify its contents manually.***

Any changes made to stack.conf that have a corresponding configuration parameter in user.conf will be overridden by the value in user.conf in the RSU's operational configuration. To update values stored in user.conf the end-user should utilise the SNMP service provided by the RSU.

4.4.3.1.1 RSU stack layer configuration parameter description

stack.conf	
Setting	**Description**
BSMEnabled	The BSMEnabled option specifies to enable or disable Basic Safety Messaging (BSM). Valid values are: • 0 – indicates to disable BSM transmission • 1 – indicates to enable BSM transmission Default value: 0 (disable BSM transmission) **Note:** As an RSU, this option should never be set to enable.
Cohda_DebugLevel	The Cohda_DebugLevel option specifies the level of debugging contained in the stderr log file located at ***/mnt/ubi/log/current/stderr***. Valid values are: • 0 – EMERG • 1 – ALERT • 2 – CRIT • 3 – ERR • 4 – WARN • 5 – NOTICE • 6 – INFO • 7 – DEBUG • 8 – TEST • 9 – VERBOSE • 127 – IRQ • 255 – ALL Default value: 4 (WARN)
Cohda_LogCaptureSTDERR	The Cohda_LogCaptureSTDERR option specifies to enable or disable the capture of the ***/mnt/ubi/log/current/stderr*** log file. Valid values are: • 0 – indicates to disable the log capture • 1 – indicates to enable the log capture Default value: 1 (enable log capture)
Cohda_LogCaptureSyslog	The Cohda_ LogCaptureSyslog option specifies to enable or disable the capture of the ***/mnt/ubi/log/current/syslog*** log file. Valid values are: • 0 – indicates to disable the log capture • 1 – indicates to enable the log capture Default value: 1 (enable log capture)

stack.conf	
Setting	**Description**
Cohda_PCAP_LoggingDisabled	The Cohda_PCAP_LoggingDisabled option specifies to disable or enable the internal interface log capability. Valid values are: • 0 – indicates to enable the log capture • 1 – indicates to disable the log capture Default value: 1 (disable the log capture) **Note:** As an RSU, the application operates it's interface logging capability based on the options listed immediately below. As such this option should remain disabled under normal RSU operation
TxALogEnableFlag	The TxALogEnableFlag option specifies to enable or disable the PCAP capture of transmitted packets on Radio A of the DSRC interface. Valid values are: • 0 – indicates to disable the log capture • 1 – indicates to enable the log capture Default value: 0 (disable the log capture) **SNMP OID:** 1.0.15628.4.1.9.1.2.2 **SNMP Format:** 1 byte
TxALogSizeLimit	The TxALogSizeLimit option specifies the size limit of the PCAP file for the transmitted packets on Radio A (in MB). When this limit is reached, the file will be closed, moved to a new file with extension with increasing numbers for each rotation **pcap.[1,2,3,…]**. At the same time a new PCAP file is opened in its place to continue logging. Valid values are: 5 – 40 (MB) Default value: 20 (MB) **SNMP OID:** 1.0.15628.4.1.9.1.3.2 **SNMP Format:** 1 byte
TxALogTimeLimit	The TxALogTimeLimit option specifies how often to rotate the PCAP file for transmitted packets on Radio A. Valid values are: 3600 - 172,800 (seconds) Default value: 86400 (seconds) (24 hours) **SNMP OID:** 1.0.15628.4.1.9.1.4.2 **SNMP Format:** 1 byte (specified as **hours**)

stack.conf	
Setting	**Description**
TxBLogEnableFlag	The TxBLogEnableFlag option specifies to enable or disable the PCAP capture of transmitted packets on Radio B of the DSRC interface. Valid values are: • 0 – indicates to disable the log capture • 1 – indicates to enable the log capture Default value: 0 (disable the log capture) **SNMP OID:** 1.0.15628.4.1.9.1.2.4 **SNMP Format:** 1 byte
TxBLogSizeLimit	The TxBLogSizeLimit option specifies the size limit of the PCAP file for the transmitted packets on Radio B (in MB). When this limit is reached, the file will be closed, moved to a new file with extension with increasing numbers for each rotation **pcap.[1,2,3,…]**. At the same time a new PCAP file is opened in its place to continue logging. Valid values are: 5 – 40 (MB) Default value: 20 (MB) **SNMP OID:** 1.0.15628.4.1.9.1.3.4 **SNMP Format:** 1 byte
TxBLogTimeLimit	The TxBLogTimeLimit option specifies how often to rotate the PCAP file for transmitted packets on Radio B. Valid values are: 3600 - 172,800 (seconds) Default value: 86400 (seconds) (24 hours) **SNMP OID:** 1.0.15628.4.1.9.1.4.4 **SNMP Format:** 1 byte (specified as **hours**)
RxALogEnableFlag	The RxALogEnableFlag option specifies to enable or disable the PCAP capture of received packets on Radio A of the DSRC interface. Valid values are: • 0 – indicates to disable the log capture • 1 – indicates to enable the log capture Default value: 0 (disable the log capture) **SNMP OID:** 1.0.15628.4.1.9.1.2.3 **SNMP Format:** 1 byte

stack.conf	
Setting	**Description**
RxALogSizeLimit	The RxALogSizeLimit option specifies the size limit of the PCAP file for the received packets on Radio A (in MB). When this limit is reached, the file will be closed, moved to a new file with extension with increasing numbers for each rotation **pcap.[1,2,3,…]**. At the same time a new PCAP file is opened in its place to continue logging. Valid values are: 5 – 40 (MB) Default value: 20 (MB) **SNMP OID:** 1.0.15628.4.1.9.1.3.3 **SNMP Format:** 1 byte
RxALogTimeLimit	The RxALogTimeLimit option specifies how often to rotate the PCAP file for received packets on Radio A. Valid values are: 3600 - 172,800 (seconds) Default value: 86400 (seconds) (24 hours) **SNMP OID:** 1.0.15628.4.1.9.1.4.3 **SNMP Format:** 1 byte (specified as **hours**)
RxBLogEnableFlag	The RxBLogEnableFlag option specifies to enable or disable the PCAP capture of received packets on Radio B of the DSRC interface. Valid values are: • 0 – indicates to disable the log capture • 1 – indicates to enable the log capture Default value: 0 (disable the log capture) **SNMP OID:** 1.0.15628.4.1.9.1.2.5 **SNMP Format:** 1 byte
RxBLogSizeLimit	The RxBLogSizeLimit option specifies the size limit of the PCAP file for the received packets on Radio B (in MB). When this limit is reached, the file will be closed, moved to a new file with extension with increasing numbers for each rotation **pcap.[1,2,3,…]**. At the same time a new PCAP file is opened in its place to continue logging. Valid values are: 5 – 40 (MB) Default value: 20 (MB) **SNMP OID:** 1.0.15628.4.1.9.1.3.5 **SNMP Format:** 1 byte

stack.conf	
Setting	**Description**
RxBLogTimeLimit	The RxBLogTimeLimit option specifies how often to rotate the PCAP file for received packets on Radio B. Valid values are: 3600 - 172,800 (seconds) Default value: 86400 (seconds) (24 hours) **SNMP OID:** 1.0.15628.4.1.9.1.4.5 **SNMP Format:** 1 byte (specified as **hours**)
OTALogEnableFlag	The OTALogEnableFlag option specifies to enable or disable the PCAP capture of transmitted packets on both Radio A and Radio B of the DSRC interface. Valid values are: • 0 – indicates to disable the log capture • 1 – indicates to enable the log capture Default value: 0 (disable the log capture) **SNMP OID:** 1.0.15628.4.1.9.1.2.1 **SNMP Format:** 1 byte
OTALogSizeLimit	The OTALogSizeLimit option specifies the size limit of the PCAP file for the transmitted packets on combined Radio A and Radio B (in MB). When this limit is reached, the file will be closed, moved to a new file with extension with increasing numbers for each rotation **pcap.[1,2,3,…]**. At the same time a new PCAP file is opened in its place to continue logging. Valid values are: 5 – 40 (MB) Default value: 20 (MB) **SNMP OID:** 1.0.15628.4.1.9.1.3.1 **SNMP Format:** 1 byte
OTALogTimeLimit	The OTALogTimeLimit option specifies how often to rotate the PCAP file for transmitted packets on combined Radio A and radio B. Valid values are: 3600 - 172,800 (seconds) Default value: 86400 (seconds) (24 hours) **SNMP OID:** 1.0.15628.4.1.9.1.4.1 **SNMP Format:** 1 byte (specified as **hours**)
SSLLogEnableFlag	The SSLLogEnableFlag option specifies to enable or disable the capture of system status log entries into a single PCAP file. Valid values are: • 0 – indicates to disable the log capture • 1 – indicates to enable the log capture Default value: 0 (disable the log capture)

stack.conf	
Setting	**Description**
Cohda_LogSystemInfo	The Cohda_LogSystemInfo option specifies to enable or disable the capture of the RSU system information to ***/mnt/ubi/log/current/info***. This information includes, • RSU uptime • Boot command • RSU application commandline statement • Network interface list Valid values are: • 0 – indicates to disable the information capture • 1 – indicates to enable the information capture Default value: 1 (enable the information capture)
Cohda_LogCaptureConf	The Cohda_ LogCaptureConf option specifies to enable or disable the capture of the initial RSU Facilities and Network Layers Stack configuration to ***/mnt/ubi/log/current/conf***. Valid values are: • 0 – indicates to disable the configuration capture • 1 – indicates to enable the configuration capture Default value: 1 (enable the configuration capture)
SecurityEnable	The SecurityEnable option specifies to enable if disable the use of 1609.2 signing and verification services. Valid values are: • 0 – indicates to disable the 1609.2 security service • 1 – indicates to enable the 1609.2 security service Default value: 1 (enable the 1609.2 security service) **Note:** For the 1609.2 service to operate, 1609.2 certificate are required to be loaded onto the RSU device by the end-user. See section 3.6.1 for more information.
Cohda_Syslog_RotateTime	The Cohda_Syslog_RotateTime option specifies when the syslog file located at ***/mnt/ubi/log/current/syslog*** is rotated. At the specified time, • The syslog file is moved to a new file with format, **Syslog-%Y%m%d-%H%M%S** • A new syslog file is created and logging continues Valid values are any chrony format string, **<minute> <hour> <day of month> <month> <day of week>** Default value: 55 23 * * 7 (23:55 on Sundays)

stack.conf	
Setting	**Description**
Cohda_Syslog_PurgeTime	The Cohda_Syslog_PurgeTime option specifies when the stale syslog files located at ***/mnt/ubi/log/current/syslog*** are deleted. Valid values are any chrony format string, **<minute> <hour> <day of month> <month> <day of week>** Default value: 10 0 * * 1 (00:10 on Mondays)
Cohda_Syslog_PurgeAge_hours	The Cohda_Syslog_PurgeAge_hours option specifies when the age syslog files located at ***/mnt/ubi/log/current/syslog*** are eligible for deletion. Valid values are: • 0 – indicates to not delete any syslog files • > 1 (hours) – indicates to delete syslog files after they are older than the specified number of hours Default value: 672 (hours) (4 weeks)

user.conf	
Setting	**Description**
WSMFwdRx_X_PSID	The WSMFwdRx_X_PSID option specifies the PSID of received WSMs to forward to an external host. The RSU supports up to 10 individual configurations for WSM forwarding, where the X indicates the configuration number [0 – 9]. Valid values are any valid WSM PSID **SNMP OID:** 1.0.15628.4.1.7.1.2.X **SNMP Format:** 2 bytes

user.conf	
Setting	**Description**
WSMFwdRx_X_DestIP	The WSMFwdRx_X_ DestIP option specifies the Desitnation IP address of an external host to forward received WSMs to. The RSU supports up to 10 individual configurations for WSM forwarding, where the X indicates the configuration number [0 – 9]. Valid values are any valid IP address. The setting is 16 bytes, which can contain either an IPv6 or IPv4 destination address, as follows: **For IPv6 destination address:** Fill out all 16 bytes with the full 128-bit IPv6 destination address. e.g. for IPv6 destination address **fe80::aabbcc** set it to: 0xfe800000000000000000000000aabbcc **For IPv4 destination address:** Zero the first 12 bytes, and set the last 4 bytes to the full 32-bit IPv4 address. e.g. for IPv4 destination address **192.168.0.1** set it to 0x000000000000000000000000c0a80001 **SNMP OID:** 1.0.15628.4.1.7.1.3.X **SNMP Format:** 16 bytes
WSMFwdRx_X_DestPort	The WSMFwdRx_X_ DestIPort option specifies the Desitnation port at an external host to forward received WSMs to. The RSU supports up to 10 individual configurations for WSM forwarding, where the X indicates the configuration number [0 – 9]. Valid values are any valid port number **SNMP OID:** 1.0.15628.4.1.7.1.4.X **SNMP Format:** 2 bytes
WSMFwdRx_X_TransportProto	The WSMFwdRx_X_ TransportProto option specifies the transport protocol to use when forwarding received WSMs to an external host. The RSU supports up to 10 individual configurations for WSM forwarding, where the X indicates the configuration number [0 – 9]. Valid values are: • 0x10 – indicates UDP • 0x01 – indicates TCP **SNMP OID:** 1.0.15628.4.1.7.1.5.X **SNMP Format:** 1 byte

user.conf	
Setting	**Description**
WSMFwdRx_X_RSSI	The WSMFwdRx_X_ RSSI option specifies RSSI threshold for forwarding received WSMs to an external host. If the received WSM's RSSI is below the specified RSSI, it is not forwarded. The RSU supports up to 10 individual configurations for WSM forwarding, where the X indicates the configuration number [0 – 9]. Valid values are: • -100 – indicates forward all received WSMs regardless of RSSI • Any other value greater then -100 – indicates the threshold that the RSSI of received WSMs must achieve before being forwarded. **SNMP OID:** 1.0.15628.4.1.7.1.6.X **SNMP Format:** 1 byte
WSMFwdRx_X_MsgSample	The WSMFwdRx_X_ MsgSample option specifies the sample rate of forwarded WSMs. The RSU supports up to 10 individual configurations for WSM forwarding, where the X indicates the configuration number [0 – 9]. Valid values are in the range [1 – 9], where • 1 – indicates forward every received WSM • 9 – indicates forward every 9th received WSM **SNMP OID:** 1.0.15628.4.1.7.1.7.X **SNMP Format:** 1 byte
WSMFwdRx_X_StartTime	The WSMFwdRx_X_ StartTime option specifies the time to begin forwarding WSMs to an external host. The RSU supports up to 10 individual configurations for WSM forwarding, where the X indicates the configuration number [0 – 9]. Valid values are any time in the format, **mm/dd/yyyy, hh:mm** **SNMP OID:** 1.0.15628.4.1.7.1.8.X **SNMP Format: YYMDHm** • year – 2 bytes, • month – 1 byte, • day – 1 byte, • hour – 1 byte, • minute – 1 byte

user.conf	
Setting	**Description**
WSMFwdRx_X_EndTime	The WSMFwdRx_X_ EndTime option specifies the time to stop forwarding WSMs to an external host. The RSU supports up to 10 individual configurations for WSM forwarding, where the X indicates the configuration number [0 – 9]. Valid values are any time in the format, **mm/dd/yyyy, hh:mm** **SNMP OID:** 1.0.15628.4.1.7.1.9.X **SNMP Format: YYMDHm** • year – 2 bytes, • month – 1 byte, • day – 1 byte, • hour – 1 byte, • minute – 1 byte
WBSS_Service_X_PSID	The WBSS_Service_X_PSID option specifies the PSID of the Xth service present in the WSA broadcast. The RSU supports up to 32 individual configurations for WSA Services, where the X indicates the service number [0 – 31]. **Note:** If security is enabled, the WSA certificate **MUST** contain the specified PSID to successfully sign the WSA Valid values are any valid PSID **SNMP OID:** 1.0.15628.4.1.13.1.2.X **SNMP Format:** 2 bytes
WBSS_Service_X_Prio	The WBSS_Service_X_Prio option specifies the priority of the Xth service present in the WSA broadcast. The RSU supports up to 32 individual configurations for WSA Services, where the X indicates the service number [0 – 31]. Valid values are any valid priority [0 – 32] **SNMP OID:** 1.0.15628.4.1.13.1.3.X **SNMP Format:** 1 byte
WBSS_Service_X_PSC	The WBSS_Service_X_PSC option specifies the provider service context string of the Xth service present in the WSA broadcast. The RSU supports up to 32 individual configurations for WSA Services, where the X indicates the service number [0 – 31]. Valid values are any valid 4 character string **SNMP OID:** 1.0.15628.4.1.13.1.4.X **SNMP Format:** 4 byte string

user.conf	
Setting	**Description**
WBSS_Service_X_IPAddress	The WBSS_Service_X_ IPAddress option specifies the IPv6 Address of the Xth service present in the WSA broadcast. The RSU supports up to 32 individual configurations for WSA Services, where the X indicates the service number [0 – 31]. If not specified, the service does not include an IP service. Valid values are any valid IPv6 address **SNMP OID:** 1.0.15628.4.1.13.1.5.X **SNMP Format:** 16 bytes
WBSS_Service_X_IPPort	The WBSS_Service_X_ IPPort option specifies the IP port of the Xth service present in the WSA broadcast. The RSU supports up to 32 individual configurations for WSA Services, where the X indicates the service number [0 – 31]. Valid values are any valid port number **SNMP OID:** 1.0.15628.4.1.13.1.6.X **SNMP Format:** 2 bytes
WBSS_Service_X_ChanId	The WBSS_Service_X_ChanId option specifies the channel of the Xth service present in the WSA broadcast. The RSU supports up to 32 individual configurations for WSA Services, where the X indicates the service number [0 – 31]. Valid values are: • SCH (Service channel) • CCH (Control Channel) • LCH (Continuous channel) **SNMP OID:** 1.0.15628.4.1.13.1.7.X **SNMP Format:** 3 byte string
WBSS_WSA_OverridePrefix	The WBSS_WSA_ OverridePrefix option specifies an override to the IPv6 address prefix of the WRA in the WSA broadcast. If not set the prefix of in the WSA will be specified based on the IPv6 address of the DSRC interface (wave-data). Valid values are any valid IPv6 address. Default value: Not set (base the prefix on the IPv6 address assigned to wave-data) **SNMP OID:** 1.0.15628.4.1.14.1.2.1 **SNMP Format:** 16 bytes

user.conf	
Setting	**Description**
WBSS_WSA_OverridePrefixLength	The WBSS_WSA_ OverridePrefixLength option specifies an override to the IPv6 prefix length of the prefix specified in the WRA of the WSA broadcast. This value is only used if the WBSS_WSA_OverridePrefix option is also specified. Valid values are any valid IPv6 address prefix length Default value: 52 **SNMP OID:** 1.0.15628.4.1.14.1.3.1 **SNMP Format:** 1 byte
WBSS_WSA_OverrideGateway	The WBSS_WSA_OverrideGateway option specifies an override to the gateway IPv6 address of the WRA in the WSA broadcast. If not set the gateway of in the WSA will be specified as the IPv6 address of the DSRC interface (wave-data). Valid values are any valid IPv6 address. Default value: Not set (use the IPv6 address assigned to wave-data) **SNMP OID:** 1.0.15628.4.1.14.1.4.1 **SNMP Format:** 16 bytes
WBSS_WSA_DNS	The WBSS_WSA_DNS option specifies the DNS entry, as an IPv6 address, of the WRA in the WSA broadcast. Valid values are any valid IPv6 address Default value: 2001:470:20::2 (Hurricane Electric IPv6 DNS server) **SNMP OID:** 1.0.15628.4.1.14.1.5.1 **SNMP Format:** 16 bytes
ForcedControlChanNum	The ForcedControlChanNum option specifies the channel number used for the Control Channel on the alternating radio. Valid values are: • 178 Default value: 178 **SNMP OID:** 1.0.15628.4.1.12.1.4.1 **SNMP Format:** 1 byte

user.conf	
Setting	**Description**
ForcedSerChanNum	The ForcedSerChanNum option specifies the channel number used for the Service Channel on the alternating radio. Valid values are: • 172 • 174 • 176 • 180 • 182 • 184 Default value: 184 **SNMP OID:** 1.0.15628.4.1.12.1.5.1 **SNMP Format:** 1 byte
ContinuousChanNum	The ContinuousChanNum option specifies the channel number used for the Continuous Radio. Valid values are: • 172 • 174 • 176 • 180 • 182 • 184 Default value: 172 **SNMP OID:** 1.0.15628.4.1.12.1.5.2 **SNMP Format:** 1 byte

5 Processing reference guide

5.1 Capabilities

As stated in section 3.4 the RSU broadly performs the following functions:

- Broadcasts SAE J2735 messages on the DSRC radio interface
- Monitors for forwarded SAE J2735 messages on its Ethernet Interface to broadcast on DSRC radio interface
- Receives Wave Short Messages (WSM)
- Transmits Wave Service Announcements (WSA)
- Routes IPv6 traffic for connected mobile units
- IEEE 1609.2 message signing and verification
- Logs transmitted and received message on DSRC radio interface
- Logs system status messages

5.1.1 Application configuration and management

The RSU application is configured by the options outlined in section 4.2.2. Many of these configuration options are configured via the SNMPv3 service running on the RSU.

Configuration options that are marked as SNMP items should be configured **ONLY** by SNMP and not by manual configuration file manipulation as the SNMP configuration is used in preference to any manual configuration changes.

Configuration options that are not marked as SNMP items should be configured either in **ONLY** ***rsu.cfg*** or ***stack.conf*** as appropriate*.*

5.1.1.1 SNMP

The RSU's SNMP service leverages **net-snmp** [3] at its core. The SNMP implementation uses SNMPv3, which include mechanisms for improved security over the v2c and v1 counterparts. Primarily, SNMP information is only accessible by authenticated SNMP users.

The RSU MIB definition file is located at **/mnt/ubi/rsu1609/snmp/mibs/** in the RSU. It is also listed in section 8 (Appendix B) of this document.

5.1.1.1.1 User creation

To create a new SNMP user account, follow the following steps.

- Log onto the RSU via SSH. See section 4.1.2 for more information
- Create a new SNMPv3 username and password using the **net-snmp-config** utility

```
## Escalate privileges
rsu@ MK5:/ $ sudo –i

## Stop any running RSU applications
root@ MK5:/ $ /opt/cohda/application/rc.local stop

## Create the SNMP user, replacing $PASSWORD and $USERNAME with appropriate strings
root@ MK5:/ $ net-snmp-config --create-snmpv3-user -A $PASSWORD -X $PASSWORD -a SHA -x
AES $USERNAME
```

```
## Re-start the RSU application
root@ MK5:/ $ /opt/cohda/application/rc.local start
```

5.1.1.1.2 SNMP Walk/Get/Set

Following the SNMP user creation outlined in section 5.1.1.1.1, an external host is capable of managing the RSU remotely via the SNMP interface (using the configured credentials). Examples that follow will utilise the net-snmp utilities for performing GET/SET/WALK operations.

SNMP GET

The values of individual SNMP MIB items can be retrieved by performing SNMP GET requests for specified SNMP OIDs. The **snmpget** utility allows either single OID retrieval or a list of OIDs.

```
snmpget -v 3 -l authPriv -u $USERNAME -A $PASSWORD -X $PASSWORD -a SHA -x AES $RSU_IP_ADDR $OID1 … $OIDn
```

SNMP WALK

The values of all (or a subset) SNMP MIB items can be retrieved by performing an SNMP WALK request for a specified SNMP OID tree. The **snmpwalk** utility allows the specification of the root of the SNMP OID tree to walk.

```
snmpwalk -v 3 -l authPriv -u $USERNAME -A $PASSWORD -X $PASSWORD -a SHA -x AES $RSU_IP_ADDR $ROOT_OID
```

SNMP SET

The value of writable SNMP MIB items can be set by performing an SNMP SET request for a specified SNMP OID and value pair. This operation is explicitly only allowed while the RSU is in **standby** mode. See sections 4.3.4 and 4.3.5 or more information on setting the mode of the RSU device. The **snmpset** utility can be used for this purpose.

```
snmpset -v 3 -l authPriv -u $USERNAME -A $PASSWORD -X $PASSWORD -a SHA -x AES $RSU_IP_ADDR $OID $TYPE $VALUE
```

5.1.1.1.3 RSU Status

The RSU provides several status indicators via the SNMP interface which are in addition to the SNMP OIDs used for configuration.

SNMP status	
Setting	**Description**
rsuRadioStatus	The rsuRadioStatus option indicates the status of the RSUs radios Status values are: • 0 – indicates both continuous and alternating radios are operational • 1 – indicates continuous radio is not operational and alternating radio is operational • 2 – indicates continuous radio is operational and alternating radio is not operational • 3 – indicates both continuous and alternating radios are not operational **SNMP OID:** 1.0.15628.4.1.0
rsuContMacAddress	The rsuContMacAddress option indicates the MAC address assigned to the continuous radio. **SNMP OID:** 1.0.15628.4.1.1

SNMP status	
Setting	**Description**
rsuAltMacAddress	The rsuAltMacAddress option indicates the MAC address assigned to the alternating radio. **SNMP OID:** 1.0.15628.4.1.2
rsuGPSStatus	The rsuGPSStatus option indicates the number of GPS satelites currently in view of the RSU. **SNMP OID:** 1.0.15628.4.1.3
rsuSysObjectID	The rsuSysObjectID option indicates the System OID of the RSU. **SNMP OID:** 1.0.15628.4.1.6.0
rsuMode	The rsuMode option indicates the current state the RSU is operating in. See section 4.3 for more information about the possible RSU states. Status values are: • 2 – indicates the RSU is in Standby mode • 4 – indicates the RSU is in Operating mode **SNMP OID:** 1.0.15628.4.1.99.1.0 **SNMP Format:** 1 byte integer

5.1.2 SAE J2735 message broadcast

The RSU application provides a service to broadcast SAE J2735 messages on the DSRC radio set. The broadcast of the SEA J2735 message is governed by the characteristics of the Active Message (template is shown in section 7 - Appendix A) such as TxInterval, DeliveryStart and DeliveryStop.

The RSU is capable of broadcasting messages based on the Active Message format that are,

- Loaded and stored, prior to the RSU application starting, as files (with extension .txt) at ***/mnt/ubi/rsu1609/msg***
- Configured via SNMP (as outlined in section **Error! Reference source not found.**)
- Forwarded to the RSU over a UDP socket whose port number is configured by the ***ActiveMsgs*** entries in **rsu.cfg** as outlined in section **Error! Reference source not found.**).

Examples of valid Traveller Information Message (TIM), Signal Phase and Timing (SPAT) and MAP messages using the Active Message format are located at ***/opt/cohda/application/rsu1609/example***.

Note: Active Message broadcasts are enabled when the RSU device is in the Operate state.

While in the Operate state, Active Messages can be added/removed/modified via SNMP and these modifications will automatically take effect without requiring the RSU to be transitioned out of the Operate state.

5.1.3 WSM forwarding

WSM messages received on the DSRC interface of the RSU can be automatically forwarded to a network-attached host. The SAE J2735 payload of the WSM is forwarded to the specified host/s. The RSU supports forwarding to up to 10 hosts, where specifically matched PSID and RSSIs can be filtered. The WSM forwarding is configured using SNMP. See section **Error! Reference source not found.** for more information on configuring the WSM forwarding.

5.1.4 System Logging

The RSU logs syslog messages to the filesystem at ***/mnt/ubi/log/current/syslog***. This log includes all standard syslog information as well as the following RSU specific information including, but not limited to

- RSU state transitions
- SNMP configuration issues
    a. Value bounds checking
    b. Failures
- Network connectivity of the RSU
    a. Connected
    b. Not Connected
- GPS acquisition failures

5.1.5 Interface Logging

The RSU logs PCAP files for the various DSRC interfaces. By default this logging is disabled, however can be configured via SNMP to enable and set the operating parameters. See section **Error! Reference source not found.** for details on how to configure the interface logging parameters.

When enabled the RSU will log to ***/mnt/ubi/log/current*** populating files that are named by the following convention

<RSU ID>-<Interface>-<Timestamp of start of capture>.pcap

For example, when the RSU is configuration with an RSU ID of ‘RSU_4_1’:

- RSU_4_1-cw-mon-rxa-20160113045245.pcap
- RSU_4_1-cw-mon-rxb-20160113045245.pcap
- RSU_4_1-cw-mon-txa-20160113045245.pcap
- RSU_4_1-cw-mon-txb-20160113045245.pcap

5.1.6 Firewall

The RSU implements a firewall capability utilising the Uncomplicated Firewall [3]. It is configured by logging into the RSU over SSH and running the **ufw** utility.

5.1.6.1 Access Control List (ACL)

An access control list can be configured for the RSU using the **ufw** utility. This capability limits access to the RSU from a specified set of IP addresses by following the procedure outlined below.

```
## Escalate privileges
rsu@ MK5:/ $ sudo –i

## Add the allowed set of IP Address (IPv4 or IPv6) to the ACL
root@ MK5:/ $ ufw allow from <IP ADDRESS>

## Set the default policy for the firewall to deny all traffic that is not specifically allowed
```

```
root@ MK5:/ $ ufw default deny incoming

## Enable the firewall
root@ MK5:/ $ ufw enable
```

WARNING! By default the RSU has no ACL configured, therefore by default all incoming traffic is allowed. It is the responsibility of the end-user to configure an appropriate ACL for the site security policy.

5.1.7 IPv6 Connectivity

IPv6 connectivity can be configured on the RSU in two different ways – Either using an IPv6 in IPv4 tunnel, or using a native IPv6 configuration.

5.1.7.1 IPv6 in IPv4 SIT tunnel

An IPv6 in IPv4 SIT tunnel may be used as the IPv6 implementation on the RSU. This service is enabled using the ***IPV6SITTunnel*** configuration discussed in section4.4.1.1. This configuration creates an IPv6 in IPv4 tunnel between two locally administered IPv6 networks as depicted in Figure 11, however does not provide IPv6 connectivity to the broader Internet - unless of course the SIT tunnel endpoint provides appropriate routing to allow this.

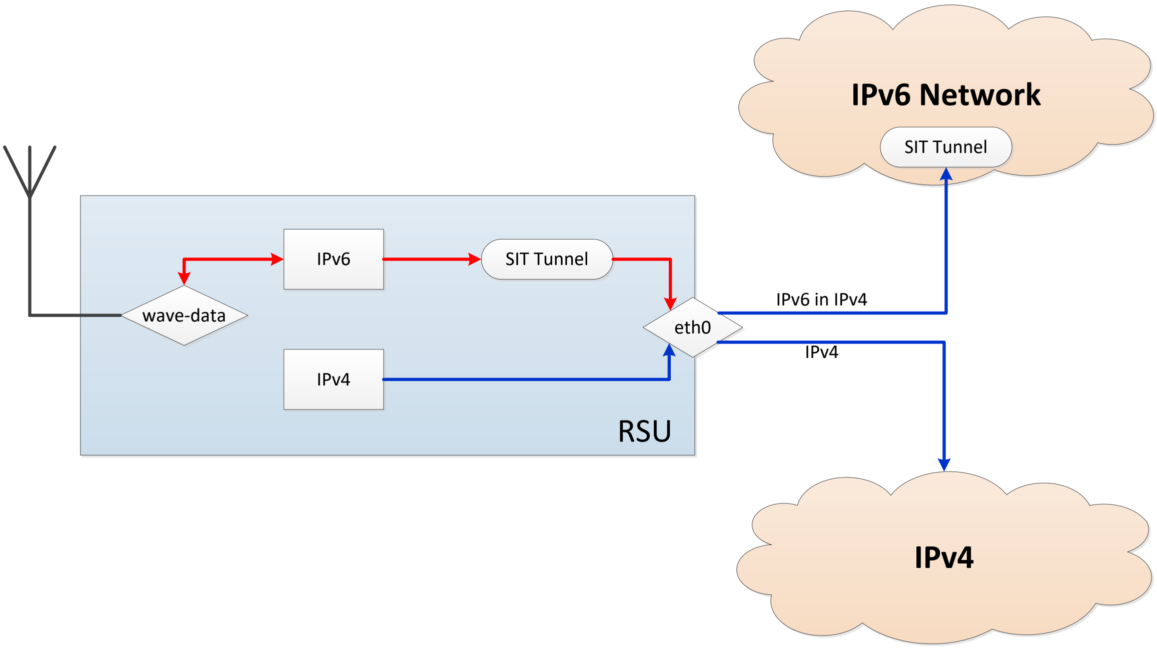

Figure 11: IPv6 in IPv4 SIT tunnel architecture

5.1.7.2 Native IPv6

Native IPv6 can be configured on the RSU using the ***IPV6NDPBridge*** configuration discussed in Section **Error! Reference source not found.**. When enabled, the RSU creates an IPv6 bridge such that an IPv6 address assigned to the eth0 interface of the RSU (through say stateless address autoconfiguration) is shared with the DSRC radio interface (wave-data) with the RSU acting as a bridge. This architecture is depicted in Figure 12.

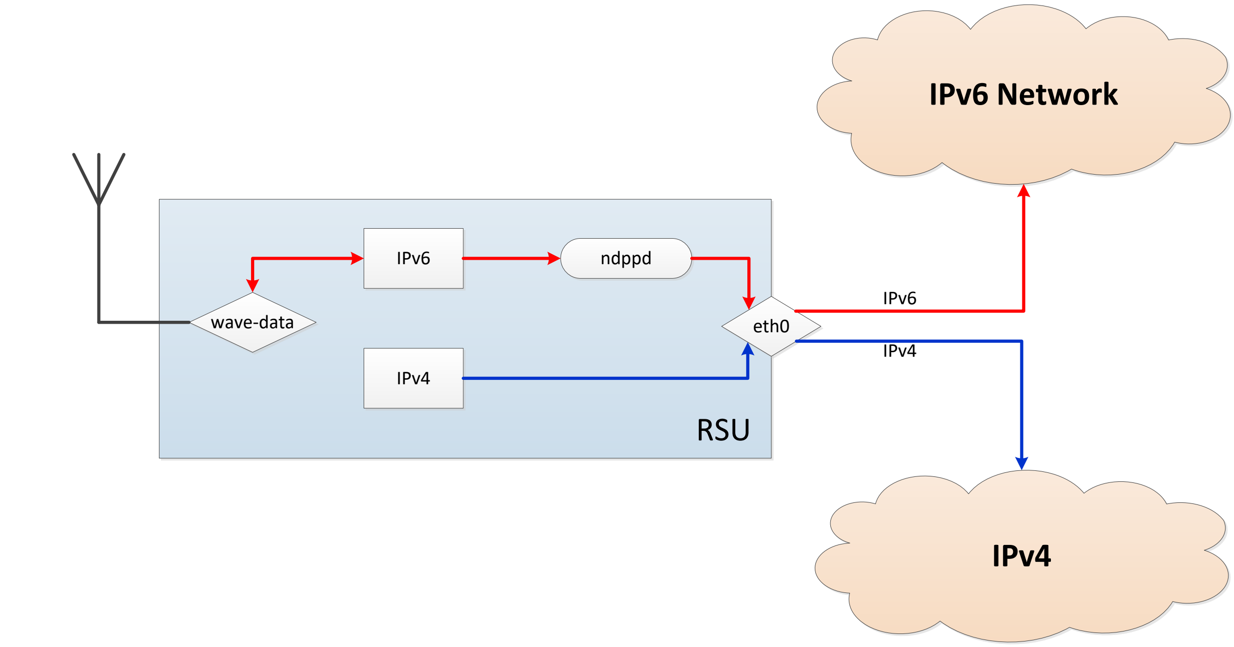

Figure 12: IPv6 auto-configured bridge architecture

5.1.8 GPS Output

The RSU can be configured to forward the GGA NMEA sentences retrieved from the on-board GPS unit to an external host. This service sends the NMEA sentences as the raw string over UDP to the host configured by the ***NMEAFwd*** option discussed in section **Error! Reference source not found.**.

A listening service at the configured external host will observe output of the form shown below.

```
$GNGGA,044848.00,3454.36594,S,13836.48506,E,1,12,0.67,-11.3,M,-3.5,M,,*57
```

5.1.9 Factory Reset

The RSU provides a mechanism to reset the device back to the ***factory (Initial)*** state.

This is made possible because the RSU root filesystem is a temporary overlay. This means that any changes to the rootfs are not persisted on reboot. For this reason any persistent data is stored under **/mnt/ubi/** which provides persistent storage across reboot cycles.

The ***factory-reset*** utility can be executed by the root user to remove all persistent data under ***/mnt/ubi/*** and then rebooting the device to set it back to the initial state.

```
root@ MK5:/ $ factory-reset
```

Output will be similar to the following.

```
root@MK5:/mnt/ubi $ factory-reset
Running: rm -rf /mnt/ubi/log/*
rm -rf /mnt/ubi/rc.local
rm -rf /mnt/ubi/rsu1609
Rebooting in 5 seconds...
root@MK5:/mnt/ubi#
Broadcast message from rsu@MK5
```

```
         (/dev/pts/0) at 0:53 ...

The system is going down for reboot NOW!
Connection to fe80::06e5:48ff:fe01:3600%eth1 closed by remote host.
```

5.2 Conventions

This paragraph is not used and has been tailored out in line with ISO 12207 guidelines.

5.3 Processing Procedures

This paragraph is not used and has been tailored out in line with ISO 12207 guidelines.

5.4 Related processing

This paragraph is not used and has been tailored out in line with ISO 12207 guidelines.

5.5 Data backup

This paragraph is not used and has been tailored out in line with ISO 12207 guidelines.

5.6 Recovery from errors, malfunctions, and emergencies

This paragraph is not used and has been tailored out in line with ISO 12207 guidelines.

5.7 Messages

The RSU application produces several log files located at ***/mnt/ubi/log***. A symbolic link, labelled *current*, will point to the active logging directory. By default the logging directory will contain the following files:

File	Description
conf	List of all currently applied configuration options.
stderr	All messages produced on the stderr stream.
*.pcap	Pcap capture of transmitted/received frames on DSRC radios.

Log files and directories may be inspected, deleted, moved or copied (locally and remotely). Remote transferring will depend on network connectivity and structure. In general the MKx secure copy tool, *scp*, may be used for basic file offload. For example, to offload to Linux host the following command may be used.

```
root@ MK5:/mnt/ubi/log/current $ scp <file> <username>@<remote_ip>:<off_load path>
```

6 Notes

6.1 Glossary

This paragraph is not used and has been tailored out in line with ISO 12207 guidelines.

6.2 Acronyms and Abbreviations

DSRC	Dedicated Short Range Communications
OBU	On-board Unit
RSU	Roadside Unit
MAP	Geographic information for a road or intersection
NDP	Neighbour Discovery Protocol
SIT	Simple Internet Translation
SPAT	Signal Phase and Timing
TIM	Traveller Information

7 Appendix A

7.1 Active Message Template

```
# Modified Date: 04/10/2014
# Version: 0.7
Version=0.7
#
# Message Dispatch Items
#
# All line beginning with # shall be removed in file sent to radio
#
# Message Type
# Values: SPAT, MAP, TIM, (other message types)
Type=<Type>
#
# Message PSID as a 2 Byte Hex value (e.g. 0x8003)
PSID=<PSID>
#
# Message Priority in the range of 0 (lowest) through 7
Priority=<priority>
#
# Transmission Channel Mode
# Allowed values: CONT, ALT
TxMode=<txmode>
# Allowed values: 172, CCH, SCH (note: “CCH” refers to DSRC Channel 178 and SCH refers to the operator configured DSRC Service Channel)
TxChannel=<channel>
#
# Transmission Broadcast Interval in Seconds
# Allowed values: 0 for Immediate-Forwarding, 1 to 5 for Store-and-Repeat
TxInterval=<txinterval>
#
# Message Delivery (broadcast) start time (UTC date and time) in the form:
# "mm/dd/yyyy, hh:mm”
# Leave value blank if Immediate Forward mode
DeliveryStart=<mm/dd/yyyy, hh:mm>
#
# Message Delivery (broadcast) stop time (UTC date and time) in the form:
# "mm/dd/yyyy, hh:mm”
# Leave value blank if Immediate Forward mode
DeliveryStop=<mm/dd/yyyy, hh:mm>
#
# Message Signature/Encryption
Signature=<True\False>
Encryption=<True\False>
#
# Message Payload (encoded according to J2735 or other definition)
Payload=<DSRC message payload>
```

8 Appendix B

8.1 SNMP RSU MIB

```
RSU-MIB DEFINITIONS ::= BEGIN

IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, Integer32,
        Counter32, NOTIFICATION-TYPE          FROM SNMPv2-SMI
        TEXTUAL-CONVENTION, DateAndTime, RowStatus,
        PhysAddress, DisplayString, MacAddress       FROM SNMPv2-TC
        MODULE-COMPLIANCE, OBJECT-GROUP              FROM SNMPv2-CONF
        Ipv6Address                                  FROM IPV6-TC;

rsuMIB MODULE-IDENTITY
        LAST-UPDATED   "201710020000Z"
        ORGANIZATION   "US-DOT"
        CONTACT-INFO   "postal:       TBD
                                       email:        TBD@TBD.com"
        DESCRIPTION           "Leidos implementation RSU 4.1 MIB based on
                                       Savari and Cohda implementation of RSU 4.0"
        REVISION              "201710020000Z"
        DESCRIPTION           "Allow RsuPsidTC length up to 4,
                                       rsuWsaProviderContext length to 32 (match dot3),
                                       rsuSRMPayload length to 2302 (match dot3)"
        REVISION              "201702200000Z"
        DESCRIPTION           "Corrections to INTEGER/Integer32 types and typos"
        REVISION              "201610310000Z"
        DESCRIPTION           "Final Draft for RSU 4.1 Spec."
        REVISION              "201608310230Z"
        DESCRIPTION           "Second Draft for RSU 4.1 Spec."
        REVISION              "201608120230Z"
        DESCRIPTION           "First Draft for RSU 4.1 Spec."
        REVISION              "201606270245Z"
        DESCRIPTION           "Combining input from Vendors"
        REVISION              "201404150000Z"          -- 15 April 2014 midnight
        DESCRIPTION           "RSU MIB Definitions"
        ::= { iso std(0) rsu(15628) version(4) 1 }



RsuTableIndex ::= TEXTUAL-CONVENTION
        DISPLAY-HINT   "d"
        STATUS         current
        DESCRIPTION
               "A valid range of values for use in table indices"
        SYNTAX         Integer32 (1..2147483647)

RsuPsidTC ::= TEXTUAL-CONVENTION
        DISPLAY-HINT   "4x"
        STATUS         current
        DESCRIPTION
               "PSID associated with a DSRC message."
        SYNTAX         OCTET STRING (SIZE(1..4))


rsuContMacAddress OBJECT-TYPE
    SYNTAX      MacAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
    "Represents an 802 MAC address of the DSRC Radio operating in
         Continuous Mode represented in the 'canonical' order defined by
         IEEE 802.1a, i.e., as if it were transmitted least significant
         bit first, even though 802.5 (in contrast to other 802.x protocols)
         requires MAC addresses to be transmitted most significant bit first"
    ::= { rsuMIB 1 }
```

```
-- add entries for multiple antennas

rsuAltMacAddress OBJECT-TYPE
    SYNTAX      MacAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents an 802 MAC address of the DSRC Radio operating in
         Alternating Mode represented in the 'canonical' order defined
         by IEEE 802.1a, i.e., as if it were transmitted least significant
         bit first, even though 802.5 (in contrast to other 802.x protocols)
         requires MAC addresses to be transmitted most significant bit first"
    ::= { rsuMIB 2 }


rsuGpsStatus OBJECT-TYPE
       SYNTAX       Integer32 (0..15)
       MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
       "Provides the number of GPS Satellites RSUxs internal GPS receiver is
              tracking"
       ::= { rsuMIB 3 }


rsuSRMStatusTable OBJECT-TYPE
       SYNTAX SEQUENCE OF RsuSRMStatusEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "Provides configuration information for each Store
       Repeat message sent by an RSU."
       ::= { rsuMIB 4 }


rsuSRMStatusEntry OBJECT-TYPE
       SYNTAX RsuSRMStatusEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
              "A row describing RSU Store and Repeat Message Status"
       INDEX    { rsuSRMIndex }
       ::= {rsuSRMStatusTable 1 }


RsuSRMStatusEntry ::= SEQUENCE {
        rsuSRMIndex             RsuTableIndex,
        rsuSRMPsid              RsuPsidTC,
        rsuSRMDsrcMsgId         Integer32,
        rsuSRMTxMode            INTEGER,
        rsuSRMTxChannel         Integer32,
        rsuSRMTxInterval        Integer32,
        rsuSRMDeliveryStart     OCTET STRING,
        rsuSRMDeliveryStop      OCTET STRING,
        rsuSRMPayload           OCTET STRING,
        rsuSRMEnable            INTEGER,
        rsuSRMStatus            RowStatus
    }

rsuSRMIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Store and Repeat Message Index "
    ::= { rsuSRMStatusEntry 1 }

rsuSRMPsid OBJECT-TYPE
    SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Store and Repeat Message PSID"
    ::= { rsuSRMStatusEntry 2 }

rsuSRMDsrcMsgId OBJECT-TYPE
    SYNTAX       Integer32
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Store and Repeat Message DSRC Message ID"
    ::= { rsuSRMStatusEntry 3 }

rsuSRMTxMode OBJECT-TYPE
        SYNTAX       INTEGER { cont(0), alt(1) }
        MAX-ACCESS   read-create
        STATUS       current
        DESCRIPTION
               "DSRC mode set for Store and Repeat Message transmit,
                Continuous or Alternating"
        ::= { rsuSRMStatusEntry 4 }

rsuSRMTxChannel OBJECT-TYPE
    SYNTAX       Integer32 (172..184)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC channel set for Store and Repeat Message transmit"
    ::= { rsuSRMStatusEntry 5 }

rsuSRMTxInterval OBJECT-TYPE
    SYNTAX       Integer32 (1..2147483647)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Time interval in milliseconds between two successive
                Store and Repeat Messages"
    ::= { rsuSRMStatusEntry 6 }

rsuSRMDeliveryStart OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0|6))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Store and Repeat Message delivery start time"
    ::= { rsuSRMStatusEntry 7 }

rsuSRMDeliveryStop OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0|6))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Store and Repeat Message delivery stop time"
        ::= { rsuSRMStatusEntry 8 }

rsuSRMPayload OBJECT-TYPE
        SYNTAX       OCTET STRING (SIZE(0..2302))
        MAX-ACCESS   read-create
        STATUS       current
        DESCRIPTION
               "Payload of Store and Repeat message.
               Length limit derived from dot3MIB."
        ::= { rsuSRMStatusEntry 9 }

rsuSRMEnable OBJECT-TYPE
        SYNTAX       INTEGER { off(0), on(1) }
        MAX-ACCESS   read-create
        STATUS       current
        DESCRIPTION
               "Set this bit to enable transmission of the message
```

```
                0=off, 1=on"
        ::= { rsuSRMStatusEntry 10 }

rsuSRMStatus OBJECT-TYPE
        SYNTAX       RowStatus
        MAX-ACCESS   read-create
        STATUS       current
        DESCRIPTION
               "create and destroy row entry"
        ::= { rsuSRMStatusEntry 11 }


rsuIFMStatusTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuIFMStatusEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Provides configuration parameters for each Immediate
        Forward message sent by an RSU."
    ::= { rsuMIB 5 }

rsuIFMStatusEntry OBJECT-TYPE
    SYNTAX       RsuIFMStatusEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "A row describing RSU Immediate Forward Message Status"
    INDEX    { rsuIFMIndex }
    ::= {rsuIFMStatusTable 1 }

RsuIFMStatusEntry ::= SEQUENCE {
    rsuIFMIndex             RsuTableIndex,
    rsuIFMPsid              RsuPsidTC,
    rsuIFMDsrcMsgId         Integer32,
        rsuIFMTxMode            INTEGER,
    rsuIFMTxChannel         Integer32,
        rsuIFMEnable            INTEGER,
        rsuIFMStatus                  RowStatus
    }


rsuIFMIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Immediate Forward Message Index "
    ::= { rsuIFMStatusEntry 1 }


rsuIFMPsid OBJECT-TYPE
    SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Immediate Forward Message PSID"
    ::= { rsuIFMStatusEntry 2}


rsuIFMDsrcMsgId OBJECT-TYPE
    SYNTAX       Integer32
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Immediate Forward Message DSRC Message ID"
    ::= { rsuIFMStatusEntry 3 }

rsuIFMTxMode OBJECT-TYPE
        SYNTAX       INTEGER { cont(0), alt(1) }
        MAX-ACCESS   read-create
        STATUS       current
        DESCRIPTION
               "Immediate Forward Message Transmit Mode
                Alternating or Continuous"
        ::= { rsuIFMStatusEntry 4 }

rsuIFMTxChannel OBJECT-TYPE
    SYNTAX       Integer32 (172..184)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC channel set for Immediate Forward Message transmit"
    ::= { rsuIFMStatusEntry 5 }

rsuIFMEnable OBJECT-TYPE
    SYNTAX       INTEGER { off(0), on(1) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Set this bit to enable transmission of the message
                0=off, 1=on"
    ::= { rsuIFMStatusEntry 6 }

rsuIFMStatus OBJECT-TYPE
        SYNTAX       RowStatus
        MAX-ACCESS   read-create
        STATUS       current
        DESCRIPTION
               "create and destroy row entry"
        ::= { rsuIFMStatusEntry 7}


rsuSysObjectID OBJECT-TYPE
    SYNTAX       OBJECT IDENTIFIER
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
       "The vendor's authoritative identification of the network
        management subsystem contained in the entity. This value
        is allocated within the DSRC subtree (1.0.15628.4) and
        provides an easy and unambiguous means for determining
        `what kind of box' is being managed. 1.0.15628.4.1.6.0
        indicates an RSU"
    ::= { rsuMIB 6 }


rsuDsrcForwardTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuDsrcForwardEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "contains the DSRC PSID being forwarded to a network host,
        the IP Address and port number of the destination host, as
        well as other configuration parameters as defined."
    ::= { rsuMIB 7}


rsuDsrcForwardEntry OBJECT-TYPE
    SYNTAX       RsuDsrcForwardEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "A row describing RSU Message Forwarding"
    INDEX   { rsuDsrcFwdIndex }
    ::= {rsuDsrcForwardTable 1 }


RsuDsrcForwardEntry ::= SEQUENCE {
        rsuDsrcFwdIndex              RsuTableIndex,
        rsuDsrcFwdPsid               RsuPsidTC,
        rsuDsrcFwdDestIpAddr         Ipv6Address,
        rsuDsrcFwdDestPort           Integer32,
        rsuDsrcFwdProtocol           INTEGER,
        rsuDsrcFwdRssi               Integer32,
        rsuDsrcFwdMsgInterval        Integer32,
        rsuDsrcFwdDeliveryStart      OCTET STRING,
        rsuDsrcFwdDeliveryStop       OCTET STRING,
        rsuDsrcFwdEnable             INTEGER,
        rsuDsrcFwdStatus             RowStatus
}

rsuDsrcFwdIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Message Forward Message Index "
    ::= { rsuDsrcForwardEntry 1 }

rsuDsrcFwdPsid OBJECT-TYPE
    SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC Message Forward PSID"
    ::= { rsuDsrcForwardEntry 2 }


rsuDsrcFwdDestIpAddr OBJECT-TYPE
    SYNTAX       Ipv6Address
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC Message Forward Destination Server IP address"
    ::= { rsuDsrcForwardEntry 3 }


rsuDsrcFwdDestPort OBJECT-TYPE
    SYNTAX       Integer32 (1024 .. 65535)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC Message Forward Destination Server Port Number"
    ::= { rsuDsrcForwardEntry 4 }

rsuDsrcFwdProtocol OBJECT-TYPE
    SYNTAX       INTEGER { tcp(1), udp(2) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC Message Forward Transport Protocol between RSU and Server"
    ::= { rsuDsrcForwardEntry 5 }

rsuDsrcFwdRssi OBJECT-TYPE
    SYNTAX       Integer32 (-100 .. -60)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Minimum Received Signal Strengh Level of DSRC Messages should be
        Forwarded to server"
    ::= { rsuDsrcForwardEntry 6 }

rsuDsrcFwdMsgInterval OBJECT-TYPE
    SYNTAX       Integer32 (1 .. 9)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Interval with which RSU forwards DSRC Messages to Server"
    ::= { rsuDsrcForwardEntry 7 }
```

```
rsuDsrcFwdDeliveryStart OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0|6))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Start time for RSU to start forwarding DSRC Messages to Server"
    ::= { rsuDsrcForwardEntry 8 }


rsuDsrcFwdDeliveryStop OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0|6))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Stop time for RSU to stop forwarding DSRC Messages to Server"
    ::= { rsuDsrcForwardEntry 9 }

rsuDsrcFwdEnable OBJECT-TYPE
    SYNTAX       INTEGER { off(0), on(1) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Stop time for RSU to stop forwarding DSRC Messages to Server"
    ::= { rsuDsrcForwardEntry 10 }

rsuDsrcFwdStatus OBJECT-TYPE
    SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "create and destroy row entry "
    ::= { rsuDsrcForwardEntry 11 }


rsuGpsOutput OBJECT IDENTIFIER ::= { rsuMIB 8 }

rsuGpsOutputPort OBJECT-TYPE
    SYNTAX       Integer32 (1024 .. 65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "GPS Out External Server Port Number"
        ::= { rsuGpsOutput 1 }

rsuGpsOutputAddress OBJECT-TYPE
       SYNTAX       Ipv6Address
       MAX-ACCESS   read-write
       STATUS       current
       DESCRIPTION
               "Remote host IPv6 address to which to send the GPS string"
       ::= { rsuGpsOutput 2 }

rsuGpsOutputInterface OBJECT-TYPE
       SYNTAX       DisplayString
       MAX-ACCESS   read-write
       STATUS       current
       DESCRIPTION
               "Local interface on which to output the GPS string"
       ::= { rsuGpsOutput 3 }

rsuGpsOutputInterval OBJECT-TYPE
       SYNTAX       Integer32 (1..18000)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Interval at which to send the GPS GPGGA NMEA String
        to external Server in seconds."
       ::= { rsuGpsOutput 4 }

rsuGpsOutputString OBJECT-TYPE
```

```
        SYNTAX       DisplayString (SIZE(0..100))
        MAX-ACCESS   read-only
        STATUS       current
        DESCRIPTION
               "Contains GPS NMEA GPGGA output string"
        ::= { rsuGpsOutput 5 }

rsuGpsRefLat OBJECT-TYPE
        SYNTAX       Integer32 (-900000000..900000000)
        MAX-ACCESS   read-write
        STATUS       current
        DESCRIPTION
               "Contains the actual GPS latitude for validation of
                reported GPS latitude in 10^-7 degrees."
        ::= { rsuGpsOutput 6 }

rsuGpsRefLon OBJECT-TYPE
        SYNTAX       Integer32 (-1800000000..1800000000)
        MAX-ACCESS   read-write
        STATUS       current
        DESCRIPTION
               "Contains the actual GPS longitude for validation of
                reported GPS longitude in 10^-7 degrees."
        ::= { rsuGpsOutput 7 }

rsuGpsRefElv OBJECT-TYPE
        SYNTAX       Integer32 (-100000..1000000)
        MAX-ACCESS   read-write
        STATUS       current
        DESCRIPTION
               "Contains the actual GPS elevation for validation of
                reported GPS elevation in centimeters."
        ::= { rsuGpsOutput 8 }

rsuGpsMaxDeviation OBJECT-TYPE
        SYNTAX       Integer32 (1..2000000)
        MAX-ACCESS   read-write
        STATUS       current
        DESCRIPTION
               "Contains the maximum allowable deviation (radius in centimeters)
                for comparison between the reported GPS coordinates and the
                static GPS coordinates."
        ::= { rsuGpsOutput 9 }


rsuInterfaceLogTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF RsuInterfaceLogEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Provides configuration information for capturing log files
        for each communication Interface x represents the
        interface for which these configurations will apply"
    ::= { rsuMIB 9 }

rsuInterfaceLogEntry OBJECT-TYPE
    SYNTAX       RsuInterfaceLogEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "A row describing RSU Interface Log"
    INDEX    { rsuIfaceLogIndex }
    ::= {rsuInterfaceLogTable 1 }

RsuInterfaceLogEntry ::= SEQUENCE {
        rsuIfaceLogIndex             RsuTableIndex,
        rsuIfaceGenerate             INTEGER,
        rsuIfaceMaxFileSize          Integer32,
        rsuIfaceMaxFileTime          Integer32,
               rsuIfaceLogByDir             INTEGER,
               rsuIfaceName                 DisplayString
   }

rsuIfaceLogIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        " Interface Logging Index "
    ::= { rsuInterfaceLogEntry 1 }

rsuIfaceGenerate OBJECT-TYPE
    SYNTAX INTEGER { off(0),
                        on(1) }
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Enable / Disable interface logging. '0x00 = OFF' and
        '0x01 = ON'"
    ::= { rsuInterfaceLogEntry 2 }

rsuIfaceMaxFileSize OBJECT-TYPE
    SYNTAX Integer32 (1..40)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Maximum Interface Log File Size in Mega Bytes,
                default is 5."
    ::= { rsuInterfaceLogEntry 3 }

rsuIfaceMaxFileTime OBJECT-TYPE
    SYNTAX Integer32 (1..48)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Maximum Collection time for Interface Logging in hrs,
                default is 24."
    ::= { rsuInterfaceLogEntry 4 }

rsuIfaceLogByDir OBJECT-TYPE
    SYNTAX       INTEGER { off(0), on(1) }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Sets whether or not to separate the log files by direction."
    ::= { rsuInterfaceLogEntry 5 }

rsuIfaceName OBJECT-TYPE
    SYNTAX       DisplayString
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Holds the name of the interface."
    ::= { rsuInterfaceLogEntry 6 }


rsuSecCredReq OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE (1))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "rovides configuration parameters for when an RSU should
        request new 1609.2 security credentials in days before
        existing credentials expire"
    ::= { rsuMIB 10 }


rsuSecCredAttachInterval OBJECT-TYPE
    SYNTAX     Integer32 (1..100)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Provides configuration parameters for when an RSU will attach
        1609.2 security credentials to a WAVE Short Message Protocol
        (WSMP) Message"
    ::= { rsuMIB 11 }


rsuDsrcChannelModeTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuDsrcChannelModeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "Provides Continuous and Alternating Channel Mode
        configurations for each DSRC interface.
        x represents the interface for which these
        configurations will apply"
    ::= { rsuMIB 12  }

rsuDsrcChannelModeEntry OBJECT-TYPE
    SYNTAX RsuDsrcChannelModeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row describing RSU Interface Log"
    INDEX    { rsuDCMIndex }
    ::= {rsuDsrcChannelModeTable 1 }

RsuDsrcChannelModeEntry ::= SEQUENCE {
        rsuDCMIndex       RsuTableIndex,
        rsuDCMRadio       DisplayString,
        rsuDCMMode        INTEGER,
    rsuDCMCCH         Integer32,
    rsuDCMSCH         Integer32
    }

rsuDCMIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        " Radio Interface Channel Mode Index "
    ::= { rsuDsrcChannelModeEntry 1 }

rsuDCMRadio OBJECT-TYPE
        SYNTAX       DisplayString
        MAX-ACCESS   read-only
        STATUS       current
        DESCRIPTION
               "Name of the radio that the configuration relates to."
        ::= { rsuDsrcChannelModeEntry 2 }

rsuDCMMode OBJECT-TYPE
    SYNTAX       INTEGER { cont(0), alt(1) }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
               "DSRC Channel Mode. '0x00 = Continuous Mode'
         and, '0x01 = Alternating Mode'"
    ::= { rsuDsrcChannelModeEntry 3 }

rsuDCMCCH OBJECT-TYPE
    SYNTAX       Integer32 (172..184)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Control Channel number to use - applies in Alternating Mode"
    ::= { rsuDsrcChannelModeEntry 4 }

rsuDCMSCH OBJECT-TYPE
```

```
    SYNTAX       Integer32 (172..184)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Service Channel number to use"
    ::= { rsuDsrcChannelModeEntry 5 }


rsuWsaServiceTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuWsaServiceEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
               "Holds general configuration parameters for the RSU WAVE
         Service Advertisement."
    ::= { rsuMIB 13 }

rsuWsaServiceEntry OBJECT-TYPE
    SYNTAX RsuWsaServiceEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row describing RSU WSA Service "
    INDEX   { rsuWsaIndex }
    ::= {rsuWsaServiceTable 1 }

RsuWsaServiceEntry ::= SEQUENCE {
        rsuWsaIndex                 RsuTableIndex,
        rsuWsaPsid                  RsuPsidTC,
        rsuWsaPriority              Integer32,
        rsuWsaProviderContext       OCTET STRING,
        rsuWsaIpAddress             Ipv6Address,
        rsuWsaPort                  Integer32,
               rsuWsaChannel                Integer32,
            rsuWsaStatus                RowStatus
    }

rsuWsaIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        " WSA Service Index "
    ::= { rsuWsaServiceEntry 1 }

rsuWsaPsid OBJECT-TYPE
       SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "WSA Service PSID"
    ::= { rsuWsaServiceEntry 2 }

rsuWsaPriority OBJECT-TYPE
    SYNTAX       Integer32 (0 .. 63)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Priority of WSA Service Advertised "
    ::= { rsuWsaServiceEntry 3 }

rsuWsaProviderContext OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE (32))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "WSA Service Specific Provider Context "
    ::= { rsuWsaServiceEntry 4 }

rsuWsaIpAddress OBJECT-TYPE
```

```
    SYNTAX       Ipv6Address
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "IPv6 address of WSA Service Advertised "
    ::= { rsuWsaServiceEntry 5 }

rsuWsaPort OBJECT-TYPE
    SYNTAX       Integer32 (1024 .. 65535)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Port Number of WSA Service Advertised "
    ::= { rsuWsaServiceEntry 6 }

rsuWsaChannel OBJECT-TYPE
       SYNTAX       Integer32 (172..184)
       MAX-ACCESS   read-create
       STATUS       current
       DESCRIPTION
              "The number of the channel on which the advertised service is provided."
       ::= { rsuWsaServiceEntry 7 }

rsuWsaStatus OBJECT-TYPE
       SYNTAX       RowStatus
       MAX-ACCESS   read-create
       STATUS       current
       DESCRIPTION
              "create or destroy rows"
       ::= { rsuWsaServiceEntry 8 }


rsuWraConfiguration OBJECT IDENTIFIER ::= { rsuMIB 14 }

rsuWraIpPrefix OBJECT-TYPE
    SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "IPv6 address prefix of WRA Service Advertised "
    ::= { rsuWraConfiguration 1 }

rsuWraIpPrefixLength OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(1))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Length of IPv6 address prefix of WRA Service Advertised "
    ::= { rsuWraConfiguration 2 }

rsuWraGateway OBJECT-TYPE
       SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "IPv6 address of Gateway of WRA Service Advertised "
    ::= { rsuWraConfiguration 3 }

rsuWraPrimaryDns OBJECT-TYPE
       SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "IPv6 address of Primary DNS Server of WRA Service Advertised "
    ::= { rsuWraConfiguration 4 }


rsuMessageStats OBJECT IDENTIFIER ::= { rsuMIB 15 }

rsuAltSchMsgSent OBJECT-TYPE
```

```
    SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages sent on Alternating Service Channel since
                start of service."
    ::= { rsuMessageStats 1 }

rsuAltSchMsgRcvd OBJECT-TYPE
       SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages received on Alternating Service Channel since
                start of service."
    ::= { rsuMessageStats 2 }

rsuAltCchMsgSent OBJECT-TYPE
       SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages sent on Alternating Control Channel since
                start of service."
    ::= { rsuMessageStats 3 }

rsuAltCchMsgRcvd OBJECT-TYPE
       SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages received on Alternating Control Channel since
                start of service."
    ::= { rsuMessageStats 4 }

rsuContSchMsgSent OBJECT-TYPE
       SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages sent on Continuous Service Channel since
                start of service."
    ::= { rsuMessageStats 5 }

rsuContSchMsgRcvd OBJECT-TYPE
       SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages received on Continuous Service Channel since
                start of service."
    ::= { rsuMessageStats 6 }

rsuContCchMsgSent OBJECT-TYPE
       SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages sent on Continuous Control Channel since
                start of service."
    ::= { rsuMessageStats 7 }

rsuContCchMsgRcvd OBJECT-TYPE
       SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages sent on Continuous Control Channel since
                start of service."
    ::= { rsuMessageStats 8 }
```

```
rsuMessageCountsByPsidTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuMessageCountsByPsidEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Provides a count of transmitted messages sorted by PSID.
                Each row is a different PSID."
    ::= { rsuMessageStats 9 }

rsuMessageCountsByPsidEntry OBJECT-TYPE
    SYNTAX RsuMessageCountsByPsidEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row describing the number of messages transmitted "
    INDEX    { rsuMessageCountsByPsidIndex }
    ::= { rsuMessageCountsByPsidTable 1 }

RsuMessageCountsByPsidEntry ::= SEQUENCE {
       rsuMessageCountsByPsidIndex        RsuTableIndex,
       rsuMessageCountsByPsidId           RsuPsidTC,
       rsuMessageCountsByPsidCounts       Counter32,
       rsuMessageCountsByPsidRowStatus    RowStatus
       }

rsuMessageCountsByPsidIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        " WSA Service Index "
    ::= { rsuMessageCountsByPsidEntry 1 }

rsuMessageCountsByPsidId OBJECT-TYPE
       SYNTAX       RsuPsidTC
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the number of seconds that have elapsed
                since the RSU was last powered on."
    ::= { rsuMessageCountsByPsidEntry 2 }

rsuMessageCountsByPsidCounts OBJECT-TYPE
       SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the number of seconds that have elapsed
                since the RSU was last powered on."
    ::= { rsuMessageCountsByPsidEntry 3 }

rsuMessageCountsByPsidRowStatus OBJECT-TYPE
       SYNTAX       RowStatus
       MAX-ACCESS   read-create
       STATUS       current
       DESCRIPTION
              "create or destroy rows"
       ::= { rsuMessageCountsByPsidEntry 4 }


rsuSystemStats OBJECT IDENTIFIER ::= { rsuMIB 16 }

rsuTimeSincePowerOn OBJECT-TYPE
       SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the number of seconds that have elapsed
                since the RSU was last powered on."
    ::= { rsuSystemStats 1 }

rsuTotalRunTime OBJECT-TYPE
       SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the number of seconds that have elapsed
                since the RSU was first powered on."
    ::= { rsuSystemStats 2 }

rsuLastLoginTime OBJECT-TYPE
       SYNTAX       DateAndTime
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the time when the last user logged in."
    ::= { rsuSystemStats 3 }

rsuLastLoginUser OBJECT-TYPE
       SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the name of the last user to log in."
    ::= { rsuSystemStats 4 }

rsuLastLoginSource OBJECT-TYPE
       SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains name or address of the remote host from which
                the last user logged in."
    ::= { rsuSystemStats 5 }

rsuLastRestartTime OBJECT-TYPE
       SYNTAX       DateAndTime
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the time when the RSU process was last started."
    ::= { rsuSystemStats 6 }

rsuIntTemp OBJECT-TYPE
       SYNTAX       Integer32 (-100..100)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the internal temperature of the RSU in degrees Celsius."
    ::= { rsuSystemStats 7 }

rsuSysDescription OBJECT IDENTIFIER ::= { rsuMIB 17 }

rsuMibVersion OBJECT-TYPE
       SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the version of this MIB."
    ::= { rsuSysDescription 1 }

rsuFirmwareVersion OBJECT-TYPE
       SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the version of firmware running on this RSU."
    ::= { rsuSysDescription 2 }
```

```
rsuLocationDesc OBJECT-TYPE
        SYNTAX       DisplayString (SIZE(0..140))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains a description of the installation location of this RSU."
    ::= { rsuSysDescription 3 }

rsuID OBJECT-TYPE
        SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the ID given to this RSU."
    ::= { rsuSysDescription 4 }

rsuManufacturer OBJECT-TYPE
        SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the name of the manufacturer of this RSU."
    ::= { rsuSysDescription 5 }

rsuSysSettings OBJECT IDENTIFIER ::= { rsuMIB 18 }

rsuTxPower OBJECT-TYPE
        SYNTAX       Integer32 (0..100)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Sets the output power of the RSU antennas as a
         percentage of full strength.  Default is 100% of 33dBm."
    ::= { rsuSysSettings 1 }

rsuNotifyIpAddress OBJECT-TYPE
        SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the IP address of the SNMP Manager that will
         receive the SNMP Notifications."
    ::= { rsuSysSettings 2 }

rsuNotifyPort OBJECT-TYPE
        SYNTAX       Integer32 (0..65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the port number of the SNMP Manager that will
                receive the SNMP Notifications.  Default is 162."
    ::= { rsuSysSettings 3 }

rsuSysLogCloseDay OBJECT-TYPE
        SYNTAX       INTEGER {        monday(1), tuesday(2), wednesday(3),
                                thursday(4), friday(5), saturday(6),
                                sunday(7) }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the day of the week on which to close the system
                log file Default is Sunday."
    ::= { rsuSysSettings 4 }

rsuSysLogCloseTime OBJECT-TYPE
        SYNTAX       OCTET STRING (SIZE(3))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the time of day at which to close the system
```

```
                log file.  Default is 23:59:00 UTC."
    ::= { rsuSysSettings 5 }

rsuSysLogDeleteDay OBJECT-TYPE
       SYNTAX      INTEGER {       monday(1), tuesday(2), wednesday(3),
                               thursday(4), friday(5), saturday(6),
                               sunday(7) }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the day of the week on which to close the system
                log file Default is Sunday."
    ::= { rsuSysSettings 6 }

rsuSysLogDeleteAge OBJECT-TYPE
       SYNTAX      Integer32
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the age at which to delete old log files.
                Default is 30 days."
    ::= { rsuSysSettings 7 }



-- System Status

rsuSystemStatus OBJECT IDENTIFIER ::= { rsuMIB 19}

rsuChanStatus OBJECT-TYPE
       SYNTAX INTEGER {
        bothOp (0), --both Continuous and Alternating modes are operational
        altOp (1),  --Alternating mode is operational,
                                     --Continuous mode is not operational
        contOp (2), --Continuous mode is operational,
                                     --Alternating mode is not operational
        noneOp (3)  --neither Continuous nor Alternating mode is operational
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
               "Indicates which channel modes are operating.
                Note: Operating means the device is functioning
                as designed, configured, and intended"
    ::= { rsuSystemStatus 1 }



-- Situation Data

rsuSitData OBJECT IDENTIFIER ::= { rsuMIB 20 }

rsuSdcDestIpAddress OBJECT-TYPE
       SYNTAX      Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the IPv6 address of the Situation Data Clearinghouse."
    ::= { rsuSitData 1 }

rsuSdcDestPort OBJECT-TYPE
       SYNTAX      Integer32 (1024..65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the port on which the Situation Data Clearinghouse
                will receive data."
    ::= { rsuSitData 2 }

rsuSdcInterval OBJECT-TYPE
```

```
        SYNTAX       Integer32 (1..18000)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the interval in seconds at which the RSU will send
                data to the Situation Data Clearinghouse."
    ::= { rsuSitData 3 }

rsuSdwIpAddress OBJECT-TYPE
        SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the IPv6 address of the Situation Data Warehouse."
    ::= { rsuSitData 4 }

rsuSdwPort OBJECT-TYPE
        SYNTAX       Integer32 (1024..65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the port on which the Situation Data Warehouse
                will receive requrests from the RSU."
    ::= { rsuSitData 5 }


-- RSU Set

rsuSet OBJECT IDENTIFIER ::= { rsuMIB 21 }

rsuSetRole OBJECT-TYPE
        SYNTAX       INTEGER {
                                             master (0),
                                             slave (1)
                              }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "The role of the RSU in a set (master or slave)"
    ::= { rsuSet 1 }

rsuSetEnable OBJECT-TYPE
        SYNTAX       INTEGER {
                                             independent (0),
                                             set (1)
                              }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "The status of the RSU set.  0 is not operating in a set;
                1 is operating in a set."
    ::= { rsuSet 2 }

rsuSetSlaveTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuSetSlaveEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Holds the configuration parameters for the slave RSUs."
    ::= { rsuSet 3 }

rsuSetSlaveEntry OBJECT-TYPE
    SYNTAX      RsuSetSlaveEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row describing the configuration of each slave RSU."
    INDEX   { rsuSetSlaveIndex }
    ::= { rsuSetSlaveTable 1 }
```

```
RsuSetSlaveEntry ::= SEQUENCE {
        rsuSetSlaveIndex              RsuTableIndex,
        rsuSetSlaveIpAddress          Ipv6Address,
        rsuSetSlaveRowStatus          RowStatus
}

rsuSetSlaveIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        " Slave RSU index "
    ::= { rsuSetSlaveEntry 1 }

rsuSetSlaveIpAddress OBJECT-TYPE
    SYNTAX       Ipv6Address
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Contains the IPv6 address of each slave RSU.  One
                slave per row."
    ::= { rsuSetSlaveEntry 2 }

rsuSetSlaveRowStatus OBJECT-TYPE
        SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "create or destroy rows"
    ::= { rsuSetSlaveEntry 3 }


-- RSU Mode

rsuMode OBJECT-TYPE
    SYNTAX      INTEGER {
                       standby  (2),
                       operate  (4),
                       off      (16)
               }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
               "Specifies the current mode of operation of the RSU."
    ::= { rsuMIB 99 }


-- Asynchronous Messages
rsuAsync OBJECT IDENTIFIER ::= { rsuMIB 100 }

-- Notifications

rsuNotifications OBJECT IDENTIFIER ::= { rsuAsync 0 }


messageFileIntegrityError NOTIFICATION-TYPE
        OBJECTS      { rsuAlertLevel, rsuMsgFileIntegrityMsg }
        STATUS       current
        DESCRIPTION
               "The SNMP agent should immediately report integrity check
                errors on select store-and-forward messages to the SNMP
                manager."
        ::= { rsuNotifications 1 }

rsuSecStorageIntegrityError NOTIFICATION-TYPE
        OBJECTS      { rsuAlertLevel, rsuSecStorageIntegrityMsg }
        STATUS       current
        DESCRIPTION
               "The SNMP agent should immediately report integrity check
                errors in secure storage to the SNMP manager."
        ::= { rsuNotifications 2 }

rsuTamperAlert NOTIFICATION-TYPE
        OBJECTS      { rsuAlertLevel, rsuTamperAlertMsg }
        STATUS       current
        DESCRIPTION
                "The SNMP agent should report any tampering to the enclosure
                 to the SNMP manager."
        ::= { rsuNotifications 3 }

rsuAuthError NOTIFICATION-TYPE
        OBJECTS      { rsuAlertLevel, rsuAuthMsg }
        STATUS       current
        DESCRIPTION
                "The SNMP agent should report an error in authorization
                 to the SNMP manager."
        ::= { rsuNotifications 4 }

rsuSignatureVerifyError NOTIFICATION-TYPE
        OBJECTS      { rsuAlertLevel, rsuSignatureVerifyMsg }
        STATUS       current
        DESCRIPTION
                "The SNMP agent should report any signature verification errors
                 to the SNMP manager."
        ::= { rsuNotifications 5 }

rsuAccessError NOTIFICATION-TYPE
        OBJECTS      { rsuAlertLevel, rsuAccessMsg }
        STATUS       current
        DESCRIPTION
                "The SNMP agent should report an access error or rejection due to
                 a violation of the Access Control List."
        ::= { rsuNotifications 6 }

rsuTimeSourceLost NOTIFICATION-TYPE
        OBJECTS      { rsuAlertLevel, rsuTimeSourceLostMsg }
        STATUS       current
        DESCRIPTION
                "The SNMP agent should report to the SNMP manager that a
                 time source was lost."
        ::= { rsuNotifications 7 }

rsuClockSkewError NOTIFICATION-TYPE
        OBJECTS      { rsuAlertLevel, rsuClockSkewMsg }
        STATUS       current
        DESCRIPTION
                "The SNMP agent should report to the SNMP manager a skew rate in
                 the clock signal that exceeds a vendor-defined value."
        ::= { rsuNotifications 8 }

rsuTimeSourceMismatch NOTIFICATION-TYPE
        OBJECTS      { rsuAlertLevel, rsuTimeSourceMismatchMsg }
        STATUS       current
        DESCRIPTION
                "The SNMP agent should report to the SNMP manager a deviation between
                 two time sources that exceeds a vendor-defined threshold."
        ::= { rsuNotifications 9 }

rsuGpsAnomaly NOTIFICATION-TYPE
        OBJECTS      { rsuAlertLevel, rsuGpsAnomalyMsg }
        STATUS       current
        DESCRIPTION
                "The SNMP agent should report any anomalous GPS readings
                 to the SNMP manager."
        ::= { rsuNotifications 10 }

rsuGpsDeviationError NOTIFICATION-TYPE
        OBJECTS      { rsuAlertLevel, rsuGpsDeviationMsg }
        STATUS       current
        DESCRIPTION
```

```
               "The SNMP agent should report to the SNMP manager a deviation in
                GPS position that is greater than the configured value."
       ::= { rsuNotifications 11 }

rsuGpsNmeaNotify NOTIFICATION-TYPE
       OBJECTS      { rsuAlertLevel, rsuGpsOutputString }
       STATUS       current
       DESCRIPTION
               "The SNMP agent should report the NMEA string to the SNMP manager
                at the configured interval."
       ::= { rsuNotifications 12 }


rsuNotificationObjects OBJECT IDENTIFIER ::= { rsuAsync 1 }

-- Notification Objects
rsuMsgFileIntegrityMsg OBJECT-TYPE
       SYNTAX       DisplayString
       MAX-ACCESS   accessible-for-notify
       STATUS       current
       DESCRIPTION
               "Contains the error message detailing an Active Message
                Integrity error "
       ::= { rsuNotificationObjects 1 }

rsuSecStorageIntegrityMsg OBJECT-TYPE
       SYNTAX       DisplayString
       MAX-ACCESS   accessible-for-notify
       STATUS       current
       DESCRIPTION
               "Contains the error message detailing a secure storage
                Integrity error "
       ::= { rsuNotificationObjects 2 }

rsuTamperAlertMsg OBJECT-TYPE
       SYNTAX       DisplayString
       MAX-ACCESS   accessible-for-notify
       STATUS       current
       DESCRIPTION
               "Contains the error message detailing an enclosure
                tampering error "
       ::= { rsuNotificationObjects 3 }

rsuAuthMsg OBJECT-TYPE
       SYNTAX       DisplayString
       MAX-ACCESS   accessible-for-notify
       STATUS       current
       DESCRIPTION
               "Contains the error message detailing an authorization error "
       ::= { rsuNotificationObjects 4 }

rsuSignatureVerifyMsg OBJECT-TYPE
       SYNTAX       DisplayString
       MAX-ACCESS   accessible-for-notify
       STATUS       current
       DESCRIPTION
               "Contains the error message detailing a signature verification
                error "
       ::= { rsuNotificationObjects 5 }

rsuAccessMsg OBJECT-TYPE
       SYNTAX       DisplayString
       MAX-ACCESS   accessible-for-notify
       STATUS       current
       DESCRIPTION
               "Contains the error message detailing an error or rejection
                due to Access Control List rules "
       ::= { rsuNotificationObjects 6 }

rsuTimeSourceLostMsg OBJECT-TYPE
```

```
        SYNTAX        DisplayString
        MAX-ACCESS    accessible-for-notify
        STATUS        current
        DESCRIPTION
                "Contains the error message indicating a time source
                 was lost"
        ::= { rsuNotificationObjects 7 }

rsuClockSkewMsg OBJECT-TYPE
        SYNTAX        DisplayString
        MAX-ACCESS    accessible-for-notify
        STATUS        current
        DESCRIPTION
                "Contains the error message detailing that a vendor-defined
                 clock skew rate was exceeded "
        ::= { rsuNotificationObjects 8 }

rsuTimeSourceMismatchMsg OBJECT-TYPE
        SYNTAX        DisplayString
        MAX-ACCESS    accessible-for-notify
        STATUS        current
        DESCRIPTION
                "Contains the error message detailing a deviation between
                 two time sources that exceeds a vendor-defined threshold "
        ::= { rsuNotificationObjects 9 }

rsuGpsAnomalyMsg OBJECT-TYPE
        SYNTAX        DisplayString
        MAX-ACCESS    accessible-for-notify
        STATUS        current
        DESCRIPTION
                "Contains the error message detailing an anomaly that was
                 detected in the GPS signal "
        ::= { rsuNotificationObjects 10 }

rsuGpsDeviationMsg OBJECT-TYPE
        SYNTAX        DisplayString
        MAX-ACCESS    accessible-for-notify
        STATUS        current
        DESCRIPTION
                "Contains the error message indicating that the reported GPS
                 position differs from the reference by more than the
                 allowed deviation "
        ::= { rsuNotificationObjects 11 }

rsuGpsNmeaNotifyInterval OBJECT-TYPE
        SYNTAX        Integer32 (0..18000)
        MAX-ACCESS    read-write
        STATUS        current
        DESCRIPTION
                "Sets the repeat interval in seconds for the Notification
                 containing the GPS NMEA GPGGA string.
                 Default is 0 (disabled)."
        ::= { rsuNotificationObjects 12 }

rsuAlertLevel OBJECT-TYPE
        SYNTAX        INTEGER {
                       info(0),
                                  notice(1),
                                  warning(2),
                                  error(3),
                                  critical(4)
                                  }
        MAX-ACCESS    accessible-for-notify
        STATUS        current
        DESCRIPTION
                "The level of importance of the notification."
        ::= { rsuNotificationObjects 13 }

END
```