Dedicated Short-Range Communications Roadside Unit Specifications

www.its.dot.gov/index.htm

April 28, 2017
FHWA-JPO-17-589
Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the work has been included only because it is essential to the contents of the work.

Quality Assurance Statement

The Federal Highway Administration (FHWA) provides high-quality information to serve Government, industry, and the public in a manner that promotes public understanding. Standards and policies are used to ensure and maximize the quality, objectivity, utility, and integrity of its information. FHWA periodically reviews quality issues and adjusts its programs and processes to ensure continuous quality improvement.
**Abstract**

The Intelligent Transportation Systems (ITS) Program definition of connected vehicles includes both 5.9 Gigahertz (GHz) Dedicated Short Range Communications (DSRC) and non-DSRC technologies as means of facilitating communication for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) applications. Non-DSRC technologies (e.g. Radio Frequency Identification (RFID), Worldwide Interoperability for Microwave Access (WiMAX), Wi-Fi, Bluetooth, and cellular communication) enable use of existing commercial infrastructure for additional capacity support, but may not meet the low-latency needs of transmitting safety-critical information.

DSRC is a two-way wireless communications protocol suite that integrates the IEEE 802.11, 1609.x standards, SAE J2735, and SAE J2945. The United States Department of Transportation (USDOT) is pursuing DSRC because of its low-latency and high-reliability performance that can be used to reduce fatalities through active safety applications, including collision avoidance, incident reporting and management, emergency response, and pedestrian safety. Furthermore, DSRC supports the close-range communication requirements to distribute Signal Phase and Timing (SPaT) information for intersection-based applications and localized roadway warnings. This document will set the requirements for roadside units (RSU) capable of acting as a network edge device for 5.9GHz DSRC infrastructure.

**Key Words**

- Dedicated Short Range Communication, DSRC, Roadside Unit, RSU, Roadside Equipment, RSE, Intelligent Transportation Systems, ITS, V2I

**Distribution Statement**

No restrictions.
# Table of Contents

**Chapter 1. Introduction** ................................................................. 1  
  What Is the Purpose of this Document? .............................................. 1  
  Who Should Read this Document? ...................................................... 1  
  How Is this Document Organized? .................................................... 1  
  How Do You Receive More Information? ........................................... 2  
  Revision History ................................................................................ 2  
  Roadside Units ................................................................................. 3  

**Chapter 2. Scope** ......................................................................... 4  
  System Overview ............................................................................... 4  
  Basic Functionality ........................................................................... 10  
  IPv6 Access ...................................................................................... 10  
  Application Layer Protocol Data Units (PDU) .................................. 11  
  Document Overview ......................................................................... 12  
  Conformance ..................................................................................... 13  
  References ......................................................................................... 13  

**Chapter 3. System Requirements** ................................................. 16  
  Power Requirements ........................................................................... 16  
  Environmental Requirements ............................................................. 17  
  Physical Requirements ...................................................................... 21  
  Functional Requirements ................................................................... 22  
  Positioning ....................................................................................... 24  
  System Log Files ............................................................................... 25  
  Interface Log Files ............................................................................ 27  
  Message Processing – Store and Repeat-Encoded Payload ......... 30  
  Message Processing – Store and Repeat-Raw Data Payload .... 33  
  Message Processing – Immediate Forward-Encoded Payload .... 34  
  Message Processing – Immediate Forward-Raw Data Payload .... 35  
  Security .......................................................................................... 37  
  USDOT Situation Data Clearinghouse and Warehouse .............. 45  
  Behavioral Requirements ................................................................. 46  
  Operational States ............................................................................ 47  
  Operational Modes .......................................................................... 48  
  Operational Configuration ............................................................... 49  
  Health and Status Monitoring .......................................................... 51  
  Performance Requirements ............................................................... 52  
  Radio Performance ........................................................................... 53  
  Interface Requirements .................................................................... 54  
  DSRC .............................................................................................. 56
| Appendix A. Terms and Definitions ........................................................... | 67 |
| Appendix B. SNMPv3 Management Information Base .............................. | 70 |
| B.1. RSU Specific MIB Objects ............................................................ | 70 |
| B.2. General MIB Objects ..................................................................... | 99 |
| B.3. IPv6 MIB Objects ......................................................................... | 103 |
| B.4. RSU Specific MIB Object Map ..................................................... | 107 |
| Appendix C. Active Message File Format ............................................. | 114 |
| Appendix D. Example WAVE Service Advertisement (WSA) .................. | 116 |

  - Context ......................................................................................................................... 116
  - WSA Example .................................................................................................................. 116
List of Tables

Table 1-1. Revision History ................................................................. 2
Table 2-1. Operational States and State Transitions ......................... 6
Table 2-2. Useful References ............................................................... 14
Table 3-1. Operating System Requirements ...................................... 16
Table 3-2. Power Requirements .......................................................... 17
Table 3-3. Environmental Requirements .......................................... 17
Table 3-4. Physical Requirements ...................................................... 21
Table 3-5. Functional Requirements .................................................. 22
Table 3-6. Positioning Requirements .................................................. 24
Table 3-7. System Logging Requirements ......................................... 26
Table 3-8. Interface Logging Requirements ....................................... 27
Table 3-9. Store and Repeat Message Requirements (Encoded Payload) 31
Table 3-10. Store and Repeat Message Requirements (Raw Data Payload) 34
Table 3-11. Immediate Forward Requirements (Encoded Payload) ........ 35
Table 3-12. Immediate Forward Requirements (Raw Data Payload) ...... 36
Table 3-13. Security Requirements .................................................... 37
Table 3-14. Situation Data Requirements .......................................... 45
Table 3-15. Behavioral Requirements ............................................... 46
Table 3-16. Operational State Requirements ..................................... 47
Table 3-17. Operational Mode Requirements .................................... 48
Table 3-18. Operational Configuration Requirements ....................... 49
Table 3-19. Health and Status Monitoring Requirements .................. 51
Table 3-20. Performance Requirements .......................................... 52
Table 3-21. Radio Requirements ....................................................... 53
Table 3-22. Interface Requirements .................................................. 54
Table 3-23. DSRC Requirements ...................................................... 56
Table 3-24. IEEE 802.11 Requirements ............................................ 56
Table 3-25. IEEE 1609.2 Requirements ........................................... 60
Table 3-26. IEEE 1609.3 Requirements ........................................... 61
Table 3-27. WSA Requirements ....................................................... 63
Table 3-28. IEEE 1609.4 Requirements ........................................... 64
List of Figures

Figure 2-1. Diagram. High-level Conceptual Diagram for the Roadside Units. ......................................................................................................................... 5
Figure 2-2. Diagram. Roadside Unit State.............................................................. 6
Figure 2-3. Diagram. Configuration for a Roadside Unit Mounted on a Mast Arm......................................................................................................................... 7
Figure 2-4. Diagram Configuration for a Roadside Unit Installed Inside a Roadside Electronics Cabinet. ................................................................. 8
Figure 2-5. Diagram. Configuration for a Roadside Unit Mounted on a Roadside Pole Base, 5–8 Feet Off the Ground. ................................................ 9
Figure 2-6. Diagram. Context Diagram for a Roadside Unit. .......................... 10
Figure D-1. Diagram. Context for Example WAVE Service Advertisement Format........................................................................................................... 116
Chapter 1. Introduction

The Intelligent Transportation Systems (ITS) Program definition of connected vehicles includes both 5.9 Gigahertz (GHz) Dedicated Short Range Communications (DSRC) and non-DSRC technologies as means of facilitating communication for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) applications. Non-DSRC technologies (e.g. Radio Frequency Identification (RFID), Worldwide Interoperability for Microwave Access (WiMAX), Wi-Fi, Bluetooth, and cellular communication) enable use of existing commercial infrastructure for additional capacity support, but may not meet the low-latency needs of transmitting safety-critical information.

DSRC is a two-way wireless communications protocol suite that integrates the IEEE 802.11, 1609.x standards, SAE J2735, and SAE J2945. The United States Department of Transportation (USDOT) is pursuing DSRC because of its low-latency and high-reliability performance that can be used to reduce fatalities through active safety applications, including collision avoidance, incident reporting and management, emergency response, and pedestrian safety. Furthermore, DSRC supports the close-range communication requirements to distribute Signal Phase and Timing (SPaT) information for intersection-based applications and localized roadway warnings.

What Is the Purpose of this Document?

This document will set the requirements for roadside units (RSU) capable of acting as a network edge device for 5.9GHz DSRC infrastructure.

Who Should Read this Document?

Suppliers interested in building roadside devices for DSRC Infrastructure Systems.

How Is this Document Organized?

The Structure of this document is as follows:

- Section 1 – Introduction: Revision History and Roadside Unit Description
- Section 2 – Scope: System Overview, Document Overview, and References.
- Section 3 – System Requirements: Describes RSU Physical, Environmental, and Functional Requirements.
How Do You Receive More Information?

Additional information is available in the documents listed in section 2.4. Questions are answered by the person responsible for this document (see section 1.5).

Revision History

Table 1-1. Revision History.

<table>
<thead>
<tr>
<th>Rev.</th>
<th>Ver.</th>
<th>Date</th>
<th>Description</th>
<th>Approved by</th>
<th>Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>2</td>
<td>05/15/2014</td>
<td>First Issue</td>
<td>Deb Curtis (FHWA)</td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>1</td>
<td>07/22/2016</td>
<td>Updates to reference current standards (SCMS EE Requirements v1.1, IEEE 802.11-2012 IEEE 1609.x-2016, SAE J2735-2016) as well as updates based on evaluations of 4.0 specification devices Added, updated, and removed various requirements for clarity and enhancement</td>
<td>Deb Curtis (FHWA)</td>
<td>Frank Perry, Kelli Raboy, Ed Leslie, Zhitong Huang</td>
</tr>
<tr>
<td>4.1</td>
<td>2</td>
<td>08/12/2016</td>
<td>Updates to address known security issues, health and monitoring functionality, and interface with the Situation Data Warehouse and Clearinghouse. New introductory section on the basic functionality of an RSU Modified Appendix B with draft revised MIB Added, updated, and removed various requirements for clarity and enhancement</td>
<td>Deb Curtis (FHWA)</td>
<td>Frank Perry, Kelli Raboy, Ed Leslie, Zhitong Huang, Drew Van Duren</td>
</tr>
<tr>
<td>4.1</td>
<td>3</td>
<td>08/31/2016</td>
<td>Updates to address stakeholder feedback, largely related to security issues and health and monitoring functionality. Modified Appendix B with revised MIB Added Appendix D: Example WAVE</td>
<td>Deb Curtis (FHWA)</td>
<td>Frank Perry, Kelli Raboy, Ed Leslie, Zhitong Huang, Drew Van Duren</td>
</tr>
</tbody>
</table>
## Roadside Units

DSRC enables communication between vehicles and roadside equipment, but does not generate data necessary to provide warnings and advisories from infrastructure to drivers. To support V2I applications, DSRC must be integrated with existing traffic equipment, such as Signal Controllers and backhaul connections to Traffic Management Centers (TMCs). DSRC devices that serve as the demarcation component between vehicles and other mobile devices and existing traffic equipment will be referred to DSRC Roadside Units (RSU) in this document.
Chapter 2. Scope

This document defines the fourth-generation of DSRC RSUs by establishing the base functionality of a carrier-grade device capable of acting as the infrastructure first point-of-contact for vehicles and other mobile devices.

A carrier-grade RSU is defined as an RSU in which both the hardware and software components operate unattended in harsh outdoor environments (temperature and precipitation extremes) for extended periods of time (typical Mean-Time-Between-Failures (MTBF) of 100,000 hours). Individual RSUs as well as groups of RSUs can be managed and monitored with existing off-the-shelf network tools with minimal modifications to support RSU specific data elements; RSUs ignore erroneous, malformed, or unexpected data received on any of its interfaces, detect and auto-recover from minor software failures, transient power spikes, and unexpected power interruptions.

These requirements apply only to the system components identified in Section 2.1 System Overview and do not extend to the supporting roadside equipment subsystems or components. RSUs procured for deployment may be subject to additional requirements based on the local design and policies of the procuring agency.

System Overview

The purpose of the RSU is to facilitate communication between transportation infrastructure and vehicles and other mobile devices by exchanging data over DSRC in compliance with industry standards, including but not limited to (IEEE 802.11, IEEE 1609.x, SAE J2735, and SAE J2945). Additionally, the RSU can be integrated with a backhaul system to enable remote management and provide vehicles and other mobile devices with services and applications delivered by back office service providers. RSUs can also be incorporated with local traffic control systems to deliver enhance traffic management services to vehicles and other mobile devices.

Figure 2-1 depicts a high-level diagram of the RSU and its role as a DSRC interface between traffic management infrastructure and vehicles and other mobile devices.
Figure 2-1. Diagram. High-level Conceptual Diagram for the Roadside Units.

The definition\(^1\) of an RSU that complies with the requirements contained in this document is a device that:

- Supports Single Channel Continuous and dual Channel Alternating DSRC Channel Modes simultaneously.
- Contains internal computer processing and permanent storage capability.
- Contains an integrated Global Positioning System (GPS) receiver for positioning and timing.
- Contains a Power-over-Ethernet (PoE) capable interface that supports both IPv4 and IPv6 connectivity, compliant with IEEE 802.3at.
- Is contained in a dedicated, NEMA 4X-rated enclosure.

For this document, Single Channel Continuous Mode is defined as operating on a single radio channel through both Time Slot 0 and Time Slot 1 as defined in IEEE 1609.4. Dual Channel Alternating Mode is defined as operating on the Control Channel (CCH) during Time Slot 0 and on a Service Channel during Time Slot 1.

The RSU will have a set of operational states as illustrated in Figure 2-2, below.

---

\(^1\) This definition is not intended to supersede FCC guidance for licensing and operation of an RSU; the FCC definition of an RSU can be found in the Electronic Code of Federal Regulations, Title 74: Telecommunications, Part 90 – Private Land Mobile Radio Services. [http://www.ecfr.gov/cgi-bin/text-idx?SID=5ea03a4e0adab6bf55092d7fd90dd701&node=47:5.0.1.1.3&rgn=div5#47:5.0.1.1.3.12.113](http://www.ecfr.gov/cgi-bin/text-idx?SID=5ea03a4e0adab6bf55092d7fd90dd701&node=47:5.0.1.1.3&rgn=div5#47:5.0.1.1.3.12.113)
Chapter 2. Scope

Figure 2-2. Diagram. Roadside Unit State.

Table 2-1. Operational States and State Transitions.

<table>
<thead>
<tr>
<th>State</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial</td>
<td>This is the initial state of the device from the factory, with no specified requirements. The device will revert to the “initial” state after a factory reset.</td>
</tr>
</tbody>
</table>
| Standby      | • Core Operating System is operational  
• DSRC radios are not operational/broadcasting  
• Interface logging is disabled;  
• Configuration changes are enabled |
| No Power     | This state results from a loss of power when the RSU is in the Operate State; this is **NOT** a graceful shutdown that would be enacted by a transition to Standby State prior to a transition to the No Power State. |
| No Power Operate | This state results from a loss of power when the RSU is in the Standby State. The unit should return to the Standby state upon power up. |
| Operate      | • All DSRC radios are operational/broadcasting  
• System log is enabled  
• Configuration changes are disabled |

The installation of the RSU is dependent upon local design, policies, and available infrastructure; an RSU can be mounted directly on a traffic pole or mast arm, or installed in an adjacent cabinet to ensure radio communication objectives can be met. This specification includes sufficient consideration of environmental exposure to cover all deployment configurations, with examples depicted in Figure 2-3 through Figure 2-5. The red boxes in these diagrams highlight the system components that are covered by this specification, including the RSU device and antennas, excluding supporting hardware and infrastructure such as gantries or mast arms and traffic controller or electronics cabinets.
Figure 2-3. Diagram. Configuration for a Roadside Unit Mounted on a Mast Arm.
Figure 2-4. Diagram Configuration for a Roadside Unit Installed Inside a Roadside Electronics Cabinet.
Furthermore, deployment locations that require the installation of multiple RSUs will be referred to as an “RSU System,” that function as a single unit and are connect to the supporting infrastructure through a single physical interface.

Figure 2-5. Diagram. Configuration for a Roadside Unit Mounted on a Roadside Pole Base, 5–8 Feet Off the Ground.
### Basic Functionality

Figure 2-6 is a basic Context Diagram highlighting Inputs and Outputs, Enablers and Controls, and Activities of an RSU.

![Diagram](image)

Figure 2-6. Diagram. Context Diagram for a Roadside Unit.

An RSU performs two core functions in a connected vehicle system:

- Provide IPv6 access to remote network hosts.
- Broadcast and receive messages as defined in SAE J2735.

### IPv6 Access

The RSU provides DSRC-equipped mobile devices with access to Back Office services by way of IPv6. This allows devices to take advantage of services such as the USDOT Situation Data Clearinghouse, Situation Data Warehouse, and Security Credential Management System (SCMS) as well as other public and private network services. In the case of the Situation Data Clearinghouse and
Situation Data Warehouse, data related to traffic conditions (speed, volume, etc.) are sent from a vehicle over DSRC through an RSU to the Situation Data Clearinghouse and Situation Data Warehouse utilizing the RSUs backhaul connection. In the case of the SCMS, a vehicle is able to send requests for updated certificates through the RSU to the SCMS and receive the updated certificates after the request is processed.

Certificates may take a significant time to process, so it is feasible that a vehicle device would make a request for certificates while it is within range of one RSU and receive them when in range of another RSU.

**Application Layer Protocol Data Units (PDU)**

The RSU transmits Application Layer Protocol Data Units (PDU) (messages) formatted in accordance with SAE J2735 using one of two mechanisms:

- Store and Repeat
- Immediate Forward

Store and Repeat messages are downloaded from a back office service and stored on the RSU. Transmit Instructions are included with each message that defines how often the message should be transmitted, when the message should start being transmitted, when the message should stop being transmitted, the channel that should be used for the transmission, the Provider Service Identifier (PSID) the message is associated with, and whether the message should be signed and/or encrypted. These transmission instructions should be extracted from the stored message and written to the appropriate Simple Network Management Protocol (SNMPv3) Object Identifier (OID). Once the message expires, it should be removed from RSU storage and the associated SNMPv3 OID should be cleared.

The RSU transmits Immediate Forward messages as they are sent to the RSU. Transmission instructions accompany messages, including the channel that should be used for the transmission, the PSID the message is associated with, and whether the message should be signed and/or encrypted. These transmission instructions should be extracted from the Immediate Forward message and written to the appropriate SNMPv3 OID. The associated SNMPv3 OID should be cleared once the Immediate Forward messages cease.

To support these two functions the RSU must obtain and manage digital certificates to sign and encrypt the messages. The RSU will have the ability to sign every nth message where n is a configurable number programmed into the RSU.

The RSU also receives messages broadcast by a DSRC-equipped mobile device and forwards them to a remote host. Messages are forwarded based on the PSID. The PSID of the message to be forwarded, the IP address and port number of the remote host, the transport protocol to use, the Receive Signal Strength, the interval at which to forward, and the time period during which to forward are all configurable. The configurable parameters are stored in an appropriate SNMPv3 OID. This allows for capabilities such as traffic monitoring, health and status reporting, and certificate requests.
Document Overview

The following section explains how the requirements nomenclature is constructed and numbered.

Each requirement contains a unique ID for traceability and configuration management. For the USDOT Roadside Unit, each requirement will begin with "USDOT_RSU-Req" which is "USDOT Roadside Unit-Requirement-XvY" were "x" is the unique ID and "Y" is the version number.

The columns in the requirements tables throughout this document have the following definitions:

- **ReqID**: a unique identifier providing a reference to a specific requirement. The ID is comprised on a system name, requirement number, and a version number.

  Example: USDOT Roadside Unit requirement 1 version 0 would be **USDOT_RSU-Req-1v0**

- **Description**: Statement of the business function or conditions the system must meet

- **Reference**: Additional requirement(s), documents, standards, etc. relating to the function or condition the system must meet

- **Verification Method**: The method utilized to verify the function or condition. The four methods utilized to verify the function or conditions the system must meet are as follows:

  1. **Inspection**: Nondestructive examination of the system using one or more of the five senses (visual, auditory, smell, tactile, taste). This may include simple physical manipulation and measurements.

  2. **Demonstration**: Manipulation of the system as it is intended to be used to verify that the results are as planned or expected.

  3. **Test**: Verification of the system using a controlled and predefined series of inputs, data, or stimuli to ensure that the system will produce a very specific and predefined output as specified by the requirements.

  4. **Analysis**: Verification of the system using models, calculations and testing equipment. Analysis allows someone to make predictive statements about the typical performance of a product or system based on the confirmed test results of a sample set or by combining the outcome of individual tests to conclude something new about the product or system. It is often used to predict the breaking point or failure of a product or system by using nondestructive tests to extrapolate the failure point.

  5. **Documentation**: Review of documentation including, but not limited to a Data Sheet, Users Guide, Operations Manual, etc.

The requirements contained in this document shall be verified by accredited test facilities. The type of facility charged with verification of each requirement will depend on whether the requirement specifies a physical or operational criterion.
Physical criteria include all technical, mechanical, power, and environmental requirements for the device and shall be evaluated by test facilities that are recognized as having the relevant expertise as defined by the standard or specification referenced in the individual requirements.

Operational criteria include all functional, performance and security requirements for the device and shall be evaluated by facilities compliant with the USDOT requirements. These requirements will be included in the final version of this document.

**Conformance**

Requirements listed in this document use the following terminology:

- **SHALL**: indicates that the definition is an absolute requirement of the specification.
- **SHALL NOT**: Indicates that the definition is an absolute prohibition of the specification.
- **SHOULD (RECOMMENDED)**: Indicates that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT (NOT RECOMMENDED)**: Indicates that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- **MAY (OPTIONAL)**: Indicates that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option SHALL be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option SHALL be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

**References**

This section contains all referenced documents, and their appropriate versions, required to meet the specifications contained in this document. The dates referenced in this table should be used as the earliest version of the references applicable to this specification; subsequent updates to the references listed below are applicable to the specifications contained in this document. Hyperlinks to the publications, or websites that offer purchase/subscription access to the publications, have been included below. In some cases, where subscription or purchase is required, temporary access may be available upon request through the Turner-Fairbank Highway Research Center library.
Table 2-2. Useful References.

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Document Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>USDOT DSRC Roadside Unit (RSU) Specification version 4.0 (2014)</td>
</tr>
<tr>
<td>2.</td>
<td>Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (IEEE 802.11-2012, or later)</td>
</tr>
<tr>
<td>4.</td>
<td>Standard for Wireless Access in Vehicular Environments (WAVE) – Security Services for Applications and Management Messages (IEEE 1609.2-2016 as modified by guidance notes, or later)</td>
</tr>
<tr>
<td>5.</td>
<td>Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services (IEEE 1609.3-2016, or later)</td>
</tr>
<tr>
<td>8.</td>
<td>Dedicated Short Range Communications (DSRC) Message Set Dictionary (SAE J2735, 2016 or later)</td>
</tr>
<tr>
<td>9.</td>
<td>Standard for Power over Ethernet (IEEE 802.3at, 2009)</td>
</tr>
<tr>
<td>10.</td>
<td>NEMA Standard for Traffic Controller Assemblies with NTCIP Requirements (NEMATS 2-2003 v02.06)</td>
</tr>
<tr>
<td>17.</td>
<td>NEMA Standard for Enclosures for Electrical Equipment (NEMA 250-2008)</td>
</tr>
<tr>
<td>18.</td>
<td>DARPA Internet Program Protocol Specification version 4 (IPv4) (as specified in IETF RFC 790 and IETF RFC 791)</td>
</tr>
<tr>
<td>19.</td>
<td>DARPA Internet Program Protocol Specification version 6 (IPv6) (as specified in IETF RFC 2460 and IETF RFC 4291)</td>
</tr>
<tr>
<td>20.</td>
<td>On-Board System Requirements for V2V Safety Communications (SAE J2945/1, 2016 or later)</td>
</tr>
<tr>
<td>21.</td>
<td>USDOT Security Credential Management System Proof–of–Concept Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.1 or later</td>
</tr>
<tr>
<td>22.</td>
<td>Federal Communications Commission (FCC) Code of Federal Regulations Title 47,</td>
</tr>
<tr>
<td>Reference Number</td>
<td>Document Name</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>23.</td>
<td>USDOT DTFH61-12-D-00020 DSRC RSU v4.0 Test Plan</td>
</tr>
<tr>
<td>26.</td>
<td>Secure Shell (SSH) Version 2 (as specified in IETF RFC 4251, IETF RFC 4252, IETF RFC 4253, and IETF RFC 4254)</td>
</tr>
</tbody>
</table>
Chapter 3. System Requirements

This section contains the system requirements to meet USDOT specifications for a DSRC Roadside Unit. These function-based specifications are not intended to prescribe any specific method of implementation, but rather to describe the minimum device functionality. The specifications are broken down into the following categories:

- Power
- Environmental
- Physical
- Functional
- Behavioral
- Performance
- Interface.

Any external agency, including state/local transportation agencies, universities or other research organizations, may specify additional requirements necessary to meet the objectives of a specific project, application, or deployment. Furthermore, individual vendors may choose to include additional functionality so long as it does not interfere with these minimum requirements.

Table 3-1. Operating System Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_343-v003</td>
<td>Operating System: The roadside unit operating system SHALL consist of a distribution mechanism in which the developer or developer community could proactively provide updates and patches to remediate vulnerabilities.</td>
<td></td>
</tr>
</tbody>
</table>

Power Requirements

This section defines the power requirements that will be expected of a compliant roadside unit.
Table 3-2. Power Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_278-v001</td>
<td>Operating Voltage: The roadside unit SHALL have a nominal operating voltage between 37 and 57 V DC, compliant with IEEE 802.3at.</td>
<td>IEEE 802.3at</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_310-v001</td>
<td>Power over Ethernet: The roadside unit SHALL support inbound power through a single, designated Ethernet port by Power-over-Ethernet (PoE) in compliance with 802.3at.</td>
<td>IEEE 802.3at</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_362-v002</td>
<td>Power Injector: any accompanying power injector SHALL be compliant with 802.3at.</td>
<td>IEEE 802.3at</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
</tbody>
</table>

Environmental Requirements

The roadside unit and all constituent equipment shall be designed to operate within the constraints of the environmental requirements described in this section.

Table 3-3. Environmental Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_312-v001</td>
<td>Ambient Temperature RSU: The roadside unit SHALL function as intended within the temperature range of -34 degrees C (-30 degrees F) to +74 degrees C (+165 degrees F).</td>
<td>NEMA TS 2-2003 v02.06</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_546-v002</td>
<td>Ambient Temperature Power Injector: any accompanying Power Injector unit SHALL function as intended within the temperature range of -34 degrees C (-30 degrees F) to +74 degrees C (+165 degrees F).</td>
<td>NEMA TS 2-2003 v02.06</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_313-v001</td>
<td>Ambient Temperature Rate of Change RSU: The roadside unit SHALL function as intended under changes in ambient temperature up to 17 degrees C (30 degrees F) per hour, throughout the required operational temperature range.</td>
<td>NEMA TS 2-2003 v02.06</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>USDOT_RSU-Req_547-v002</td>
<td>Ambient Temperature Rate of Change Power Injector: Any accompanying Power Injector unit SHALL function as intended under changes in ambient temperature up to 17 degrees C (30 degrees F) per hour, throughout the required operational temperature range.</td>
<td>NEMA TS 2-2003 v02.06</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_314-v001</td>
<td>Storage Temperature RSU: The roadside unit SHALL function as intended after storage at a temperature range of -45 degrees C (-50 degrees F) to +85 degrees C (+185 degrees F).</td>
<td>NEMA TS 2-2003 v02.06</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_548-v002</td>
<td>Storage Temperature Power Injector: Any accompanying Power Injector unit SHALL function as intended after storage at a temperature range of -45 degrees C (-50 degrees F) to +85 degrees C (+185 degrees F).</td>
<td>NEMA TS 2-2003 v02.06</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_315-v001</td>
<td>Humidity – Average Temperatures RSU: The roadside unit SHALL be capable of continuous operation under a relative humidity of 95% non-condensing over the temperature range of +4.4 degrees C (+40.0 degrees F) to +43.3 degrees C (+110.0 degrees F).</td>
<td>NEMA TS 2-2003 v02.06</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_549-v002</td>
<td>Humidity – Average Temperatures Power Injector: Any accompanying Power Injector unit SHALL be capable of continuous operation under a relative humidity of 95% non-condensing over the temperature range of +4.4 degrees C (+40.0 degrees F) to +43.3 degrees C (+110.0 degrees F).</td>
<td>NEMA TS 2-2003 v02.06</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_316-v001</td>
<td>Rain: The roadside unit SHALL pass the rain test with a rainfall rate of 1.7 mm/min (4in/hour), wind speed of 18 m/sec (40 mph) and 30 minutes on each surface of the device as called out in MIL-STD-810 G method 506.5 Procedure 1.</td>
<td>MIL-STD-810 G method 506.5 Procedure 1</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>USDOT_RSU-Req_317-v001</td>
<td>Salt Fog: The roadside unit SHALL pass the salt fog test with 5% saline exposure for 2 cycles x 48 hours (24 hours wet/24 hours dry) as called out in MIL-STD-810 G method 509.5.</td>
<td>MIL-STD-810 G method 509.5</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_318-v001</td>
<td>Wind: The roadside unit mounting bracket SHALL be able to withstand winds up to 150 miles per hour per AASHTO Special Wind Regions Specification.B19</td>
<td>AASHTO Standard Specifications for Structural Supports for Highway Signs, Luminaires, and Traffic Signals, version 6 - Section 3.8.</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_319-v002</td>
<td>Operating Shock and Vibration RSU: The roadside unit SHALL comply with the United States Military Standard MIL-STD-810G.</td>
<td>MIL-STD-810G (Ground Transportation Random Vibration and Mechanical Shock) Methods 514.5C-17 and 516.5</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_320-v001</td>
<td>Shock and Vibration Testing RSU: The roadside unit SHALL pass environmental testing conducted in accordance with the procedures specified in IEC-60068 and IEC-60721.</td>
<td>IEC-60068 (Environmental Testing) Section 2-6 Procedures B1, C1 and IEC-60721 (Classification of Environmental Conditions) Section 3-4 Class 4M3</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>USDOT_RSU-Req_551-v002</td>
<td>Shock and Vibration Testing Power Injector: Any accompanying Power Injector unit SHALL pass environmental testing conducted in accordance with the procedures specified in IEC-60068 and IEC-60721.</td>
<td>IEC-60068 (Environmental Testing) Section 2-6 Procedures B1, C1 IEC-60721 (Classification of Environmental Conditions) Section 3-4 Class 4M4</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_439-v001</td>
<td>Transportation Shock and Vibration (RSU packaged for shipment): The roadside unit SHALL comply with the United States Military Standard MIL-STD-810G, Test Method 514.6, Procedure I, Category 4. (Heavy truck profile) for packaging and shipping. Note: Intended to provide reasonable assurance that materiel can withstand transportation and handling including field installation, removal, and repair.</td>
<td>MIL-STD-810G, Test Method 514.6, Procedure I, Category 4. (Heavy truck profile)</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_321-v001</td>
<td>Electrical Emissions Susceptibility RSU: The roadside unit SHALL be immune to radio frequency (RF)/Electromagnetic Interference (EMI) per SAE J1113.</td>
<td>SAE J1113</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_552-v002</td>
<td>Electrical Emissions Susceptibility Power Injector: Any accompanying Power Injector unit SHALL be immune to radio frequency (RF)/Electromagnetic Interference (EMI) per SAE J1113.</td>
<td>SAE J1113</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_322-v001</td>
<td>Electrostatic Discharge RSU: The roadside unit SHALL be able to withstand electrostatic discharges from the air up to +/-15kiloVolts (kV) and electrostatic discharges on contact up to +/-8 kiloVolts (kV), in compliance with IEC EN61000-3-2.</td>
<td>IEC EN61000-3-2</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
</tbody>
</table>
### Physical Requirements

This section contains the physical specifications that a compliant roadside unit will be expected to meet.

#### Table 3-4. Physical Requirements

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_324-v001</td>
<td>Weight: The weight of the roadside unit, excluding antennas, mounting hardware and Power-over-Ethernet (PoE) Power Injector, SHALL NOT exceed fifteen (15) pounds</td>
<td>-</td>
<td>Inspection: weighed using a calibrated scale</td>
</tr>
<tr>
<td>USDOT_RSU-Req_325-v001</td>
<td>Enclosure: The roadside unit SHALL be housed in a corrosion-resistant enclosure that is compliant with the NEMA4X (IP66) rating.</td>
<td>NEMA 250-2008</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_328-v001</td>
<td>Power over Ethernet Connector: The external Power-over-Ethernet (PoE) connector SHALL be compliant with the Outdoor IP66 rating.</td>
<td>NEMA 250-2008 IEEE 802.3at</td>
<td>Test: A &quot;Pass&quot; indication contained in a Test Report from an accredited test facility</td>
</tr>
<tr>
<td>USDOT_RSU-Req_329-v001</td>
<td>Mounting: The roadside unit SHALL support installation on a shelf, wall, or pole (horizontal or vertical).</td>
<td>-</td>
<td>Inspection</td>
</tr>
<tr>
<td>USDOT_RSU-Req_331-v001</td>
<td>Power Indication: The roadside unit SHALL include an LED to indicate the power status of the device in accordance with the following protocol: Off - No Power Solid Green - Device is powered on</td>
<td>-</td>
<td>Demonstration: verify the status and color of the LED with the device powered off and powered on</td>
</tr>
</tbody>
</table>
### Status Indication

The roadside unit SHALL include an LED to indicate the operational status of the device in accordance with the following protocol:

- **Off - No Power**
- **Blinking Green - Device Start-Up**
- **Solid Green - Device Operational**
- **Amber - Firmware Update In Progress**
- **Red - Fault**

---

## Functional Requirements

This section contains the specifications for all functions that a roadside unit will be expected to perform. SNMPv3 is expected to be used for all device configurations.

### Table 3-5. Functional Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_361-v002</td>
<td>RSU Set: At installation locations that require multiple roadside units to provide the required DSRC coverage, all RSUs SHALL be configured to operate as a single functional unit.</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_576-v001</td>
<td>RSU Set Master: 1 roadside unit in the RSU Set SHALL be configured as the Set &quot;Master&quot; which will be the basis for the configuration of the other RSUs in the Set.</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_577-v001</td>
<td>RSU Set Configuration: All non-Master RSUs in the RSU Set SHALL be automatically configured based on the configuration of the Set &quot;Master&quot; RSU</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_580-v002</td>
<td>RSU Set Backhaul: If the RSU Set has a backhaul connection, all data between the Back Office and the RSU Set SHALL route through a single device connecting the RSU Set Master to the other roadside units in the backhaul.</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| USDOT_RSU-Req_437-v005 | DSRC Message Forwarding: The roadside unit SHALL forward WSMP messages received on any DSRC interface, containing a specified PSID, to a specified network host, as configured in SNMPv3 MIB OID 1.0.15628.4.1.7.  
Note: The WSMP Message Forwarding SNMPv3 MIB Object contains the following information:  
-PSID  
-Dest_IP Address  
-Dest_Port  
-TransPort_Protocol  
-RSSI  
-MsgForwardInterval (RSU forwards every nth message received)  
-DeliveryStart  
-DeliveryStop  
See the SNMPv3 MIB OID 1.0.15628.4.1.7 in Appendix B for more information | Test:                                                                                         |                                   |
| USDOT_RSU-Req_438-v004 | GPS Output: The roadside unit SHALL send the GPGGA NMEA String to a specified UDP port at a specified rate, upon acquisition of 3 or more Satellites, as configured in SNMPv3 MIB OID 1.0.15628.4.1.8, which contains the following data.  
-destination IP Address  
-port (default is 5115)  
-sample period (default is 1 second, with a valid range of 1-18000 seconds, in increments of 1 second)  
See the SNMPv3 MIB OID 1.0.15628.4.1.8 in Appendix B for more information | Req_363                                                                                   | Test:                                                                                         |
| USDOT_RSU-Req_513-v003 | System Time: The roadside unit SHALL maintain a system clock based on timing information from a local positioning system that manages leap second corrections in accordance with Req_363, IS-GPS-200H Sections 3.3.4, 20.3.3.5.2.4, and 30.3.3.6.2 | Test:                                                                                   |                                   |
### Chapter 3. System Requirements

#### Intelligent Transportation Systems Joint Program Office

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS-GPS-200H</td>
<td>Note: GPS is intended to serve as the primary time source and the NTP server is intended to be available as a secondary, backup time source in the event that the RSU loses GPS.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_514-v002</td>
<td>System Time Standard: The roadside unit SHALL conform to the Universal Time, Coordinated (UTC) standard with epoch 1 January 1970 00:00:00.</td>
<td>Req_363</td>
<td>Test:</td>
</tr>
</tbody>
</table>
| USDOT_RSU-Req_618-v002 | The roadside unit SHALL notify a remote host via SNMPv3:  
• if a time source input has been lost for a configurable period of time or has failed after a configurable number of query attempts (note: the time source itself shall also be indicated) (OID 1.0.15628.4.1.100.0.7)  
• if the value of an internal clock drift (skew rate) has exceeded a configurable tolerance (OID 1.0.15628.4.1.100.0.8)  
• if the deviation between two or more time sources has exceeded a configurable threshold (OID 1.0.15628.4.1.100.0.9) |             | Test:               |

### Positioning

#### Table 3-6. Positioning Requirements

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_510-v002</td>
<td>Position Determination: The roadside unit SHALL utilize a local subsystem to determine its position on the surface of the earth using a sample rate of 1 Hz or better</td>
<td>Req_363</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_511-v001</td>
<td>Positioning Failure Log Entry: The roadside unit SHALL write a CRITICAL entry to the System Log if it is not able to acquire a minimum of 3 Satellites within 20 seconds after entering the &quot;Operate&quot; state</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>USDOT_RSU-Req_512-v002</td>
<td>Positioning Corrections: The roadside unit SHALL utilize WAAS corrections, when available</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_602-v001</td>
<td>GPS Reference: The roadside unit SHALL store a reference set of GPS coordinates for itself</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_613-v002</td>
<td>The roadside unit SHOULD evaluate GPS sub-frame data to indicate the legitimacy of the GPS data frame source</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_614-v002</td>
<td>The roadside unit SHALL notify a remote host via SNMPv3: • if its GPS position deviates from the stored reference by more than a configurable radius (OID 1.0.15628.4.1.100.0.11) • if a suspicious GPS signal is detected (OID 1.0.15628.4.1.100.0.10) • of its current NMEA GPGGA string at a configurable interval (OID 1.0.15628.4.1.100.0.12)</td>
<td></td>
<td>Test:</td>
</tr>
</tbody>
</table>

**System Log Files**

This section contains requirements related to the RSUs operating system log (syslog) files. The RSU is expected to generate system log file entries at the appropriate priority level depending on the system event. Typical Linux operating system Log files contain the following priority levels:

- **EMERGENCY** (Level 1) – The application has completely crashed and is no longer functioning. Normally, this will generate a message on the console as well as all root terminals. This is the most serious error possible. This should not normally be used for applications outside of the system level (file systems, kernel, etc.). This usually means the entire system has crashed.
- **ALERT** (Level 2) – The application is unstable and a crash is imminent. This will generate a message on the console and on root terminals. This should not normally be used for applications outside of the system level (file systems, kernel, etc.).
- **CRITICAL** (Level 3) – A serious error occurred during application execution. Someone (systems administrators and/or developers) should be notified and should take action to correct the issue.
- **ERROR** (Level 4) – An error occurred that should be logged, however it is not critical. The error may be transient by nature, but it should be logged to help debug future problems via error message trending. For example, if a connection to a remote server failed, but it will be retried automatically and is fairly self-healing, it is not critical. But if it fails every night at 2AM, you can look through the logs to find the trend.
• WARNING (Level 5) – The application encountered a situation that it was not expecting, but it can continue. The application should log the unexpected condition and continue on.

• NOTICE (Level 6) – The application has detected a situation that it was aware of, it can continue, but the condition is possibly incorrect.

• INFO (Level 7) – For completely informational purposes, the application is simply logging what it is doing. This is useful when trying to find out where an error message is occurring during code execution.

• DEBUG (Level 8) – Detailed error messages describing the exact state of internal variables that may be helpful when debugging problems.

Table 3-7. System Logging Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_500-v001</td>
<td>System Log File: The roadside unit SHALL log system events to a standard operating system Log (Syslog) File</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_501-v001</td>
<td>System Log Event Priorities: The Priority Level of events that are recorded in the roadside unit System Log file SHALL consist of all priorities available for the operating system</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_503-v001</td>
<td>System Log Default Event Priority: The roadside unit SHALL write an entry in the System Log file for INFO events and above, by default</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_502-v001</td>
<td>System Log Event Priority Configuration: The Priority Level of events that are recorded in the roadside unit System Log file SHALL be configurable by authorized users</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_504-v002</td>
<td>System Log Time Period-Close: The roadside unit SHALL close open System Log files once per week at a configurable time</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_505-v002</td>
<td>System Log Time Period-Open: Upon closing a System Log file, the roadside unit SHALL open a new System Log file.</td>
<td>Test:</td>
<td></td>
</tr>
</tbody>
</table>
### Chapter 3. System Requirements

#### Intelligent Transportation Systems Joint Program Office

#### Dedicated Short Range Communications Roadside Unit Specifications

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_506-v003</td>
<td>System Log File Storage: At a configurable time, the roadside unit SHALL delete system log files that are older than a configurable age (i.e. the length of time since the file was closed).</td>
<td>See the SNMPv3 MIB OID 1.0.15628.4.1.18 in Appendix B for more information</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_559-v001</td>
<td>System Log File Access: The roadside unit SHALL allow authorized users to view System Log Files stored in the System Log File directory on the device through an Ethernet interface.</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_450-v001</td>
<td>Network Host Connection State Change: The roadside unit SHALL write a WARNING entry to the System Log File when a non-DSRC network host connection changes state. The entry will contain the following data:</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Date and Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- new state (connected, not connected)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Interface Log Files

The RSU will provide operators the ability to capture packets transmitted and received on any enabled communication interface for troubleshooting purposes. Interface logs are not intended for long term data capturing.

#### Table 3-8. Interface Logging Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_516-v001</td>
<td>Interface Log File: The roadside unit SHALL have the ability to log all transmitted and received packets across all enabled communication interfaces, while in the “Operate” State.</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| USDOT_RSU-Req_542-v002 | Interface Log File Default Configurations: All Interface Log File configurations contained in SNMPv3 MIB OID 1.0.15628.4.1.9 SHALL have the following default values:  
- generate=off  
- Max file size=20MB  
- Max collection time=24 hr. | See the SNMPv3 MIB 1.0.15628.4.1.9 in Appendix B for more information | Test:               |
| USDOT_RSU-Req_539-v003 | Interface Log File Begin Generation: An Interface Log File SHALL be generated for a roadside unit communication interface upon setting the "generate" flag in SNMPv3 MIB OID 1.0.15628.4.1.9 for that interface to "on."  
Note: when set to "on" both transmitted and received packets are logged | See the SNMPv3 MIB 1.0.15628.4.1.9 in Appendix B for more information | Test:               |
<p>| USDOT_RSU-Req_560-v002 | Interface Log File Stop Generation: An Interface Log File SHALL stop being generated for a roadside unit communication interface upon setting the &quot;generate&quot; flag in SNMPv3 MIB OID 1.0.15628.4.1.9 for that interface to &quot;off.&quot; | See the SNMPv3 MIB 1.0.15628.4.1.9 in Appendix B for more information | Test:               |
| USDOT_RSU-Req_518-v003 | Interface Log File-Separation by each direction of an Interface: A separate and independent Interface log file SHALL be generated for each direction (transmit and receive) of a roadside unit communication interface when the SNMPv3 MIB OIB 1.0.15628.4.1.9 for that interface is set to &quot;on.&quot; | See the SNMPv3 MIB 1.0.15628.4.1.9 in Appendix B for more information | Test:               |</p>
<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
</table>
| USDOT_RSU-Req_541-v002 | Interface Log File format: Each Interface Log File SHALL be generated in the industry standard packet capture (pcap) format and contain the following data:  
- Date and Time (in UTC, when the packet was logged)  
- RSSI (for Packets Received over DSRC)  
- TxPower (for Packets Transmitted over DSRC)  
- packet (complete transmitted or received packet) | Test: | Test: |
| USDOT_RSU-Req_521-v003 | Interface Log File Close-Max file size: The roadside unit SHALL close an active Interface Log File upon reaching the configured "Max file size" in SNMPv3 MIB OID 1.0.15628.4.1.9.  
See the SNMPv3 MIB 1.0.15628.4.1.9 in Appendix B for more information | Test: | Test: |
| USDOT_RSU-Req_522-v001 | Interface Log File Close-transition to Standby: The roadside unit SHALL close all active Interface Log Files when transitioning to "standby" state. | Test: | Test: |
| USDOT_RSU-Req_543-v003 | Interface Log File Close-Time Limit: The roadside unit SHALL close an active Interface Log File upon reaching the configured "Max collection time" in SNMPv3 MIB OID 1.0.15628.4.1.9.  
See the SNMPv3 MIB 1.0.15628.4.1.9 in Appendix B for more information | Test: | Test: |
| USDOT_RSU-Req_523-v003 | Interface Log File Generation-Max file size: The roadside unit SHALL generate a new Interface Log File upon closing a previously active Interface Log File when the configured "Max file size" in SNMPv3 MIB OID 1.0.15628.4.1.9 is reached.  
See the SNMPv3 MIB 1.0.15628.4.1.9 in Appendix B for more information | Test: | Test: |
## Interface Log File Name Convention

Each roadside unit Interface Log File SHALL be named according to the following convention:

- RSU ID (see MIB OID 1.0.15628.4.1.17)
- Interface ID
- transmit, receive, or both
- date and time (UTC date and time when the file was created)

## Interface Log File Access

The roadside unit SHALL allow authorized users to view Interface Log Files stored in the Interface Log File directory on the device through an Ethernet interface.

## Message Processing – Store and Repeat-Encoded Payload

The roadside unit will transmit DSRC messages based on Active Message text files loaded on the device. Each text file will contain the transmission instructions and encoded payload for 1 DSRC message and include the following data elements:

- Message Type/Description
- Message PSID
- Message Priority
- Transmission Channel Mode
- Transmission Channel
- Transmission Interval
- Message Delivery (transmission) start time
- Message Delivery (transmission) stop time
- Signature
- Encryption
- Payload.

The file format is contained in Appendix C.
<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-</td>
<td>Store &amp; Repeat Message Start of Transmission: The roadside unit SHALL begin transmitting the payload of an Active Message text file over a DSRC interface, based on the transmission instructions contained in the Active Message text file, on or after the start time specified in the transmission instructions of the Active Message text file for each Active Message text file stored on the unit. Note: Appendix C contains the message format</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>Req_468-v001</td>
<td></td>
<td>-----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>USDOT_RSU-</td>
<td>Store &amp; Repeat Message End of Transmission: The roadside unit SHALL stop transmitting the payload of an Active Message text file as a DSRC message at end time specified in the transmission instructions of the Active Message text file for each Active Message text file stored on the unit.</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>Req_470-v001</td>
<td></td>
<td>-----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>USDOT_RSU-</td>
<td>Store &amp; Repeat Message Storage: The roadside unit SHALL store at least 100 Active Message text files in an Active Message directory.</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>Req_452-v002</td>
<td></td>
<td>-----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>USDOT_RSU-</td>
<td>Store &amp; Repeat Active Message file installation: The roadside unit SHALL allow authorized users to add/remove Active Message text files to/from the Active Message directory through SNMPv3 OID 1.0.15628.4.1.4.x.</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>Req_453-v003</td>
<td></td>
<td>-----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>USDOT_RSU-</td>
<td>Store &amp; Repeat Active Message file removal: The roadside unit SHALL allow authorized users to remove Messages from the Active Message directory through SNMPv3 OID 1.0.15628.4.1.4.</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>Req_454-v003</td>
<td></td>
<td>-----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>USDOT_RSU-</td>
<td>Store &amp; Repeat Active Message review: The roadside unit SHALL allow authorized users to view the contents of Active Messages in the Active Message directory through SNMPv3 OID 1.0.15628.4.1.4.</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>Req_455-v003</td>
<td></td>
<td>-----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>USDOT_RSU-Req_457-v003</td>
<td>Store &amp; Repeat Active Message Modification: The roadside unit SHALL allow authorized users to modify an Active Message through SNMPv3 OID 1.0.15628.4.1.4.</td>
<td></td>
<td>Test:</td>
</tr>
</tbody>
</table>
| USDOT_RSU-Req_459-v001 | Store & Repeat Active Message Authorized Access Log Entry: The roadside unit SHALL write an INFO entry to the System Log File for each authorized access to an Active Message text file containing the following data:  
- Date and Time  
- File Name (name of the Active Message text file as stored in the Active Message directory)  
- Successful operation (installation, removal, or modification)  
- user ID |           | Test:               |
| USDOT_RSU-Req_469-v001 | Store & Repeat Active Message Failed Access Log Entry: The roadside unit SHALL write a WARNING entry to the System Log File for each failed access attempt to an Active Message text file containing the following data:  
- Date and Time  
- File Name (name of the Active Message text file as stored in the Active Message directory)  
- Failed operation (install, remove, modify)  
- user ID |           | Test:               |
<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
</table>
| USDOT_RSU-Req_462-v001 | Store & Repeat Active Message Transmission Log Entry: The roadside unit SHALL write a NOTICE entry to the System Log File when an Active Message changes transmission status resulting from a user initiated device shut down, device boot up, message start time or message end time. Each entry will contain the following data:  
- Date and Time  
- File Name (name of the Active Message text file as stored in the Active Message directory)  
- Transmission Status (Start/Stop) |           | Test: |

**Message Processing – Store and Repeat-Raw Data Payload**

If supported, the roadside unit will transmit DSRC messages based on configuration text files containing raw, un-encoded data, loaded on the device. Each text file will contain the transmission instructions and human readable data elements for 1 DSRC message and include the following data elements:

- Message Type/Description
- Message PSID
- Message Priority
- Transmission Channel Mode
- Transmission Channel
- Transmission Interval
- Message Delivery (transmission) start time
- Message Delivery (transmission) stop time
- Signature
- Encryption
- <list of raw data elements>. 
Table 3-10. Store and Repeat Message Requirements (Raw Data Payload).

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_562-v001</td>
<td>Raw Data Text File: The roadside unit MAY store raw data text files for encoding into messages to be transmitted over a DSRC interface. Note: This is similar to the Store &amp; Repeat functionality described in Section 3.4.4 with the exception that the file stored on the RSU would contain raw, un-encoded, data to be encoded prior to being transmitted over DSRC. For Example a human readable/configurable Map configuration file</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_563-v001</td>
<td>Raw Data Text File Encoding: The roadside unit MAY encode raw data contained in a text file residing on the RSU into messages to be transmitted over a DSRC interface. Note: This is similar to the Store &amp; Repeat functionality described in Section 3.4.4 with the exception that the RSU would encode the raw data contained in the stored file into a DSRC Payload of the appropriate format prior to transmitting over DSRC. For Example a human readable/configurable Map configuration file</td>
<td></td>
<td>Test:</td>
</tr>
</tbody>
</table>

Message Processing – Immediate Forward-Encoded Payload

The roadside unit will transmit DSRC messages based on information received from a network host. Each Immediate Forward (IF) message received from a network host will contain the transmission instructions and payload for 1 DSRC message and include the following data elements:

- Message Type/Description
- Message PSID
- Message Priority
- Transmission Channel Mode
- Transmission Channel
- Transmission Interval (set to Null)
• Message Delivery (transmission) start time (set to Null)
• Message Delivery (transmission) stop time (set to Null)
• Signature
• Encryption
• Payload.

Appendix C contains the format of the Immediate Forward Message.

Table 3-11. Immediate Forward Requirements (Encoded Payload)

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_554-v001</td>
<td>Immediate Forward Message Receive: The roadside unit SHALL receive messages for Immediate Forward from network hosts on default UDP port 1516</td>
<td>Note: Appendix C contains the Immediate Forward message format</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_471-v003</td>
<td>Immediate Forward Message Transmission: The roadside unit SHALL transmit over a DSRC interface each message payload received from a network host upon receipt of the message and according to the transmission instructions contained in the message header.</td>
<td>Note: Appendix C contains the Immediate Forward message format</td>
<td>Test:</td>
</tr>
</tbody>
</table>

**Message Processing – Immediate Forward-Raw Data Payload**

If supported, the roadside unit will transmit DSRC messages based on raw, un-encoded, data received from a network host. Each data stream will include raw data elements for 1 DSRC message. The following transmission instructions should be applied to each message:

- Message Type/Description
- Message PSID
- Message Priority
- Transmission Channel Mode
- Transmission Channel
- Transmission Interval (set to Null)
- Message Delivery (transmission) start time (set to Null)
- Message Delivery (transmission) stop time (set to Null)
- Signature
- Encryption.

Table 3-12. Immediate Forward Requirements (Raw Data Payload)

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
</table>
| USDOT_RSU-Req_565-v001 | Raw Data Stream: The roadside unit MAY accept raw data over a non-DSRC Interface for encoding into messages to be transmitted over a DSRC interface  
Note: This is similar to the Immediate Forward functionality described in Section 3.4.6 with the exception that the RSU will receive raw, un-encoded, data from a network host that must be encoded prior to being transmitted over DSRC. For example: raw SPaT data from a Signal Controller |           | Test                |
| USDOT_RSU-Req_566-v001 | Data Stream Message Encoding: The roadside unit MAY encode raw data received on a non-DSRC interface into messages to be transmitted over a DSRC interface  
Note: This is similar to the Immediate Forward functionality described in Section 3.4.6, with the exception that the RSU will encode the raw data into a DSRC Payload of the appropriate format prior to transmitting over DSRC. For example: raw SPaT data from a Signal Controller. |           | Test                |
### Security

Table 3-13. Security Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_567-v001</td>
<td>Physical Security: The roadside unit SHALL be compliant with Federal Information Processing Standard (FIPS) 140-2 Level 2 Physical Security Requirements</td>
<td>FIPS 140-2</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_585-v001</td>
<td>Physical Security: The roadside unit SHOULD be compliant with Federal Information Processing Standard (FIPS) 140-2 Level 3 Physical Security Requirements that require a tamper response mechanism, such as sending off an indicator to the backhaul network.</td>
<td>FIPS 140-2</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_344-v002</td>
<td>Authentication: The roadside unit SHALL be protected by a password compliant with either local operator security policies or a policy based on existing standards (e.g., FIPS 140- Level 3 and 4 in Section 4.3.3)</td>
<td>FIPS 140-2 Section 4.3.3</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_467-v001</td>
<td>Authentication: The roadside unit SHALL support multiple SNMPv3 users each with an individual password</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_345-v001</td>
<td>Authentication: The roadside unit SHOULD support multi-factor authentication.</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_632-v002</td>
<td>Authentication: The roadside unit SHOULD enforce multi-factor authentication on all SSH Version 2 sessions, and, if supported, all TLS-based remote access sessions to the roadside unit.</td>
<td>Secure Shell (SSH) Version 2 (as specified in IETF RFC 4251, IETF RFC 4252, IETF RFC 4253, and IETF RFC 4254) and Transport Layer Security (TLS) Protocol Version 1.2 (IETF RFC 5246, August 2008)</td>
<td>Test:</td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>USDOT_RSU-Req_346-v002</td>
<td>Authentication: The roadside unit SHALL support password recovery for the RSU User Accounts that cannot be violated by physical access alone.</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_347-v002</td>
<td>Configuration: The roadside unit configuration files SHOULD enforce digital signatures to prevent unauthorized modifications.</td>
<td>FIPS 186-4</td>
<td>Test:</td>
</tr>
</tbody>
</table>
| USDOT_RSU-Req_348-v001 | Access Control: The roadside unit SHALL restrict remote network access based on an IP Address Access Control List (ACL)  
Note: The RSU can only be accessed from the IP Addresses contain in the ACL.  |           | Test:               |
| USDOT_RSU-Req_350-v001 | Data Protection: The roadside unit local file system SHOULD be encrypted    |           | Test:               |
| USDOT_RSU-Req_351-v002 | Interfaces: Each roadside unit Ethernet interface SHALL be protected by a configurable firewall with a default to be closed. |           | Test:               |
| USDOT_RSU-Req_440-v002 | Access Control: If so equipped, Web-Based access to the roadside unit SHALL only be through Hypertext Transfer Protocol Secure (HTTPS) |           | Test:               |
| USDOT_RSU-Req_442-v002 | Data Protection: The roadside unit SHOULD synchronize its system clock to a Network Time Protocol (NTP) Service in the event that it loses GPS fix. |           | Test: if available  |
| USDOT_RSU-Req_355-v001 | Authentication: If the roadside unit synchronizes its system clock to a Network Time Protocol (NTP) service, the device SHALL authenticate messages received from the NTP service | Req_442   | Test: if available  |
| USDOT_RSU-Req_356-v003 | Access Control: The roadside unit SHALL only be accessible through the following network protocols:  
Secure Shell version 2 (SSHv2)  
SNMPv3  
SCP  
TLS (HTTPS) |           | Test: log in attempts will be made using SSHv2 |
<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
</table>
| USDOT_RSU-Req_583-v001 | Configuration: network protocol Secure Shell version 2 SHOULD be configured as follows:  
Root Login Disable root  
Use certificate-based authentication, rate-limited (to slow down brute-force attempts)  
use FIPS 140-2-compliant cryptography | FIPS 140-2      | Test:               |
| USDOT_RSU-Req_606-v001 | Data Protection: The roadside unit SHALL immediately apply integrity protections to the store-and-repeat message data following SNMP-secured download to the roadside unit. | Section 3.4.4, Section 3.4.5, Req_607 | Test:               |
| USDOT_RSU-Req_607-v001 | Data Protection: The roadside unit SHALL verify the integrity of the store-and-repeat message data prior to generating and transmitting IEEE 1609.2-secured messages that are derived from the message data. | Section 3.4.4 and Section 3.4.5 | Test:               |
| USDOT_RSU-Req_609-v001 | Data Protection: The roadside unit SHALL inhibit construction and transmission of an IEEE 1609.2-secured message derived from an integrity-failed store-and-repeat message. | Section 3.4.4 and Section 3.4.5 | Test:               |
| USDOT_RSU-Req_615-v001 | Notification: The roadside unit SHALL notify a remote host via SNMPv3:  
if an Active Message fails an Integrity check  
if a configurable number of consecutive authentication attempts have failed  
if the signature of a signed DSRC message has failed verification  
of any access control errors and rejections | | Test:               |
<p>| USDOT_RSU-Req_616-v001 | Notification: If secure storage is available, the roadside unit SHALL notify a remote host via SNMPv3 if the secure parameters stored in secure storage have failed an Integrity check. | Req_579   | Test:               |</p>
<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_617-v001</td>
<td>Notification: If FIPS 140-2 level 3 is implemented, the roadside unit SHALL notify a remote host via SNMPv3 if the enclosure has been tampered with according to FIPS 140-2 Section 4.5 Level 3 tamper indication requirements.</td>
<td>FIPS 140-2 Section 4.5 Level 3</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_619-v001</td>
<td>Access Control: The roadside unit SHALL enforce clear associations between roles, services and the distinct authentication and authorizations required to access those services.</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_620-v001</td>
<td>Access Control: Access to sensitive services SHALL require an authenticated, authorized role.</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_621-v001</td>
<td>Access Control: Access to sensitive data SHALL require an authenticated, authorized role.</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_622-v001</td>
<td>Authentication: The roadside unit SHALL be configurable to limit the number of repeated authentication attempts for services requiring authentication.</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_623-v002</td>
<td>Authentication: The roadside unit SHOULD utilize certificate pinning to secure all TLS sessions with the SCMS Device Configuration Manager and other SCMS nodes to which it connects.</td>
<td>Transport Layer Security (TLS) Protocol Version 1.2 (IETF RFC 5246 and IETF RFC 7469) with cipher suites pinned to USDOT Security Credential Management System Design: Security Credential Management System Proof–of–Concept Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.1, published May, 2016, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>USDOT_RSU-Req_625-v001</td>
<td>Authentication: The roadside unit SHALL terminate a TLS session if the server public key certificate signature verification fails during TLS session establishment.</td>
<td>Transport Layer Security (TLS) Protocol Version 1.2 (IETF RFC 5246, August 2008)</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_627-v001</td>
<td>Authentication: The roadside unit should verify the IEEE 1609.2 digital signature on all messages previously signed by the TMC or other backhaul services prior to forwarding over the DSRC interface.</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_628-v002</td>
<td>Authentication: Services requiring role- or identity-based authentication SHALL meet the authentication requirements of FIPS 140-2, Section 4.3 Level 2 and any supporting FIPS 140-2 implementation guidance.</td>
<td>FIPS 140-2, Section 4.3 Level 2 and Level 3</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_629-v001</td>
<td>Authentication: Services requiring authentication SHALL meet the single attempt and multiple attempt authentication strength requirements of FIPS 140-2, Section 4.3.</td>
<td>FIPS 140-2, Section 4.3</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_630-v001</td>
<td>Authentication: The roadside unit SHALL require SSH Version 2 or TLS Version 1.2 using mutual (two way) public key credential authentication for all authorized user sessions.</td>
<td>Secure Shell (SSH) Version 2 (as specified in IETF RFC 4251, IETF RFC 4252, IETF RFC 4253, and IETF RFC 4254)</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_631-v001</td>
<td>Authentication: The roadside unit SHALL require HTTPS using mutual (two way) public key credential authentication for all HTTPS connections to the roadside unit.</td>
<td>Transport Layer Security (TLS) Protocol Version 1.2 (IETF RFC 5246, August 2008)</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_635-v001</td>
<td>Configuration: The roadside unit SHALL be configurable regarding the maximum frequency (number per second) or ratio (percentage) of DSRC message digital signatures to verify based on PSID.</td>
<td>Section 3.4.4 and Section 3.4.5</td>
<td>Test:</td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>USDOT_RSU-Req_636-v001</td>
<td>Configuration: The roadside unit SHALL be able to be configured whether to accept, drop, or respond to application-specific messages signed with expired certificates.</td>
<td>Section 3.4.4 and Section 3.4.5</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_638-v001</td>
<td>Data Protection: The roadside unit SHALL cryptographically protect the integrity of all configuration information provided by the SCMS Device Configuration Manager (DCM).</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_639-v002</td>
<td>Data Protection: All cryptographic keys SHALL be established or generated using a FIPS Approved and allowed key generation and key establishment mechanisms.</td>
<td>FIPS 140-2 Annex A and Annex D</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_640-v001</td>
<td>Data Protection: All sensitive roadside unit system files and application files SHALL be digitally signed using a digital signature algorithm listed in FIPS 186-4.</td>
<td>FIPS 186-4</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_641-v001</td>
<td>Data Protection: The roadside unit SHALL successfully verify the digital signature on all sensitive roadside unit system and application files prior to exposing any services.</td>
<td></td>
<td>Test:</td>
</tr>
</tbody>
</table>
| USDOT_RSU-Req_642-v001 | Data Protection: The roadside unit SHALL implement a secure mechanism in software to securely store and provide strict access controls to all sensitive security parameters, including:  
  - TLS public and private keys (as used for HTTPS or other TLS tunneling, including with the SCMS)  
  - SSH public and private keys  
  - Passwords  
  - SNMP keys and passphrases  
  - Any sensitive security parameters not stored in a hardware secure storage mechanism | Req_579                                       | Test:               |
<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
</table>
| USDOT_RSU-Req_643-v001 | Data Protection: Software secure storage SHALL:  
- prevent read-access to all stored security parameters,  
- maintain integrity of all security parameters, including associations of keys with entities and processes  
- check the integrity of stored security parameters when accessing  
- prevent unauthorized modification of security parameters, except by authorized users  
- prevent unauthorized addition of security parameters, except by authorized users  
- prevent unauthorized substitution of security parameters, except by authorized users  
- encrypt all sensitive security parameters when not in use                                                                 | Req_579   | Test:               |
<p>| USDOT_RSU-Req_644-v001 | Data Protection: The roadside unit SHALL store passwords in secure storage only after modifying via a one-way cryptographic function.                                                                                                                                         | Req_579   | Test:               |
| USDOT_RSU-Req_645-v001 | Data Protection: The roadside unit SHALL zeroize all non-factory installed parameters, cryptographic keys, applications, data and configurations when undergoing a factory reset.                                                                                        | Req_568   | Test:               |
| USDOT_RSU-Req_646-v001 | Data Protection: Upon sudden loss of external power, the roadside unit SHALL undergo a shutdown procedure that preserves file system integrity.                                                                                                                                 |           | Test:               |</p>
<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_647-v001</td>
<td>Interfaces: The roadside unit SHALL utilize TLS versions and cipher suites consistent with SCMS interface specifications.</td>
<td>USDOT Security Credential Management System Design: Security Credential Management System Proof-of-Concept Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.1, published May, 2016, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_648-v001</td>
<td>Interfaces: Services and protocols SHALL be able to be inhibited according to physical interface, source/destination IP address and source/destination ports</td>
<td>USDOT Security Credential Management System Design: Security Credential Management System Proof-of-Concept Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.1, published May, 2016, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_649-v002</td>
<td>Logging: The roadside unit SHALL write the following entries to the System Log File: GPS location and time data on a configurable interval metrics on packet integrity or transmission/reception errors all authentication parameter modifications attempts to perform a service allocated to a role(s) for which the entity is not authenticated authorization failures when a role or identity attempts access services and data requiring authorization input and output protocol violations, including encoding errors and invalid parameters session management failures in each of the session-based network protocols it supports all additions, modifications and removal of secret, public and private</td>
<td>FIPS 186-4</td>
<td>Test:</td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td>cryptographic keys success or failure of digitally signing all sensitive roadside unit system and application files using a digital signature algorithm listed in FIPS 186-4 any expired IEEE 1609.2 public key credentials it has stored any expired X.509 public key credentials it has stored pending expirations of all public key credentials to a configurable warning time value</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**USDOT Situation Data Clearinghouse and Warehouse**

If supported the roadside unit will deposit Intersection Situation Data into the USDOT Situation Data Clearinghouse and retrieve geographic relevant Traveler information messages from the USDOT Situation Data Warehouse.

Table 3-14. Situation Data Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_589-v001</td>
<td>Situation Data Clearinghouse: if transmitting Intersection Safety Awareness messages, the roadside unit SHOULD deposit an Intersection Situation Data (ISD) Protocol Data Unit (PDU) (message) into the USDOT Situation Data Clearinghouse once every 2 seconds. Intersection Situation Data Protocol Data Units are comprised of 1 SAE Signal Phase and Timing Message (SPaT) and 1 SAE Map Message. See the SNMPv3 MIB OID 1.0.15628.4.1.20 in Appendix B for more information</td>
<td>USDOT Connected Vehicle Support Services SEMI_v2.3.0_070616.asn or later</td>
<td>Test:</td>
</tr>
</tbody>
</table>
### Behavioral Requirements

This section contains the specifications for the expected behavior of a compliant roadside unit.

#### Table 3-15. Behavioral Requirements

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_496-v002</td>
<td>Configuration Updates-updateconfig command: The roadside unit SHALL update all configuration parameters upon receiving an &quot;updateconf&quot; command from an authorized user</td>
<td>USDOT Connected Vehicle Support Services SEMI_v2.3.0_070616.asn or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_497-v002</td>
<td>Configuration Updates-SNMPv3 MIB: The roadside unit SHALL update all configuration parameters upon receiving changes to any writable SNMPv3 MIB objects from an authorized user</td>
<td>USDOT Connected Vehicle Support Services SEMI_v2.3.0_070616.asn or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_604-v002</td>
<td>Antenna Output Power: the roadside unit transmit output power SHOULD be configurable</td>
<td>USDOT Connected Vehicle Support Services SEMI_v2.3.0_070616.asn or later</td>
<td>Test:</td>
</tr>
</tbody>
</table>
# Operational States

## Table 3-16. Operational State Requirements

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_475-v002</td>
<td>State Transition - Initial to Standby: The roadside unit SHALL transition from the &quot;Initial&quot; State to the &quot;Standby State&quot; upon power on. Note: Transition from the &quot;initial&quot; state to the &quot;standby&quot; state only happens the first time the device is powered on after manufacturing or after factory reset. The device will only return to the &quot;initial&quot; state if a factory reset is initiated.</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_476-v002</td>
<td>State Transition - Operate to Standby: The roadside unit SHALL transition from the &quot;Operate&quot; State to the &quot;Standby&quot; State upon receiving a &quot;standby&quot; command from an authorized user</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_479-v002</td>
<td>State Transition - Standby to Operate: The roadside unit SHALL transition from the &quot;Standby&quot; State to the &quot;Operate&quot; state upon receiving a &quot;run&quot; command from an authorized user</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_480-v002</td>
<td>State Transition - Current to No Power: The roadside unit SHALL transition from its current State to the &quot;No Power&quot; State upon loss of power or user initiated shut down without corrupting or damaging the file system or files contained on the unit.</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_575-v001</td>
<td>State Transition - No Power to Previous State: When power is restored, the roadside unit SHALL transition from the “No Power” state to the State (&quot;Standby&quot; or &quot;Operate&quot;) the roadside unit was in when power was lost.</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>USDOT_RSU-Req_568-v002</td>
<td>Factory Reset: The roadside unit SHALL support a &quot;Factory Reset&quot; mechanism (command, button, etc.) for authenticated, authorized local users to remove all configuration parameters and operator installed files, returning the device to its original Factory Settings and &quot;Initial&quot; State</td>
<td></td>
<td>Test:</td>
</tr>
</tbody>
</table>

**Operational Modes**

Table 3-17. Operational Mode Requirements

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
</table>
| USDOT_RSU-Req_482-v001 | Operation Mode-Connected: The roadside unit SHALL operate with full functionality while connected to an operations center.  
Note: "Connected Mode" implies that the RSU is intended to continuously be connected to an operation center                                                                 |           | Test:               |
| USDOT_RSU-Req_484-v001 | Operation Mode-"Standalone": The roadside unit SHALL operate with full functionality while not connected to an operations center, until the device’s security credentials expire. |           | Test:               |
## Operational Configuration

Table 3-18. Operational Configuration Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_435-v001</td>
<td>SNMPv3: roadside unit Configuration, Management, and Status information SHALL be provided through SNMPv3. The RSU Management Information Base (MIB) is contained in Appendix B.</td>
<td>Simple Network Management Protocol Version 3 (SNMPv3) (as specified in IETF RFC 3411, IETF RFC 3412, IETF RFC 3413, IETF RFC 3414, IETF RFC 3415, IETF RFC 3416, IETF RFC 3417, and IETF RFC 3418)</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_487-v001</td>
<td>SNMPv3 MIB Configurations: The roadside unit SHALL operate based on parameters contained in the SNMPv3 MIB stored on the device.</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_489-v001</td>
<td>SNMPv3 MIB Configuration Default Parameters: The roadside unit SHALL have default values for each configuration parameter in the SNMPv3 MIB.</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_498-v001</td>
<td>SNMPv3 MIB Configuration Parameter Valid Range: The value of each SNMPv3 MIB Object SHALL be restricted to a valid range in which the roadside unit will operate.</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_490-v001</td>
<td>SNMPv3 MIB Walk: The roadside unit SHALL allow an authorized user to perform a MIB walk on the SNMPv3 MIB to produce a complete list of all supported MIBs and OIDs and the current setting for each Object.</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_491-v002</td>
<td>SNMPv3 MIB Parameter Modification: The roadside unit SHALL allow an authorized user to modify the value of any writeable SNMPv3 MIB Object within its valid range.</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| USDOT_RSU-Req_492-v002 | SMNPv3 MIB Modification Validation-System Status Log File entry: The roadside unit SHALL write an INFO entry to the System Status Log File if the value of a writable SNMPv3 MIB Object is modified to an out of range value. The log entry will contain the following data elements:  
  - Date and Time  
  - file name (name of the MIB file)  
  - "MIB Object Value Out-of-Range"  
  - OID (of the Object whose value is out of range)  
  - user ID  
  - attempted value                                                                                                           | Test:     |                     |
| USDOT_RSU-Req_499-v001 | SMNPv3 MIB Modification Validation-retain current value: The roadside unit SHALL retain the current value for a writable SNMPv3 MIB Object that is modified to an out of range value                                                                 | Test:     |                     |
| USDOT_RSU-Req_493-v001 | SMNPv3 MIB installation: The roadside unit SHALL allow authorized users to copy/move a SNMPv3 MIB from a network host to the SMNPv3 MIB directory on the device through an Ethernet Interface.                                                                                   | Test:     |                     |
| USDOT_RSU-Req_494-v001 | SMNPv3 MIB copy: The roadside unit SHALL allow authorized users to copy the SNMPv3 MIB from the SNMPv3 MIB directory to a network host through an Ethernet Interface.                                                                                              | Test:     |                     |
### Chapter 3. System Requirements

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
</table>
| USDOT_RSU-Req_495-v002 | SNMPv3 MIB Installation Validation-System Status Log File entry: The roadside unit SHALL write a CRITICAL entry in the System Status log file if a SNMPv3 MIB that contains out of range values for a writable Object is copied/moved into the SNMPv3 MIB directory. The log entry will contain the following data elements:  
  * Date and Time  
  * file name (name of the MIB file)  
  * "MIB Object Value Out-of-Range:"  
  * OID (of the Object whose value is out of range)  
  * user ID  
  * offending value | | Test: |

### Health and Status Monitoring

Table 3-19. Health and Status Monitoring Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
</table>
| USDOT_RSU-Req_592-v002 | The roadside unit SHALL report over SNMPv3:  
  status of its memory (OID ucdavis.4)  
  status of its CPU load  
  status of its non-volatile storage  
  standard system load average values  
  time elapsed since it entered the "Operate" state  
  time elapsed since it was first powered on  
  last user to log in  
  time the last user logged in  
  source IP address of the last user to log in  
  number of messages | UCD-SNMP-MIB | Test: |
<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_601-v001</td>
<td>The roadside unit SHOULD report over SNMPv3 its internal temperature</td>
<td></td>
<td>Test:</td>
</tr>
</tbody>
</table>

### Performance Requirements

This section contains the specifications for the expected performance of a compliant roadside unit.

**Table 3-20. Performance Requirements.**

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_340-v001</td>
<td>Mean-Time-Between-Failure (MTBF): The roadside unit SHALL remain operational for an average of 100,000 hours.</td>
<td></td>
<td>Analysis: using MIL-HDBK-217 calculation methods</td>
</tr>
<tr>
<td>USDOT_RSU-Req_341-v002</td>
<td>Availability: The roadside unit SHALL meet the operational availability requirements of 99.9%. Note: This does not include scheduled maintenance.</td>
<td></td>
<td>Analysis:</td>
</tr>
</tbody>
</table>
Radio Performance

Table 3-21. Radio Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_432-v004</td>
<td>DSRC Radio Receive Range: The roadside unit SHALL receive DSRC messages throughout a range of 1m to 300m, with a maximum Packet Error Rate of 10.0%, in an open field under the following conditions: When receiving on an 802.11 Operating class 17 channel (even 10 MHz Service Channel, numbers 172 through 184). When receiving Part 1 of the SAE J2735 defined Basic Safety Message (BSM) With a BSM transmit rate of 10 Hz With a Data Rate of 6 Mbps With an RSU antenna centerline height of 8 meters With a BSM transmit power of VRPMax, as defined in SAE J2945/1</td>
<td>FCC Title 47, Part 90.377 SAE J2945/1</td>
<td>Test: Measure the Packet Error Rate of received Basic Safety Messages on Service Channel 172 at specified distances from the RSU Antenna</td>
</tr>
</tbody>
</table>
Chapter 3. System Requirements

### Smart Roadside Unit Specifications

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_433-v003</td>
<td>DSRC Radio Transmission Range: The roadside unit SHALL transmit DSRC messages throughout a range of 1m to 300m, with a maximum Packet Error Rate of 10.0%, in an open field under the following conditions: When transmitting on an 802.11 Operating class 17 channel (even 10 MHz Service Channel, numbers 172 through 184). When transmitting Wave Service Advertisements (WSA), as defined in IEEE 1609.3 With a WSA Transmission Rate of 10 Hz With a Data Rate of 6 Mbps With an RSU antenna centerline height of 8 meters With a maximum WSA transmit EIRP Using a Receiver conforming to SAE J2945/1 Section 6.4.2</td>
<td>FCC Title 47, Part 90 SAE J2945/1 Section 6.4.2</td>
<td>Test: Transmit a DSRC message on each of the even 10MHz Service Channel and measure the Packet Error Rate at specified distances from the RSU Antenna</td>
</tr>
</tbody>
</table>

### Interface Requirements

This section contains the specifications for the internal and external interfaces of a compliant roadside unit.

**Table 3-22. Interface Requirements.**

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_363-v001</td>
<td>GPS: The roadside unit SHALL include an integrated GPS receiver (for positioning and UTC time).</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>USDOT_RSU-Req_364-v003</td>
<td>RSU Set Interface: At installation locations that require multiple roadside units, the “master” roadside unit in the set SHALL be functional as the Ethernet interface between other non-master RSUs and the backhaul communication.</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_326-v001</td>
<td>Physical Ethernet Interface: The roadside unit SHALL, at a minimum, include a 1x10/100 Base-T Ethernet (RJ45) port that supports 48V DC and is compliant with 802.3at Power-over-Ethernet (PoE), including IPv4 and IPv6.</td>
<td>IEEE 802.3at</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_327-v001</td>
<td>Virtual Ethernet Interfaces: The roadside unit SHALL support multiple, independent IPv4 and IPv6 networks.</td>
<td>IPv4, IPv6, and IEEE 802.3</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_584-v002</td>
<td>Interfaces: If the roadside unit contains additional integrated wireless interfaces, such as: -802.11b/g/n/a/acother Wi-Fi -Cellular 3G/4G -others those interfaces SHALL be inhibited or implement equivalent security access controls, authentication, integrity, and confidentiality to the services available over the wired Power-over-Ethernet (PoE) interface.</td>
<td></td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_354-v001</td>
<td>Interfaces: The roadside unit SHOULD support NAT64 protocol</td>
<td></td>
<td>Test: If available</td>
</tr>
</tbody>
</table>
## Dedicated Short-Range Communications

### Table 3-23. DSRC Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_367-v001</td>
<td>FCC Regulation 47 CFR Compliance: The roadside unit SHALL comply with Federal Communications Commission (FCC) Code of Federal Regulations Title 47 Parts 0, 1, 2, 15, 90, and 95.</td>
<td>Federal Communications Commission (FCC) Code of Federal Regulations Title 47 Parts 0, 1, 2, 15, 90, and 95</td>
<td>Test:</td>
</tr>
</tbody>
</table>

### 802.11

### Table 3-24. IEEE 802.11 Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_372-v002</td>
<td>IEEE 802.11 Conformance: The roadside unit SHALL conform to IEEE Std. 802.11 with Management Information Base (MIB) variable <code>dot11OCBActivated</code> set to &quot;true&quot; and as bounded by the general requirement to fully support the IEEE 1609.x protocol specification set.</td>
<td>802.11-2012 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>USDOT_RSU-Req_373-v003</td>
<td>IEEE 802.11 Physical Layer: The roadside unit SHALL implement the Orthogonal frequency division multiplexing (OFDM) physical layer of the Open Systems Interconnection (OSI) model defined in Clause 18 of IEEE 802.11, unless otherwise indicated (including all data rates for 10 MHz channel spacing and 20 MHz channel spacing in 18.2.3.4).</td>
<td>802.11-2012 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, or later, Clause 18</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_375-v001</td>
<td>IEEE 802.11 Default Values: The roadside unit SHALL use the default values defined in IEEE 802.11 unless otherwise indicated (including the slot time in 18.3.8.7).</td>
<td>802.11-2012 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_376-v001</td>
<td>IEEE 802.11 Quality of Service: The roadside unit SHALL send 802.11 data frames using the Quality of Service (QoS) Data subtype.</td>
<td>802.11-2012 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>USDOT_RSU-Req_377-v001</td>
<td>Arbitration Interframe Spacing Value: The roadside unit SHALL configure an AIFSN of a given access category with an integer value from 2 to X, where the value of X is based on the chip set used – as defined by the vendor. Note: Vendor should provide the limit for X, based on the chip set used</td>
<td>802.11-2012 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_378-v001</td>
<td>Transmission Opportunity Value: The TXOP Limit of a given AC SHALL be capable of being set to 0.</td>
<td>802.11-2012 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_379-v001</td>
<td>Contention Window Minimum Value: The CWmin of a given AC SHALL take any value of the form ((2^k) - 1), for (k = 1) through (Y). Note: Vendor should provide the limit for (Y), based on the chip set used.</td>
<td>802.11-2012 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>USDOT_RSU-Req_382-v001</td>
<td>IEEE 802.11 Basic Service Set: The roadside unit SHALL send MAC Protocol data units (MPDUs) outside the context of a basic service set (BSS), i.e. with Management Information Base (MIB) variable dot11OCBActivated is set to &quot;true.&quot;</td>
<td>802.11-2012 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_383-v001</td>
<td>IEEE 802.11 Operating Class 17: The roadside unit SHALL support Operating class 17 (even 10 MHz channels in the range 172 to 184).</td>
<td>802.11-2012 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_384-v003</td>
<td>IEEE 802.11 Operating Class 18: The roadside unit SHALL support Operating class 18 (odd 20 MHz channels in the range 175 to 181).</td>
<td>802.11-2012 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements</td>
<td>Test:</td>
</tr>
<tr>
<td>ReqID</td>
<td>Description</td>
<td>Reference</td>
<td>Verification Method</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>USDOT_RSU-Req_385-v001</td>
<td>IEEE 802.11 Enhanced Distributed Channel Access: The roadside unit SHALL have a configurable EDCA parameter with a default as defined in IEEE 802.11.</td>
<td>802.11-2012 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, or later, Table 8-106</td>
<td>Test:</td>
</tr>
</tbody>
</table>

**IEEE 1609.2**

Table 3-25. IEEE 1609.2 Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_388-v002</td>
<td>IEEE 1609.2 Conformance: The roadside unit SHALL conform to IEEE 1609.2</td>
<td>IEEE 1609.2-2016 IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages, as modified by guidance notes, or later</td>
<td>Test:</td>
</tr>
</tbody>
</table>
### Chapter 3. System Requirements

#### USDOT Security Credential Management System

**Conformance:** The roadside unit SHALL conform to the USDOT Security Credential Management System End Entity Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
</table>

**Secure Storage:** The roadside unit SHOULD store all digital certificates and public and private key pairs in secure storage, such as that contained in a Hardware Security Module.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_579-v001</td>
<td>Secure Storage: The roadside unit SHOULD store all digital certificates and public and private key pairs in secure storage, such as that contained in a Hardware Security Module.</td>
<td>USDOT Security Credential Management System Design: Security Credential Management System Proof-of-Concept Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.1, published May, 2016, or later</td>
<td>Documentation:</td>
</tr>
</tbody>
</table>

**IEEE 1609.3**

Table 3-26. IEEE 1609.3 Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_412-v002</td>
<td>IEEE 1609.3 Conformance: The roadside unit SHALL conform to IEEE 1609.3.</td>
<td>IEEE 1609.3-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services, or later</td>
<td>Test:</td>
</tr>
</tbody>
</table>
Chapter 3. System Requirements

### Dedicated Short Range Communications Roadside Unit Specifications

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_413-v001</td>
<td>IEEE 1609.3 IP Data: The roadside unit SHALL process both transmitted and received IPv6 packets. Note: At a minimum, IP based communications over DSRC will be used for the exchange of data between the onboard equipment and the 1609.2 security credential management system.</td>
<td>IEEE 1609.3-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services. or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_414-v001</td>
<td>IEEE 1609.3 WSMP Data: The roadside unit SHALL process (both transmit and receive) WAVE Short Message Protocol (WSMP) messages.</td>
<td>IEEE 1609.3-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services. or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_415-v001</td>
<td>IEEE 1609.3 PSID-Specific User Priority: The roadside unit SHALL assign a configurable PSID value (default to the value specified for the associated application area defined in IEEE 1609.12-2016, or later) and a configurable User Priority value (default to 2) to each data frame.</td>
<td>IEEE 1609.3-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services. or later, IEEE P1609.12-2016 or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_416-v001</td>
<td>IEEE 1609.3 WSMP-N- Header Options: The following WSMP-N- header options SHALL be configured on the roadside unit: Data Rate Transmit Power Used</td>
<td>IEEE 1609.3-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services. or later</td>
<td>Test:</td>
</tr>
</tbody>
</table>

**WAVE Service Advertisements**

Appendix D contains an Example WSA for an RSU advertising Intersection.
Table 3-27. WSA Requirements.

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_586-v001</td>
<td>WSA Security Profile: The roadside unit SHALL conform to the WAVE Service Advertisement (WSA) Security Profile defined in IEEE 1609.3-2016 Annex H.1</td>
<td>IEEE 1609.3-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_587-v001</td>
<td>WSA Broadcast Channel: The roadside unit SHALL broadcast WAVE Service Advertisements (WSA) on the Control Channel (CCH)</td>
<td>IEEE 1609.3-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_588-v001</td>
<td>WSA Broadcast Time Slot: the roadside Unit SHALL broadcast WAVE Service Advertisements (WSA) during Time Slot 0</td>
<td>IEEE 1609.3-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_570-v002</td>
<td>WSA Configuration_General: The roadside unit WAVE Service Advertisement (WSA) SHALL include DSRC Service Channel (SCH) Services from WSA MIB OID 1.0.15628.4.1.13</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_571-v001</td>
<td>WSA Configuration_S&amp;R Messages: The roadside unit WAVE Service Advertisement (WSA) SHALL include DSRC Service Channel (SCH) Services based on the Store and Repeat messages contained in MIB OID 1.0.15628.4.1.4</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_572-v001</td>
<td>WSA Configuration_IF Messages: The roadside unit WAVE Service Advertisement (WSA) SHALL include DSRC Service Channel (SCH) Services based on Immediate Forward messages received on non-DSRC interfaces as listed in MIB OID 1.0.15628.4.1.5</td>
<td>Test:</td>
<td></td>
</tr>
</tbody>
</table>
### Chapter 3. System Requirements

**U.S. Department of Transportation**  
**Office of the Assistant Secretary for Research and Technology**  
**Intelligent Transportation Systems Joint Program Office**  
**Dedicated Short Range Communications Roadside Unit Specifications**

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_573-v002</td>
<td>Control Channel Store &amp; Repeat Messages: Store &amp; Repeat messages transmitted on the DSRC Control Channel (CCH), 178 SHALL NOT be included in the WAVE Service Advertisement</td>
<td>Test:</td>
<td></td>
</tr>
<tr>
<td>USDOT_RSU-Req_574-v001</td>
<td>Control Channel Immediate Forward Messages: Immediate Forward messages transmitted on the DSRC Control Channel (CCH), 178 SHALL NOT be included in the WAVE Service Advertisement</td>
<td>Test:</td>
<td></td>
</tr>
</tbody>
</table>

### IEEE 1609.4

**Table 3-28. IEEE 1609.4 Requirements.**

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_419-v001</td>
<td>IEEE 1609.4 Standard Conformance: Each DSRC radio contained in the roadside unit SHALL conform to IEEE 1609.4.</td>
<td>IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_420-v002</td>
<td>IEEE 1609.4 Radio Operating Modes: Each DSRC radio in the roadside unit SHALL be configurable to operate either in &quot;Continuous&quot; (operating continuously on a single Service Channel) or &quot;Alternating&quot; (switched between two Service Channels (or the Control Channel and a Service Channel)) Mode, as shown in Figure 9 of IEEE 1609.4-2016.</td>
<td>IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, Figure 9, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_360-v002</td>
<td>Channel Modes: The roadside unit SHALL support Continuous Mode and Alternating Mode radio operations simultaneously</td>
<td>USDOT_RSU-Req_420-v001</td>
<td>Test:</td>
</tr>
</tbody>
</table>

---

*U.S. Department of Transportation*  
*Office of the Assistant Secretary for Research and Technology*  
*Intelligent Transportation Systems Joint Program Office*  
*Dedicated Short Range Communications Roadside Unit Specifications*
<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_421-v001</td>
<td>IEEE 1609.4 Radio Channel Usage: Each DSRC radio in the roadside unit SHALL be configurable to send messages either on Channel 178 during the Control Channel (CCH) interval or on any of the 10 MHz or 20 MHz channels with no time interval restrictions.</td>
<td>IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_422-v001</td>
<td>IEEE 1609.4 Continuous Channel Mode: Roadside unit DSRC Radios in Continuous Mode SHALL be configurable for operation on any 10 MHz or 20 MHz channel (default 10 MHz Channel 172) with no time interval restrictions.</td>
<td>IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_423-v001</td>
<td>IEEE 1609.4 CCH Alternating Channel Mode: Roadside unit DSRC Radios in Alternating Mode SHALL broadcast WAVE Service Advertisements and WAVE Short Messages on Channel 178 during the Control Channel (CCH) interval</td>
<td>IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_436-v001</td>
<td>IEEE 1609.4 SCH Alternating Channel Mode: Roadside unit DSRC Radios in Alternating Mode SHALL be configurable to operate on any 10 MHz or 20 MHz channel during the Service Channel (SCH) Interval. Note: Service Channel configuration is part of the SNMPv3 MIB, see Appendix B.</td>
<td>IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_424-v002</td>
<td>Service Channel Interval: Roadside unit DSRC Radios in Alternating Mode SHALL be capable of switching to the configured Service Channel every Service Channel interval with no time interval restrictions.</td>
<td>IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, or later</td>
<td>Test:</td>
</tr>
</tbody>
</table>
### Chapter 3. System Requirements

<table>
<thead>
<tr>
<th>ReqID</th>
<th>Description</th>
<th>Reference</th>
<th>Verification Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>USDOT_RSU-Req_425-v002</td>
<td>RSU Sets-Service Channel Alternating Mode: All non-master roadside unit DSRC radios in Alternating Mode within the same RSU set SHALL automatically operate on the same service channel(s) as the configuration of the “master” roadside unit.</td>
<td>IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_429-v001</td>
<td>IEEE 1609.4 Synchronized Collision: Roadside unit DSRC radios in Alternating Mode SHALL avoid the synchronized collision phenomenon described in Annex B of IEEE 1609.4 when broadcasting messages on during the Control Channel interval.</td>
<td>IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, Annex B, or later</td>
<td>Test:</td>
</tr>
<tr>
<td>USDOT_RSU-Req_430-v001</td>
<td>IEEE 1609.4 Readdressing Option: The roadside unit SHALL implement the readdressing option defined in IEEE 1609.4</td>
<td>IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation Clause 6.6, or later</td>
<td>Test:</td>
</tr>
</tbody>
</table>
## Appendix A. Terms and Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AASHTO</td>
<td>American Association of State Highway and Transportation Officials</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>AIFSN</td>
<td>Arbitration Interframe Space Number, See IEEE 802.11</td>
</tr>
<tr>
<td>BSM</td>
<td>Basic Safety Message</td>
</tr>
<tr>
<td>C</td>
<td>Celsius (Unit of Temperature)</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CAMP</td>
<td>Crash Avoidance Metrics Partnership</td>
</tr>
<tr>
<td>CCH</td>
<td>Control Channel</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>Channel Mode</td>
<td>Single Channel Continuous or Dual Channel Alternating as defined in IEEE 1609.4.</td>
</tr>
<tr>
<td>CML</td>
<td>Communications Message Log</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List</td>
</tr>
<tr>
<td>CSW</td>
<td>Curve Speed Warning</td>
</tr>
<tr>
<td>CWmin</td>
<td>Contention Window Minimum Size</td>
</tr>
<tr>
<td>dBm</td>
<td>Decibel-milliwatts</td>
</tr>
<tr>
<td>DARPA</td>
<td>Defense Advanced Research Projects Agency</td>
</tr>
<tr>
<td>DC</td>
<td>Direct Current</td>
</tr>
<tr>
<td>DSRC</td>
<td>Dedicated Short-Range Communication</td>
</tr>
<tr>
<td>EDCA</td>
<td>Enhanced Distributed Channel Access</td>
</tr>
<tr>
<td>EMI</td>
<td>Electromagnetic Interference</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>GHz</td>
<td>Gigahertz</td>
</tr>
<tr>
<td>GNSS</td>
<td>Global Navigation Satellite System</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronic Engineers</td>
</tr>
<tr>
<td>Immediate</td>
<td>Dynamic messages from ancillary devices connected to an RSU. An Example</td>
</tr>
<tr>
<td>Forward</td>
<td>would be SPaT. The RSU transmits Immediate Forward messages only when</td>
</tr>
<tr>
<td>Messages</td>
<td>the RSU receives them.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol version 6 (IPv6) is a protocol upgrade of for IPv4 (the current basis of the internet. IPv6 uses 128 bit addresses as opposed to the 32 bit IPv4 address. The basics of IPv6 are similar to those of IPv4 -- devices can use IPv6 as source and destination addresses to pass packets over a network, and tools like ping work for network testing as they do in IPv4, with some slight variations, however network appliance (switches, routers, firewalls, etc.) must specifically support IPv6.</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>ITS</td>
<td>Intelligent Transportation Systems</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LED</td>
<td>Light Emitting Diode</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MB</td>
<td>Megabyte</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>MHz</td>
<td>Megahertz</td>
</tr>
<tr>
<td>MPDUs</td>
<td>MAC Protocol Units</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time Between Failure</td>
</tr>
<tr>
<td>NEMA</td>
<td>National Electrical Manufacturers Association</td>
</tr>
<tr>
<td>NTCIP</td>
<td>National Transportation Communications for Intelligent Transportation System Protocol</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OID</td>
<td>Object Identifier (SNMP MIB OID)</td>
</tr>
<tr>
<td>OFDM</td>
<td>Orthogonal Frequency Division Multiplexing</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>PDU</td>
<td>Protocol Data Unit</td>
</tr>
<tr>
<td>PHY</td>
<td>Physical Layer, refers to a specific layer in the Open Systems Interconnection (OSI) reference model</td>
</tr>
<tr>
<td>PoE</td>
<td>Power-over-Ethernet</td>
</tr>
<tr>
<td>PSID</td>
<td>Provider Service Identifier</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
</tr>
<tr>
<td>Roadside Equipment</td>
<td>Traffic Management equipment installed along the roadside to convey traffic or traveler information to passing drivers or to connected said management equipment to a Traffic Management Center or other back office services and applications.</td>
</tr>
<tr>
<td>RSU</td>
<td>Roadside Unit</td>
</tr>
<tr>
<td>SAE</td>
<td>Society of Automotive Engineers</td>
</tr>
<tr>
<td>SCH</td>
<td>Service Channel</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SCMS</td>
<td>A Connected Vehicle Security Credential Management System (SCMS) provides DSRC devices with digital certificates that the devices use to sign (authenticate) and encrypt DSRC messages. The SCMS also revokes certificates, when warranted and provides a certificate revocation list (CRL) to remaining devices.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SPaT</td>
<td>Signal Phase and Timing</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>Store and Repeat Messages</td>
<td>Static messages that are loaded on RSUs for transmission to passing vehicles. An Example would be a Curve Speed Warning (CSW) Message that contains the geometry of the subject curve and an advised speed in which to traverse the curve. These messages are loaded as individual text files that contain the transmission strategy (how often the message is transmitted, what (DSRC) channel the messages is transmitted on, etc.) and the message payload.</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TMC</td>
<td>Traffic Management Center</td>
</tr>
<tr>
<td>TXOP</td>
<td>Transmission Opportunity Value</td>
</tr>
<tr>
<td>USDOT</td>
<td>United States Department of Transportation</td>
</tr>
<tr>
<td>UTC</td>
<td>Universal Time, Coordinated</td>
</tr>
<tr>
<td>V2I</td>
<td>Vehicle-to-Infrastructure</td>
</tr>
<tr>
<td>V2V</td>
<td>Vehicle-to-Vehicle</td>
</tr>
<tr>
<td>VSC3</td>
<td>Vehicle Safety Communications 3 (Consortium)</td>
</tr>
<tr>
<td>WAAS</td>
<td>Wide Area Augmentation System</td>
</tr>
<tr>
<td>WAVE</td>
<td>Wireless Access in Vehicular Environments</td>
</tr>
<tr>
<td>WiMAX</td>
<td>Worldwide Interoperability for Microwave Access</td>
</tr>
<tr>
<td>WSA</td>
<td>WAVE Service Announcement</td>
</tr>
<tr>
<td>WSM</td>
<td>WAVE Short Message</td>
</tr>
<tr>
<td>WSMP</td>
<td>WAVE Short Message Protocol</td>
</tr>
</tbody>
</table>
Appendix B. SNMPv3 Management Information Base

B.1. RSU Specific MIB Objects

This section contains the RSU specific MIB OIDs

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 "201702200000Z"
   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 "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 "2x"
   STATUS current
   DESCRIPTION "PSID associated with a DSRC message."
SYNTAX OCTET STRING (SIZE(1..2))

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..1500))
MAX-ACCESS   read-create
STATUS       current
DESCRIPTION
"Payload of Store and Repeat message.
Length limit derived from UDP size limit."
::= { 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
Appendix B. SNMPv3 Management Information Base

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 }
Appendix B. SNMPv3 Management Information Base

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 Strength 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
Appendix B. SNMPv3 Management Information Base

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."
Appendix B. SNMPv3 Management Information Base

::= { 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 }

rsuInterfaceLogByDir 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 }

rsuInterfaceName 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
"Provides 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
Appendix B. SNMPv3 Management Information Base

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 (4))
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"
Appendix B. SNMPv3 Management Information Base

::= { 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."
Appendix B. SNMPv3 Management Information Base

::= { 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."
Appendix B. SNMPv3 Management Information Base

::= { 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 }

U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems Joint Program Office

Dedicated Short Range Communications Roadside Unit Specifications
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 requests 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
Appendix B. SNMPv3 Management Information Base

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
B.2. General MIB Objects

This section contains a list of MIB Objects for a typical Linux device. The RSU is expected to, at a minimum, support these or similar Objects with corresponding Object Identifiers.

sysDescr OBJECT-TYPE 1.3.6.1.2.1.1.1
sysObjectID OBJECT-TYPE 1.3.6.1.2.1.1.2
sysUpTime OBJECT-TYPE 1.3.6.1.2.1.1.3
sysContact OBJECT-TYPE 1.3.6.1.2.1.1.4
sysName OBJECT-TYPE 1.3.6.1.2.1.1.5
sysLocation OBJECT-TYPE 1.3.6.1.2.1.1.6
sysServices OBJECT-TYPE 1.3.6.1.2.1.1.7
ifNumber OBJECT-TYPE 1.3.6.1.2.1.2.1
ifTable OBJECT-TYPE 1.3.6.1.2.1.2.2
ifEntry OBJECT-TYPE 1.3.6.1.2.1.2.2.1
ifIndex OBJECT-TYPE 1.3.6.1.2.1.2.2.1.1
ifDescr OBJECT-TYPE 1.3.6.1.2.1.2.2.1.2
ifType OBJECT-TYPE 1.3.6.1.2.1.2.2.1.3
ifMtu OBJECT-TYPE 1.3.6.1.2.1.2.2.1.4
ifSpeed OBJECT-TYPE 1.3.6.1.2.1.2.2.1.5
ifPhysAddress OBJECT-TYPE 1.3.6.1.2.1.2.2.1.6
ifAdminStatus OBJECT-TYPE 1.3.6.1.2.1.2.2.1.7
ifOperStatus OBJECT-TYPE 1.3.6.1.2.1.2.2.1.8
ifLastChange OBJECT-TYPE 1.3.6.1.2.1.2.2.1.9
ifInOctets OBJECT-TYPE 1.3.6.1.2.1.2.2.1.10
ifInUcastPkts OBJECT-TYPE 1.3.6.1.2.1.2.2.1.11
ifInNUcastPkts OBJECT-TYPE 1.3.6.1.2.1.2.2.1.12
ifInDiscards OBJECT-TYPE 1.3.6.1.2.1.2.2.1.13
ifInErrors OBJECT-TYPE 1.3.6.1.2.1.2.2.1.14
ifInUnknownProtos OBJECT-TYPE 1.3.6.1.2.1.2.2.1.15
ifOutOctets OBJECT-TYPE 1.3.6.1.2.1.2.2.1.16
ifOutUcastPkts OBJECT-TYPE 1.3.6.1.2.1.2.2.1.17
ifOutNUcastPkts OBJECT-TYPE 1.3.6.1.2.1.2.2.1.18
ifOutDiscards OBJECT-TYPE 1.3.6.1.2.1.2.2.1.19
ifOutErrors OBJECT-TYPE 1.3.6.1.2.1.2.2.1.20
ifOutQLen OBJECT-TYPE 1.3.6.1.2.1.2.2.1.21
ifSpecific OBJECT-TYPE 1.3.6.1.2.1.2.2.1.22
atTable OBJECT-TYPE 1.3.6.1.2.1.3.1
atEntry OBJECT-TYPE 1.3.6.1.2.1.3.1.1
atIfIndex OBJECT-TYPE 1.3.6.1.2.1.3.1.1.1
atPhysAddress OBJECT-TYPE 1.3.6.1.2.1.3.1.1.2
### Appendix B. SNMPv3 Management Information Base

The table below lists some of the SNMPv3 Management Information Base (MIB) objects and their corresponding Object Identifiers (OIDs).

<table>
<thead>
<tr>
<th>Object Name</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>atNetAddress</td>
<td>1.3.6.1.2.1.3.1.1.3</td>
</tr>
<tr>
<td>ipForwarding</td>
<td>1.3.6.1.2.1.4.1</td>
</tr>
<tr>
<td>ipDefaultTTL</td>
<td>1.3.6.1.2.1.4.2</td>
</tr>
<tr>
<td>ipInReceives</td>
<td>1.3.6.1.2.1.4.3</td>
</tr>
<tr>
<td>ipInHdrErrors</td>
<td>1.3.6.1.2.1.4.4</td>
</tr>
<tr>
<td>ipInAddrErrors</td>
<td>1.3.6.1.2.1.4.5</td>
</tr>
<tr>
<td>ipFwdDatagrams</td>
<td>1.3.6.1.2.1.4.6</td>
</tr>
<tr>
<td>ipInUnknownProtos</td>
<td>1.3.6.1.2.1.4.7</td>
</tr>
<tr>
<td>ipInDiscards</td>
<td>1.3.6.1.2.1.4.8</td>
</tr>
<tr>
<td>ipInDelivers</td>
<td>1.3.6.1.2.1.4.9</td>
</tr>
<tr>
<td>ipOutRequests</td>
<td>1.3.6.1.2.1.4.10</td>
</tr>
<tr>
<td>ipOutDiscards</td>
<td>1.3.6.1.2.1.4.11</td>
</tr>
<tr>
<td>ipOutNoRoutes</td>
<td>1.3.6.1.2.1.4.12</td>
</tr>
<tr>
<td>ipReasmTimeout</td>
<td>1.3.6.1.2.1.4.13</td>
</tr>
<tr>
<td>ipReasmReqs</td>
<td>1.3.6.1.2.1.4.14</td>
</tr>
<tr>
<td>ipReasmOKs</td>
<td>1.3.6.1.2.1.4.15</td>
</tr>
<tr>
<td>ipReasmFails</td>
<td>1.3.6.1.2.1.4.16</td>
</tr>
<tr>
<td>ipFragOKs</td>
<td>1.3.6.1.2.1.4.18</td>
</tr>
<tr>
<td>ipFragFails</td>
<td>1.3.6.1.2.1.4.18</td>
</tr>
<tr>
<td>ipFragCreates</td>
<td>1.3.6.1.2.1.4.19</td>
</tr>
<tr>
<td>ipAddrTable</td>
<td>1.3.6.1.2.1.4.20</td>
</tr>
<tr>
<td>ipAddrEntry</td>
<td>1.3.6.1.2.1.4.20.1</td>
</tr>
<tr>
<td>ipAdEntAddr</td>
<td>1.3.6.1.2.1.4.20.1.1</td>
</tr>
<tr>
<td>ipAdEntIfIndex</td>
<td>1.3.6.1.2.1.4.20.1.2</td>
</tr>
<tr>
<td>ipAdEntNetMask</td>
<td>1.3.6.1.2.1.4.20.1.3</td>
</tr>
<tr>
<td>ipAdEntBcastAddr</td>
<td>1.3.6.1.2.1.4.20.1.4</td>
</tr>
<tr>
<td>ipAdEntReasmMaxSize</td>
<td>1.3.6.1.2.1.4.20.1.5</td>
</tr>
<tr>
<td>ipRouteTable</td>
<td>1.3.6.1.2.1.4.21</td>
</tr>
<tr>
<td>ipRouteDest</td>
<td>1.3.6.1.2.1.4.21.1</td>
</tr>
<tr>
<td>ipRouteEntry</td>
<td>1.3.6.1.2.1.4.21.1.1</td>
</tr>
<tr>
<td>ipRouteIfIndex</td>
<td>1.3.6.1.2.1.4.21.1.2</td>
</tr>
<tr>
<td>ipRouteMetric1</td>
<td>1.3.6.1.2.1.4.21.1.3</td>
</tr>
<tr>
<td>ipRouteMetric2</td>
<td>1.3.6.1.2.1.4.21.1.4</td>
</tr>
<tr>
<td>ipRouteMetric3</td>
<td>1.3.6.1.2.1.4.21.1.5</td>
</tr>
<tr>
<td>ipRouteMetric4</td>
<td>1.3.6.1.2.1.4.21.1.6</td>
</tr>
<tr>
<td>ipRouteNextHop</td>
<td>1.3.6.1.2.1.4.21.1.7</td>
</tr>
<tr>
<td>ipRouteType</td>
<td>1.3.6.1.2.1.4.21.1.8</td>
</tr>
<tr>
<td>ipRouteProto</td>
<td>1.3.6.1.2.1.4.21.1.9</td>
</tr>
<tr>
<td>ipRouteAge</td>
<td>1.3.6.1.2.1.4.21.1.10</td>
</tr>
<tr>
<td>ipRouteMask</td>
<td>1.3.6.1.2.1.4.21.1.11</td>
</tr>
<tr>
<td>ipRouteMetric5</td>
<td>1.3.6.1.2.1.4.21.1.12</td>
</tr>
</tbody>
</table>
Appendix B. SNMPv3 Management Information Base

U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems Joint Program Office

Dedicated Short Range Communications Roadside Unit Specifications

<table>
<thead>
<tr>
<th>OBJECT-ATYPE</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipRouteInfo OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.4.21.1.13</td>
</tr>
<tr>
<td>ipNetToMediaTable OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.4.22</td>
</tr>
<tr>
<td>ipNetToMediaEntry OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.4.22.1</td>
</tr>
<tr>
<td>ipNetToMediaType OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.4.22.1.1</td>
</tr>
<tr>
<td>ipNetToMediaPhysAddress OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.4.22.1.2</td>
</tr>
<tr>
<td>ipNetToMediaNetAddress OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.4.22.1.3</td>
</tr>
<tr>
<td>ipNetToMediaType OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.4.22.1.4</td>
</tr>
<tr>
<td>ipRoutingDiscards OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.4.23</td>
</tr>
<tr>
<td>icmpInMsgs OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.1</td>
</tr>
<tr>
<td>icmpInErrors OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.2</td>
</tr>
<tr>
<td>icmpInDestUnreachs OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.3</td>
</tr>
<tr>
<td>icmpInTimeExcds OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.4</td>
</tr>
<tr>
<td>icmpInParmProbs OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.5</td>
</tr>
<tr>
<td>icmpInSrcQuenchs OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.6</td>
</tr>
<tr>
<td>icmpInRedirects OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.7</td>
</tr>
<tr>
<td>icmpInEchos OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.8</td>
</tr>
<tr>
<td>icmpInEchoReps OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.9</td>
</tr>
<tr>
<td>icmpInTimestamps OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.10</td>
</tr>
<tr>
<td>icmpInTimestampReps OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.11</td>
</tr>
<tr>
<td>icmpInAddrMasks OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.12</td>
</tr>
<tr>
<td>icmpInAddrMaskReps OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.13</td>
</tr>
<tr>
<td>icmpOutMsgs OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.14</td>
</tr>
<tr>
<td>icmpOutErrors OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.15</td>
</tr>
<tr>
<td>icmpOutDestUnreachs OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.16</td>
</tr>
<tr>
<td>icmpOutTimeExcds OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.17</td>
</tr>
<tr>
<td>icmpOutParmProbs OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.18</td>
</tr>
<tr>
<td>icmpOutSrcQuenchs OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.19</td>
</tr>
<tr>
<td>icmpOutRedirects OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.20</td>
</tr>
<tr>
<td>icmpOutEchos OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.21</td>
</tr>
<tr>
<td>icmpOutEchoReps OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.22</td>
</tr>
<tr>
<td>icmpOutTimestamps OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.23</td>
</tr>
<tr>
<td>icmpOutTimestampReps OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.24</td>
</tr>
<tr>
<td>icmpOutAddrMasks OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.25</td>
</tr>
<tr>
<td>icmpOutAddrMaskReps OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.5.26</td>
</tr>
<tr>
<td>tcpRtoAlgorithm OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.6.1</td>
</tr>
<tr>
<td>tcpRtoMin OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.6.2</td>
</tr>
<tr>
<td>tcpRtoMax OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.6.3</td>
</tr>
<tr>
<td>tcpMaxConn OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.6.4</td>
</tr>
<tr>
<td>tcpActiveOpens OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.6.5</td>
</tr>
<tr>
<td>tcpPassiveOpens OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.6.6</td>
</tr>
<tr>
<td>tcpAttemptFails OBJECT-ATYPE</td>
<td>1.3.6.1.2.1.6.7</td>
</tr>
</tbody>
</table>
Appendix B. SNMPv3 Management Information Base

<table>
<thead>
<tr>
<th>OBJECT-TYPE</th>
<th>OBJECT IDENTIFIER</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcpEstabResets</td>
<td>1.3.6.1.2.1.6.8</td>
</tr>
<tr>
<td>tcpCurrEstab</td>
<td>1.3.6.1.2.1.6.9</td>
</tr>
<tr>
<td>tcpInSegs</td>
<td>1.3.6.1.2.1.6.10</td>
</tr>
<tr>
<td>tcpOutSegs</td>
<td>1.3.6.1.2.1.6.11</td>
</tr>
<tr>
<td>tcpRetransSegs</td>
<td>1.3.6.1.2.1.6.12</td>
</tr>
<tr>
<td>the TCP Connection table</td>
<td>1.3.6.1.2.1.6.13</td>
</tr>
<tr>
<td>tcpConnEntry</td>
<td>1.3.6.1.2.1.6.13.1</td>
</tr>
<tr>
<td>tcpConnState</td>
<td>1.3.6.1.2.1.6.13.1.1</td>
</tr>
<tr>
<td>tcpConnLocalAddress</td>
<td>1.3.6.1.2.1.6.13.1.2</td>
</tr>
<tr>
<td>tcpConnLocalPort</td>
<td>1.3.6.1.2.1.6.13.1.3</td>
</tr>
<tr>
<td>tcpConnRemAddress</td>
<td>1.3.6.1.2.1.6.13.1.4</td>
</tr>
<tr>
<td>tcpConnRemPort</td>
<td>1.3.6.1.2.1.6.13.1.5</td>
</tr>
<tr>
<td>tcpInErrs</td>
<td>1.3.6.1.2.1.6.14</td>
</tr>
<tr>
<td>tcpOutRsts</td>
<td>1.3.6.1.2.1.6.15</td>
</tr>
<tr>
<td>udpInDatagrams</td>
<td>1.3.6.1.2.1.6.16</td>
</tr>
<tr>
<td>udpNoPorts</td>
<td>1.3.6.1.2.1.6.16.1</td>
</tr>
<tr>
<td>udpInErrors</td>
<td>1.3.6.1.2.1.6.16.3</td>
</tr>
<tr>
<td>udpOutDatagrams</td>
<td>1.3.6.1.2.1.6.16.4</td>
</tr>
<tr>
<td>udpTable</td>
<td>1.3.6.1.2.1.6.16.5</td>
</tr>
<tr>
<td>udpEntry</td>
<td>1.3.6.1.2.1.6.16.6</td>
</tr>
<tr>
<td>udpLocalAddress</td>
<td>1.3.6.1.2.1.6.16.7</td>
</tr>
<tr>
<td>udpLocalPort</td>
<td>1.3.6.1.2.1.6.16.8</td>
</tr>
<tr>
<td>egpInMsgs</td>
<td>1.3.6.1.2.1.6.17</td>
</tr>
<tr>
<td>egpInErrors</td>
<td>1.3.6.1.2.1.6.17.1</td>
</tr>
<tr>
<td>egpOutMsgs</td>
<td>1.3.6.1.2.1.6.17.2</td>
</tr>
<tr>
<td>egpOutErrors</td>
<td>1.3.6.1.2.1.6.17.3</td>
</tr>
<tr>
<td>egpNeighTable</td>
<td>1.3.6.1.2.1.6.17.4</td>
</tr>
<tr>
<td>egpNeighEntry</td>
<td>1.3.6.1.2.1.6.17.5</td>
</tr>
<tr>
<td>egpNeighAddr</td>
<td>1.3.6.1.2.1.6.17.6</td>
</tr>
<tr>
<td>egpNeighAs</td>
<td>1.3.6.1.2.1.6.17.7</td>
</tr>
<tr>
<td>egpNeighInMsgs</td>
<td>1.3.6.1.2.1.6.17.8</td>
</tr>
<tr>
<td>egpNeighInErrs</td>
<td>1.3.6.1.2.1.6.17.9</td>
</tr>
<tr>
<td>egpNeighOutMsgs</td>
<td>1.3.6.1.2.1.6.17.10</td>
</tr>
<tr>
<td>egpNeighOutErrs</td>
<td>1.3.6.1.2.1.6.17.11</td>
</tr>
<tr>
<td>egpNeighIntervalHello</td>
<td>1.3.6.1.2.1.6.17.12</td>
</tr>
<tr>
<td>egpNeighIntervalPoll</td>
<td>1.3.6.1.2.1.6.17.13</td>
</tr>
</tbody>
</table>
Appendix B. SNMPv3 Management Information Base

egpNeighMode OBJECT-TYPE 1.3.6.1.2.1.8.5.1.14
egpNeighEventTrigger OBJECT-TYPE 1.3.6.1.2.1.8.5.1.15
egpAs OBJECT-TYPE 1.3.6.1.2.1.8.6
the Transmission group 1.3.6.1.2.1.10
the SNMP group 1.3.6.1.2.1.11
snmpInPkts OBJECT-TYPE 1.3.6.1.2.1.11.1
snmpOutPkts OBJECT-TYPE 1.3.6.1.2.1.11.2
snmpInBadVersions OBJECT-TYPE 1.3.6.1.2.1.11.3
snmpInBadCommunityNames OBJECT-TYPE 1.3.6.1.2.1.11.4
snmpInBadCommunityUses OBJECT-TYPE 1.3.6.1.2.1.11.5
snmpInASNParseErrs OBJECT-TYPE 1.3.6.1.2.1.11.6
snmpInTooBigs OBJECT-TYPE 1.3.6.1.2.1.11.8
snmpInNoSuchNames OBJECT-TYPE 1.3.6.1.2.1.11.9
snmpInBadValues OBJECT-TYPE 1.3.6.1.2.1.11.10
snmpInReadOnlys OBJECT-TYPE 1.3.6.1.2.1.11.11
snmpInGenErrs OBJECT-TYPE 1.3.6.1.2.1.11.12
snmpInTotalReqVars OBJECT-TYPE 1.3.6.1.2.1.11.13
snmpInTotalSetVars OBJECT-TYPE 1.3.6.1.2.1.11.14
snmpInGetRequests OBJECT-TYPE 1.3.6.1.2.1.11.15
snmpInGetNexts OBJECT-TYPE 1.3.6.1.2.1.11.16
snmpInSetRequests OBJECT-TYPE 1.3.6.1.2.1.11.17
snmpInGetResponses OBJECT-TYPE 1.3.6.1.2.1.11.18
snmpInTraps OBJECT-TYPE 1.3.6.1.2.1.11.19
snmpOutTooBigs OBJECT-TYPE 1.3.6.1.2.1.11.20
snmpOutNoSuchNames OBJECT-TYPE 1.3.6.1.2.1.11.21
snmpOutBadValues OBJECT-TYPE 1.3.6.1.2.1.11.22
snmpOutGenErrs OBJECT-TYPE 1.3.6.1.2.1.11.24
snmpOutGetRequests OBJECT-TYPE 1.3.6.1.2.1.11.25
snmpOutGetNexts OBJECT-TYPE 1.3.6.1.2.1.11.26
snmpOutSetRequests OBJECT-TYPE 1.3.6.1.2.1.11.27
snmpOutGetResponses OBJECT-TYPE 1.3.6.1.2.1.11.28
snmpOutTraps OBJECT-TYPE 1.3.6.1.2.1.11.29
snmpEnableAuthenTraps OBJECT-TYPE 1.3.6.1.2.1.11.30

B.3. IPv6 MIB Objects

This section contains a list of IPv6 MIB Objects for a typical Linux device. The RSU is expected to, at a minimum, support these, or similar Objects with corresponding Object Identities.

ipv6Forwarding OBJECT-TYPE 1.3.6.1.2.1.55.1.1.0
Appendix B. SNMPv3 Management Information Base

ipv6DefaultHopLimit OBJECT-TYPE  1.3.6.1.2.1.55.1.2.0
ipv6Interfaces OBJECT-TYPE  1.3.6.1.2.1.55.1.3.0
ipv6IfTableLastChange OBJECT-TYPE  1.3.6.1.2.1.55.1.4.0
ipv6IfTable OBJECT-TYPE  1.3.6.1.2.1.55.1.5
ipv6IfEntry OBJECT-TYPE  1.3.6.1.2.1.55.1.5.1
ipv6IfIndex OBJECT-TYPE  1.3.6.1.2.1.55.1.5.1.1
ipv6IfDescr OBJECT-TYPE  1.3.6.1.2.1.55.1.5.1.2
ipv6IfLowerLayer OBJECT-TYPE  1.3.6.1.2.1.55.1.5.1.3
ipv6IfEffectiveMtu OBJECT-TYPE  1.3.6.1.2.1.55.1.5.1.4
ipv6IfReasmMaxSize OBJECT-TYPE  1.3.6.1.2.1.55.1.5.1.5
ipv6IfIdentifier OBJECT-TYPE  1.3.6.1.2.1.55.1.5.1.6
ipv6IfIdentifierLength OBJECT-TYPE  1.3.6.1.2.1.55.1.5.1.7
ipv6IfPhysicalAddress OBJECT-TYPE  1.3.6.1.2.1.55.1.5.1.8
ipv6IfAdminStatus OBJECT-TYPE  1.3.6.1.2.1.55.1.5.1.9
ipv6IfOperStatus OBJECT-TYPE  1.3.6.1.2.1.55.1.5.1.10
ipv6IfLastChange OBJECT-TYPE  1.3.6.1.2.1.55.1.5.1.11
ipv6IfStatsTable OBJECT-TYPE  1.3.6.1.2.1.55.1.6
ipv6IfStatsEntry OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1
ipv6IfStatsInReceives OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.1
ipv6IfStatsInHdrErrors OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.2
ipv6IfStatsInTooBigErrors OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.3
ipv6IfStatsInNoRoutes OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.4
ipv6IfStatsInAddrErrors OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.5
ipv6IfStatsInUnknownProtos OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.6
ipv6IfStatsInTruncatedPkts OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.7
ipv6IfStatsInDiscards OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.8
ipv6IfStatsInDelivers OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.9
ipv6IfStatsOutForwDatagrams OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.10
ipv6IfStatsOutRequests OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.11
ipv6IfStatsOutDiscards OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.12
ipv6IfStatsOutFragOKs OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.13
ipv6IfStatsOutFragFails OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.14
ipv6IfStatsOutFragCreates OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.15
ipv6IfStatsReasmReqs OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.16
ipv6IfStatsReasmOKs OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.17
ipv6IfStatsReasmFails OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.18
ipv6IfStatsInMcastPkts OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.19
ipv6IfStatsOutMcastPkts OBJECT-TYPE  1.3.6.1.2.1.55.1.6.1.20
ipv6AddrPrefixTable OBJECT-TYPE  1.3.6.1.2.1.55.1.7.0.0
ipv6AddrPrefixEntry OBJECT-TYPE  1.3.6.1.2.1.55.1.7.1
ipv6AddrPrefix OBJECT-TYPE  1.3.6.1.2.1.55.1.7.1.1
Appendix B. SNMPv3 Management Information Base

ipv6AddrPrefixLength OBJECT-TYPE 1.3.6.1.2.1.55.1.7.1.2
ipv6AddrPrefixOnLinkFlag OBJECT-TYPE 1.3.6.1.2.1.55.1.7.1.3
ipv6AddrPrefixAutonomousFlag OBJECT-TYPE 1.3.6.1.2.1.55.1.7.1.4
ipv6AddrPrefixAdvPreferredLifetime OBJECT-TYPE 1.3.6.1.2.1.55.1.7.1.5
ipv6AddrPrefixAdvValidLifetime OBJECT-TYPE 1.3.6.1.2.1.55.1.7.1.6
ipv6AddrTable OBJECT-TYPE 1.3.6.1.2.1.55.1.8
ipv6AddrEntry OBJECT-TYPE 1.3.6.1.2.1.55.1.8.1
ipv6AddrAddress OBJECT 1.3.6.1.2.1.55.1.8.1.1
ipv6AddrPfxLength OBJECT-TYPE 1.3.6.1.2.1.55.1.8.1.2
ipv6AddrType OBJECT-TYPE 1.3.6.1.2.1.55.1.8.1.3
ipv6AddrAnycastFlag OBJECT-TYPE 1.3.6.1.2.1.55.1.8.1.4
ipv6AddrStatus OBJECT-TYPE 1.3.6.1.2.1.55.1.8.1.5
ipv6RouteNumber OBJECT-TYPE 1.3.6.1.2.1.55.1.9.0
ipv6DiscardedRoutes OBJECT-TYPE 1.3.6.1.2.1.55.1.10.0
ipv6RouteTable OBJECT-TYPE 1.3.6.1.2.1.55.1.11.0
ipv6RouteEntry OBJECT-TYPE 1.3.6.1.2.1.55.1.11.1.0
ipv6RouteDest OBJECT-TYPE 1.3.6.1.2.1.55.1.11.1.1
ipv6RoutePfxLength OBJECT-TYPE 1.3.6.1.2.1.55.1.11.1.2
ipv6RouteIfIndex OBJECT-TYPE 1.3.6.1.2.1.55.1.11.1.3
ipv6RouteIfIndex OBJECT-TYPE 1.3.6.1.2.1.55.1.11.1.4
ipv6RouteNextHop OBJECT-TYPE 1.3.6.1.2.1.55.1.11.1.5
ipv6RouteType OBJECT-TYPE 1.3.6.1.2.1.55.1.11.1.6
ipv6RouteProtocol OBJECT-TYPE 1.3.6.1.2.1.55.1.11.1.7
ipv6RoutePolicy OBJECT-TYPE 1.3.6.1.2.1.55.1.11.1.8
ipv6RouteAge OBJECT-TYPE 1.3.6.1.2.1.55.1.11.1.9
ipv6RouteNextHopRDI OBJECT-TYPE 1.3.6.1.2.1.55.1.11.1.10
ipv6RouteMetric OBJECT-TYPE 1.3.6.1.2.1.55.1.11.1.11
ipv6RouteWeight OBJECT-TYPE 1.3.6.1.2.1.55.1.11.1.12
ipv6RouteInfo OBJECT-TYPE 1.3.6.1.2.1.55.1.11.1.13
ipv6RouteValid OBJECT-TYPE 1.3.6.1.2.1.55.1.11.1.14
ipv6NetToMediaTable OBJECT-TYPE 1.3.6.1.2.1.55.1.12.0
ipv6NetToMediaEntry OBJECT-TYPE 1.3.6.1.2.1.55.1.12.1.0
ipv6NetToMediaNetAddress OBJECT-TYPE 1.3.6.1.2.1.55.1.12.1.1
ipv6NetToMediaPhysAddress OBJECT-TYPE 1.3.6.1.2.1.55.1.12.1.2
ipv6NetToMediaType OBJECT-TYPE 1.3.6.1.2.1.55.1.12.1.3
ipv6IfNetToMediaState OBJECT-TYPE 1.3.6.1.2.1.55.1.12.1.4
ipv6IfNetToMediaLastUpdated OBJECT-TYPE 1.3.6.1.2.1.55.1.12.1.5
ipv6NetToMediaValid OBJECT-TYPE 1.3.6.1.2.1.55.1.12.1.6
ipv6Notifications OBJECT IDENTIFIER 1.3.6.1.2.1.55.2
ipv6NotificationPrefix OBJECT IDENTIFIER 1.3.6.1.2.1.55.2.0
ipv6IfStateChange NOTIFICATION-TYPE 1.3.6.1.2.1.55.2.0.1
ipv6Conformance OBJECT IDENTIFIER 1.3.6.1.2.1.55.3
ipv6Compliances OBJECT IDENTIFIER 1.3.6.1.2.1.55.3.1
ipv6Groups OBJECT IDENTIFIER 1.3.6.1.2.1.55.3.2
ipv6Compliance MODULE-COMPLIANCE 1.3.6.1.2.1.55.3.2.1
### B.4. RSU Specific MIB Object Map

This section contains a mapping of the RSU specific MIB OIDs from section 0 above.

<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
<th>Max-Access</th>
<th>Syntax</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous MAC Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuContMacAddress</td>
<td>1.1</td>
<td>read-only</td>
<td>MacAddress</td>
<td></td>
</tr>
<tr>
<td>Alternating Mac Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuAltMacAddress</td>
<td>1.2</td>
<td>read-only</td>
<td>MacAddress</td>
<td></td>
</tr>
<tr>
<td>GPS Status</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuGPSStatus</td>
<td>1.3</td>
<td>read-only</td>
<td>Integer32</td>
<td>0..15</td>
</tr>
<tr>
<td>Store and Repeat</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuSRMStatusTable</td>
<td>1.4</td>
<td>not-accessible</td>
<td>SEQUENCE OF</td>
<td></td>
</tr>
<tr>
<td>rsuSRMStatusEntry</td>
<td>1.4.1</td>
<td>not-accessible</td>
<td>RsuSRMStatusEntry</td>
<td></td>
</tr>
<tr>
<td>rsuSRMIndex</td>
<td>1.4.1.1</td>
<td>not-accessible</td>
<td>RsuTableIndex</td>
<td></td>
</tr>
<tr>
<td>rsuSRMPsid</td>
<td>1.4.1.2</td>
<td>read-create</td>
<td>RsuPsidTC</td>
<td></td>
</tr>
<tr>
<td>rsuSRMDsrcMsgId</td>
<td>1.4.1.3</td>
<td>read-create</td>
<td>Integer32</td>
<td></td>
</tr>
<tr>
<td>rsuSRMTxMode</td>
<td>1.4.1.4</td>
<td>read-create</td>
<td>INTEGER</td>
<td>0</td>
</tr>
<tr>
<td>rsuSRMTxChannel</td>
<td>1.4.1.5</td>
<td>read-create</td>
<td>Integer32</td>
<td>172..184</td>
</tr>
<tr>
<td>rsuSRMTxInterval</td>
<td>1.4.1.6</td>
<td>read-create</td>
<td>Integer32</td>
<td>1..2147483647</td>
</tr>
<tr>
<td>rsuSRMDeliveryStart</td>
<td>1.4.1.7</td>
<td>read-create</td>
<td>OCTET STRING</td>
<td>SIZE(0</td>
</tr>
<tr>
<td>rsuSRMDeliveryStop</td>
<td>1.4.1.8</td>
<td>read-create</td>
<td>OCTET STRING</td>
<td>SIZE(0</td>
</tr>
<tr>
<td>rsuSRMPayload</td>
<td>1.4.1.9</td>
<td>read-create</td>
<td>OCTET STRING</td>
<td>SIZE(0..1500)</td>
</tr>
<tr>
<td>rsuSRMEnable</td>
<td>1.4.1.10</td>
<td>read-create</td>
<td>INTEGER</td>
<td>0</td>
</tr>
<tr>
<td>rsuSRMStatus</td>
<td>1.4.1.11</td>
<td>read-create</td>
<td>RowStatus</td>
<td></td>
</tr>
<tr>
<td>Immediate Forward</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuIFMStatusTable</td>
<td>1.5</td>
<td>not-accessible</td>
<td>SEQUENCE OF</td>
<td></td>
</tr>
<tr>
<td>rsuIFMStatusEntry</td>
<td>1.5.1</td>
<td>not-accessible</td>
<td>RsuIFMStatusEntry</td>
<td></td>
</tr>
</tbody>
</table>
## Appendix B. SNMPv3 Management Information Base

<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
<th>Max-Access</th>
<th>Syntax</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsuIFMIndex</td>
<td>1.5.1.1</td>
<td>not-accessible</td>
<td>RsuTableIndex</td>
<td></td>
</tr>
<tr>
<td>rsuIFMPsid</td>
<td>1.5.1.2</td>
<td>read-create</td>
<td>RsuPsidTC</td>
<td></td>
</tr>
<tr>
<td>rsuIFMDsrcMsgId</td>
<td>1.5.1.3</td>
<td>read-create</td>
<td>Integer32</td>
<td></td>
</tr>
<tr>
<td>rsuIFMTxMode</td>
<td>1.5.1.4</td>
<td>read-create</td>
<td>INTEGER</td>
<td>0</td>
</tr>
<tr>
<td>rsuIFMTxChannel</td>
<td>1.5.1.5</td>
<td>read-create</td>
<td>Integer32</td>
<td>172..184</td>
</tr>
<tr>
<td>rsuIFMEnable</td>
<td>1.5.1.6</td>
<td>read-create</td>
<td>INTEGER</td>
<td>0</td>
</tr>
<tr>
<td>rsuIFMStatus</td>
<td>1.5.1.7</td>
<td>read-create</td>
<td>RowStatus</td>
<td></td>
</tr>
<tr>
<td>Device ID</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuSysObjectID</td>
<td>1.6</td>
<td>read-only</td>
<td>OBJECT IDENTIFIER</td>
<td></td>
</tr>
<tr>
<td>GPS Config</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuDsrcForwardTable</td>
<td>1.7</td>
<td>not-accessible</td>
<td>SEQUENCE OF</td>
<td></td>
</tr>
<tr>
<td>rsuDsrcForwardEntry</td>
<td>1.7.1</td>
<td>not-accessible</td>
<td>RsuDsrcForwardEntry</td>
<td></td>
</tr>
<tr>
<td>rsuDsrcForwardIndex</td>
<td>1.7.1.1</td>
<td>not-accessible</td>
<td>RsuTableIndex</td>
<td></td>
</tr>
<tr>
<td>rsuDsrcFwdPsid</td>
<td>1.7.1.2</td>
<td>read-create</td>
<td>RsuPsidTC</td>
<td></td>
</tr>
<tr>
<td>rsuDsrcFwdDestIPAddr</td>
<td>1.7.1.3</td>
<td>read-create</td>
<td>Ipv6Address</td>
<td></td>
</tr>
<tr>
<td>rsuDsrcFwdDestPort</td>
<td>1.7.1.4</td>
<td>read-create</td>
<td>Integer32</td>
<td>1024..65535</td>
</tr>
<tr>
<td>rsuDsrcFwdProtocol</td>
<td>1.7.1.5</td>
<td>read-create</td>
<td>INTEGER</td>
<td>1</td>
</tr>
<tr>
<td>rsuDsrcFwdRssi</td>
<td>1.7.1.6</td>
<td>read-create</td>
<td>Integer32</td>
<td>-100..-60</td>
</tr>
<tr>
<td>rsuDsrcFwdMsgInterval</td>
<td>1.7.1.7</td>
<td>read-create</td>
<td>Integer32</td>
<td>1..9</td>
</tr>
<tr>
<td>rsuDsrcFwdDeliveryStart</td>
<td>1.7.1.8</td>
<td>read-create</td>
<td>OCTET STRING</td>
<td>SIZE(0</td>
</tr>
<tr>
<td>rsuDsrcFwdDeliveryStop</td>
<td>1.7.1.9</td>
<td>read-create</td>
<td>OCTET STRING</td>
<td>SIZE(0</td>
</tr>
<tr>
<td>rsuDsrcFwdEnable</td>
<td>1.7.1.10</td>
<td>read-create</td>
<td>INTEGER</td>
<td>0</td>
</tr>
<tr>
<td>messageForwardingRowStatus</td>
<td>1.7.1.11</td>
<td>read-create</td>
<td>RowStatus</td>
<td></td>
</tr>
</tbody>
</table>

### U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems Joint Program Office

Dedicated Short Range Communications Roadside Unit Specifications
<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
<th>Max-Access</th>
<th>Syntax</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsuGpsOutputInterface</td>
<td>1.8.3</td>
<td>read-write</td>
<td>DisplayString</td>
<td></td>
</tr>
<tr>
<td>rsuGpsOutputInterval</td>
<td>1.8.4</td>
<td>read-write</td>
<td>Integer32</td>
<td>1..18000</td>
</tr>
<tr>
<td>rsuGpsOutputString</td>
<td>1.8.5</td>
<td>read-only</td>
<td>DisplayString</td>
<td>SIZE(0..100)</td>
</tr>
<tr>
<td>rsuGpsRefLat</td>
<td>1.8.6</td>
<td>read-write</td>
<td>Integer32</td>
<td>-9000000000..9000000000</td>
</tr>
<tr>
<td>rsuGpsRefLon</td>
<td>1.8.7</td>
<td>read-write</td>
<td>Integer32</td>
<td>-1800000000..18000000000</td>
</tr>
<tr>
<td>rsuGpsRefElv</td>
<td>1.8.8</td>
<td>read-write</td>
<td>Integer32</td>
<td>-100000..1000000</td>
</tr>
<tr>
<td>rsuGpsMaxDeviation</td>
<td>1.8.9</td>
<td>read-write</td>
<td>Integer32</td>
<td>1..2000000</td>
</tr>
<tr>
<td>Interface Logging Config</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuInterfaceLogTable</td>
<td>1.9</td>
<td>not-accessible</td>
<td>SEQUENCE OF</td>
<td></td>
</tr>
<tr>
<td>rsuInterfaceLogEntry</td>
<td>1.9.1</td>
<td>not-accessible</td>
<td>RsuInterfaceLogEntry</td>
<td></td>
</tr>
<tr>
<td>rsuIfaceLogIndex</td>
<td>1.9.1.1</td>
<td>not-accessible</td>
<td>RsuTableIndex</td>
<td></td>
</tr>
<tr>
<td>rsuIfaceGenerate</td>
<td>1.9.1.2</td>
<td>read-write</td>
<td>INTEGER</td>
<td>0</td>
</tr>
<tr>
<td>rsuIfaceMaxFileSize</td>
<td>1.9.1.3</td>
<td>read-write</td>
<td>Integer32</td>
<td>5..40</td>
</tr>
<tr>
<td>rsuIfaceMaxFileTime</td>
<td>1.9.1.4</td>
<td>read-write</td>
<td>Integer32</td>
<td>1..48</td>
</tr>
<tr>
<td>rsuIfaceLogByDir</td>
<td>1.9.1.5</td>
<td>read-write</td>
<td>INTEGER</td>
<td>0</td>
</tr>
<tr>
<td>rsuIfaceName</td>
<td>1.9.1.6</td>
<td>read-only</td>
<td>DisplayString</td>
<td></td>
</tr>
<tr>
<td>Cert requests</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuSecCredReq</td>
<td>1.10</td>
<td>read-write</td>
<td>OCTET STRING</td>
<td>SIZE(1)</td>
</tr>
<tr>
<td>1609.2 Config</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuSecCredAttachInterval</td>
<td>1.11</td>
<td>read-write</td>
<td>INTEGER</td>
<td>1..100</td>
</tr>
<tr>
<td>DSRC Interface Config</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuDsrcChannelModeTable</td>
<td>1.12</td>
<td>not-accessible</td>
<td>SEQUENCE OF</td>
<td></td>
</tr>
<tr>
<td>rsuDsrcChannelModeEntry</td>
<td>1.12.1</td>
<td>not-accessible</td>
<td>RsuDsrcChannelModeEntry</td>
<td></td>
</tr>
<tr>
<td>rsuDCMIndex</td>
<td>1.12.1.1</td>
<td>not-accessible</td>
<td>RsuTableIndex</td>
<td></td>
</tr>
<tr>
<td>rsuDCMRadio</td>
<td>1.12.1.2</td>
<td>read-only</td>
<td>DisplayString</td>
<td></td>
</tr>
<tr>
<td>rsuDCMMode</td>
<td>1.12.1.3</td>
<td>read-write</td>
<td>INTEGER</td>
<td>0</td>
</tr>
<tr>
<td>rsuDCMCCCH</td>
<td>1.12.1.4</td>
<td>read-write</td>
<td>Integer32</td>
<td>172..184</td>
</tr>
</tbody>
</table>
### Appendix B. SNMPv3 Management Information Base

<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
<th>Max-Access</th>
<th>Syntax</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsuDCMSCH</td>
<td>1.12.1.5</td>
<td>read-write</td>
<td>Integer32</td>
<td>172..184</td>
</tr>
<tr>
<td><strong>WSA Message Config</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuWsaServiceTable</td>
<td>1.13</td>
<td>not-accessible</td>
<td>SEQUENCE OF</td>
<td></td>
</tr>
<tr>
<td>rsuWsaServiceEntry</td>
<td>1.13.1</td>
<td>not-accessible</td>
<td>RsuWsaServiceEntry</td>
<td></td>
</tr>
<tr>
<td>rsuWsaIndex</td>
<td>1.13.1.1</td>
<td>not-accessible</td>
<td>RsuTableIndex</td>
<td></td>
</tr>
<tr>
<td>rsuWsaPsid</td>
<td>1.13.1.2</td>
<td>read-create</td>
<td>RsuPsidTC</td>
<td></td>
</tr>
<tr>
<td>rsuWsaPriority</td>
<td>1.13.1.3</td>
<td>read-create</td>
<td>INTEGER</td>
<td>0..63</td>
</tr>
<tr>
<td>rsuWsaProviderContext</td>
<td>1.13.1.4</td>
<td>read-create</td>
<td>DisplayString</td>
<td>SIZE(4)</td>
</tr>
<tr>
<td>rsuWsaIpPrefix</td>
<td>1.13.1.5</td>
<td>read-create</td>
<td>Ipv6Address</td>
<td></td>
</tr>
<tr>
<td>rsuWsaPort</td>
<td>1.13.1.6</td>
<td>read-create</td>
<td>Integer32</td>
<td>1024..65535</td>
</tr>
<tr>
<td>rsuWsaChannel</td>
<td>1.13.1.7</td>
<td>read-create</td>
<td>Integer32</td>
<td>172..184</td>
</tr>
<tr>
<td>rsuWsaStatus</td>
<td>1.13.1.8</td>
<td>read-create</td>
<td>RowStatus</td>
<td></td>
</tr>
<tr>
<td><strong>WRA Config</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuWraConfiguration</td>
<td>1.14</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuWralpPrefix</td>
<td>1.14.1</td>
<td>read-write</td>
<td>Ipv6Address</td>
<td></td>
</tr>
<tr>
<td>rsuWralpPrefixLength</td>
<td>1.14.2</td>
<td>read-write</td>
<td>OCTET STRING</td>
<td>SIZE(1)</td>
</tr>
<tr>
<td>rsuWraGateway</td>
<td>1.14.3</td>
<td>read-write</td>
<td>Ipv6Address</td>
<td></td>
</tr>
<tr>
<td>rsuWraPrimaryDns</td>
<td>1.14.4</td>
<td>read-write</td>
<td>Ipv6Address</td>
<td></td>
</tr>
<tr>
<td><strong>Message Statistics</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuMessageStats</td>
<td>1.15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuAltSchMsgSent</td>
<td>1.15.1</td>
<td>read-only</td>
<td>Counter32</td>
<td>0-2^32</td>
</tr>
<tr>
<td>rsuAltSchMsgRcvd</td>
<td>1.15.2</td>
<td>read-only</td>
<td>Counter32</td>
<td>0-2^32</td>
</tr>
<tr>
<td>rsuAltCchMsgSent</td>
<td>1.15.3</td>
<td>read-only</td>
<td>Counter32</td>
<td>0-2^32</td>
</tr>
<tr>
<td>rsuAltCchMsgRcvd</td>
<td>1.15.4</td>
<td>read-only</td>
<td>Counter32</td>
<td>0-2^32</td>
</tr>
<tr>
<td>rsuContSchMsgSent</td>
<td>1.15.5</td>
<td>read-only</td>
<td>Counter32</td>
<td>0-2^32</td>
</tr>
<tr>
<td>rsuContSchMsgRcvd</td>
<td>1.15.6</td>
<td>read-only</td>
<td>Counter32</td>
<td>0-2^32</td>
</tr>
<tr>
<td>rsuContCchMsgSent</td>
<td>1.15.7</td>
<td>read-only</td>
<td>Counter32</td>
<td>0-2^32</td>
</tr>
</tbody>
</table>
### Appendix B. SNMPv3 Management Information Base

<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
<th>Max-Access</th>
<th>Syntax</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsuContCchMsgRcvd</td>
<td>1.15.8</td>
<td>read-only</td>
<td>Counter32</td>
<td>0-2^32</td>
</tr>
<tr>
<td>rsuMessageCountsByPsidTable</td>
<td>1.15.9</td>
<td>not-accessible</td>
<td>SEQUENCE OF</td>
<td></td>
</tr>
<tr>
<td>rsuMessageCountsByPsidEntry</td>
<td>1.15.9.1</td>
<td>not-accessible</td>
<td>RsuMessageCountsByPsidEntry</td>
<td></td>
</tr>
<tr>
<td>rsuMessageCountsByPsidIndex</td>
<td>1.15.9.1.1</td>
<td>not-accessible</td>
<td>RsuTableIndex</td>
<td></td>
</tr>
<tr>
<td>rsuMessageCountsByPsidId</td>
<td>1.15.9.1.2</td>
<td>read-create</td>
<td>RsuPsidTC</td>
<td></td>
</tr>
<tr>
<td>rsuMessageCountsByPsidCounts</td>
<td>1.15.9.1.3</td>
<td>read-create</td>
<td>Counter32</td>
<td>0-2^32</td>
</tr>
<tr>
<td>rsuMessageCountsByPsidRowStatus</td>
<td>1.15.9.1.4</td>
<td>read-create</td>
<td>RowStatus</td>
<td></td>
</tr>
<tr>
<td><strong>System Statistics</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuSystemStats</td>
<td>1.16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuTimeSincePowerOn</td>
<td>1.16.1</td>
<td>read-only</td>
<td>Counter32</td>
<td>0-2^32 sec</td>
</tr>
<tr>
<td>rsuTotalRunTime</td>
<td>1.16.2</td>
<td>read-only</td>
<td>Counter32</td>
<td>0-2^32 sec</td>
</tr>
<tr>
<td>rsuLastLoginTime</td>
<td>1.16.3</td>
<td>read-only</td>
<td>DateAndTime</td>
<td></td>
</tr>
<tr>
<td>rsuLastLoginUser</td>
<td>1.16.4</td>
<td>read-only</td>
<td>DisplayString</td>
<td>SIZE(0..32)</td>
</tr>
<tr>
<td>rsuLastLoginSource</td>
<td>1.16.5</td>
<td>read-only</td>
<td>DisplayString</td>
<td>SIZE(0..32)</td>
</tr>
<tr>
<td>rsuLastRestartTime</td>
<td>1.16.6</td>
<td>read-only</td>
<td>DateAndTime</td>
<td></td>
</tr>
<tr>
<td>rsuIntTemp</td>
<td>1.16.7</td>
<td>read-only</td>
<td>Integer32</td>
<td>-100..100</td>
</tr>
<tr>
<td><strong>System Description</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuSysDescription</td>
<td>1.17</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuMibVersion</td>
<td>1.17.1</td>
<td>read-only</td>
<td>DisplayString</td>
<td>SIZE(0..32)</td>
</tr>
<tr>
<td>rsuFirmwareVersion</td>
<td>1.17.2</td>
<td>read-only</td>
<td>DisplayString</td>
<td>SIZE(0..32)</td>
</tr>
<tr>
<td>rsuLocationDesc</td>
<td>1.17.3</td>
<td>read-write</td>
<td>DisplayString</td>
<td>SIZE(0..140)</td>
</tr>
<tr>
<td>rsuid</td>
<td>1.17.4</td>
<td>read-write</td>
<td>DisplayString</td>
<td>SIZE(0..32)</td>
</tr>
<tr>
<td>rsuManufacturer</td>
<td>1.17.5</td>
<td>read-only</td>
<td>DisplayString</td>
<td>SIZE(0..32)</td>
</tr>
<tr>
<td><strong>System Settings</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuSysSettings</td>
<td>1.18</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuTxPower</td>
<td>1.18.1</td>
<td>read-write</td>
<td>Integer32</td>
<td>0..100</td>
</tr>
<tr>
<td>rsuNotifyIpAddress</td>
<td>1.18.2</td>
<td>read-write</td>
<td>Ipv6Address</td>
<td></td>
</tr>
</tbody>
</table>
### Appendix B. SNMPv3 Management Information Base

<table>
<thead>
<tr>
<th>Name</th>
<th>OID 15628.4.x</th>
<th>Max-Access</th>
<th>Syntax</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsuNotifyPort</td>
<td>1.18.3</td>
<td>read-write</td>
<td>Integer32</td>
<td>0..65535</td>
</tr>
<tr>
<td>rsuSysLogCloseDay</td>
<td>1.18.4</td>
<td>read-write</td>
<td>INTEGER</td>
<td>1..7</td>
</tr>
<tr>
<td>rsuSysLogCloseTime</td>
<td>1.18.5</td>
<td>read-write</td>
<td>OCTET STRING</td>
<td>SIZE(3)</td>
</tr>
<tr>
<td>rsuSysLogDeleteDay</td>
<td>1.18.6</td>
<td>read-write</td>
<td>INTEGER</td>
<td>1..7</td>
</tr>
<tr>
<td>rsuSysLogDeleteAge</td>
<td>1.18.7</td>
<td>read-write</td>
<td>Integer32</td>
<td></td>
</tr>
</tbody>
</table>

**System Status**

<table>
<thead>
<tr>
<th>Name</th>
<th>OID 1.19.1</th>
<th>Max-Access</th>
<th>Syntax</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsuChanStatus</td>
<td></td>
<td>read-only</td>
<td>INTEGER</td>
<td>0..3</td>
</tr>
</tbody>
</table>

**Situation Data**

<table>
<thead>
<tr>
<th>Name</th>
<th>OID 1.20</th>
<th>Max-Access</th>
<th>Syntax</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsuSitData</td>
<td>1.20</td>
<td>read-write</td>
<td>IPv6Address</td>
<td></td>
</tr>
<tr>
<td>rsuSdcDestIpAddress</td>
<td>1.20.1</td>
<td>read-write</td>
<td>Integer32</td>
<td>1024..65535</td>
</tr>
<tr>
<td>rsuSdcDestPort</td>
<td>1.20.2</td>
<td>read-write</td>
<td>Integer32</td>
<td>1..18000</td>
</tr>
<tr>
<td>rsuSdcInterval</td>
<td>1.20.3</td>
<td>read-write</td>
<td>Integer32</td>
<td></td>
</tr>
<tr>
<td>rsuSdwIpAddress</td>
<td>1.20.4</td>
<td>read-write</td>
<td>IPv6Address</td>
<td></td>
</tr>
<tr>
<td>rsuSdwPort</td>
<td>1.20.5</td>
<td>read-write</td>
<td>Integer32</td>
<td>1024..65535</td>
</tr>
</tbody>
</table>

**RSU Set**

<table>
<thead>
<tr>
<th>Name</th>
<th>OID 1.21</th>
<th>Max-Access</th>
<th>Syntax</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsuSet</td>
<td>1.21</td>
<td>read-write</td>
<td>INTEGER</td>
<td>0</td>
</tr>
<tr>
<td>rsuSetRole</td>
<td>1.21.1</td>
<td>read-write</td>
<td>INTEGER</td>
<td>0</td>
</tr>
<tr>
<td>rsuSetEnable</td>
<td>1.21.2</td>
<td>read-write</td>
<td>INTEGER</td>
<td></td>
</tr>
<tr>
<td>rsuSetSlaveTable</td>
<td>1.21.3</td>
<td>not-access</td>
<td>SEQUENCE OF</td>
<td></td>
</tr>
<tr>
<td>rsuSetSlaveEntry</td>
<td>1.21.3.1</td>
<td>not-access</td>
<td>RsuSetSlaveEntry</td>
<td></td>
</tr>
<tr>
<td>rsuSetSlaveIndex</td>
<td>1.21.3.1.1</td>
<td>not-access</td>
<td>RsuTableIndex</td>
<td></td>
</tr>
<tr>
<td>rsuSetSlaveIpAddress</td>
<td>1.21.3.1.2</td>
<td>read-create</td>
<td>IPv6Address</td>
<td></td>
</tr>
<tr>
<td>rsuSetSlaveRowStatus</td>
<td>1.21.3.1.3</td>
<td>read-create</td>
<td>RowStatus</td>
<td></td>
</tr>
</tbody>
</table>

**Mode**

<table>
<thead>
<tr>
<th>Name</th>
<th>OID 1.99</th>
<th>Max-Access</th>
<th>Syntax</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsuMode</td>
<td>1.99</td>
<td>read-write</td>
<td>INTEGER</td>
<td>2</td>
</tr>
</tbody>
</table>

**Notifications**

<table>
<thead>
<tr>
<th>Name</th>
<th>OID 1.100.0.1</th>
<th>Max-Access</th>
<th>Syntax</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsuMsgFileIntegrityError</td>
<td></td>
<td>read-write</td>
<td>NOTIFICATION-TYPE</td>
<td></td>
</tr>
</tbody>
</table>
## Appendix B. SNMPv3 Management Information Base

**U.S. Department of Transportation**  
Office of the Assistant Secretary for Research and Technology  
Intelligent Transportation Systems Joint Program Office  
Dedicated Short Range Communications Roadside Unit Specifications

<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
<th>Max-Access</th>
<th>Syntax</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsuSecStorageIntegrityError</td>
<td>1.100.0.2</td>
<td></td>
<td>NOTIFICATION-TYPE</td>
<td></td>
</tr>
<tr>
<td>rsuTamperAlert</td>
<td>1.100.0.3</td>
<td></td>
<td>NOTIFICATION-TYPE</td>
<td></td>
</tr>
<tr>
<td>rsuAuthError</td>
<td>1.100.0.4</td>
<td></td>
<td>NOTIFICATION-TYPE</td>
<td></td>
</tr>
<tr>
<td>rsuSignatureVerifyError</td>
<td>1.100.0.5</td>
<td></td>
<td>NOTIFICATION-TYPE</td>
<td></td>
</tr>
<tr>
<td>rsuAccessError</td>
<td>1.100.0.6</td>
<td></td>
<td>NOTIFICATION-TYPE</td>
<td></td>
</tr>
<tr>
<td>rsuTimeSourceLost</td>
<td>1.100.0.7</td>
<td></td>
<td>NOTIFICATION-TYPE</td>
<td></td>
</tr>
<tr>
<td>rsuClockSkewError</td>
<td>1.100.0.8</td>
<td></td>
<td>NOTIFICATION-TYPE</td>
<td></td>
</tr>
<tr>
<td>rsuTimeSourceMismatch</td>
<td>1.100.0.9</td>
<td></td>
<td>NOTIFICATION-TYPE</td>
<td></td>
</tr>
<tr>
<td>rsuGpsAnomaly</td>
<td>1.100.0.10</td>
<td></td>
<td>NOTIFICATION-TYPE</td>
<td></td>
</tr>
<tr>
<td>rsuGpsDeviationError</td>
<td>1.100.0.11</td>
<td></td>
<td>NOTIFICATION-TYPE</td>
<td></td>
</tr>
<tr>
<td>rsuGpsNmeaNotify</td>
<td>1.100.0.12</td>
<td></td>
<td>NOTIFICATION-TYPE</td>
<td></td>
</tr>
<tr>
<td><strong>Notification Objects</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rsuMsgFile IntegrityMsg</td>
<td>1.100.1.1</td>
<td>accessible-for-notify</td>
<td>DisplayString</td>
<td></td>
</tr>
<tr>
<td>rsuSecStorageIntegrityMsg</td>
<td>1.100.1.2</td>
<td>accessible-for-notify</td>
<td>DisplayString</td>
<td></td>
</tr>
<tr>
<td>rsuTamperAlertMsg</td>
<td>1.100.1.3</td>
<td>accessible-for-notify</td>
<td>DisplayString</td>
<td></td>
</tr>
<tr>
<td>rsuAuthMsg</td>
<td>1.100.1.4</td>
<td>accessible-for-notify</td>
<td>DisplayString</td>
<td></td>
</tr>
<tr>
<td>rsuSignatureVerifyMsg</td>
<td>1.100.1.5</td>
<td>accessible-for-notify</td>
<td>DisplayString</td>
<td></td>
</tr>
<tr>
<td>rsuAccessMsg</td>
<td>1.100.1.6</td>
<td>accessible-for-notify</td>
<td>DisplayString</td>
<td></td>
</tr>
<tr>
<td>rsuTimeSourceLostMsg</td>
<td>1.100.1.7</td>
<td>accessible-for-notify</td>
<td>DisplayString</td>
<td></td>
</tr>
<tr>
<td>rsuClockSkewMsg</td>
<td>1.100.1.8</td>
<td>accessible-for-notify</td>
<td>DisplayString</td>
<td></td>
</tr>
<tr>
<td>rsuTimeSourceMismatch</td>
<td>1.100.1.9</td>
<td>accessible-for-notify</td>
<td>DisplayString</td>
<td></td>
</tr>
<tr>
<td>rsuGpsAnomalyMsg</td>
<td>1.100.1.10</td>
<td>accessible-for-notify</td>
<td>DisplayString</td>
<td></td>
</tr>
<tr>
<td>rsuGpsDeviationMsg</td>
<td>1.100.1.11</td>
<td>accessible-for-notify</td>
<td>DisplayString</td>
<td></td>
</tr>
<tr>
<td>rsuGpsNmeaNotifyInterval</td>
<td>1.100.1.12</td>
<td>read-write</td>
<td>Integer32</td>
<td>0..18000</td>
</tr>
<tr>
<td>rsuAlertLevel</td>
<td>1.100.1.13</td>
<td>accessible-for-notify</td>
<td>INTEGER</td>
<td>0..4</td>
</tr>
</tbody>
</table>
Appendix C. Active Message File Format

The format for both encoded Store & Repeat Messages and encoded Immediate Forward messages is contained below

# Message File Format
# 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>
Appendix D. Example WAVE Service Advertisement (WSA)

Context

Figure D-1 indicates the context for an example Signed WSA format, as indicated in IEEE 1609.3-2016.

![Diagram](image)

Figure D-1. Diagram. Context for Example WAVE Service Advertisement Format.

WSA Example

Table D-1 provides the format of a basic WSA for an RSU that advertises Intersection Safety Awareness and IPv6 Routing services

Table D-1: Format of a Basic WSA for an RSU.

<table>
<thead>
<tr>
<th>Header</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSA Version and Option Indicator</td>
<td>0x3F</td>
<td>WSA Version = 3 (4 bits) Option Indicator = 0b1111 (4 bits) all Header Extensions are present</td>
</tr>
<tr>
<td>WSA ID and Content Count</td>
<td>0x11</td>
<td>WSA ID =1 (4 bits) Content Count = 1 (4 bits)</td>
</tr>
<tr>
<td>Repeat Rate</td>
<td>32</td>
<td>indicates the WSA is repeated 50 times per 5 seconds</td>
</tr>
<tr>
<td>3DLocation</td>
<td></td>
<td>based on RSU Location</td>
</tr>
<tr>
<td>Advertiser ID</td>
<td></td>
<td>ASCII content representing the RSU Owner</td>
</tr>
</tbody>
</table>
### Service Info Segment 1

<table>
<thead>
<tr>
<th>PSID</th>
<th>0x82</th>
<th>Intersection Safety Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Index</td>
<td>0x09</td>
<td>Chan Index = 1 (5 bits)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>reserved = 0b00 (2 bits)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Opt Ind=0b1 (1 bit)</td>
</tr>
<tr>
<td>PSC</td>
<td></td>
<td>ASCII representation of &quot;Intersection Safety Awareness&quot;</td>
</tr>
<tr>
<td>RCPI Threshold</td>
<td></td>
<td>-95dBm</td>
</tr>
<tr>
<td>WSA Count Threshold</td>
<td>5</td>
<td>5: Indicates the receiving devices should ignore the Advertised Services if it receives less than 5 WSAs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: The WSA Count Threshold Interval is not present, indicating a default value of 1 second</td>
</tr>
</tbody>
</table>

### Service Info Segment 2

<table>
<thead>
<tr>
<th>PSID</th>
<th>0x10 20 40 7E</th>
<th>IPv6 Routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Index</td>
<td>0x11</td>
<td>Chan Index = 2 (5 bits)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>reserved = 0b00 (2 bits)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Opt Ind=0b1 (1 bit)</td>
</tr>
<tr>
<td>PSC</td>
<td></td>
<td>ASCII representation of &quot;IPv6 Routing&quot;</td>
</tr>
<tr>
<td>RCPI Threshold</td>
<td></td>
<td>-90dBm</td>
</tr>
<tr>
<td>WSA Count Threshold</td>
<td>5</td>
<td>5: Indicates the receiving devices should ignore the Advertised Services if it receives less than 5 WSAs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: The WSA Count Threshold Interval is not present, indicating a default value of 1 second</td>
</tr>
</tbody>
</table>
## Appendix D. Example WAVE Service Advertisement (WSA)

<table>
<thead>
<tr>
<th>Channel Info Instance Advertise SPaT and Map</th>
<th>Operating Class</th>
<th>0x0E</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Number</td>
<td>0xAC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmit Power</td>
<td>0x14</td>
<td>20dBm</td>
<td></td>
</tr>
<tr>
<td>Adaptable and Data Rate</td>
<td>0x0C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Channel Info Option Indicator</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Channel Access</td>
<td>0</td>
<td>Continuous Access during both Time Slot 0 and Time Slot 1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Channel Info Instance Advertise IPv6 Routing</th>
<th>Operating Class</th>
<th>0x0E</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Number</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmit Power</td>
<td>0x14</td>
<td>20dBm</td>
<td></td>
</tr>
<tr>
<td>Adaptable and Data Rate</td>
<td>0x0C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Channel Info Option Indicator</td>
<td>0x01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Channel Access</td>
<td>0x02</td>
<td>Alternating Access during Time Slot 1 only</td>
<td></td>
</tr>
</tbody>
</table>

### WRA

- Router Lifetime (deployment specific)
- IP Prefix
- Prefix Length
- Default Gateway
- Primary domain name system (DNS)
- Secondary DNS
- Gateway MAC Address

---

U.S. Department of Transportation  
Office of the Assistant Secretary for Research and Technology  
Intelligent Transportation Systems Joint Program Office  
Dedicated Short Range Communications Roadside Unit Specifications