Savari

STREETWAVE™ User Guide

Release 5.9.2

Document Version 1.7

November 28, 17

savari.net // +1 408 833 6369

Regulatory Compliance

FCC Class B Information

IMPORTANT NOTE: FCC Compliance statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

IMPORTANT NOTE: FCC Operation Guide

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: FCC Caution Statement

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

IMPORTANT NOTE: FCC RF exposure statement

The antenna(s) used for this device must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

IMPORTANT NOTE: FCC Shielded cable statement

This unit was tested with shielded cables on the peripheral devices. Shielded cables must be used with the unit to insure compliance.

Table of Contents

LIST OF FIGURES

REVISION HISTORY

Sl No	Date	Chapter	Description	Version
1	31-Oct-17	All	Reorganized the document and revised content in all sections	1.4

1 Introduction

SW-1000™ is the next generation Road-side Unit (RSU) developed by Savari Inc. primarily for the USDOT (United States Department of Transportation) Connected Vehicles program. It is the latest addition to the StreetWAVE™ family of products. The SW-1000™ is architecturally compliant to US-DOT v4.1 RSU specification and is capable of transmitting signed or unsigned Immediate Forward messages (ex: Signal Phase information), Store and Repeat messages (ex: TIM) and providing IPv6 connectivity to OBUs over a dedicated short-range communications (DSRC) 5.9 Gigahertz (GHz) wireless networks. SW-1000™ uses following protocol stack and other standards associated with DSRC for vehicular communications:

- IEEE 802.11p
- IEEE 1609-1 through 1609-4
- J2735 (2016 version)
- USDOT RSU v4.1 specification

StreetWAVE™ has a provisioning/test interface for managing the device:

- Receive and load new versions of software
- Update configurations
- User credentials management
- Logging functions and download log messages to an external device.

Note: The terms “RSU” and “StreetWAVE™” have been used interchangeably throughout this document.

2 Abbreviations

The following are the abbreviations used throughout this document:

Abbreviation	Expansion
ASN1	Abstract Syntax Notation 1
CA	Certificate Authority
CSV	Comma Separated Value
DHCP	Dynamic Host Control Protocol
DNS	Dynamic Naming Service
DSRC	Dedicated Short Range Communication
GID	Geometric Intersection Description
GPS	Global Positioning Satellite
HTTP	Hypertext Transfer Protocol
IFM	Immediate Forward Message
ITS	Intelligent Transportation Systems
IT IS	International Traveler Information Systems
IP	Internet Protocol
LED	Light Emitting Device
LTM	Left Turn Movement
MAP	Map Data
MIB	Management Information Base
NTCIP	National Transportation Communications for ITS Protocol
OBU/OBE	On-Board Equipment/On-Board Unit
PCAP	Packet Capture

PSID	Provider Service Identifier
RDNSS	Recursive DNS Server
RFC	Request for Comments
RSE/RSU	Roadside Equipment/Roadside Unit
RNDF	Route Network Definition File
RTM	Right Turn Movement
RX	Receive
SAE	Society for Automotive Engineers
SSH	Secure Shell
SPaT	Signal Phase and Timing
SNMP	Simple Network Management Protocol
SRM	Signal Request Message
TC	Traffic Controller
TCID	Traffic Controller Interface Device
TCP	Transmission Control Protocol
TM	Through Movement
TIM	Traveler Information Message
TX	Transmit
UDP	User Datagram Protocol
WAVE	Wireless Access in Vehicular Environments
WSA	WAVE Service Announcement

3 Specifications

Please refer to the StreetWAVE™ Installation Guide for more details on the StreetWAVE™ hardware components and installation procedures.

Hardware and Software Specifications

Item	Description
Processor	800 MHz dual core i.MX6
Memory	4GB DDR3 DRAM
Storage	8GB eMMC
DSRC Radio	Two IEEE 802.11p Radios, -94dB receiver sensitivity
GPS	U-blox. Tracking sensitivity -160 dBm
Secure Flash	Infineon HSM SLI97
Ethernet	10/100 RJ-45 ports with Auto Uplink.
Power Supply	802.3at Compliant
Temperature	-35C to +75C
Standards Compliance	IEEE 802.11p, IEEE 1609.2, IEEE 1609.3, IEEE 1609.4, SAE J2735 (2016)
Security	SSL, Firewall, 1609.2, HSM
Physical	8” (L) x 8.5” (H) x 2.75” (D)
RF Antenna Connectors	SMB Male FAKRA. Type C Blue GPS, Type Z Light Green DSRC0, Type Z Light Green DSRC1.
Power Consumption	Nominal < 10W
LED	Indicators for power, status and diagnostics (as per US-DOT RSU v4.1 specification)

3.1 Connection Description

The top and bottom views of the SW-1000™ are displayed below.

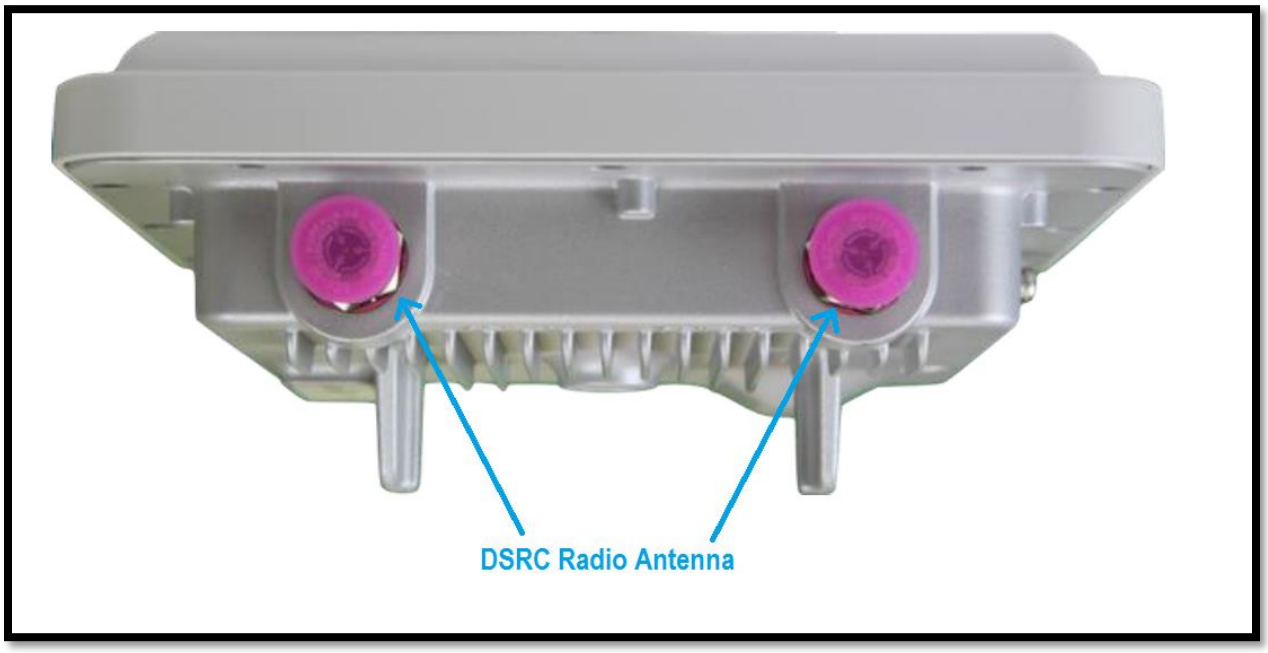

Figure 1: StreetWAVE™ Top View

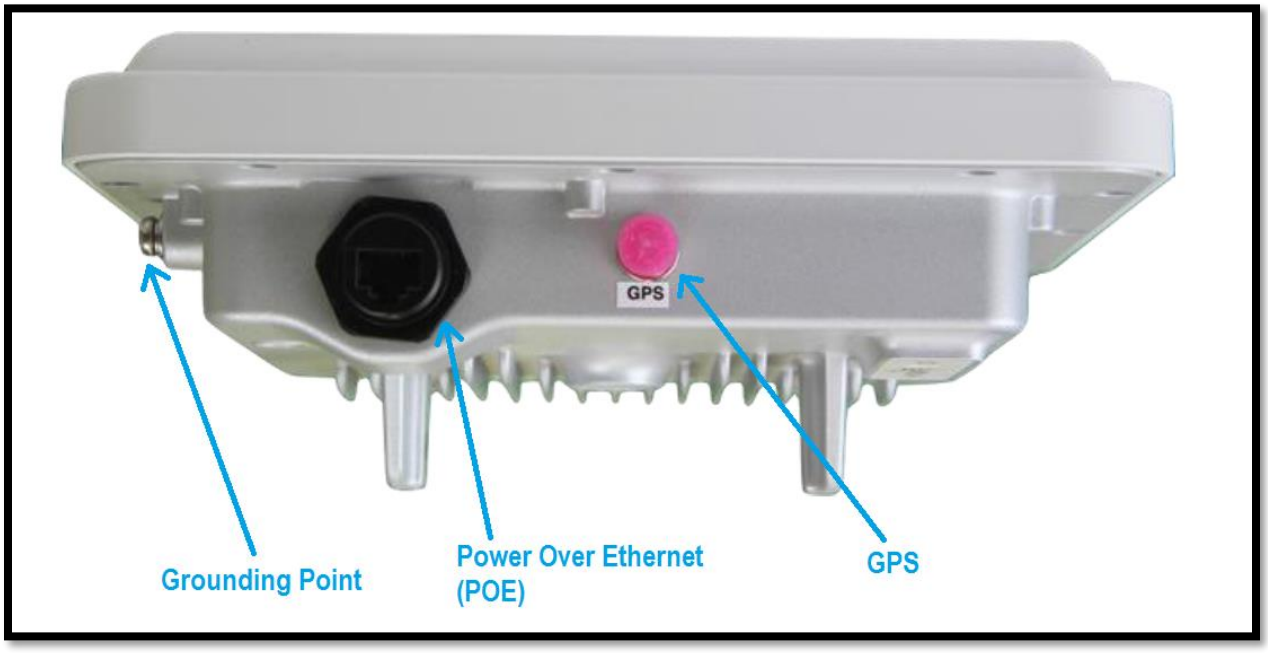

Figure 2: StreetWAVE™ Bottom View

3.2 Power

StreetWAVE™ can be powered by using an IEEE 803.at compliant Power Over Ethernet (POE) device. Savari has tested with a Trendnet TI-IG30 PoE.

3.3 GNSS

StreetWAVE™ comes with a multi-constellation GNSS that can provide the following:

- 1 Hz update rate
- Location accuracy of < 2 m with WAAS (2.5 m without WAAS) under clear sky

Note: WAAS is enabled by default.

Note: For GNSS functionality, StreetWAVE™ needs to be connected to an external GPS antenna.

3.4 DSRC Radios

DSRC radios support 802.11p in the hardware and transmit power capabilities of up to 20 dBm. The range of these radios is 450-500m and can be adjusted using the TX power setting.

3.5 Antennas

StreetWAVE™ ships with the following antennas that directly mount to the main unit:

- Two 5 GHz DSRC Omni-directional
- One magnetic GNSS

3.6 Storage

StreetWAVE™ has 4GB of integrated compact flash memory.

Note: StreetWAVE™ supports uploading the log data to an external platform for post analysis.

3.7 LED

StreetWAVE™ unit is installed with three LEDs on the panel to indicate power, device operation state and diagnostics.

3.8 Ethernet

StreetWAVE™ consists of one Ethernet port (eth0) on the panel.

3.9 Enclosure

StreetWAVE™ enclosure is IP66 rated outdoor quality unit.

4 StreetWAVE™ Features

This chapter explains the salient features of the StreetWAVE™ roadside equipment.

Following is the architecture diagram of StreetWAVE™. Each component is explained briefly in the following subsections:

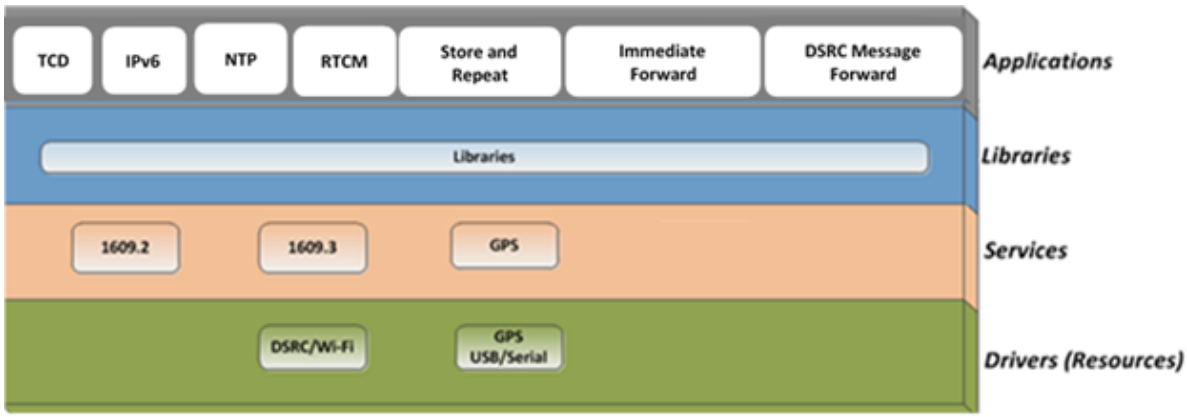

Figure 3: StreetWAVE Architecture Diagram

StreetWAVE™ features are explained briefly in the following subsections:

4.1 DSRC Radio Pair

Each StreetWAVE™ unit consists of two (2) integrated high power DSRC radios, which are exposed as the following two interfaces:

- Radio 1
- Radio 2

StreetWAVE™ radio configuration is very flexible. Any or both radios can be configured on any of the following channel modes:

- Alternating Channel Access
- Continuous Channel Access

The following applications can be configured to use any of the two interfaces (Radio1 or Radio2):

- Immediate Forward
- Store and Repeat
- IPv6-provider
- DSRC Message Forward
- TCD
- RTCM
- NTP

However, radio configuration between the applications should be consistent. i.e. each of the enabled applications should have a valid channel configuration.

4.1.1 Radio configurations in Hub-Spoke Model

You can operate multiple StreetWAVE™ units in a hub-and-spoke configuration in which the hub unit originates a message. It broadcasts those messages on its configured DSRC interface to OBUs as well as on Ethernet interface to the spoke StreetWAVE™ units in Savari 's proprietary format. The spoke StreetWAVE™ units receive them and broadcast them on their DSRC interfaces, essentially working as DSRC repeaters. This configuration is useful at an intersection where no specific location has line of sight to all approaches to the intersection. The Hub unit does not have to be in the traffic controller cabinet. It can be one of the units on the pole if it has Ethernet connectivity to the cabinet.

4.2 IPv6 Networking

StreetWAVE™ unit consists of one Ethernet interface (eth0) and 2 radio Interfaces (ath0, ath1)

StreetWAVE™ provides support for both IPv6 networking on eth0 and IPV6 support for the Radio interfaces (ath0 (i.e., Radio 1) and ath1 (i.e, Radio 2).

StreetWAVE™ can forward both IPv6 packets between its interfaces (Ethernet and DSRC) acting as a router. It also supports both IPv6 firewalls allowing the following:

- Source and destination IPv6 addresses
- Port-based rules

4.3 Immediate Forward

StreetWAVE™ Immediate Forward application supports the forwarding feature in addition to the following features.

4.3.1 UDP Listener

StreetWAVE™ Immediate Forward application listens on configured UDP ports. If any message is received on these ports in the format specified in USDOT RSU requirements, RSU signs the message using the 1609.2 protocol, if specified in incoming message, and immediately transmits on the configured DSRC interface with the PSID and channel specified in the incoming message. Incoming messages could specify different priorities, but it must specify the same transmit mode (TxMode) and transmit channel (TxChannel). This feature is applied when an intermediate device (TCD or Battelle device) is sending periodic Immediate Forward messages to a RSU

4.3.2 UDP Streaming

The StreetWAVE™ can be configured to receive data from other StreetWAVE™ and stream it over DSRC. This allows the StreetWAVE™ to function as a repeater. In this setup, one StreetWAVE™ is configured as the Hub unit and all other StreetWAVE™ that are connected to it as Spoke units (that are not capable of independently transmitting Store and Repeat, Immediate Forward etc. and are depending on the Hub to provide this data). The Hub transmits the data over the air as well as to the Spoke unit typically over an Ethernet link. The Spoke unit, upon reception of the Hub's packet, decodes and applies rules that are present in the packet, signs (if certificate is present in the forwarded packet) and forwards the packet over DSRC. The ability of the StreetWAVE™ to function in this manner can be used for streaming the packet data (in Savari proprietary format) from TMCs or back-end servers over the air. This arrangement could be useful in scenarios where a single StreetWAVE™ may not provide ample coverage for the geographic area of interest.

4.4 Spat / MAP

StreetWAVE™ supports transmission of SPAT and MAP messages. The SPaT message provides current signal status by lane and when the status is expected to change. The MAP message provides geometrical layout of an intersection/roadway. SPaT and MAP messages can be either be generated on RSU or can be compiled outside RSU and broadcasted via RSU to its listeners.

4.4.1 TCD

StreetWAVE™ can be configured to interact with Traffic-Controller device for current signal-phase information and/or for requesting either a priority signal or a preemption signal

4.5 Store and Repeat

StreetWAVE™ supports transmission of Store and Repeat messages. The Store and Repeat application, which runs on the StreetWAVE™ unit, transmits on the configured channel over the Radio 1 (default configuration) interface.

Store and Repeat application is configured in a data store inside the StreetWAVE™. The data store supports up to 10 Secured or 100 Unsecured Store and Repeat messages. The Store and Repeat messages are stored in the form of active message files. Each file contains the transmissions parameters and the actual data of the Store and Repeat message. Each Store and Repeat message can be scheduled differently based on the instructions mentioned in the active message file. The active message files follow the USDOT RSU 4.1 Specification.

4.5.1 Store-And-Repeat Active Message

StreetWAVE™ supports the USDOT Active Message Configuration file format for configuring active Store and Repeat messages.

US DOT Active Message Configuration file format

This format is defined in section ***US DOT RSU v4.1 requirements***. Each Store and Repeat active message should be defined in a separate file.

4.6 1609.3 IPv6 Provider

StreetWAVE™ supports WSAs as per the 1609.3-2016 protocol. If enabled, StreetWAVE™ switches channels on the configured interface between the following:

- 178 (control channel)
- Configured service channel.

StreetWAVE™ runs IPv6 traffic on a service channel in the configured service channel interval. Such IPv6 traffic is transparent to StreetWAVE™. It merely routes IPv6 traffic from/to DSRC interface from the Ethernet interface.

StreetWAVE™ announces this service availability using WSAs including Service Info and WRA elements. The WSA Service Info elements consists of PSID, channel information Index, Service IP and Port if any, and the service channel. WRAs consist of router IPv6 prefix, gateway address, and DNS addresses. WRA is announced if the service running behind the RSU (and RSU is merely acting as a gateway for this service). The OBEs will then use the service so that OBEs can configure their IPv6 addresses, default gateway, and DNS servers.

4.7 RTCM

StreetWAVE™ supports transmission of RTCM corrections-message. RTCM message is used to encapsulate RTCM differential corrections for GPS and other radio navigation signals as defined by the RTCM (Radio Technical Commission for Maritime Services) special committee number 104 in its various standards. In DSRC context, RTCM messages are "wrapped" for transport on the DSRC media, and are then re-constructed back into the final expected formats defined by the RTCM standard and used directly by various positioning systems to increase the absolute and relative accuracy estimates produced.

4.8 GPSOUT

StreetWAVE™ provides an option to transmit its current location (NMEA string) to a back-office server. This information can be used by back-office applications for developing a host of

applications, ex: plotting RSU's on a map, identifying GPS errors in a location, etc.

4.9 1609.2 Security

StreetWAVE™ supports 1609.2 Draft 9.3 security protocol. It supports signed Immediate Forward, signed Store and Repeat messages and signed WSAs to announce IPv6 services. The security feature can be individually enabled or disabled on Immediate Forward, Store and Repeat, and WSA.

StreetWAVE™ ships with the following pre-generated certificates supplied by US DOT:

- One root certificate
- Five different message signing certificates
- One WSA signing certificate

The following security profile is used for signing Immediate Forward, and Store and Repeat messages:

SPAT (Immediate Forward)

Field	Value	Notes
include_generation_time	True	SPAT profile requires true
include_expiration_time	false	SPAT profile requires false
message_life_time	0	not used in SPAT
include_generation_location	True	SPAT profile requires false

MAP (Immediate Forward)

Field	Value	Notes
include_generation_time	True	MAP profile requires true
include_expiration_time	false	MAP profile requires false
message_life_time	0	not used in MAP
include_generation_location	false	MAP profile requires false

Store and Repeat

Field	Value	Notes
include_generation_time	true	TIM profile requires true
include_expiration_time	false	TIM profile requires false
message_life_time	0	not used in TIM

include_generation_location	false	TIM profile requires false

WSA

Field	Value	Notes
certificate_interval	1000	
include_generation_time	true	
include_generation_location	true	
include_expiration_time	true	
check_replays	true	
check_relevance_generation_time	true	
check_relevance_generation_location	true	
check_relevance_expiry_time	true	

4.10 DSRC Message Forward

StreetWAVE™ supports the DSRC Message Forward feature as outlined in USDOT RSU 4.1 specification. This application provides the capability to forward any DSRC message received over the air to an external server over an ethernet link. The specification USDOT RSU 4.1 lists certain filter criteria that must be met for the messages to be forwarded. The DSRC Message Forward feature transparently forwards all messages if the filter criterion is successful. The application does not terminate the packet with regards to security or content.

5 RSU Initial Configuration

5.1 Accessing Methods

The StreetWAVE™ can be accessed from any PC or laptop using any of the following modes:

- SSH
- SNMP

Note: Serial port access is not available in StreetWAVE™.

5.1.1 Accessing the RSU via SSH

Follow these instructions to connect to the RSU via SSH

1. Connect RSU and local-pc using ethernet (PC IP address should be in the same network as default RSU IP).
2. Open Putty or Linux-terminal on local-pc. Check appendix for instructions on using putty.
3. If using Linux-terminal, execute the following command

   >ssh <username>@<Default IP Address> -p <port number>

   Username: root

   Password: 1[8V:2<J5*W;2I16H1nu

   Default IPv4 Address: 192.168.100.1

   Port number: 51012

5.2 StreetWAVE™ Initial Configuration Flowchart

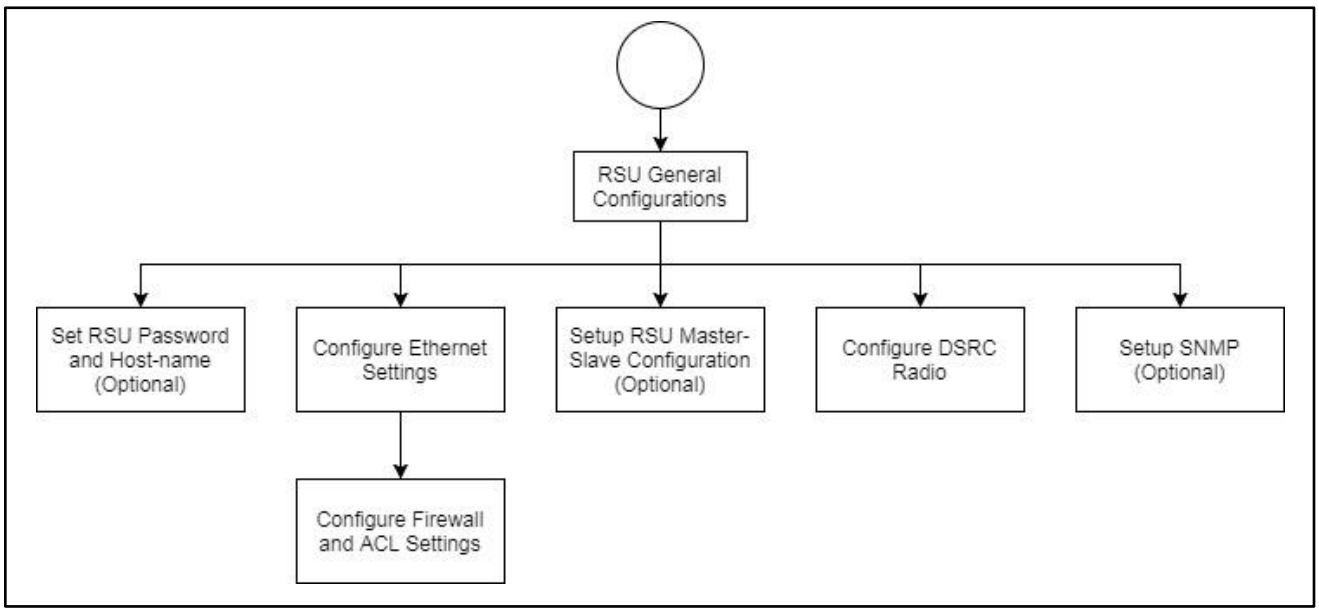

Figure 4: Initial Configuration Flowchart

5.3 Networking & Firewall

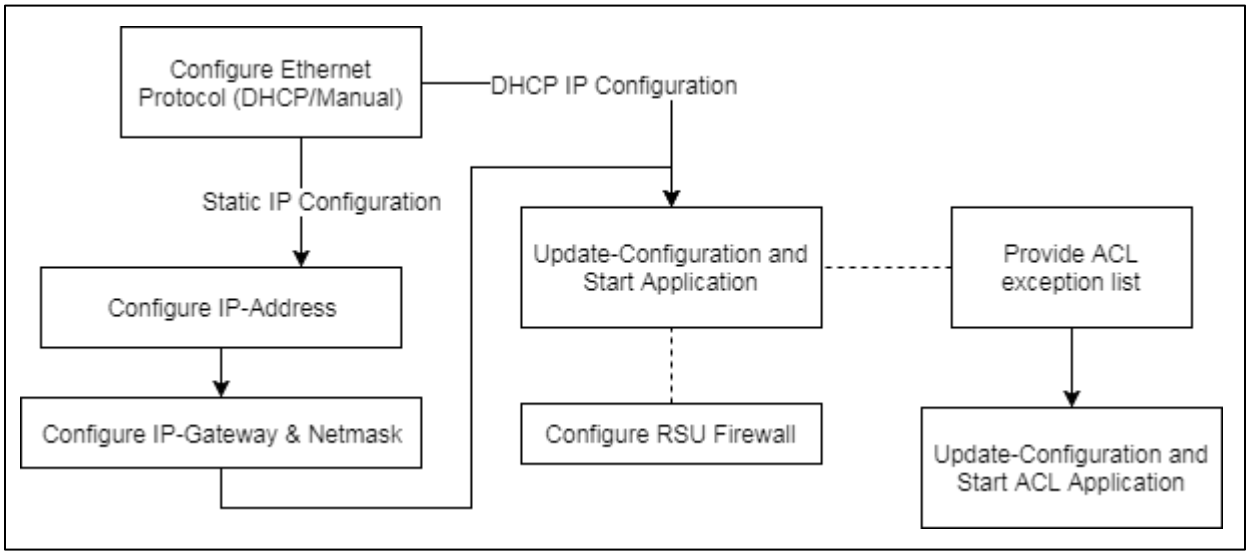

Figure 5: Networking and Firewall Configuration Flowchart

5.3.1 Networking

You can configure the IP addresses, subnet and gateway for Ethernet, Radio-1 and Radio-2 devices of RSU.

Follow these steps to configure network parameters for eth0 (for Radio-1, Radio-2 configurations use ath0, ath1 respectively in place of eth0 in the instructions)

Note: Eth0 protocol can be configured in either static or dynamic. Savari suggests using static mode configuration. DHCP is not recommended. unless until the operator has a method to identify IP address assigned to RSU.

For static Eth0 IP Configuration

1. Set eth0 to static mode

   > config system network eth0 proto static
2. Set eth0 IP-address

   > config system network eth0 ip address 10.0.0.101
3. Set eth0 gateway

   > config system network eth0 ip gateway 10.0.0.1
4. Set eth0 netmask

   > config system network eth0 ip netmask 255.255.255.0
5. Set eth0 ip6 address

   > config system network eth0 ip6 address

   For Example: <FD01:1234:0118:9000::1111/64>
6. Set eth0 ip6 gateway

> config system network eth0 ip6 gateway

For Example: <FD01:1234:0118:9000::1>

7. Restart network configuration with new-changes.

> config system network eth0 updateconf

For dhcp based Eth0 IP configuration

1. Set eth0 to dhcp mode

> config system network eth0 proto dhcp

2. Restart network configuration with new-changes.

> config system network eth0 updateconf

Note: Before configuring the eth0 proto mode to DHCP, we suggest you note down the eth0 MAC information of the board.

For static Radio-1 IP Configuration (ipv6 only)

1. Set radio1 to static mode

> config system network radio1 proto static

2. Set IP6 address for radio 1 interface

> config system network radio1 ip6 address < IPv6 address>

For Example: <FD01:1234:0118:8000::1111/64>

3. Set IP6 address for radio 1 gateway

> config system network radio1 ip6 gateway < IPv6 gateway>

For Example: <FD01:1234:0118:8000::1>

4. Commits network configuration with new-changes.

> config system network radio1 updateconf

Note: Radio-1 protocol can be configured in either static or dynamic. Savari suggests using static mode configuration

For static Radio-2 IP Configuration (ipv6 only)

1. Set radio-2 to static mode

> config system network radio2 proto static

2. Set IP6 address for radio-2 interface

> config system network radio2 ip6 address < IPv6 address>

For Example: <FD01:1234:0118:8000::1112/64>

3. Set IP6 address for radio-2 gateway

> config system network radio2 ip6 gateway < IPv6 gateway>

For Example: <FD01:1234:0118:8000::1>

4. Commits network configuration with new-changes.

> config system network radio2 updateconf

Note: Radio-2 protocol can be configured in either static or dynamic. Savari suggests using static mode configuration

5.3.2 Firewall

Various Firewalls rules can be configured for IPV4, IPV6 independently.

Follow the steps to configure RSU Firewall rules

1. To add firewall port forwarding rule for IPv4 (or) IPv6.
   > config system firewall add <ipv4/ipv6>
2. Restart Firewall with new configuration changes.
   > config system firewall updateconf

5.3.3 ACL (Access Control List)

By default, RSU blocks any remote-access requests from a different subnet. To allow remote-machines to login, access RSU, include the remote-machine details (IP addresses) in the RSU-ACL details.

Follow the steps to include a remote-machine to RSU's ACL

1. Add remote-machine's IPv4 (or) IPv6 address to ACL
   > config system acl add <ipv4/ipv6>
2. Restart with new configuration changes.
   > config system acl updateconf

This step is mandatory to access the RSU using an SNMP MIB browser. (Only in case of MIB browser in different subnet).

5.4 SNMP Configuration

5.4.1 SNMP Access Details

The details for accessing RSU via SNMP are

IP Address: RSU Eth0 IPV4 or IPV6 address

Default eth0 IPv4 address: 192.168.100.1

Port number: 161

StreetWAVE™ provides 3 sets of user-credentials for access via SNMP. Each of the SNMP-user has different access-privileges. For the list of privileges of each user, refer section *"User Management"*

1. ***Admin***

   Username: admin

   Password:

   MD5 tUrnFrf@1rb@nk$

   DES tUrnGrf@1rb@nk$

2. ***Public***

   Username: public

   Password: <No Password>

3. ***Savari***

   Username: savari

   Password: tUrnErf@1rb@nk$

5.4.2 User Management

StreetWAVE™, by default has 3 user configurations

1. **Public**: A Public user does not need any authentication and has no privacy (messages are not encrypted). Public users are provided with read-only permissions.
2. **Savari**: A Savari user needs authentication to access RSU, but has no privacy (messages are not encrypted).
3. **Admin**: An Admin user needs authentication to access RSU. privacy is also enabled for the user (all messages are encrypted).

Follow these steps to add new users to SNMP

1. Add new user to SNMP users list

   > utils snmp add-user <username>

2. Define new-user's privacy and authentication level

   Choose user security level: Enter Option: **<1-3>**

   1 - No Authentication, No Privacy

   2 - Authentication, No Privacy

   3 - Authentication and Privacy

3. Define authentication password for the new-user

   Password: <Enter any password>

   Note: Password should be min 8 characters long with at least 1 uppercase and 1 special character

4. Select SNMP Security Protocol when prompted for

   Enter Option: <1 - 2>

   1. MDA5

2. SHA

5.5 GPS

No additional GPS configurations are required on SW1000 device. Ensure GPS 3D-fix is available on the device before configuring the SW1000 applications.

Following command provides RSU's current GPS status:

> show system gpsstatus

5.6 Radio Configuration

StreetWAVE™ allows users to configure the radios (Radio 1 and Radio 2) in two service channels (both continuous) or one radio in alternating and one in continuous.

5.6.1 Default radio configuration

- DSRC radio 1 (Radio 1): This radio is configured in channel switching mode with IPv6 support on service channel 174 and WSAs (with WRAs) on control channel 178. WSAs announce the same IPv6 which is configurable through the CLI.
- DSRC radio 2 (Radio 2): This radio is configured in the continuous channel mode for channel 172.

5.6.2 Channel Configuration

Follow these steps to configure DSRC radios:

1. Configure radio in service or control channel

   > config app radio <radio1/radio2> <cch/svc>

   cch for control channel

   svc for service channel

2. Configure radio in continuous or alternating channel mode.

   > config app radio <radio1/radio2> chan_mode <0/1>

   0 for continuous channel mode

   1 for alternating channel mode

5.7 RSU Master-Slave Model

RSU can be configured in a master-slave model. This type of constellation allows RSU to extend its communication range. In the master-slave model, one RSU is set as master, and one or more RSU(s) are set as slave(s).

Follow these steps to configure an RSU as master (master in master-slave model)

1. Set an RSU as a master device

   > config rsu-set master enable

2. Include RSU-slaves for the selected RSU-master

   > config rsu-set add <slave-ip address>

   Slave-ip address: provide IP address of slave RSU.

   Note: Execute this command multiple times to add all the slave RSU(s) into the master RSU

3. Restart RSU master-slave service to reflect updated configuration

   > config rsu-set updateconf

Follow these steps in each of the other RSU(s) to configure an RSU as slave (slave in master-slave model)

1. Set an RSU as slave device

   > config rsu-set master disable

2. Restart RSU master-slave service to reflect updated configuration

   > config rsu-set updateconf

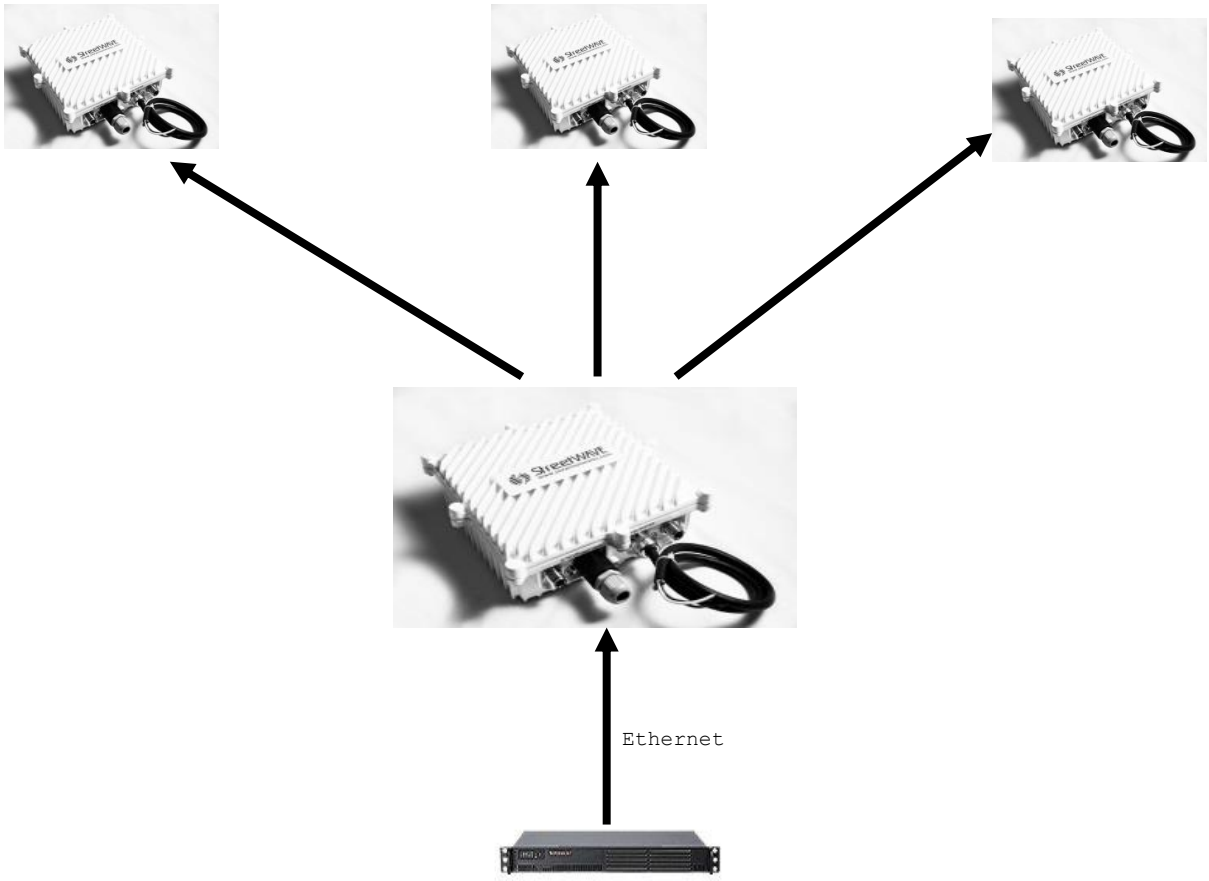

Figure 6: Master-Slave Model Deployment

6 Application and Service Activation

This section explains the parameters and statistical counters of individual applications. Counters are reset when the user places the StreetWAVE™ into a 'run' state from a corresponding 'halt' (standby) state. These counters also reset when the updateconf command is applied for configuration changes to the application.

List of applications & services supported by StreetWAVE

- Store-Repeat service
    - TIM
- Immediate-Forward service
    - SPAT
    - MAP
- GPS-Output application
- IPv6-provider application
    - SCMS
- DSRC-message-forward application
- NTP-client application
- RTCM application

6.1 Flowchart to configure the RSU Services

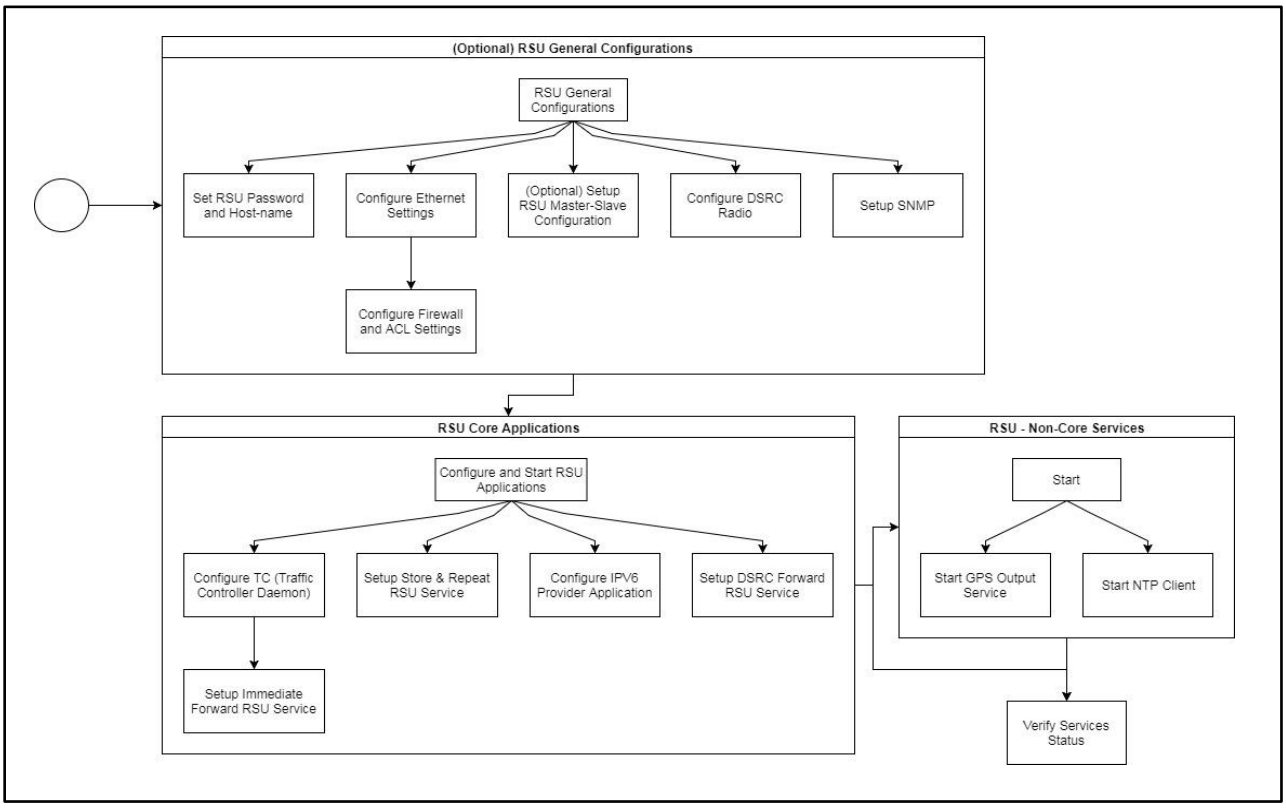

Figure 7: StreetWAVE™ Applications and Services Configurations Flowchart

6.1.1 **Common Configuration**

Before configuring individual applications or services, confirm the configurations and running state of mentioned services.

1. DSRC Radio Configuration
   Refer section *'Radio Configuration'* for configuration instructions
2. SNMP Configurations
   Refer section *'SNMP Configuration*' for configuration instructions
3. Network Firewall Settings
   Refer section '*Networking & Firewall*' for configuration instructions
4. Traffic Controller Interface
   Refer section *'Traffic Controller Interface Daemon*' for configuration instructions

6.1.2 **Traffic Controller Interface Daemon**

Follow these steps to configure Traffic-Controller Interface daemon

1. Configure Traffic-Controller Interface Mode
   > config app tcd mode <tcd-mode>

tcd-mode: Traffic Controller Daemon supports: *ntcip*, *broadcast*

2. Configure Traffic-Controller Interface network details
    a. Steps if Traffic-Controller was configured in broadcast mode
        i. Configure Traffic-Controller port
        > config app tcd broadcast port <port-number>
        port-number: provide a port number between 1024 - 65535
    ***Note**: For ports other than 6053, the corresponding firewall related changes must also be made.*
    b. Steps if Traffic-Controller was configured in ntcip mode
        i. Configure Traffic-Controller IP address
        > config app tcd ntcip tc-ipaddr <IP-address>
        IP-address: provide traffic-controller ip-address (IPv4 or IPv6)
        ii. Configure Traffic-Controller port
        > config app tcd ntcip tc-port <port-number>
        port-number: provide traffic-controller-port number between 1024 - 65535
        iii. Configure Traffic-Controller type (model)
        > config app tcd ntcip tc-type <tc-type>
        tc-type: Following traffic-controller types are currently supported: *Generic, econolite, d4, Siemens*

3. Enable Traffic-Controller Daemon
    > config app tcd enable
4. Restart Traffic-Controller application to reflect updated configuration
    > config app tcd updateconf

Note: For advanced Traffic-Controller Interface configuration refer StreetWAVE™ CLI guide, section: 'Configuring tcd'

6.2 Store-Repeat (TIM)

StreetWAVE™ Store and Repeat application can be configured in 2 modes:

- Streaming Mode (For Hub-Spoke Mode)
  Multiple RSU(s) are transmitting same message
- Standalone Mode (For local file)
  Single RSU is transmitting the Store-Repeat message

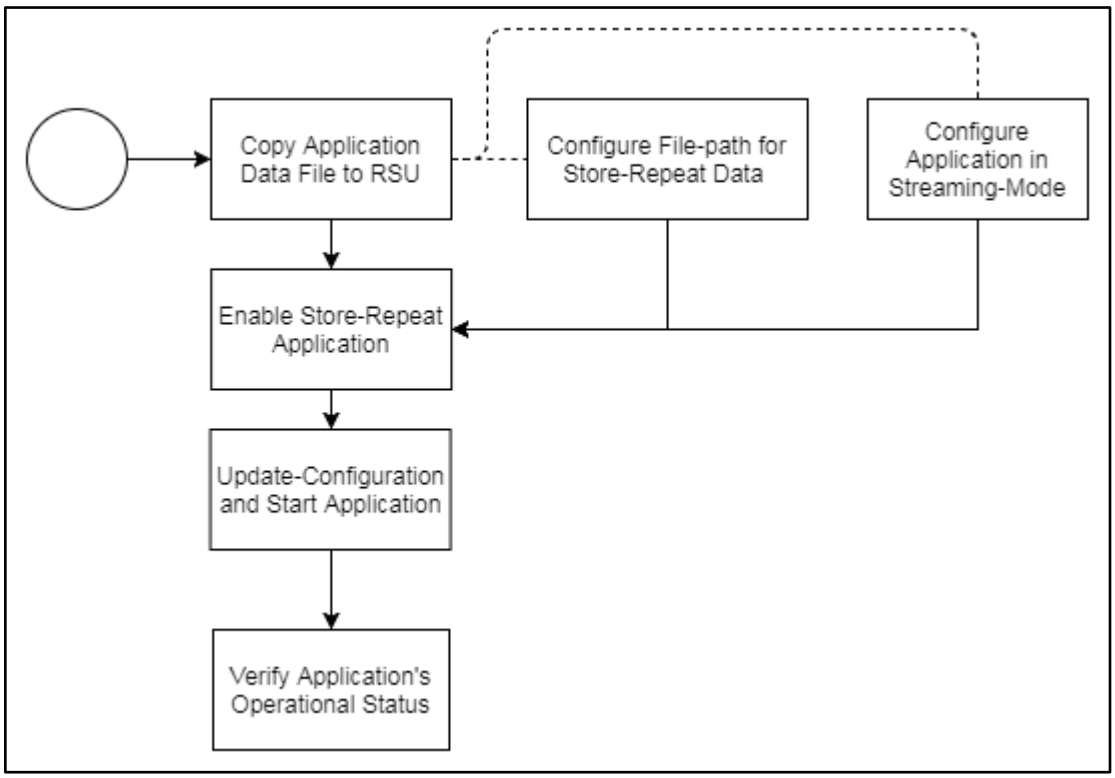

Figure 8: StreetWAVE™ TIM Application Configuration Flowchart

6.2.1 **Streaming Mode**

Follow these steps to configure Store-Repeat service alone in streaming mode

1. Copy store and repeat message file to Hub and spoke RSU's

   > utils copy <remote_username>**:scp://**<remote_server_IP>**:/**<path/to/file.image>

   timdb:<file.db>

   Ex: utils copy root:scp://192.168.20.115:/TimData/ActiveList.db timdb:ActiveList.db

Configuration Steps for RSU(s) in Hub-Spoke configuration.

Configuration Steps in Hub-RSU:

1. Add all spoke-RSU IP addresses

   > config app store-repeat streaming ipaddr <spoke-RSU IP address>

   Spoke-RSU IP address: You can include either multicast, broadcast, unicast addresses
2. Configure store-repeat streaming port

   > config app store-repeat streaming port <port>

   Port: provide a port number between 1024 - 65535
3. Enable streaming mode

   > config app store-repeat streaming mode enable send
4. Update the configuration using following command to reflect the above changes

   > config app store-repeat updateconf

Note: Check StreetWAVE™ CLI guide for advanced streaming-mode settings such as security.

Configuration Steps in Spoke-RSU:

1. Enable streaming-receive mode in spoke-RSU

   > config app store-repeat streaming mode enable receive

2. Update the configuration using the following command to reflect the above changes

   > config app store-repeat updateconf

Note: Check StreetWAVE™ CLI guide for advanced streaming-mode settings such as security.

6.2.2 Standalone Mode

Follow these steps to configure Store-Repeat service in standalone mode

1. Copy store and repeat message file to StreetWAVE

   > utils copy <remote_username>**:scp://**<remote_server_IP>**:/**<path/to/file.image>

   timdb:<file.db>

   Ex: utils copy root:scp://192.168.20.115:/TimData/ActiveList.db timdb:ActiveList.db

2. Enable store-repeat application

   > config app store-repeat enable

3. Restart store-repeat application to reflect updated configuration

   > config app store-repeat updateconf

6.3 SPAT & MAP Message Configuration

SPAT & MAP DSRC messages can be formulated in 2 ways in Master/HUB RSU

1. Based on streaming information received from upstream server (Backoffice)
   a. Refer section SPAT & MAP Streaming Configuration
2. Generated on StreetWAVE™ via Traffic-Controller application
   a. Refer to sections *'SPAT Configuration', 'MAP Configuration'* for configuring SPAT, MAP messages respectively.

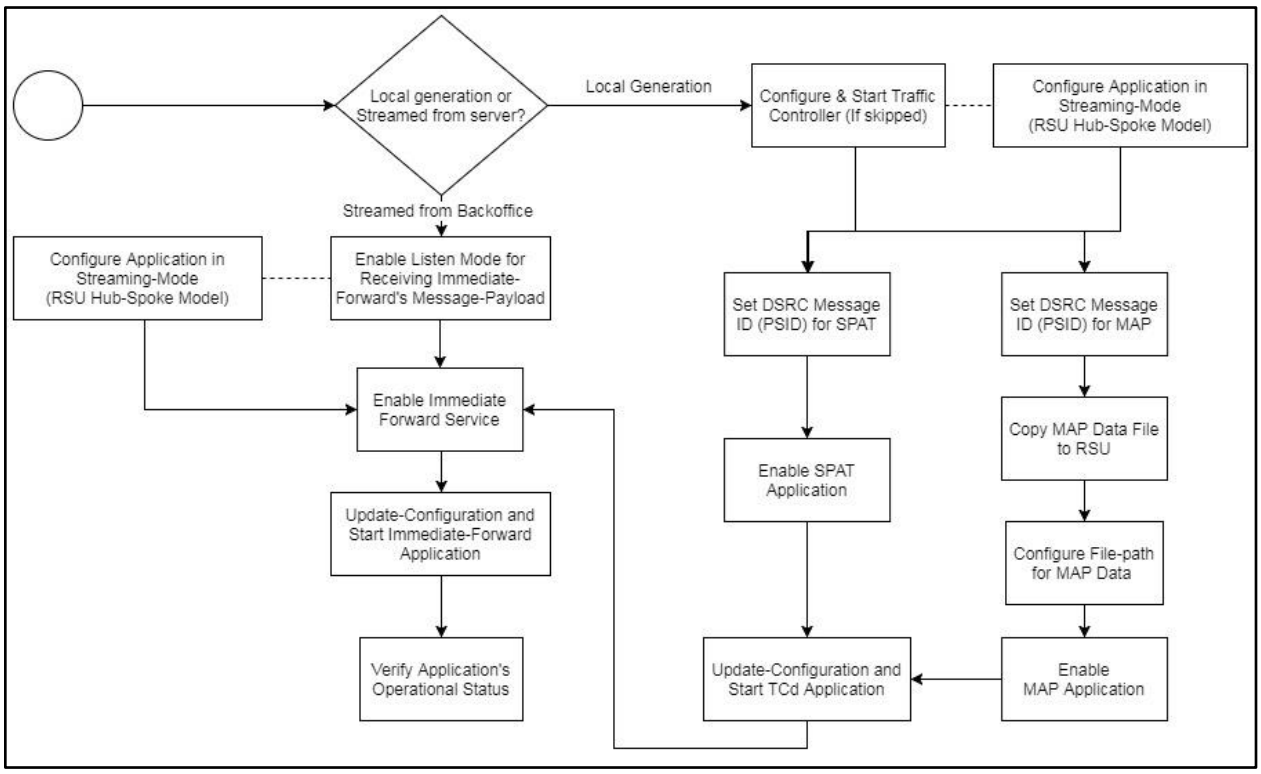

Figure 9: StreetWAVE™ SPAT & MAP Application Configuration Flowchart

6.3.1 SPAT & MAP Streaming Configuration

Follow these steps to configure SPAT & MAP in streaming-mode.

1. Configure listening mode

   > config app immediate-message-forward listenerport <port>

   Port: provide a port number between 1024 - 65535
2. Configure MAP message PSID

   > config app tcd map psid <PSID>

   PSID values range between: <0x0000 to 0XBFFF> and Default PSID: 0x8002
3. Configure SPAT message PSID

   > config app tcd spat psid <PSID>

   PSID values range between: <0x0000 to 0XBFFF> and Default PSID: 0x8002
4. Restart Traffic-Controller application to reflect updated configuration

   > config app tcd updateconf

Note: If either SPAT/MAP messages' PSID is updated, copy relevant security certificates for the new PSID.

6.3.2 MAP Configuration

Follow these steps to configure MAP message

1. Configure MAP message PSID

> config app tcd map psid <PSID>

PSID values range between: <0x0000 to 0XBFFF> and Default PSID: 0xBFF0

2. List all the MAP data file(s) on StreetWAVE™ device

   > utils list tcd

3. Configure MAP data file

   > config app tcd map mapfile <mapfile >

   Mapfile - Provide a MAP file in xml file format

   Ex: Sample_Map_Haggerty_12mile.xml

4. Restart Traffic-Controller application to reflect updated configuration

   > config app tcd updateconf

Note: For additional MAP configuration refer StreetWAVE™ CLI guide, section: 'Configuring tcd', option: 'MAP'

6.3.3 SPAT Configuration

Before configuring SPAT message, ensure traffic-controller is configured and running. Check section: *'Traffic Controller Interface Daemon'* for instructions on setting traffic-controller daemon.

Follow these steps to configure SPAT message

1. Configure SPAT message PSID

   > config app tcd spat psid <PSID>

   PSID values range between: <0x0000 to 0XBFFF> and Default PSID: 0xBFE0

2. Configure the traffic controller IP address

   > config app tcd ntcip tc-ipaddr <IP_Address>

   IP address: provide IP address of traffic-controller (providing signal information)

3. Restart Traffic-Controller application to reflect updated configuration

   > config app tcd updateconf

Note: For additional SPAT configuration refer StreetWAVE™ CLI guide, section: 'Configuring tcd', option: 'spat'

6.4 Immediate Forward

StreetWAVE™ Immediate Forward application requires the following two configurations:

- The main configuration file containing the UDP configuration.
- Incoming stream of messages as specified in USDOT RSU requirements

UDP streaming configuration is not needed if only one StreetWAVE™ unit is used at a given intersection.

StreetWAVE™ Store and Repeat application can be configured in 2 modes:

- **Streaming Mode:** Multiple RSU(s) are transmitting same message
- **Standalone Mode** (local file): Single RSU is transmitting the immediate-forward message

6.4.1 Streaming Mode

Streaming mode configuration allows RSU to replicate Immediate-Message in downstream RSUs.

Prerequisites: Ensure Traffic Controller Daemon is active, and MAP, SPAT messages are configured before configuring Immediate-forward message in standalone mode.

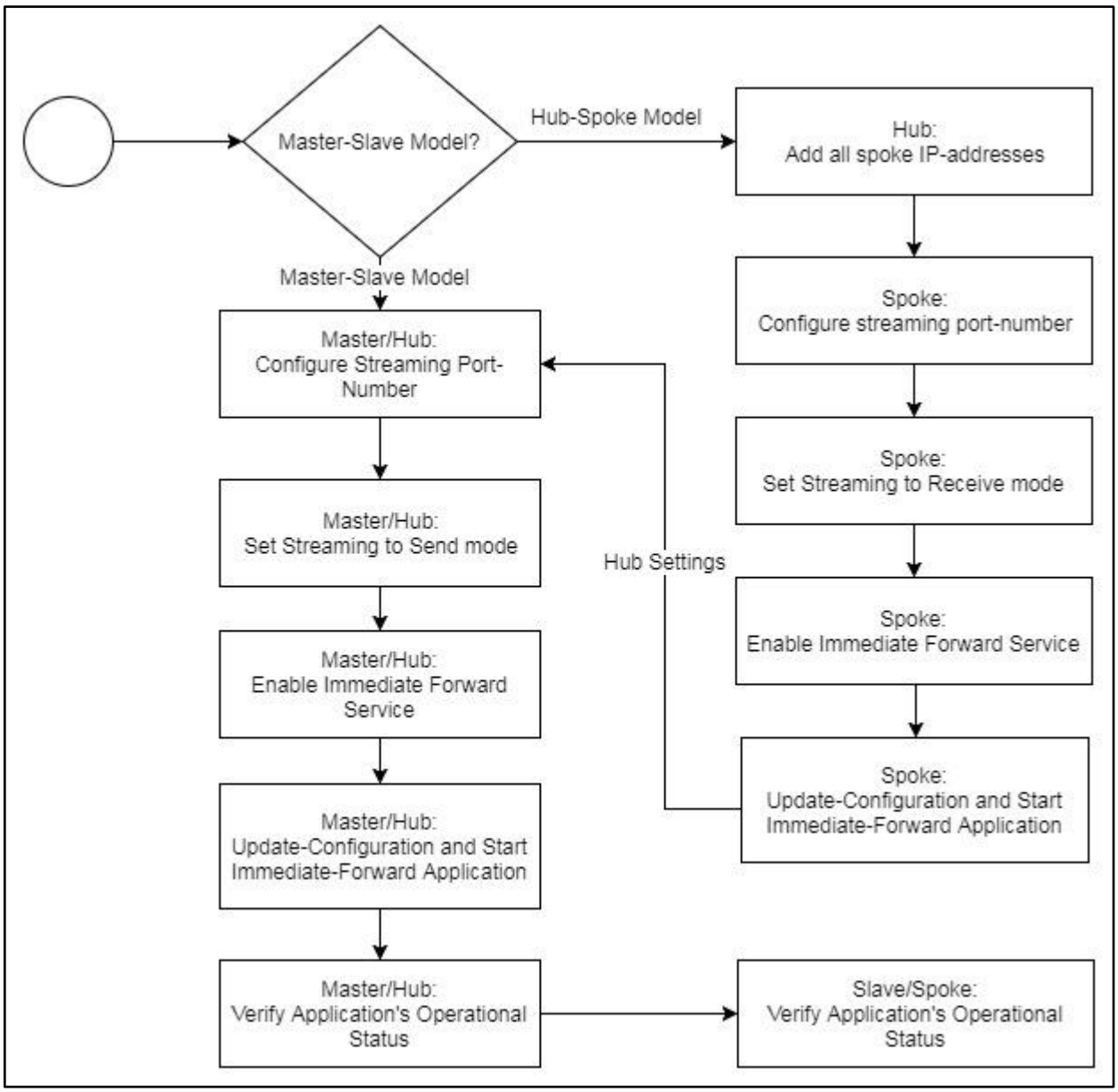

Figure 10: StreetWAVE™ Immediate Forward Application Configuration Flowchart

Streaming Mode Configurations for Master-Slave Mode

Configuration Steps in case of an RSU Master-Slave configuration.

1. Configure immediate-forward streaming port

   > config app immediate-forward streaming port <port>

   Port: provide a port number between 1024 - 65535
2. Enable streaming mode

   > config app immediate-forward streaming mode enable send
3. Enable Immediate forward application

   > config app immediate-forward enable
4. Configure the TCD Listen in Immediate Forward Application.

   > config app immediate-forward tcdlisten enable
5. Restart immediate-forward application to reflect updated configuration

   > config app immediate-forward updateconf

Note: Master RSU automatically configures slave RSU settings (no explicit settings in slave RSUs are required)

Streaming Mode Configurations for Hub-Spoke Model

Follow these steps to configure immediate-forward service in streaming mode

1. Configure HUB RSU to send streaming information to Spoke RSUs
2. Configure Spoke RSU to receive streaming information from Hub RSUs

Configuration Steps in Hub-RSU

Follow these steps to configure immediate-forward service in streaming mode in Hub RSU:

1. Add all spoke-RSU IP addresses

   > config app immediate-forward streaming ipaddr <spoke-RSU IP address>

   Spoke-RSU IP address: You can include either multicast, broadcast, unicast addresses
2. Configure immediate-forward streaming port

   > config app immediate-forward streaming port <port>

   Port: provide a port number between 1024 - 65535
3. Enable streaming mode

   > config app immediate-forward streaming mode enable send
4. Enable Immediate forward application

   > config app immediate-forward enable
1. Restart Immediate-forward application to reflect updated configuration

   > config app immediate-forward updateconf

Configuration Steps in Spoke-RSU

Follow these steps to configure immediate-forward service in streaming mode in Spoke RSU:

1. Enable streaming-receive mode in spoke-RSU

   > config app immediate-forward streaming mode enable receive

2. Enable Immediate-forward application

   > config app immediate-forward enable

3. Restart Immediate-forward application to reflect updated configuration

   > config app immediate-forward updateconf

6.4.2 Standalone Mode

Follow these steps to configure Immediate-forward service in standalone mode

1. Enable Immediate-forward application

   > config app immediate-forward enable

2. Restart immediate-forward application to reflect updated configuration

   > config app immediate-forward updateconf

Note: Ensure Traffic Controller Daemon is active, and MAP, SPAT messages are configured before configuring Immediate-forward message in standalone mode.

6.5 RTCM

RTCM application connects to RTCM server, and generates RTCM messages for its listeners.

Follow these steps to configure RTCM application on StreetWAVE

1. Configure RTCM DSRC message PSID

   > config app rtcm <psid>

   PSID values range between: <0x0000 to 0XBFFF>, and default PSID: 0x8000

2. Configure RTCM local port

   > config app rtcm localPort <port-number>

   port-number: provide traffic-controller-port number between 1024 - 65535

3. Configure backhouse server port for accessing RTCM information

   > config app rtcm <imfPort>

   imfPort: Provide IMF port number.

4. Enable RTCM application

   > config app rtcm enable

5. Restart RTCM application to reflect updated configuration

   > config app rtcm updateconf

Note: For advanced RTCM configuration refer StreetWAVE™ CLI guide, section: **'Configuring rtcm'**

6.6 GPSOUTPUT

The StreetWAVE™ unit shall send the NMEA string to a specific UDP port at a specified rate, upon acquisition of 3 or more satellites.

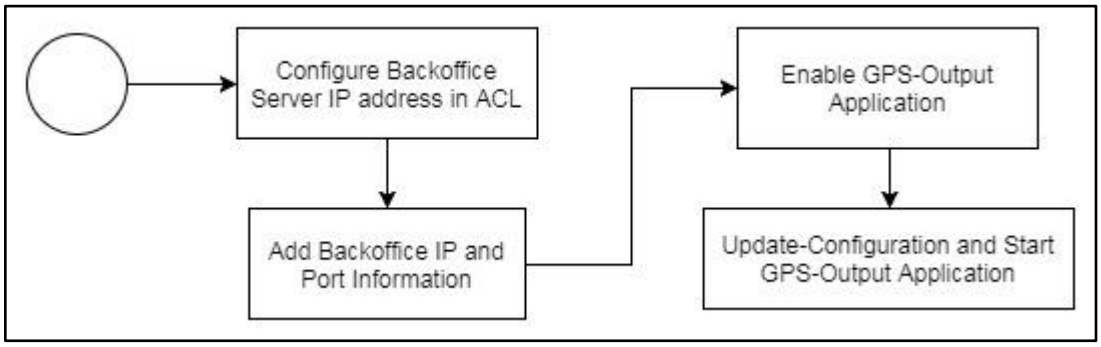

Figure 11: StreetWAVE™ GPSOUTPUT Application Configuration Flowchart

Follow these steps to configure GPS-Output application on StreetWAVE™

1. Configure backhouse server IP address for forwarding GPS information

   > config app gpsoutput <destination ip-address>

   destination ip-address: Provide backhouse server IP-address.

2. Configure backhouse server port for forwarding GPS information

   > config app gpsoutput <destination port>

   destination port: Provide backhouse server port number.

3. Configure GPS-Output Interval

   > config app GPS-Output Interval <time-interval>

   Time-interval: Provide time-interval (in seconds) for sending gps-output details to back-office.

   Valid input: 1 to 18000 (sec)

   Default-value: 1 (sec)

4. Configure Reference Position (for detecting RSU GPS deviations)

   a. Configure reference latitude

      > config app GPS-Output reference latitude <ref-latitude>

      Ref-latitude: Provide reference latitude value (in 10^{-7} degrees) for RSU device (valid input: -900000000 to 900000000)

   b. Configure Reference Longitude

      > config app GPS-Output reference longitude <ref-longitude>

      Ref-longitude: Provide reference longitude (in 10^{-7} degrees) value for RSU device

      Valid input: -1800000000 to 1800000000

c. Configure Reference Elevation

> config app GPS-Output reference elevation <ref-elevation>

Ref-elevation: Provide reference elevation (in meters) value for RSU device.

Valid input: -4095 to 61439

5. Configure Maximum Deviation

> config app GPS-Output max-deviation <max_deviation>

max_deviation: provide maximum allowable deviation (radius in centimeters) for comparison between the reported GPS coordinates and the static GPS coordinates.

Valid values: 100 to 500

Default value: 100 (meters)

6. Enable GPSOutput application

> config app gpsoutput enable

7. Restart GPSOutput application to reflect updated configuration

> config app gpsoutput updateconf

Note: For additional GPSOutput configuration and trap configuration, refer StreetWAVE™ CLI guide, section: 'Configuring gpsoutput'

6.7 DSRC Forward

StreetWAVE™ when configured can capture selected DSRC messages and send the information to a backhouse server for further processing. The RSU can also be configured to start streaming the data to backhouse at specific time of the day.

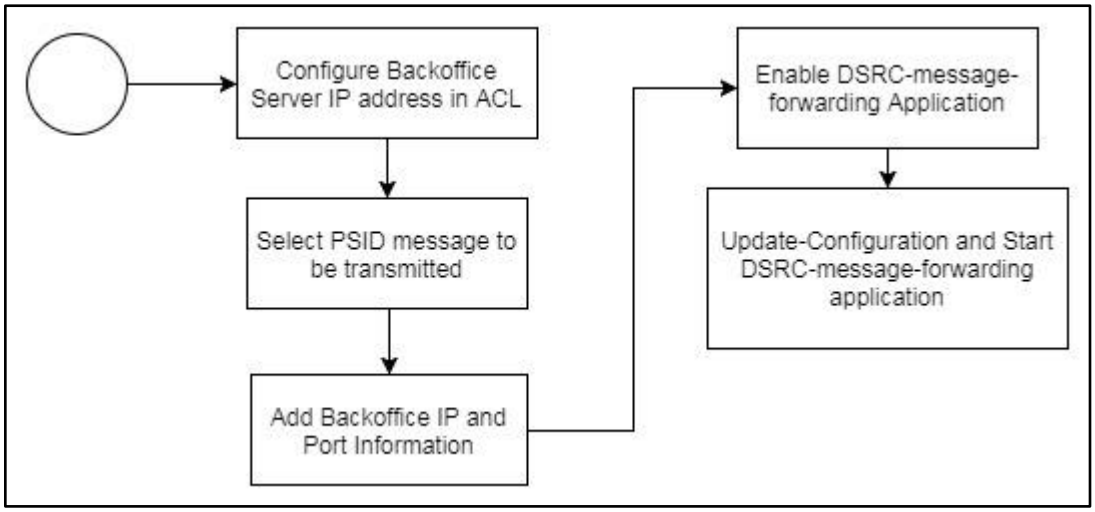

Figure 12: StreetWAVE™ DSRC Forward Application Configuration Flowchart

Follow these steps to configure DSRC-Forward application on StreetWAVE™

1. Configure DSRC-Forward message PSID

   > config app dsrc-message-forward psid <PSID>

   PSID values range between: <0x0000 to 0XBFFF>

2. Configure backhouse server IP address for forwarding selected PSID message.

   > config app dsrc-message-forward psid <PSID> destination ip <destination ip-address>

   PSID: Enter the PSID value from Step-1

   destination ip-address: Provide backhouse server ip-address. Ensure the configured IP address is reachable from RSU eth0 interface

3. Configure backhouse server port for forwarding selected PSID message.

   > config app dsrc-message-forward psid <PSID> destination port <destination port>

   PSID: Enter the PSID value from Step-1

   destination port: Provide backhouse server port number.

4. Enable DSRC-Forward application

   > config app dsrc-message-forward enable

5. Restart DSRC-forward application to reflect updated configuration

   > config app dsrc-message-forward updateconf

6.8 IPV6 App Provider

IPV6 provider application provides Onboard-devices to connect to StreetWAVE™ device. This service is an enabler for RSU/OBU to request/post non-generic information (such-as: uploading OBU data-logs, downloading security-certificates)

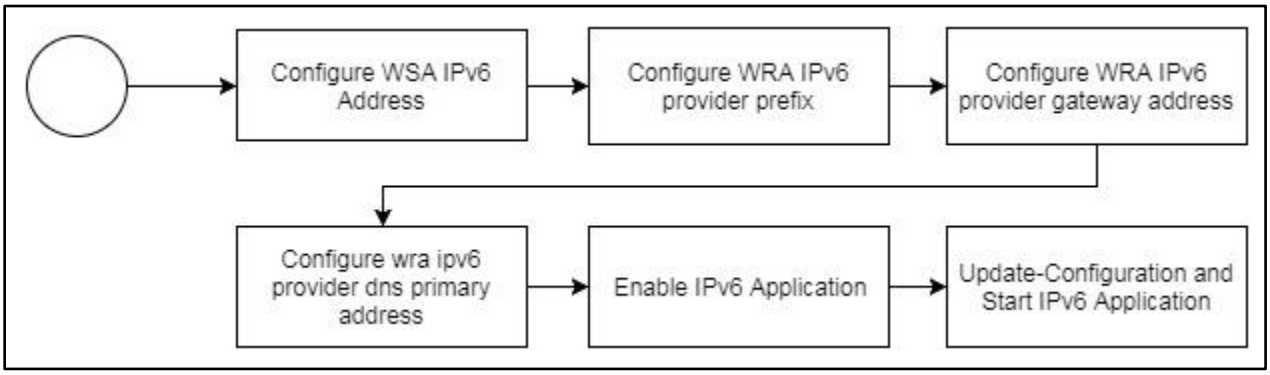

Figure 13: IPV6 Provider App Configuration Flowchart

Follow these steps to configure IPV6 application on StreetWAVE™

1. Configure wsa ipv6 provider address

   > config app ipv6-provider wsa ipv6addr <IPv6 Address>

   IPv6 Address: IPv6 address of SW-1000

   Ex: FD01:1234:0114:9000::1234/64

2. Configure wra ipv6 provider prefix

   > config app ipv6-provider wra prefix < IPv6 Prefix>

   IPV6 Prefix: prefix value to be announced in WRA

   Ex: FD01:1234:0114:8000::

3. Configure wra ipv6 provider gateway address

   > config app ipv6-provider wra gateway-address ipv6 <IPv6 gateway address>

   IPv6 gateway address: gateway MAC address to announce in WRA

   Ex: FD01:1234:0114:8000::1111

4. Configure wra ipv6 provider dns primary address

   > config app ipv6-provider wra dns primary <Primary DNS address>

   Primary DNS address provide primary DNS address value

   Ex: FD01:1234:0114:9000::1111

5. Enable IPV6 provider application

   > config app ipv6-provider enable

6. Restart IPv6-provider application to reflect updated configuration

   > config app ipv6-provider updateconf

Note: For advanced IPv6 application configuration refer ‘StreetWAVE™ CLI guide’, section:

'Configuring ipv6-provider'

Consider the following to ensure the RSU connections are secure

- Ping SCMS Server from RSU to ensure SCMS Server is accessible.
- Reboot the RSU
- On Reboot, MW Should be able to connect to RSU
- ASD Should get IP address in the domain 'fdca:39c0:a830:4444::
- ASD should also set its default Gateway as 'fdca:39c0:a830:4444::1.
- ASD should be able to ping RSU and SCMS.

6.9 Logging

6.9.1 Interface Logging

StreetWAVE™ supports logging all DSRC and IP messages transmitted and received in the PCAP format to the persistent memory. All packet activity on all interfaces are captured and logged in the PCAP format. The PCAP files can then be seen in Wireshark after file offload has transferred the PCAP files to a back-office server. In addition, the system-status log messages are logged to separate files. There is ~3GB of space set aside for this total logging.

Follow these steps to configure Interface logging in StreetWAVE

1. Enable system interface log generation
   StreetWAVE>> **config system interface-log <interface> generate enable**
   Interface: provide interface details. Ex: ath1, ath0
2. Restart interface-log application to reflect updated configuration
   StreetWAVE>> **config system interface-log updateconf**

6.9.2 System Logging

StreetWAVE™ supports logging nearly all system events. The system log files can be transferred to a back-office server for further analysis like, checking system performance, detecting security breaches, identify system errors, etc.

StreetWAVE™ supports multiple logging levels based on the need of the user. The levels have been defined as per ITS RSU standard spec 4.1

- 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 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.
- 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.

Sample list of system events logged in StreetWAVE™ device:

1. Current RSU GPS location.
2. User-access details (ex: failed login entry, file accessed, etc.)
3. Ethernet connection status changes (ex: link up/down)
4. Kernel errors
5. Application events (ex: store & repeat application start/end time)
6. Security failures (ex: security signing failures, list of expired public-keys on RSU)

Follow these steps to configure System logging in StreetWAVE™

Note: System logging is enabled by default in all StreetWAVE™ devices

1. Set system log level for writing system-events

   StreetWAVE>> **config system system-log loglevel <level>**

   Level: Provide a level value between 1 to 8.

   Note: By default, the RSU device is set to log all events of level-7 (or lower).

2. Set system log deletion day value. (system files meeting deletion criteria will be deleted on the specific day of the week)

   StreetWAVE>> **config system system-log deleteday <day>**

   Day: Day of the week <1(Monday) - 7(Sunday)>

3. Set system log deletion age (all system files older than provided days will be deleted on the set day of the week)

   StreetWAVE>> **config system system-log deleteage <age>**

   Age: Select a value between 1 to 30 (days)

4. Enable system log generation

   StreetWAVE>> **config system system-log enable**

5. Restart system-log application to reflect updated configuration

   StreetWAVE>> **config system system-log updateconf**

7 System Monitoring

7.1 Visual Status LED Indicators

The following table displays the details about the LED status indicators:

LED Name	Indication	Description
"STATUS"	Off	The system is in "Standby" state or all applications (Store and Repeat, DSRC Message Forward Immediate Forward, and IPv6) are disabled.
	Green On	The system is in "run" state and at least one application (Store and Repeat, DSRC Message Forward, Immediate Forward, and IPv6) is enabled and functioning properly.
	Green Blinking	The system is in "run" state and at least one application is malfunctioning.
	Amber Blinking	System upgrade is initiated
"POWER"	On	The device is powered on.
	Off	The device is powered off.

7.2 Understanding RSU Monitoring Parameters

7.3 RSU Status

StreetWAVE™ provides CLI commands for knowing the status of RSU and its applications.

7.3.1 GPS Status

The GPS Fix status of the board can be displayed using the following show command

> show system gpsstatus

StreetWAVE™ Sample Output

```
3D fix (Lat: 12.945319, Lon: 77.586183, Elev: 912.10)
```

7.3.2 Application Status

Execute the following command in StreetWAVE™ CLI to generate RSU application status.

> show system app-status

Description:

- Enabled:
  - Y: Application is enabled

- N: Application is disabled

- Idle:
  - Y: Application is running, but is idle (not receiving/transmitting any messages)
- Running:
  - Y: Application is up and running (either transmitting, receiving, or both)
- Not-Running:
  - Y: Application is not running (either crashed or manually stopped)

Execution results example:

Service:	**Enabled**	**Idle**	**Running**	**Not-Running**
SPAT	N	-	-	-
MAP	N	-	-	-
STORE-REPEAT	N	-	-	-
WSA/IPV6	N	-	-	-
DSRC-MSG-FORWD	N	-	-	-
RTCM	-	-	-	Y
Oper Mode:				
IFM(MASTER)	N	-	-	-
SRM(MASTER)	N	-	-	-
IFM(SLAVE)	N	-	-	-
SRM(SLAVE)	N	-	-	-
Halt Last Executed On: _ Run Last Executed On: _				

Sample show-app status scenario(s)

Scenario-1: The below screenshot shows the WSA/IPV6, DSRC-Msg-Forward and MAP applications in a ‘Running’ state with data transmission whereas STORE-REPEAT, and SPAT applications are shown as in an ‘Enabled’ state but with no data transmission (Idle).

Service:	**Enabled**	**Idle**	**Running**	**Not-Running**
SPAT	Y	Y	-	-
MAP	Y	-	Y	-
STORE-REPEAT	Y	Y	-	-
WSA/IPV6	Y	-	Y	-
DSRC-MSG-FORWD	Y	-	Y	-

RTCM	-	-	-	Y
Oper Mode:				
IFM(MASTER)	N	-	-	-
SRM(MASTER)	N	-	-	-
IFM(SLAVE)	N	-	-	-
SRM(SLAVE)	N	-	-	-
Halt Last Executed On: Fri Oct 06 06:18:44 UTC 2017 Run Last Executed On: Fri Oct 06 06:19:01 UTC 2017				

Scenario-2: The below screenshot shows an RSU with a halt operation performed, which then places all the enabled services into a 'Not-Running' state.

Service:	**Enabled**	**Idle**	**Running**	**Not-Running**
SPAT	Y	-	-	Y
MAP	Y	-	-	Y
STORE-REPEAT	Y	-	-	Y
WSA/IPV6	Y	-	-	Y
DSRC-MSG-FORWD	Y	-	-	Y
RTCM	Y	-	-	Y
Oper Mode:				
IFM(MASTER)	N	-	-	-
SRM(MASTER)	N	-	-	-
IFM(SLAVE)	N	-	-	-
SRM(SLAVE)	N	-	-	-
Halt Last Executed On: Fri Oct 06 06:28:41 UTC 2017 Run Last Executed On: Fri Oct 06 06:30:23 UTC 2017				

Scenario-3: The below screen shows the services in a completely disabled state.

Service:	**Enabled**	**Idle**	**Running**	**Not-Running**
SPAT	N	-	-	-
MAP	N	-	-	-

STORE-REPEAT	N	-	-	-
WSA/IPV6	N	-	-	-
DSRC-MSG-FORWD	N	-	-	-
RTCM	N	-	-	-
Oper Mode:				
IFM(MASTER)	N	-	-	-
SRM(MASTER)	N	-	-	-
IFM(SLAVE)	N	-	-	-
SRM(SLAVE)	N	-	-	-
Halt Last Executed On: Fri Oct 06 07:28:41 UTC 2017 Run Last Executed On: Fri Oct 06 07:30:23 UTC 2017				

GPS Output

Execute the following command in StreetWAVE™ CLI to check gpsoutput application status.

> show app gpsoutput status

Execution results example:

```
status = gpsoutput app is enabled
```

Traffic Controller Daemon

Execute the following command in StreetWAVE™ CLI to TCD application status.

> show app tcd status

Execution results example:

```
status = enable
```

7.3.3 **Log Status**

System Log

Execute the following command in StreetWAVE™ CLI to check system-logging application status.

> show system system-log status

Execution results example:

```
enable = 1
```

Interface Log

Execute the following command in StreetWAVE™ CLI to check interface-logging application status.

> show system interface-log status

Execution results example:

```
interface_log = enable
```

7.4 RSU Application Statistics

StreetWAVE™ provide CLI commands for generating statistics of running applications and services.

Parameter	Description
Tx Packet (or) Tx	Number of message packets transmitted to the DSRC radio.
Udp Tx Packet (or) Udp Tx	Number of message packets transmitted over UDP streaming (Hub-Spoke)
Rx Packet (or) Rx	Number of message packets received on DSRC radio.
Signing Failures	Count of messages with signing failure.
Active List Files	Number of active list files (ex: number of store-and-repeat message active list files on RSU)
Transmit Channel	The DSRC channel on which given message packets are transmitted.
PSID	PSID of the selected message
Drop	Number of messages dropped due to signing failures or malformed packets

7.4.1 All Applications

Execute the following command in StreetWAVE™ CLI to check application stats of all RSU applications.

> show system rsu-stats all

Execution results example:

```
Status:
        Running
```

```
Stats:
        STORE-REPEAT:
                Tx Packet               : 2606
                Udp Tx Packet           : 0
                Signing Failures        : 0
                Num Active List Files   : 1
                Transmit Channel        : 178
Status:
        Running
Stats:
        IMMEDIATE-FORWARD:
                SPAT:
                        Spat Rx         : 9690
                        Spat Tx         : 9690
                        Spat Udp Tx     : 0
                MAP:
                        Map Rx          : 0
                        Map Tx          : 0
                        Map Udp Tx      : 0
                RTCM:
                        RTCM Rx         : 0
                        RTCM Tx         : 0
                        RTCM Udp Tx     : 0
Status:
        Running
Stats:
        IPV6-PROVIDER:
                IpService Enabled       : 0
                Signing Enabled         : 0
                Current Service Channel : 0
                Wsa Tx Packet           : 25915
Status:
        Running
Stats:
                RTCM:
                        RTCM Rx         : 0
                        RTCM Tx         : 0
                        RTCM Udp Tx     : 0
```

```
Status:
        Not Running
Stats:
        DSRC-MESSAGE-FORWARD:
                PSID Based Stats For ath0:
                PSID            Rx              Tx              Drop
                0x8007          0               0               0
                0x20            0               0               0
                0x8003          0               0               0
                0x8002          0               0               0
                0x8000          0               0               0

                PSID Based Stats For ath1:
                PSID            Rx              Tx              Drop
                0x8007          0               0               0
                0x20            0               0               0
                0x8003          0               0               0
                0x8002          0               0               0
                0x8000          0               0               0
```

7.4.2 **Store and Repeat Messages**

The following parameters are displayed in the Store and Repeat app status command:

> show system rsu-stats store-repeat

Execution results example:

```
Status:
        Running
Stats:
        STORE-REPEAT:
                Tx Packet               : 197
                Udp Tx Packet           : 0
                Signing Failures        : 0
                Num Active List Files   : 1
                Transmit Channel        : 178
```

The above example displays the Store and Repeat application in ‘Running’ state for 1 Active Message List.

7.4.3 **Immediate Forward Message**

The following parameters and counters are displayed in the Immediate Forward status.

> show system rsu-stats immediate-forward

Execution results example:

```
Status:
        Running
Stats:
        IMMEDIATE-FORWARD:
                SPAT:
                        Spat Rx          : 2336461
                        Spat Tx          : 2336461
                        Spat Udp Tx      : 0
                MAP:
                        Map Rx           :233227
                        Map Tx           :233227
                        Map Udp Tx       : 0
                RTCM:
                        RTCM Rx          : 0
                        RTCM Tx          : 0
                        RTCM Udp Tx      : 0
```

Note: “Immediate Forward UDP Tx” is applicable when the StreetWAVE™ is configured as a “Hub” StreetWAVE™. It represents the Immediate Forward messages forwarded to the “Spoke” StreetWAVE™.

7.4.4 **IPv6 Provider Application**

The following parameters are displayed in the IPv6 Provider app status command:

> show system rsu-stats ipv6-provider

Execution results example:

```
Status:
        Running
Stats:
        IPV6-PROVIDER:
                IpService Enabled        : 0
                Signing Enabled          : 0
```

```
Current Service Channel  : 0
Wsa Tx Packet            : 26512
```

7.4.5 **RTCM Application**

The following parameters are displayed in the RTCM app status command:

> show system rsu-stats rtcm_msg_fwd

Execution results example:

```
Status:
        Running
Stats:
                RTCM:
                        RTCM Rx         : 0
                        RTCM Tx         : 0
                        RTCM Udp Tx     : 0
```

7.4.6 **DSRC Message Forward Application**

The following parameters are displayed in the DSRC message forward app status command:

> show system rsu-stats dsrc-message-forward

Execution results example:

```
Status:
        Not Running
Stats:
        DSRC-MESSAGE-FORWARD:
                PSID Based Stats For ath0:
                PSID    Rx              Tx              Drop
                0x8007          0               0               0
                0x20            0               0               0
                0x8003          0               0               0
                0x8002          0               0               0
                0x8000          0               0               0

                PSID Based Stats For ath1:
                PSID    Rx              Tx              Drop
                0x8007          0               0               0
```

0x20	0	0	0
0x8003	0	0	0
0x8002	0	0	0
0x8000	0	0	0

7.5 RSU System Statistics

7.5.1 Disk Usage

The following command can be used to display the current disk usage

> show system disk-usage

Execution results example:

Filesystem	Size	Used	Available	Use%	Mounted on
rootfs	189.5M	97.1M	88.5M	52%	/
/dev/root	189.5M	97.1M	88.5M	52%	/
tmpfs	881.3M	68.0K	881.2M	0%	/tmp
/dev/mmcblk0p3	3.3G	7.3M	3.1G	0%	/nojournal
tmpfs	512.0K	0	512.0K	0%	/dev

7.5.2 Memory Usage

The following command can be used to display the current memory usage.

> show system memory-usage

Execution results example:

	total	used	free	shared	buffers
Mem:	1804852	48952	1755900	88	348
-/+ buffers:		48604	1756248		
Swap:	0	0	0		

7.5.3 CPU Usage

The following command can be used to display the current CPU usage for each process

> show system cpu-usage

Execution results example:

09:08:46	CPU	%usr	%nice	%sys	%iowait	%irq	%soft	%steal	%guest	%idle
09:08:47	0	0.00	0.00	4.08	0.00	0.00	0.00	0.00	0.00	95.92

7.6 RSU Networking & Security Services Information

The following parameters are displayed in the RSU networking & security services status command:

> show system network all

Execution results example:

```
eth0:
 proto          = static
 ipaddr         = 10.0.0.114
 macaddr        = DE:B4:A8:3B:59:23
 netmask        = 255.255.255.0
 gateway        = 10.0.0.1
 ip6addr        = FD01:1234:0114:9000::1111/64
 ip6gw          = FD01:1234:0114:9000::1

radio1:
 proto          = static
 macaddr        = 00:20:62:06:AA:00
 ip6addr        = FD01:1234:0114:8000::1111/64
 ip6gw          = FD01:1234:0114:8000::1

radio2:
 proto          = static
 macaddr        = 00:20:62:06:BB:00
 ip6addr        = FD01:1234:0114:7000::1111/64
 ip6gw          = FD01:1234:0114:7000::1
```

7.6.1 Network

The following command can be used to display the ethernet configuration of the board

> show system network eth0 all

Execution results example:

```
 proto          = static
 ipaddr         = 10.0.0.114
 macaddr        = DE:B4:A8:3B:59:23
 netmask        = 255.255.255.0
 gateway        = 10.0.0.1
```

```
ip6addr      = FD01:1234:0114:9000::1111/64
ip6gw        = FD01:1234:0114:9000::1
```

7.6.2 **Firewall**

StreetWAVE™ will be protected by the configured incoming firewall port.

The following firewall parameters are configured for IPv4 by default:

> show system firewall list ipv4

Execution results example:

```
config rule 'udp_0_1516'
        option src 'lan'
        option proto 'udp'
        option dest_port '1516'
        option target 'ACCEPT'

config rule 'udp_0_6053'
        option src 'lan'
        option proto 'udp'
        option dest_port '6053'
        option target 'ACCEPT'

config rule 'udp_0_3334'
        option src 'lan'
        option proto 'udp'
        option dest_port '3334'
        option target 'ACCEPT'

config rule 'udp_0_16092'
        option src 'lan'
        option proto 'udp'
        option dest_port '16092'
        option target 'ACCEPT'

config rule 'udp_0_51015'
        option src 'lan'
        option proto 'udp'
        option dest_port '51015'
```

```
        option target 'ACCEPT'

config rule 'udp_0_'
        option src 'lan'
        option proto 'udp'
        option dest_port ''
        option target 'ACCEPT'
        option src_port '501'

config rule 'udp_0_501'
        option src 'lan'
        option proto 'udp'
        option dest_port '501'
        option target 'ACCEPT'
```

The following firewall parameters are configured for IPv6 by default:

> show system firewall list ipv6

Execution results example:

```
config rule 'udp_1_1516'
        option src 'lan'
        option proto 'udp'
        option dest_port '1516'
        option target 'ACCEPT'

config rule 'udp_1_6053'
        option src 'lan'
        option proto 'udp'
        option dest_port '6053'
        option target 'ACCEPT'

config rule 'udp_1_3334'
        option src 'lan'
        option proto 'udp'
        option dest_port '3334'
        option target 'ACCEPT'

config rule 'udp_1_16092'
```

```
        option src 'lan'
        option proto 'udp'
        option dest_port '16092'
        option target 'ACCEPT'

config rule 'udp_1_51015'
        option src 'lan'
        option proto 'udp'
        option dest_port '51015'
        option target 'ACCEPT'

config rule 'udp_1_'
        option src 'lan'
        option proto 'udp'
        option dest_port ''
        option target 'ACCEPT'
        option src_port '501'

config rule 'udp_1_501'
        option src 'lan'
        option proto 'udp'
        option dest_port '501'
        option target 'ACCEPT'
```

7.6.3 Access Control List

The following parameters are displayed in the access-control list command:

> show system acl list all

The following ACL lists are configured by default in RSU.

```
IPv4  = 202.123.3.4
IPv6  = fd01:1
```

7.6.4 SNMP Notifications

The following parameters are displayed in the SNMP notifications command:

> show system snmp-notification all

Execution results example:

```
ipaddr                = FF02::25
port                  = 162
```

7.7 RSU Uptime Information

This section explains system and its applications uptime information. StreetWAVE™ also maintains an application specific counter containing number of application restarts.

Application -counter is reset to 0 in following scenarios:

1. RSU reboot/restart
2. Utils Standby & Run
3. System Upgrade

7.7.1 RSU uptime

RSU uptime shows the last system start-time.

Execute the following command to check the RSU system uptime details:

> show system uptime

Execution results example:

```
09:27:53 up  2:21,  load average: 2.18, 2.11, 2.12
```

7.7.2 GPS service uptime

GPS uptime shows the time since the GPS service was up and a restart-counter indicating number of application restarts since RSU uptime.

Execute the following command to check the GPS service uptime details:

> show system rsu-uptime gpsd

Execution results example:

```
up 10 days 03:50:15
restarted: 0 times
```

7.7.3 Service Manager

ServiceManager uptime shows the time since the service-manager was up and a restart-counter indicating number of application restarts since RSU uptime.

Execute the following command to check the service-manager uptime details:

> show system rsu-uptime smgrd

Execution results example:

```
up 10 days 03:50:45
restarted: 0 times
```

7.7.4 DSRC Message Forward

DSRC message forward service uptime shows the time since the dsrc message forward service was up and a restart-counter indicating number of application restarts since RSU uptime.

Execute the following command to check the DSRC message forward service uptime details:

> show system rsu-uptime dsrc-message-forward

Execution results example:

```
up 10 days 03:01:00
restarted: 0 times
```

7.7.5 **Store-Repeat Applications**

Store-Repeat service uptime shows the time since the Store-Repeat service was up and a restart-counter indicating number of application restarts since RSU uptime.

Execute the following command to check the Store-Repeat service uptime details:

> show system rsu-uptime store-repeat

Execution results example:

```
up 10 days 03:48:51
restarted: 0 times
```

7.7.6 **Immediate Forward Application**

Immediate forward service uptime shows the time since the Immediate forward service was up and a restart-counter indicating number of application restarts since RSU uptime.

Execute the following command to check the Immediate forward service uptime details:

StreetWAVE>> show system rsu-uptime immediate-forward

Execution results example:

```
up 10 days 3:47:038
restarted: 0 times
```

7.7.7 **TCD applications**

Traffic-Controller service uptime shows the time since the Traffic-controller daemon was up and a restart-counter indicating number of application restarts since RSU uptime.

Execute the following command to check the Traffic Controller daemon uptime details:

StreetWAVE>> show system rsu-uptime tcd

Execution results example:

```
up 10 days 03:12:29
restarted: 0 times
```

7.7.8 Security Services

Security service uptime shows the time since the Security service was up and a restart-counter indicating number of application restarts since RSU uptime.

Execute the following command to check the Security service uptime details:

StreetWAVE>> show system rsu-uptime security-services

Execution results example:

```
up 0 days 00:48:46
restarted: 0 times
```

7.7.9 Savari1609.3 Daemon Radio 1

Radio-1 uptime shows the time since the radio-1 was active and a restart-counter indicating number of the service had restarted

Execute the following command to check the Radio-1 uptime details:

> show system rsu-uptime savari16093d-radio1

Execution results example:

```
up 10 days 03:49:31
restarted: 0 times
```

7.7.10 Savari1609.3 Daemon Radio 2

Radio-2 uptime shows the time since the radio-2 was active and a restart-counter indicating number of the service had restarted

Execute the following command to check the Radio-2 uptime details:

> show system rsu-uptime savari16093d-radio2

Execution results example:

```
up 10 days 03:50:07
restarted: 0 times
```

7.7.11 Snmpd

SNMP-daemon uptime shows the time since the SNMP daemon was up and a restart-counter indicating number of application restarts since RSU uptime.

Execute the following command to check the SNMP daemon uptime details:

> show system rsu-uptime snmpd

Execution results example:

```
up 10 days 03:33:16
restarted: 0 times
```

7.7.12 IPv6 Provider Application

IPv6 provider application uptime shows the application start time and a restart-counter indicating number of application restarts since RSU uptime.

Execute the following command to check the Immediate forward service uptime details:

> show system rsu-uptime ipv6-provider

Execution results example:

```
up 10 days 03:51:16
restarted: 0 times
```

7.8 RSU Process List

StreetWAVE™ process-list provides a snapshot of currently running processes in the StreetWAVE.

Execute the following command to

> show system process-list

Execution results example:

```
  PID USER      VSZ STAT COMMAND
19832 root     1100 R    /usr/sbin/dropbear -F -P /var/run/dropbear.1.pid -p
19844 root     7996 S    /usr/local/bin/sav_cmd
22291 root     2960 S    /usr/local/bin/savari/rtcm_msg_fwd
22422 root     6292 S    /usr/local/bin/savari/immediate_forward
22423 root     7068 S    /usr/local/bin/savari/Tcd
```

8 System Maintenance

8.1 Log File Handling

RSU collects, stores and/or sends different types of log files when in service. This section provides details about log-file format and about handling log-files.

8.1.1 Types of StreetWAVE™ Logs

Interface Logs

This is a repository for all the packets received and transmitted from all interface radio 1, radio 2 and Ethernet.

System Logs

All the StreetWAVE™ system log-files such as application logs, monitoring-logs, etc.

Support Logs

Support logs generate additional log information for Savari Engineering team to debug and identifying root-cause of an issue.

8.1.2 Log File Name Format for Tx/Rx Packet(s)

TX/RX Packet log file names are in the following format:

<fileprefix>_<interface>_<out/in>_YYYY_MM_DD_HH_MM_SS.pcap, where

<fileprefix> is configured prefix

<interface> is eth/dsrc0/dsrc1

<out/in> is out for outgoing packets and in for incoming packets

YYYY_MM_DD_HH_MM_SS is the timestamp in UTC when the file was opened.

For example:

```
root@StreetWAVE:/nojournal/pcaplogs# pwd
/nojournal/pcaplogs
root@StreetWAVE:/nojournal/pcaplogs# ls -l
-rw-r--r-- 1 root    root       42808 Jul 20 00:47 StreetWAVE_eth_out_2011_07_20_00_47_26.pcap
-rw-r--r-- 1 root    root       1594308 Jul 20 01:01 StreetWAVE_dsrc0_in_2011_07_20_00_47_55.pcap
```

8.1.3 **Log Retrieval**

Users can copy log-files to a remote machine. The log files are encoded in simple text-format, and can be opened in any standard text-editor

Follow these steps to remove log-file(s) from StreetWAVE

NOTE: Replace <log file-type>, with interface-log or system-log,

1. List out all the log-filename(s).

   > utils list <log file-type>

2. Copy a log-file from StreetWAVE

   > utils copy src <log file-type>:<log-file-name>

   <remote_username>:scp://<remote-ip-address>:<destination path>

   Log-file-name: provide name of the log-file to be copied to remote-machine

   Remote_username: provide username of remote-machine

   Remote-ip-address: provide ip-address of remote machine

   Destination path: provide destination folder-path for copying log files

   Ex: utils copy src system-log:*syslog_2017_05_25_12_17_51.txt*

   savari:scp://192.168.10.1:home/savari/logs

NOTE: Logs have the following naming convention: *syslog_2017_05_25_12_17_51.txt*

8.1.4 **Log Deletion**

StreetWAVE™ by default purges old log files, once the directory occupancy of 80% (of the disk capacity) is reached. This helps StreetWAVE™ to make space for new log-files to be saved. Users can also delete selected log-files as needed.

NOTE: Ensure the files are copied before deleting them.

Follow these steps to remove log-file(s) from StreetWAVE

NOTE: Replace log file-type, with interface-log or system-log.

1. List out all the log-filename(s)

   > utils list <log file-type>

2. Delete a log-file from StreetWAVE

   > utils remove <log file-type> <log-file-name>

8.2 Support-Log Generation

StreetWAVE™ Support-log file contains a snapshot of StreetWAVE™ system state at a point of time. This log-file helps Savari Engineering team in identifying and solving errors.

Follow these steps to generate the support-log and to copy the file to local-machine.

1. Generate support-log file

   > show support-log

2. Copy support-log file to local-machine

   > utils copy support-log:../root/test.txt

   <remote_username>:scp://<remote_server_IP>:/<destination_path>

8.3 PCAP File Handling

8.3.1 Packet Logging Configuration

StreetWAVE™ generates per interface per direction packet log files as per configuration below. Log file names are in the following format:

- Ethernet interface outgoing : <fileprefix>_eth_out_YYYY_MM_DD_HH_MM_SS.pcap
- Ethernet interface incoming : <fileprefix>_eth_in_YYYY_MM_DD_HH_MM_SS.pcap
- DSRC0 interface outgoing : <fileprefix>_dsrc0_out_YYYY_MM_DD_HH_MM_SS.pcap
- DSRC0 interface incoming : <fileprefix>_dsrc0_in_YYYY_MM_DD_HH_MM_SS.pcap
- DSRC1 interface outgoing : <fileprefix>_dsrc1_out_YYYY_MM_DD_HH_MM_SS.pcap
- DSRC1 interface incoming : <fileprefix>_dsrc1_in_YYYY_MM_DD_HH_MM_SS.pcap

8.3.2 Retrieving the PCAP Files

The .pcap files can be retrieved only from StreetWAVE™ to any external device through SCP.

NOTE: Please use manual log file transfer when the system is in “standby” mode.

8.3.3 Deleting the PCAP Files

Once pcap files are copied out of StreetWAVE™, it is advisable to delete them from StreetWAVE™. This helps to conserve disk space on the StreetWAVE™ for further TX Packet logging. Check “Log deletion” process mentioned below for deleting files.

9 System Upgrade Procedure (Using CLI)

This section contains procedure to upgrade firmware.

Use the following procedure to upgrade **(5.x to 5.x)** the STREETWAVE™ firmware using the CLI:

1. Connect a local PC to the STREETWAVE™ via Ethernet.

   Note: If the StreetWAVE™ is already configured and part of a local-subnet, ensure the PC's IP-address is already added into the StreetWAVE™ ACL list.

2. After connecting the Ethernet to STREETWAVE™, assign the IP address to the PC, in the same subnet of the STREETWAVE™.

   StreetWAVE>> **sudo ifconfig eth0** < IP address for local-PC >

   IP address for local-PC: Assign an IP address to the PC in the same subnet of the SW-1000

3. Download the image to be upgraded from the Savari FTP site to the PC.

   For FTP site details and login credentials, please contact Savari-Support team at support@savari.net

4. Login to the STREETWAVE™ from the PC using SSH with the following credentials:

   Login: root

   Password: provide StreetWAVE™ root-password

   Default Root-Password: 1[8V:2<J5*W;2I16H1nu

5. Copy the firmware image using the CLI command in StreetWAVE

   StreetWAVE>> **utils copy** <remote_username>**:scp://**<ipaddr>**:**<path/to/file.image> **image:**<file.image>

   ex: utils copy savari:scp://tmp/SW1000/SW1000_rel_5.8.0.image image:new.image

6. After copying the file using the above command, verify the same using the below command.

   StreetWAVE>> **utils list rsu-image**

7. In the terminal (or putty) use one of the below mentioned option to initiate image upgrade using one of the below options:

   Replace <Firmware image name> with the name of the firmware image copied in the Image folder (/tmp)

   a. (suggested option) If you want to retain ONLY the network configuration data post upgradation:

```
StreetWAVE>> utils rsu-upgrade -n < Firmware image name >
```

b. For a clean installation (reset all configuration data in config-files):

Note: All configurations (including, network, and wireless) will be lost, and they may need to be configured again.

```
StreetWAVE>> utils rsu-upgrade -c < Firmware image name >
```

c. If you want to retain all the configuration information from the previous version:

```
StreetWAVE>> utils rsu-upgrade < Firmware image name >
```

Note: This is not recommended option, as any new configuration parameter added in the new image wouldn't get updated.