

**Plug Fest Interoperability Test Cases**

|  |  |
| --- | --- |
| Version: | 1.3 |
| Revision Date: | 5/3/2017 |

**Table of Contents**

[1 Scope 3](#_Toc481578613)

[1.1 References 3](#_Toc481578614)

[2 Abbreviations 4](#_Toc481578615)

[3 Prerequisites and Test Configurations 4](#_Toc481578616)

[3.1 Test Configurations 4](#_Toc481578617)

[4 WSM Packets 5](#_Toc481578618)

[4.1 Validation 5](#_Toc481578619)

[4.1.1 IOP TC WSM 1 5](#_Toc481578620)

[4.2 Transmit WSM with N Header / T Header 5](#_Toc481578621)

[4.2.1 IOP TC WSM 2 5](#_Toc481578622)

[4.2.2 IOP TC WSM 3 6](#_Toc481578623)

[4.2.3 IOP TC WSM 4 6](#_Toc481578624)

[4.3 Transmission of WSMs with payload exceeding WsmMaxLength 6](#_Toc481578625)

[4.3.1 IOP TC WSM 5 6](#_Toc481578626)

[4.4 WSM communications with continuous channel 7](#_Toc481578627)

[4.4.1 IOP TC WSM 6 7](#_Toc481578628)

[4.5 WSM communication with alternative channel access 7](#_Toc481578629)

[4.5.1 IOP TC WSM 7 7](#_Toc481578630)

[5 BSM 8](#_Toc481578631)

[5.1 Generation and reception 8](#_Toc481578632)

[5.1.1 IOP TC BSM 1 8](#_Toc481578633)

[5.1.2 IOP TC BSM 2 9](#_Toc481578634)

[5.1.3 IOP TC BSM 3 9](#_Toc481578635)

[5.1.4 IOP TC BSM 4 10](#_Toc481578636)

[5.1.5 IOP TC BSM 5 10](#_Toc481578637)

[5.1.6 IOP TC BSM 6 11](#_Toc481578638)

[5.1.7 IOP TC BSM 7 11](#_Toc481578639)

[6 WSA 12](#_Toc481578640)

[6.1 Transmission and reception 12](#_Toc481578641)

[6.1.1 IOP TC WSA 1 12](#_Toc481578642)

[6.1.2 IOP TC WSA 2 12](#_Toc481578643)

[6.1.3 IOP TC WSA 3 13](#_Toc481578644)

[6.1.4 IOP TC WSA 4 14](#_Toc481578645)

[6.1.5 IOP TC WSA 5 14](#_Toc481578646)

[6.1.6 IOP TC WSA 6 14](#_Toc481578647)

[7 IPv6 15](#_Toc481578648)

[7.1 IP Configuration 15](#_Toc481578649)

[7.1.1 IOP TC IP 1 15](#_Toc481578650)

[7.2 Communication using IPv6 16](#_Toc481578651)

[7.2.1 IOP TC IP 2 16](#_Toc481578652)

[7.2.2 IOP TC IP 3 16](#_Toc481578653)

[8 SPAT / MAP 17](#_Toc481578654)

[8.1 Transmission 17](#_Toc481578655)

[8.1.1 IOP TC SPATMAP 1 17](#_Toc481578656)

[8.1.2 IOP TC SPATMAP 2 18](#_Toc481578657)

[8.2 Reception and processing 18](#_Toc481578658)

[8.2.1 IOP TC SPATMAP 3 18](#_Toc481578659)

[8.2.2 IOP TC SPATMAP 4 18](#_Toc481578660)

[Revision History 19](#_Toc481578661)

[Known Issues 19](#_Toc481578662)

# Scope

This document provides the test cases expected to be conducted as a part of the Plugfest interoperability that will be held at Southwest Research Institute’s facilities in San Antonio, Texas in May of 2017. Some test cases may not be applicable if certificates are not available by the time of the Plugfest.

## References

The following referenced documents are necessary for the application of the present document.

[1] SAE J2945/1 MAR2016: “Surface Vehicle Standard - On-board System Requirements for V2V Safety Communications”

[2] SAE J2735 (2016-01): “Dedicated Short Range Communication (DSRC) Message Set Dictionary”

[3] IEEE Std. 802.11™-2012: “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”. Latest issue.

[4] IEEE Std. 1609.2-2016: "IEEE Draft Standard for Wireless Access in Vehicular Environments - security Services for Applications and Management Messages".

[5] IEEE Std 1609.3-2016 “IEEE Standard for Wireless Access in Vehicular Environments (WAVE) — Network Services”

[6] IEEE Std. 1609.4-2016 “IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation”.

[7] TCIS (V0.6.0): “Test Control Interface Specification.”: Revision date 4/21/2017, download from <https://github.com/certificationoperatingcouncil/TCI_ASN1>

[8] USDOT RSU Specification 4.1: “DSRC Roadside Unit (RSU) Specification Document v4.1

# Abbreviations

**SAE** Society of Automotive Engineers

**IEEE** Institute of Electrical and Electronics Engineers

**MAC** Media Access Control

**PHY** Physical Layer

**WAVE** Wireless Access in Vehicular Environments

**V2V** Vehicle-to-Vehicle

**DSRC** Dedicated Short Range Communications

**LAN** Local Area Network

**IUT** Implementation Under Test

**COC** Certification Operating Council

**RSU** Road Side Unit

**TCI** Test Control Interface

**IOP** Interoperability

**CFG** Configuration

**STD** Standard

**WSM** WAVE Short Message

**TPID** Transport Protocol Identifier

**PSID** Provider Service Identifier

**BSM** Basic Safety Message

**ID** Identifier

**WSA** Wave Service Advertisement

**TX** Transmit

**UDP** User Datagram Protocol

**IP** Internet Protocol

**IPv6** Internet Protocol Version 6

**I/F** Interface

# Prerequisites and Test Configurations

## Test Configurations

**IOP CFG 1**: Two IUTs are placed a short distance away from each other to allow for easy communication. One IUT may be replaced by a system provided by the COC specifically when an RSU functionality is required.

**IOP CFG 2**: IUT transmission is tested with a DSRC sniffer.

# WSM Packets

## Validation

### IOP TC WSM 1

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC WSM 1 | | |
| **Summary:** | Transmit WSM with version number and ethertype | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [5] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit WSMs  Device B can receive WSMs | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is configured to transmit WSM |
| 2 | Stimulus | Device A transmits WSM |
| 3 | Verify | Reception of WSM by Device B |
|  | 4 | Verify | Received WSM contains:   * uses EPD in the LLC sublayer * LLC sublayer contains Ethertype Type indicating value 0x88DC * WSM header version indicates version 3 |
|  |  |  |  |

## Transmit WSM with N Header / T Header

### IOP TC WSM 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC WSM 2 | | |
| **Summary:** | Transmit WSM with N Header containing WAVE Information Element Extensions | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [5] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit WSMs  Device B can receive WSMs | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is configured to transmit WSM containing WSM-N-Header containing:   * Channel Number * Data Rate * Transmit Power Used |
| 2 | Stimulus | Device A transmits WSM |
| 3 | Verify | WSM header information included in the WSM-N-Header WAVE Information Element Extensions matches actually used Channel Number, Data Rate and Transmit Power Used. |
|  | 4 | Verify | Device B received WSMs with WSM-N-Header containing WAVE Information Element Extensions |
|  | 5 | Procedure | Repeat Steps 1-4 using different Channels |
|  | 6 | Procedure | Repeat Steps 1-4 using different Data Rates |
|  | 7 | Procedure | Repeat Steps 1-4 using different Transmit Powers |
|  |  |  |  |

### IOP TC WSM 3

| **Identifier:** | IOP TC WSM 3 | | |
| --- | --- | --- | --- |
| **Summary:** | Transmit WSM with N Header without WAVE Information Element Extensions | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [5] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit WSMs  Device B can receive WSMs | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is configured to transmit WSM containing WSM-N-Header without any optional WAVE Information Element Extensions. |
| 2 | Stimulus | Device A transmits WSM |
| 3 | Verify | Actually used Channel Number, Data Rate corresponds those specified in the WSM configuration |
|  | 4 | Verify | Device B can receive and process WSMs with WSM-N-Header containing no WAVE Information Element Extensions |
|  | 5 | Procedure | Repeat Steps 1-4 using different Channels |
|  | 6 | Procedure | Repeat Steps 1-4 using different Data Rates |
|  | 7 | Procedure | Repeat Steps 1-4 using different Transmit Powers |
|  |  |  |  |

### IOP TC WSM 4

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC WSM 4 | | |
| **Summary:** | Transmit WSM with T Header, and WSM Data, testing different PSID lengths | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [5] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit WSMs  Device B can receive WSMs | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is configured to transmit WSM containing TPID, PSID, WSM Length, and WSM Data |
| 2 | Stimulus | Device A transmits WSM |
| 3 | Verify | Device B can receive and process WSMs |
|  | 4 | Verify | Repeat steps 1-3 for each PSID length i.e. 1, 2, 3, and 4 octets |
|  |  |  |  |

## Transmission of WSMs with payload exceeding WsmMaxLength

### IOP TC WSM 5

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC WSM 5 | | |
| **Summary:** | Confirm that WSM with payload exceeding WsmMaxLength are not transmitted | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [5] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit WSMs  Device B can receive WSMs  Channels and WSM Repeat Rate to be defined between two parties. | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is configured to transmit WSM with payload equal to WsmMaxLength – H – 1, where H is the length of the WSMP header (in octets). |
| 2 | Stimulus | Device A transmits WSM at defined channels and repeat rate |
| 3 | Verify | Device B **does** receive WSM from Device A |
|  | 4 | Configure | Device A is configured to transmit WSM with payload equal or greater to WsmMaxLength – H, where H is the length of the WSMP header (in octets). |
|  | 5 | Stimulus | Device A transmits WSM at defined channels and repeat rate |
|  | 6 | Verify | Device B **does not** detect/receive WSM from Device A |
|  |  |  |  |

## WSM communications with continuous channel

### IOP TC WSM 6

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC WSM 6 | | |
| **Summary:** | Transmit WSMs in continuous operation on a selected channel with specific repeat rate | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [5] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit WSMs  Device B can receive WSMs.  Channel and WSM Repeat Rate to be defined between two parties. | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is configured to transmit WSM |
| 2 | Stimulus | Device A transmits WSM at defined channel and repeat rate |
| 3 | Verify | Reception of WSM by Device B |
|  | 4 | Verify | Device B receives continuous streams of WSMs and verifies the channel used. |
|  | 5 | Verify | Average repeat period of the messages received by the Device B does not deviate from the expected (i.e. configured in Step 1) repeat period by more than 10%. Repeat period is defined as the inverse of the repeat rate. |
|  |  |  |  |

## WSM communication with alternative channel access

### IOP TC WSM 7

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC WSM 7 | | |
| **Summary:** | Transmit WSMs in alternating operation on selected channels | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [5] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit WSMs  Device B can receive WSMs  Channels and WSM Repeat Rate to be defined between two parties. | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is configured to transmit 2 streams of WSMs:   * WSM1 on CH1 during TimeSlot1 * WSM2 on CH2 during TimeSlot2   Where CH1 different from CH2 |
| 2 | Configure | Device B is configured to receive WSMs in alternating operation on   * CH1 during TimeSlot1 * CH2 during TimeSlot2 |
| 3 | Stimulus | Device A transmits WSM1 and WSM2s with defined repeat periods |
| 4 | Verify | Device B received both WSM1 and WSM2 on the corresponding channels. |
|  | 5 | Verify | Device B detects WSMs on defined channels |
|  | 6 | Verify | Average repeat period for WSM1 and WSM2 doesn’t vary from the specified repeat period (i.e. specified in Step 2) by more than 10%. |
|  | 7 | Configure | Change Device B configuration to receive WSMs on   * CH1 during TimeSlot2 * CH2 during TimeSlot1   (i.e. inverse time slots)  Device A continues to transmit WSM1 and WSM2 per Step 3 |
|  | 8 | Verify | Device B does not receive WSM1 and does not receive WSM2 |
|  |  |  |  |

# BSM

## Generation and reception

### IOP TC BSM 1

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC BSM 1 | | |
| **Summary:** | Generate valid BSM security header | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [4] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit BSMs  Device B can receive BSMs  Devices A and B loaded with necessary 1609.2 security credentials | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is configured to transmit BSM |
| 2 | Stimulus | Device A transmits BSMs using built-in default application rules |
| 3 | Verify | Emitted BSMs contain:   * protocol version and content in Ieee1609Dot2Data. * hashId in signedData. * Protocol version, content in tbsData. * Psid, generationTime * Does not include expiryTime, generationLocation in headerInfo |
|  | 4 | Verify | Device B received and verified BSM signatures successfully |
|  |  |  |  |

### IOP TC BSM 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC BSM 2 | | |
| **Summary:** | Test transmission and reception of “generic” BSMs | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [2] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit BSMs  Device B can receive BSMs  Devices A and B loaded with necessary 1609.2 security credentials | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is configured to transmit BSM |
| 2 | Stimulus | Device A transmits BSM |
| 3 | Verify | BSM is transmitted using WSM containing:   * Version = 3 * No optional WAVE Element Extensions included * PSID = 0p20 |
| 4 | Verify | WSM is signed using 1609.2 |
| 5 | Verify | BSM is transmitted using J2735 MSG\_MessageFrame containing BSMcoreData containing:   * msgCnt, * id * secMark * lat * long * elev * accuracy: semiMajor, semiMinor, orientation * transmission * speed * heading * angle * accelSet: long, lat, vert, yaw * brakes: wheelBrakes, traction, abs, scs, brakeBoost, auxBrakes * size: width, length |
| 6 | Verify | Device B can receive and decode BSMs |
|  |  |  |  |

### IOP TC BSM 3

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC BSM 3 | | |
| **Summary:** | Test transmission of BSMs with vehicle event flags | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [3] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit BSMs  Device B can receive BSMs  Devices A and B loaded with necessary 1609.2 security credentials  Event can be triggered in the BSM transmitter (Device A), e.g. using CAN interface, TCI interface or some other means, which will cause the Device A to emit BSMs and include Part II subframe. | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is transmitting BSM messages and no event flags activated. |
| 2 | Stimulus | An event flag triggered in Device A |
| 3 | Verify | BSM is transmitted using J2735 MSG\_MessageFrame containing BSMcoreData |
|  |  | MSG\_MessageFrame contains DF\_VehicleSafetyExtensions, which is constructed using the following elements (some elements are optional):   * events * pathHistory:   + initialPosition: utcTime, long, lat, elevation, heading, speed, posAccuracy, timeConfidence, posConfidence, speedConfidence   + currGNSSstatus   + crumbData: latOffset, lonOffset, elevationOffset, timeOffset, speed, posAccuracy (semiMajor, semiMinor, orientation), heading * pathPrediction: radiusOfCurve, confidence * lights |
|  |  |  |

### IOP TC BSM 4

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC BSM 4 | | |
| **Summary:** | Test message number rollover and Temporary ID of BSMs | | |
| **Configuration:** | IOP CFG 2 | | |
| **References:** | [4] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit BSMs  Devices A is loaded with necessary 1609.2 security credentials  Wireless sniffer to capture and analyze BSMs  BSM signing certificate doesn’t change during this test | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A transmit BSMs where DE\_MsgCount is less than 127 |
| 2 | Procedure | BSMs are captured using wireless sniffer for further analysis |
| 3 | Stimulus | Device A transmits BSM where DE\_MsgCount is greater than 1 |
| 4 | Verify | DE\_MsgCount is incremented by one for every BSM until it reaches 127, then the next BSM DE\_MsgCount is equal to one and continues to increment by one for subsequent BSMs. |
| 5 | Verify | DE\_TemporaryIDs is unchanged for all captured BSMs |

### IOP TC BSM 5

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC BSM 5 | | |
| **Summary:** | Test data randomization of BSMs | | |
| **Configuration:** | IOP CFG 2 | | |
| **References:** | [5] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit BSMs  Devices A is loaded with necessary 1609.2 security credentials  Wireless sniffer to capture and analyze BSMs | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A transmits BSM  Record DE\_MsgCount, DE\_TemporaryID and DSRC MAC Address |
| 2 | Stimulus | Restart Device A.  Use wireless sniffer to capture BSMs after the restart |
| 3 | Procedure | Record DE\_MsgCount, DE\_TemporaryID and DSRC MAC Address of the 1st BSM after the Device A restart |
| 4 | Procedure | Repeat steps 2-3 several times |
|  | 5 | Verify | DE\_MsgCount, DE\_TemporaryID and DSRC MAC Address are selected randomly after Device A restart |

### IOP TC BSM 6

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC BSM 6 | | |
| **Summary**: | Test that BSMs contain full certificates after vMaxCertDigestInterval (5min) or more has passed since the previous transmission of a certificate | | |
| **Configuration:** | IOP CFG 2 | | |
| **References:** | [4] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit BSMs  Devices A is loaded with necessary 1609.2 security credentials  Wireless sniffer to capture and analyze BSMs | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is configured to transmit BSM |
| 2 | Stimulus | Device A transmits BSM with the full certificate attached |
| 3 | Stimulus | Wait for the next BSM with full certificate attached to be transmitted |
| 4 | Verify | A BSM is transmitted with a full certificate attached within interval not exceeding vMaxCertDigestInterval |
|  |  |  |  |

### IOP TC BSM 7

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC WSM 7 | | |
| **Summary:** | Test whether IUT continues sending valid BSMs after receiving invalid data frames/elements | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [6] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit BSMs  Device B can receive BSMs  Devices A and B loaded with necessary 1609.2 security credentials | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | A test surrogate device is configured to transmit signed BSMs where 1609.2 signature cannot be successfully verified. (For this test special test setup may be required). |
| 2 | Stimulus | A series of improper BSMs transmitted |
| 3 | Verify | Device A continues sending valid BSMs throughout the test and ignore invalid BSMs |

# WSA

## Transmission and reception

### IOP TC WSA 1

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC WSA 1 | | |
| **Summary:** | Transmit WSM with valid WSM header and WSA payload message | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [5] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit WSAs  Device B can receive and process WSAs | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is configured to transmit WSAs containing:   * WSA Header   + Repeat Rate, 3D Location, Advertiser ID * Service Info (2 segments)   + Segment 1     - PSID, PSC   + Segment 2     - PSID, PSC, IPv6, Service Port, Provider MAC address * Channel Info Segment   + Channel Number, Power Level, Data Rate, Adaptable, EDCA values, alternating SCH |
| 2 | Stimulus | Device A transmits WSAs |
| 3 | Verify | WSA messages are transmitted as WSM with N-Header containing Subtype, TPID, PSID = 0p80-07 and WSM Data containing WSA in Ieee1609dot2Data, WSA version is 3 |
| 4 | Verify | WSA contents include all fields configured in step 1 |
| 5 | Verify | WSA transmitted with repeat period which vary by no more than 10% from the expected rate included in Step 1 |
| 6 | Verify | Device B received WSM/WSAs and updated its MIB UserAvailableServiceTable with WSA contents |
|  |  |  |  |

### IOP TC WSA 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC WSA 2 | | |
| **Summary:** | Transmit WSA containing WRA | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [5] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit WSAs  Device B can receive and process WSAs | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is configured to transmit WSAs containing:   * WSA Header   + Repeat Rate, 3D Location, Advertiser ID * Service Info (2 segments)   + Segment 1     - PSID, PSC, Channel Index   + Segment 2     - PSID, PSC, Channel Index, IPv6, Service Port, Provider MAC address, RcpiThreshold, WsaCountThreshold, WsaCountThresholdInterval * Channel Info Segment   + Channel Number, Power Level, Data Rate, Adaptable, EDCA values, alternating SCH * WAVE Router Advertisement   + Lifetime, ipPrefix, ipPrefixLength, defaultGateway, primaryDns, Gateway MAC, Secondary DNS |
| 2 | Stimulus | Device A transmits WSAs |
| 3 | Verify | WSA messages are transmitted as WSMs with N-Header containing Subtype, TPID, PSID = 0p80-07 and WSM Data containing WSA in Ieee1609dot2Data, WSA version is 3 |
| 4 | Verify | WSA contents include all fields configured in step 1 |
| 5 | Verify | WSA transmitted with repeat period which vary by no more than 10% from the expected rate included in Step 1 |
| 6 | Verify | Device B received WSM/WSAs and updated its MIB UserAvailableServiceTable with WSA contents |
|  |  |  |  |

### IOP TC WSA 3

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC WSA 3 | | |
| **Summary:** | Transmit WSA with valid 1609.2 security header | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [4] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit WSAs  Device B can receive and process WSAs | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is configured to transmit WSA |
| 2 | Stimulus | Device A transmits WSA |
| 3 | Verify | Received WSA contains:   * protocolVersion and content in Ieee1609Dot2Data. * protocolVersion and content in tbsData. * psid, generationTime, expirtyTime and generationLocation in headerInfo |
|  | 4 | Verify | Device B can receive WSA and updated its MIB UserAvailableServiceTable with WSA contents |
|  |  |  |  |

### IOP TC WSA 4

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC WSA 4 | | |
| **Summary:** | Checking validity of WSA signature | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [4] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit WSAs  Device B can receive and process WSAs  Required 1609.2 credentials are loaded on Device A and B | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is configured to transmit WSA with valid signature |
| 2 | Stimulus | Device A transmits WSA |
| 3 | Verify | Device B receives WSAs and verify WSA signature using certificate in WSA |
|  |  |  |  |

### IOP TC WSA 5

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC WSA 5 | | |
| **Summary:** | Detection of invalid WSAs | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [4] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A is configured to receive WSAs | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | A test surrogate device is configured to transmit signed WSA where WSA signature cannot be successfully verified. (For this test special test setup may be required). |
| 2 | Stimulus | WSA is transmitted |
| 3 | Verify | Device A received WSAs |
|  | 4 | Verify | Device A discards WSA which didn’t pass signature verification. |
|  |  |  |  |

### IOP TC WSA 6

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC WSA 6 | | |
| **Summary:** | Change WSA Contents | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [5] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit WSAs  Device B can receive and process WSAs | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A transmits WSAs containing one ServiceInfoSegment. |
| 2 | Configure | Device B receives WSAs updated its MIB UserAvailableServiceTable with the WSA contents |
| 3 | Stimulus | Device B added another service to the WSA ServiceInfoSegment |
| 4 | Verify | Device B receives WSAs and updated its MIB UserAvailableServiceTable to add the additional service |
|  | 5 | Stimulus | Device B deleted one of the services in the WSA ServiceInfoSegment |
|  | 6 | Verify | Device B receives WSAs and updated its MIB UserAvailableServiceTable to delete the service removed in step 5. |

# IPv6

## IP Configuration

### IOP TC IP 1

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC IP 1 | | |
| **Summary:** | Assignment and change of IPv6 address on OBU | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [5] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit WSAs  Device B can receive and process WSAs | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A transmits WSAs configured with the configuration parameters from the IOP TC WSA 2 Step 1 |
| 2 | Configure | Device B is configured to receive WSAs and join/activate service with PSID listed in the Service Info Segment 2 |
| 3 | Verify | Device B does not have IPv6 global address assigned to its DSRC radio interface |
| 4 | Stimulus | Device A transmits WSAs and Device B activates the PSID service |
| 5 | Verify | Device B DSRC radio is assigned link-local IPv6 address which is derived from Device B MAC address |
|  | 6 | Verify | Device B DSRC radio is assigned link-global IPv6 address, where the IPv6 address is derived from the WRA ipPrefix and Device B MAC address |
|  | 7 | Stimulus | Device A WSA transmissions stopped and Device B deactivate the service |
|  | 8 | Verify | Device B DSRC radio link-global IPv6 address is removed |
|  | 9 | Stimulus | Device A transmits WSAs and Device B activates the PSID service |
|  | 10 | Verify | Device B DSRC radio is assigned link-local IPv6 address different from the one used in step 5 (due to change in MAC address) |
|  | 11 | Verify | Device B DSRC radio is assigned link-global IPv6 address, where the IPv6 address is derived from the WRA ipPrefix and Device B MAC address (which changed compared to Step 6) |
|  | 12 | Procedure | Repeat steps 7 – 11 several times |
|  | 13 | Verify | Device B MAC address changes to new random values when Device B activates the WSA service, which lead to corresponding changes with link-local and link-global IPv6 addresses. |
|  |  |  |  |

## Communication using IPv6

### IOP TC IP 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC IP 2 | | |
| **Summary:** | IPv6 communication between RSU and OBU using link-local IPv6 | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [5] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A can transmit WSAs  Device B can receive and process WSAs | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A transmits WSAs configured with the configuration parameters from the IOP TC WSA 1 Step 1, where Service Info Segment 2   * IPv6 address is the link-local IPv6 of the Device A DSRC radio interface * Provider MAC Address is the MAC address of the DSRC radio of the Device A. |
| 2 | Configure | Device B is configured to receive WSAs and join/activate service with PSID listed in the Service Info Segment 2 |
| 3 | Stimulus | Device A transmits WSAs and Device B activates the PSID service |
| 4 | Verify | Device B DSRC radio is assigned link-local IPv6 address |
| 5 | Verify | Device B sends ping6 to the link-local IPv6 address of Device A and receives ping6 echo |
| 6 | Verify | Device A sends ping6 to the link-local IPv6 address of Device B and receives ping6 echo |
| 7 | Stimulus | Device A stops transmitting WSAs and Device B deactivates the PSID service |
| 8 | Verify | Device B sends ping6 to the link-local IPv6 address of Device A and receives no ping6 echo back |
| 9 | Verify | Device A sends ping6 to the link-local IPv6 address of Device B and receives no ping6 echo back |
|  |  |  |  |

### IOP TC IP 3

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC IP 3 | | |
| **Summary:** | IPv6 communication between RSU and OBU using link-global IPv6 | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [5] | | |
|  | | | |
| **Pre-test**  **conditions:** | Device A is configured to transmit WSAs.  Device A is connected to a PC laptop. Device A can ping laptop using link-global IPv6 address of the laptop and receive echo messages back  Device B is configured to receive WSAs | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A transmits WSAs configured with the configuration parameters from the IOP TC WSA 2 Step 1, where  For Service Info Segment 2   * IPv6 address is the link-global IPv6 of the PC laptop * Provider MAC Address is omitted   For WRA Info   * ipPrefix corresponds to the RSU DSRC radio network segment * defaultGateway is the link-global IPv6 of the RSU * Gateway MAC is the MAC addres of the RSU DSRC radio |
| 2 | Configure | Device B is configured to receive WSAs and join/activate service with PSID listed in the Service Info Segment 2 |
| 3 | Stimulus | Device A transmits WSAs and Device B activates the PSID service |
| 4 | Verify | Device B DSRC radio is assigned link-local and link-global IPv6 address |
| 5 | Verify | Device B sends ping6 to the link-global IPv6 address of the PC laptop and receives ping6 echo |
| 6 | Verify | PC laptop sends ping6 to the link-global IPv6 address of Device B and receives ping6 echo |
| 7 | Stimulus | Device A stops transmitting WSAs and Device B deactivates the PSID service |
| 8 | Verify | Device B sends ping6 to the link-global IPv6 address of PC laptop and receives no ping6 echo back |
| 9 | Verify | PC laptop sends ping6 to the link-global IPv6 address of Device B and receives no ping6 echo back |
|  |  |  |  |

# SPAT / MAP

## Transmission

### IOP TC SPATMAP 1

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC SPATMAP 1 | | |
| **Summary:** | Verify transmission of SPAT messages | | |
| **Configuration:** | IOP CFG 2 | | |
| **References:** | [8] | | |
|  | | | |
| **Pre-test**  **conditions:** | Channel is selected (default 172) for transmission of SPAT  Device A contains 1609.2 security credentials for SPAT/MAP | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is configured to use “Immediate Forward” application for SPAT messages. |
| 2 | Stimulus | SPAT messages sent via Ethernet to a UDP port on the Device A. |
|  | Verify | Device A transmits a WSM with PSID p80-02 on the selected channel |
|  | Verify | WSMs contain SPAT payload encoded per J2735 [2]  and required 1609.2 security envelope |
|  |  |  |

### IOP TC SPATMAP 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC SPATMAP 2 | | |
| **Summary:** | Verify transmission of MAP messages | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [8] | | |
|  | | | |
| **Pre-test**  **conditions:** | Channel is selected (default 172) for transmission of MAP  Device A contains 1609.2 security credentials for SPAT/MAP | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device A is configured to use Store & Forward application.  MAP message is loaded on the RSU using configuration file listed in [8] or RSU SNMP MIB |
| 2 | Stimulus | Device A transmits a WSMs with MAP |
| 3 | Verify | Device A transmits WSM with PSID p80-02 containing MAP message on the selected channel |
|  | 4 | Verify | WSMs contain MAP payload encoded per J2735 [2]  and required 1609.2 security envelope |

## Reception and processing

### IOP TC SPATMAP 3

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC SPATMAP 3 | | |
| **Summary:** | Verify reception of SPAT messages | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [8] | | |
|  | | | |
| **Pre-test**  **conditions:** | Channel is selected (default 172) for transmission of MAP  Device A and B contain 1609.2 security credentials for SPAT/MAP | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device B configured to receive WSM messages with PSID p80-02 |
| 2 | Stimulus | Device A transmits WSMs with PSID p80-02 containing SPAT messages on CH 172 |
| 3 | Verify | Device B receives WSMs on CH172 |
|  | 4 | Verify | Device B can decode the contents of the SPAT message |

### IOP TC SPATMAP 4

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier:** | IOP TC SPATMAP 4 | | |
| **Summary:** | Verify reception of MAP messages | | |
| **Configuration:** | IOP CFG 1 | | |
| **References:** | [8] | | |
|  | | | |
| **Pre-test**  **conditions:** | Channel is selected (default 172) for transmission of MAP  Device A and B contain 1609.2 security credentials for SPAT/MAP | | |
|  | | | |
| **Test Sequence:** | **Step** | **Type** | **Description** |
| 1 | Configure | Device B configured to receive WSM messages with PSID p80-02 |
| 2 | Stimulus | Device A transmits WSMs with PSID p80-02 containing MAP messages on CH 172 |
| 3 | Verify | Device B receives WSMs on CH172 |
|  | 4 | Verify | Device B can decode the contents of the MAP message |

Revision History

|  |  |  |
| --- | --- | --- |
| V1.1 | Nov 2016 | Version prepared for the Plugfest in Novi, MI |
| V1.2 | May 2017 | Revised previously defined test cases  Renumbered test cases  Added test cases for SPAT, MAP |
| V1.3 | May 2017 | Reworked Test Cases in BSM section  Updated test configurations |

Known Issues

None

◙ End of Document ◙