

PAWS
Internet-Draft
Intended status: Standards Track
Expires: April 6, 2013

V. Chen, Ed.
Google
S. Das
Applied Communication Sciences
Z. Lei
Huawei
J. Malyar
Telcordia Technologies Inc.
P. McCann
Huawei
October 3, 2012

Protocol to Access Spectrum Database
draft-vchen-paws-protocol-00

Abstract

Portions of the radio spectrum that are allocated to licensees are available for non-interfering use. This available spectrum is called "White Space." Allowing secondary users access to available spectrum "unlocks" existing spectrum to maximize its utilization and to provide opportunities for innovation, resulting in greater overall spectrum utilization.

One approach to manage spectrum sharing uses databases to report spectrum availability to devices. To achieve interoperability among multiple devices and databases, a standardized protocol must be defined and implemented. This document defines such a protocol, the "Protocol to Access White Space database" (PAWS).

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 6, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	4
2. Conventions and Terminology	4
2.1. Conventions Used in This Document	4
2.2. Terminology	5
3. Protocol Overview	5
4. Protocol Functionalities	6
4.1. Indicating Errors	6
4.2. Database Discovery	6
4.3. Initialization	7
4.3.1. INIT_REQ	7
4.3.2. INIT_RESP	8
4.4. Device Registration	9
4.4.1. REGISTRATION_REQ	9
4.4.2. REGISTRATION_RESP	10
4.5. Available Spectrum Query	10
4.5.1. AVAIL_SPECTRUM_REQ	13
4.5.2. AVAIL_SPECTRUM_RESP	14
4.5.3. AVAIL_SPECTRUM_BATCH_REQ	15
4.5.4. AVAIL_SPECTRUM_BATCH_RESP	16
4.5.5. SPECTRUM_USE_NOTIFY	18
4.5.6. SPECTRUM_USE_RESP	19
4.6. Device Validation	19
4.6.1. DEV_VALID_REQ	21
4.6.2. DEV_VALID_RESP	21
5. Protocol Parameters	22
5.1. ProtocolInfo	22
5.2. ResponseInfo	22
5.3. GeoLocation	23
5.3.1. Regulatory Specifics	23
5.4. DeviceIdentifier	24

5.4.1. Regulatory Specifics	24
5.5. AntennaCharacteristics	25
5.5.1. Regulatory Specifics	25
5.6. DeviceCapabilities	25
5.7. DeviceOwner	26
5.8. RulesetInfo	27
5.8.1. RegulatorySpecifics	27
5.9. Spectrum	28
5.10. FrequencyRange	28
5.11. EventTime	29
5.12. SpectrumSchedule	29
5.13. GeoSpectrumSchedule	30
5.14. DeviceValidity	30
5.15. Response Codes	31
6. Message Encoding	31
7. HTTPS Binding	31
8. Example Messages	32
9. IANA Considerations	32
10. Security Considerations	32
10.1. Assurance of Proper Database	33
10.2. Protection Against Modification	33
10.3. Protection Against Eavesdropping	33
10.4. Client Authentication Considerations	33
11. Contributors	34
12. Acknowledgments	34
13. References	35
13.1. Normative References	35
13.2. Informative References	35
Appendix A. Changes / Author Notes	35
Authors' Addresses	36

1. Introduction

This section provides some high level introductory material. Readers are strongly encouraged to read [I-D.ietf-paws-problem-stmt-usecases-rqmts] for use cases, requirements, and additional background.

A geospatial database can track available spectrum (in accordance with the rules of one or more regulatory domains) and make this information available to devices. This approach shifts the complexity of spectrum-policy conformance out of the device and into the Database. This approach also simplifies adoption of policy changes, limiting updates to a handful of databases, rather than numerous devices. It opens the door for innovations in spectrum management that can incorporate a variety of parameters, including user location and time. In the future, it can include other parameters, such as user priority, time, signal type and power, spectrum supply and demand, payment or micro-auction bidding, and more.

In providing this service, a database records and updates information necessary to protect primary users -- for example, this information may include parameters such as a fixed transmitter's call sign, its geo-location, antenna height, power, and periods of operation. The rules that the Database must follow, including its schedule for obtaining and updating protection information, protection rules, and information reported to devices, vary according to regulatory domain. Such variations, however, should be handled by each database, and exposure to the variations by devices should be minimized.

This specification defines an extensible protocol to obtain available spectrum from a geospatial database by a device with geo-location capability. It enables a device to operate in any regulatory domain that implements the same protocol and in which the device is authorized to operate. The document describes the use of HTTP/TLS as transport for the protocol.

2. Conventions and Terminology

2.1. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2.2. Terminology

Database or Spectrum Database: A database that provides spectrum availability information to devices.

Master Device: A device with geo-location capability that queries a database to find available spectrum.

Slave Device: A device without geo-location capability that uses the spectrum made available by a Master Device. It does not query the Database directly.

RAT: Radio Access Technology

3. Protocol Overview

A Master Device uses the PAWS protocol to obtain a schedule of available spectrum at its location. The security necessary to ensure the accuracy, privacy, and confidentiality of the Device's location is described in the Security Considerations (Section 10). This document assumes that the Master Device and the Database are connected to the Internet.

A typical sequence of PAWS operations is outlined as follows. See Protocol Functionalities (Section 4) and Protocol Parameters (Section 5) for details:

1. The Master Device locates or discovers the regulatory domain for its location and the URI for the Database to send subsequent PAWS messages. [Editor's Note: It is an open item whether database discovery should be a separate document.]
2. The Master Device establishes an HTTPS session with database.
3. The Master Device optionally sends an initialization message to the Database to exchange capabilities.
4. If the Database receives an initialization message, it responds with a message in the body of the HTTP response.
5. If required by regulatory domain, the Database registers the Master Device.
6. The Master Device sends an available-spectrum request message to the Database.
7. If the Master Device is obtaining the schedule on behalf of a Slave Device, if required by the regulatory domain, the Database validates the Slave Device.
8. The database responds with an available-spectrum response message in the body of the HTTP response.
9. Depending on regulatory domain requirements and database implementation, the Master Device sends a spectrum-usage notification message to the Database.

10. If the Database receives a spectrum-usage notification message, it responds by sending the Master Device a spectrum-usage acknowledgement message.

4. Protocol Functionalities

The PAWS protocol consists of several components:

- o Database Discovery (Section 4.2) MUST be supported by Master Device
- o Initialization (Section 4.3) MAY be used by the Master Device and MUST be implemented by the Database.
- o Device Registration (Section 4.4) MAY be used by the Master Device and MAY be implemented by the Database.
- o Available Spectrum Query (Section 4.5) MUST be supported by Master Device and the Database.
- o Device Validation (Section 4.6) MAY be used by the Master Device and MUST be implemented by the Database if the regulatory domain requires device validation.

This section describes the protocol components and their messages. Section 5 contains a more thorough discussion of the parameters that comprise the PAWS request and response messages. Section 6 provides details of the message encodings. Section 7 describes the use of HTTPS [RFC2818] for transporting PAWS messages and optional device authentication.

4.1. Indicating Errors

Each PAWS response messages contains a "responseInfo" parameter (see Section 5.2). When the Database encounters an error, it MUST report the error code using the "responseInfo" parameter and SHOULD include an optional error message. The message MAY be in any language. When the Database reports an error, it MAY omit otherwise required portions of the response message.

Note that all PAWS-level errors are reported within a successful transport-level response, e.g., 200 OK HTTPS response. Valid error codes are listed in Section 5.15.

4.2. Database Discovery

A device MUST determine the URI for the Database and applicable regulatory domain before it can send PAWS messages. The URI for the Database SHOULD be obtained from an authorized and authenticated entity, but it MAY be statically configured into the device.

[Editor's Note: It is an open item whether database discovery should

be a separate document.]

4.3. Initialization

A Master Device SHOULD use the initialization procedure to exchange capability information with the Database whenever the Master Device powers up or initiates communication with the Database. The initialization response informs the Master Device of specific regulatory-dependent parameterized-rule values, such as threshold distances and time periods beyond which the device must update its available-spectrum data (see Section 5.8). The Master Device MAY manually configure these parameterized-rule values. The initialization messages also represents extension points for database implementations or regulatory domains that require the extra handshake.

The Initialization request procedure is depicted in Figure 1.

- o INIT_REQ (Section 4.3.1) is the initialization request message
- o INIT_RESP (Section 4.3.2) is the initialization response message

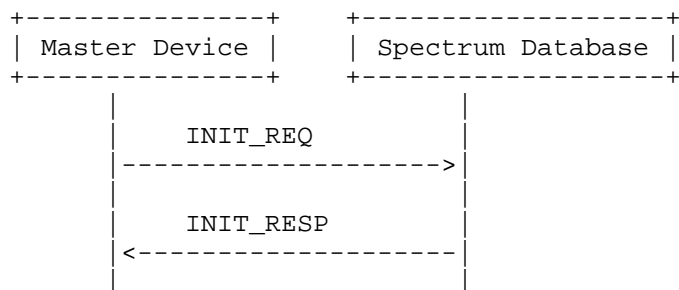


Figure 1

4.3.1. INIT_REQ

The initialization request message allows a device to initiate exchange of capabilities with a database.

INIT_REQ	
protocolInfo:ProtocolInfo	required
deviceId:DeviceIdentifier	required
location:GeoLocation	required
.....
*other:any	depends

Parameters:

protocolInfo: The protocol info (Section 5.1) for this message is REQUIRED. The "messageType" parameter MUST be "INIT_REQ".

deviceId: The device identifier (Section 5.4) for the device is REQUIRED. If the Database does not support the regulatory domain specified by the "authority" parameter, it MUST return an error code (TBD value) in the response.

location: The geo-location (Section 5.3) for the device is REQUIRED.

other: Depending on the regulatory domain or database implementation, the Master Device MAY specify additional handshake parameters in the INIT_REQ message. A database MUST ignore all parameters it does not understand.

4.3.2. INIT_RESP

The initialization response message communicates database parameters to the requesting device.

+-----+ INIT_RESP +-----+	
protocolInfo:ProtocolInfo	required
responseInfo:ResponseInfo	required
rulesetInfo:RulesetInfo	required*
.....
*other:any	depends
+-----+	

Parameters:

protocolInfo: The protocol info (Section 5.1) for this message is REQUIRED. The messageType parameter MUST be "INIT_RESP".

responseInfo: The response info (Section 5.2) is REQUIRED and contains the response code, timestamp, etc.

rulesetInfo: This ruleset info (Section 5.8) parameter MUST be included in the response if "responseInfo" does not contain an error code. If there is an error, "rulesetInfo" MUST NOT be included in the response message. This parameter specifies the regulatory domain and parameters applicable for that domain. The database MUST specify the same "authority" as that specified in the "deviceId" parameter of the INIT_REQ message.

other: Depending on the regulatory domain or database implementation, the Database MAY include additional handshake parameters in the INIT_RESP message. The Master Device MUST ignore all parameters it does not understand.

4.4. Device Registration

When a regulatory domain requires registration of a Master Device, the device **MUST** send its registration information to the Database to establish certain operational parameters. FCC rules, for example, require that a 'Fixed Device' **MUST** register its owner and operator contact information, its device identifier, its location, and its antenna height.

The database **MAY** support device registration as a separate Device Registration component, or as part of the Spectrum Availability component. If a database does not support a separate Device Registration request, it **MUST** return an error in the registration response message.

The Device Registration request procedure is depicted in Figure 2.

- o REGISTRATION_REQ (Section 4.4.1) is the device-registration request message
- o REGISTRATION_RESP (Section 4.4.2) is the device-registration response message

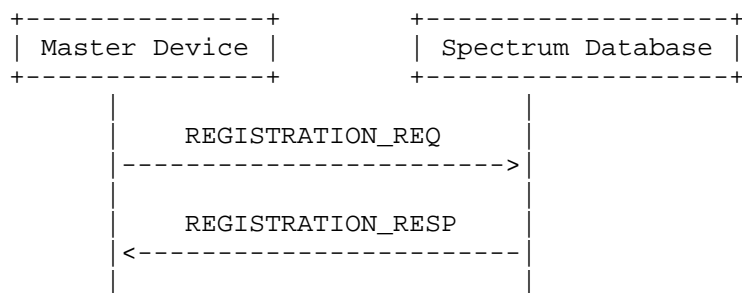


Figure 2

4.4.1. REGISTRATION_REQ

The registration request message contains the required registration parameters.

REGISTRATION_REQ	
protocolInfo:ProtocolInfo	required
deviceId:DeviceIdentifier	required
location:GeoLocation	required
deviceOwner:DeviceOwner	required
.....
*other:any	depends

```
+-----+-----+
```

Parameters:

protocolInfo: The protocol info (Section 5.1) for this message is REQUIRED. The "messageType" parameter MUST be "REGISTRATION_REQ".

deviceId: The device identifier (Section 5.4) for the device is REQUIRED.

location: The geo-location (Section 5.3) for the device is REQUIRED.

deviceOwner: The device-owner (Section 5.7) information is REQUIRED.

other: Regulatory domains MAY require additional registration parameters. To simplify its registration logic, a device MAY send a union of the registration information required by all supported regulatory domains. A database MUST ignore all parameters it does not understand.

4.4.2. REGISTRATION_RESP

The registration response message simply acknowledges receipt of the request.

```
+-----+
|REGISTRATION_RESP|
+-----+
|protocolInfo:ProtocolInfo| required|
|responseInfo:ResponseInfo| required|
+-----+
```

Parameters:

protocolInfo: The protocol info (Section 5.1) for this message is REQUIRED. The "messageType" parameter MUST be "REGISTRATION_RESP".

responseInfo: The response info (Section 5.2) is REQUIRED and contains the response code, timestamp, etc.

4.5. Available Spectrum Query

To obtain the available spectrum from a database, a Master Device sends a request that contains its geo-location and any parameters required by the regulatory rules (such as device identifier, capabilities, and characteristics). The database returns a response that describes what frequencies are available, at what permissible operating power levels, and a schedule of when they are available.

The Available Spectrum Query procedure is depicted in Figure 3.

- o AVAIL_SPECTRUM_REQ (Section 4.5.1) is the available-spectrum request message
- o AVAIL_SPECTRUM_RESP (Section 4.5.2) is the available-spectrum response message
- o AVAIL_SPECTRUM_BATCH_REQ (Section 4.5.3) is an OPTIONAL batch version of the available-spectrum request message that allows multiple locations to be specified in the request
- o AVAIL_SPECTRUM_BATCH_RESP (Section 4.5.4) is the response message for the batch version of the available-spectrum request that contains available spectrum for each location
- o SPECTRUM_USE_NOTIFY (Section 4.5.5) is the spectrum-usage notification message
- o SPECTRUM_USE_RESP (Section 4.5.6) is the spectrum-usage acknowledgment message

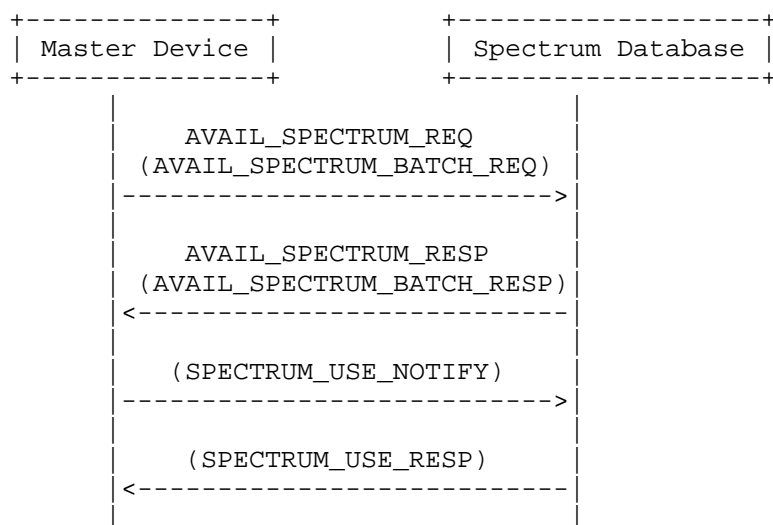


Figure 3

1. First, the Master Device sends an available-spectrum request message to a database.
2. The database it MUST respond with an error message (error code TBD) if:
 - * registration information is required, and
 - * the request does not include registration information, and
 - * the device has not previously registered
3. If the location specified in the request is outside the regulatory domain, the Database MUST respond with an error message (error code TBD).

4. The database MAY perform other validation of the request, (e.g., checking for missing required parameters, authorizations). It MUST return an error message with appropriate error code, if validation fails.
5. If the request is valid, the Database responds with an available-spectrum response message. If the regulatory domain requires that devices must report anticipated spectrum usage, the Database MUST indicate so in the response message.
6. If the available-spectrum response indicates that the Master Device must send a spectrum-usage notification message, the Master Device MUST send the notification message to the Database.
7. If the Database receives a spectrum-usage notification message, it MUST send a spectrum-usage acknowledgment message to the Master Device.

The procedure for asking for available spectrum on behalf of a slave device is similar, except that the process is initiated by the slave device. Also, the device identifier, capabilities, and characteristics communicated in the AVAIL_SPECTRUM_REQ message SHALL be those of the slave device. Although the communication and protocol between the slave device and Master Device is outside the scope of this document, the expected message sequence is shown in Figure 4.

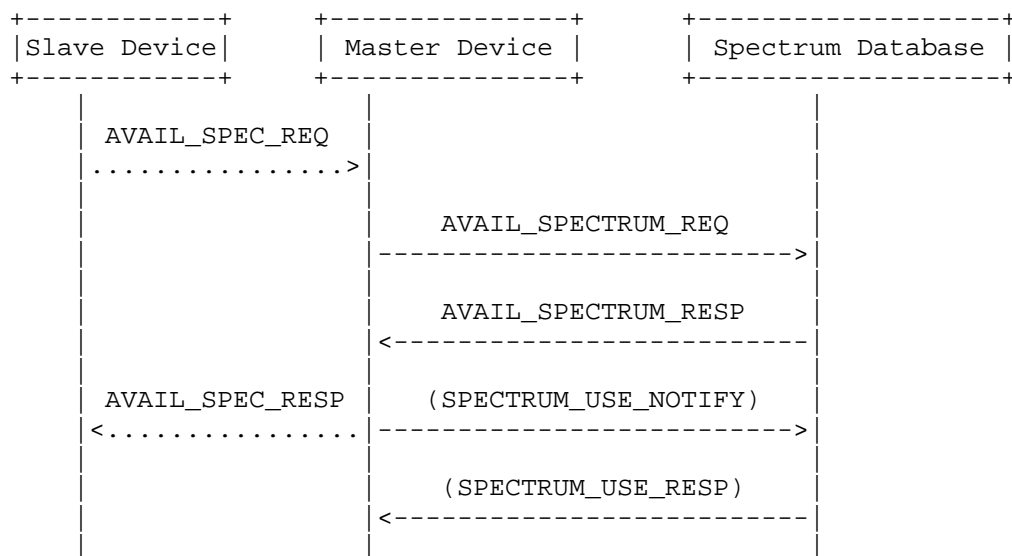


Figure 4

4.5.1. AVAIL_SPECTRUM_REQ

The request message for the Available Spectrum Query protocol MUST include the device's geo-location.

+-----+ AVAIL_SPECTRUM_REQ +-----+	
protocolInfo:ProtocolInfo	required
deviceId:DeviceIdentifier	required
location:GeoLocation	required
antenna:AntennaCharacteristics	depends on regulatory domain
owner:DeviceOwner	depends on regulatory domain
capabilities:DeviceCapabilities	optional
+-----+	

Parameters:

protocolInfo: The protocol info (Section 5.1) for this message is REQUIRED. The "messageType" parameter MUST be "AVAIL_SPECTRUM_REQ".

deviceId: The device identifier (Section 5.4) for the device is REQUIRED.

location: The geo-location (Section 5.3) for the device is REQUIRED. The location SHOULD be the current location of the device. Depending on the regulatory domain, the location MAY be an anticipated position of the device.

antenna: Depending on the device type and regulatory domain, the antenna characteristics (Section 5.5) MAY be required.

owner: Depending on the device type and regulatory domain, the device owner (Section 5.7) information MAY be included to register the device with the Database. This enables a device to register and get spectrum-availability information in a single request.

capabilities: The Master Device MAY include its device capabilities (Section 5.6) to limit the available-spectrum response to the spectrum that is compatible with its capabilities. The database SHOULD NOT return spectrum that is not compatible with the specified capabilities.

4.5.1.1. Regulatory Specifics

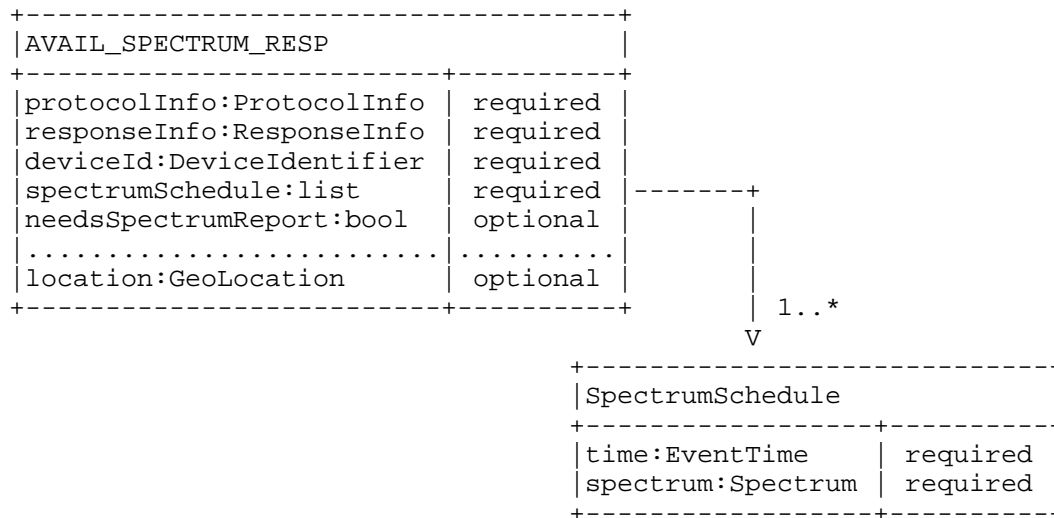
For the US / FCC TV-Band devices:

- o The "antenna" parameter is REQUIRED for FIXED device types. It MUST specify the antenna height and height type.
- o The "owner" parameter is REQUIRED for FIXED device types and if the device has not been registered yet with the Database or if the Database does not implement a separate device registration

request.

4.5.2. AVAIL_SPECTRUM_RESP

The response message for the Available Spectrum Query contains a schedule of available spectrum for the device.



Parameters:

protocolInfo: The protocol info (Section 5.1) for this message is REQUIRED. The "messageType" parameter MUST be "AVAIL_SPECTRUM_RESP"

responseInfo: The response info (Section 5.2) is REQUIRED and contains the response code, timestamp, etc.

deviceId: The database MUST include the device identifier (Section 5.4) specified in the AVAIL_SPECTRUM_REQ message

spectrumSchedule: The schedule (Section 5.12) of available spectrum. The Database MAY return more than one schedule to represent future changes to the available spectrum. How far in advance a schedule may be provided depends on the regulatory domain.

needsSpectrumReport: For regulatory domains that require a spectrum-usage report from devices, the Database MUST return true for this parameter. The default value is false.

location: The database MAY copy other elements from the request, such as the geo-location (Section 5.3) of the device. The device MUST ignore any parameters it does not understand.

When the stop time specified in the schedule has been reached, a device:

- o MUST obtain a new spectrum-availability schedule, either by using the next one in the list (if provided) or making another Available Spectrum Query (Section 4.5)
- o If the new schedule indicates the in-use spectrum is no longer available, the device MUST stop operation immediately.
- o If the device is unable to contact the Database to obtain a new schedule, depending on the regulatory domain, the device MAY continue to operate for a period of time, as indicated by parameters returned in the INIT_RESP (Section 4.3.2) message.

When the device moves beyond a threshold distance (established by regulatory rules) away from the actual location and all anticipated location(s) it reported in previous AVAIL_SPECTRUM_REQ or AVAIL_SPECTRUM_BATCH_REQ requests (see "maxLocationChange" in Section 5.8), it:

- o MUST obtain a new spectrum-availability schedule by making another Available Spectrum Query (Section 4.5).
- o If the new response indicates the in-use spectrum is no longer available, the device MUST stop operation immediately.
- o If the device is unable to contact the Database to obtain a new schedule, depending on the regulatory domain, the device MUST stop operation immediately.

4.5.3. AVAIL_SPECTRUM_BATCH_REQ

The Database MAY support the batch request that allows multiple locations to be specified. This allows a portable Master Device to get available spectrum for a sequence of anticipated locations using a single request. Each location is treated independently such that a single batch request is equivalent to multiple AVAIL_SPECTRUM_REQ (Section 4.5.1) requests. The request message for the batch Available Spectrum Query protocol MUST include at least one geo-location. If the Database does not support batch requests, it MUST return a NOT_SUPPORTED error.

+-----+ AVAIL_SPECTRUM_BATCH_REQ +-----+		
protocolInfo:ProtocolInfo	required	
deviceId:DeviceIdentifier	required	
locations:list	required	--+
antenna:AntennaCharacteristics	depends on regulatory domain	
owner:DeviceOwner	depends on regulatory domain	
capabilities:DeviceCapabilities	optional	1..*
+-----+		V
		+-----+
		GeoLocation
		+-----+

Parameters:

protocolInfo: The protocol info (Section 5.1) for this message is REQUIRED. The "messageType" parameter MUST be "AVAIL_SPECTRUM_BATCH_REQ".

deviceId: The device identifier (Section 5.4) for the device is REQUIRED.

locations: The list of geo-locations (Section 5.3) for the device is REQUIRED. This allows a device to specify its actual location plus additional anticipated locations, when allowed by the regulatory domain. At least one location MUST be included. This specification places no upper limit on the number of locations, but the Database MAY restrict the number of locations it supports by returning a response with fewer locations than specified in the request.

antenna: Depending on the device type and regulatory domain, the antenna characteristics (Section 5.5) MAY be required.

owner: Depending on the device type and regulatory domain, the device owner (Section 5.7) information MAY be included to register the device with the Database. This enables a device to register and get spectrum-availability information in a single request.

capabilities: The Master Device MAY include its device capabilities (Section 5.6) to limit the available-spectrum response to the spectrum that is compatible with its capabilities. The database SHOULD NOT return spectrum that is not compatible with the specified capabilities.

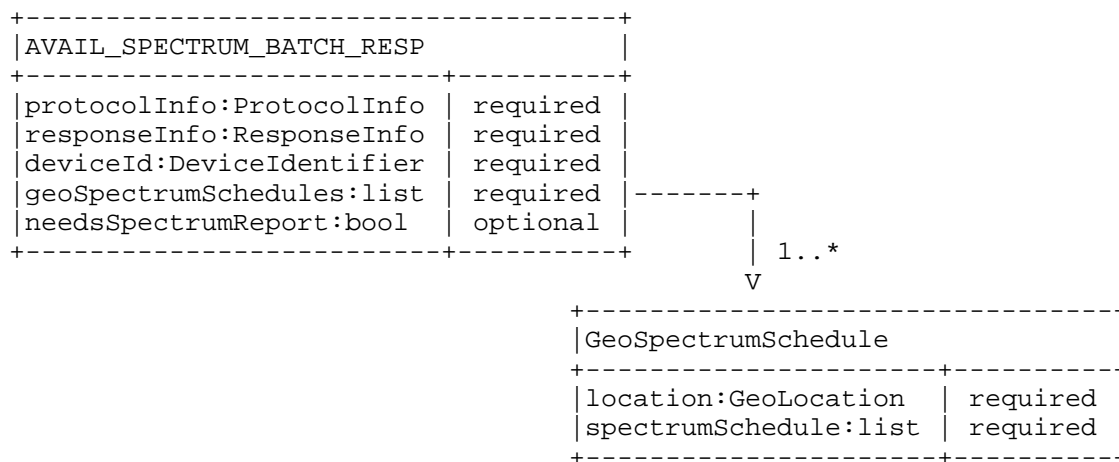
4.5.3.1. Regulatory Specifics

For the US / FCC TV-Band devices:

- o The "antenna" parameter is REQUIRED for FIXED device types. It MUST specify the antenna height and height type.
- o The "owner" parameter is REQUIRED for FIXED device types and if the device has not been registered yet with the Database or if the Database does not implement a separate device registration request.

4.5.4. AVAIL_SPECTRUM_BATCH_RESP

The response message for the batch Available Spectrum Query contains a schedule of available spectrum for the device at multiple locations.



Parameters:

protocolInfo: The protocol info (Section 5.1) for this message is REQUIRED. The "messageType" parameter MUST be "AVAIL_SPECTRUM_BATCH_RESP"

responseInfo: The response info (Section 5.2) is REQUIRED and contains the response code, timestamp, etc.

deviceId: The database MUST include the device identifier (Section 5.4) specified in the AVAIL_SPECTRUM_REQ message

geoSpectrumSchedules: The list of spectrum-availability schedules for a location (Section 5.13) is REQUIRED. For each location, the Database MAY return more than one schedule to represent future changes to the available spectrum. How far in advance a schedule may be provided depends on the regulatory domain. The Database MAY return available spectrum for fewer locations than requested. The Device MUST NOT make any assumptions on the order of the entries in the list and MUST use the location value in each GeoSpectrumSchedule entry to match available spectrum to a location.

needsSpectrumReport: For regulatory domains that require a spectrum-usage report from devices, the Database MUST return true for this parameter. The default value is false.

When the stop time specified in the schedule has been reached, a device:

- o MUST obtain a new spectrum-availability schedule, either by using the next one in the list (if provided) or making another Available Spectrum Query (Section 4.5)

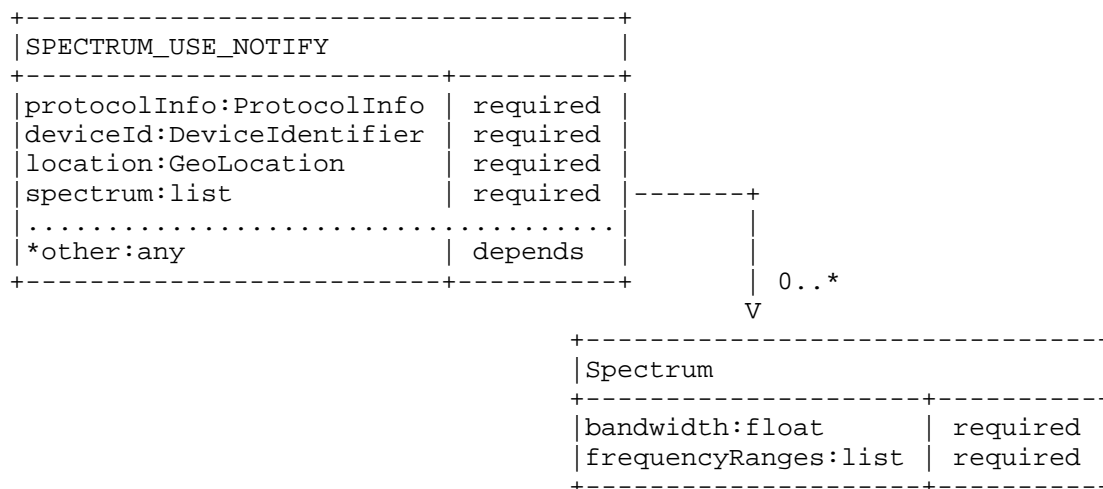
- o If the new schedule indicates the in-use spectrum is no longer available, the device MUST stop operation immediately.
- o If the device is unable to contact the Database to obtain a new schedule, depending on the regulatory domain, the device MAY continue to operate for a period of time, as indicated by parameters returned in the INIT_RESP (Section 4.3.2) message.

When the device moves beyond a threshold distance (established by regulatory rules) away from all actual or anticipated location(s) it reported in the AVAIL_SPECTRUM_BATCH_REQ message (see "maxLocationChange" in Section 5.8), it:

- o MUST obtain a new spectrum-availability schedule by making another Available Spectrum Query (Section 4.5).
- o If the new schedule indicates the in-use spectrum is no longer available, the device MUST stop operation immediately.
- o If the device is unable to contact the Database to obtain a new schedule, depending on the regulatory domain, the device MUST stop operation immediately.

4.5.5. SPECTRUM_USE_NOTIFY

The spectrum-use notification message MUST contain the geo-location of the device and parameters required by the regulatory domain.



Parameters:

protocolInfo: The protocol info (Section 5.1) for this message is REQUIRED. The "messageType" parameter MUST be "SPECTRUM_USE_NOTIFY".

deviceId: The device identifier (Section 5.4) for the device is REQUIRED.

location: The geo-location (Section 5.3) for the device is REQUIRED.

spectrum: The spectrum (Section 5.9) is REQUIRED and specifies the spectrum anticipated to be used by the device, which includes frequency ranges and maximum power levels. For consistency, the "bandwidth" value SHOULD match that from one of the Spectrum elements in the corresponding AVAIL_SPECTRUM_RESP message, and the maximum power levels in the Spectrum element MUST be expressed as total power (EIRP) computed over the specified "bandwidth" value. The actual bandwidth to be used (as computed from the start and stop frequencies) MAY be different from the "bandwidth" value. As an example, when regulatory rules express maximum power spectral density in terms of maximum power over any 100 kHz band, then the "bandwidth" value should be set to 100 kHz, even though the actual bandwidth used is 20 kHz.

other: Depending on the regulatory domain, other parameters MAY be required. To simplify its logic, the device MAY include the union of all parameters required by all supported regulatory domains. The database MUST ignore all parameters it does not understand.

4.5.6. SPECTRUM_USE_RESP

The spectrum-use response message simply acknowledges receipt of the notification.

```
+-----+
|SPECTRUM_USE_RESP|
+-----+
|protocolInfo:ProtocolInfo| required |
|responseInfo:ResponseInfo| required |
+-----+
```

Parameters:

protocolInfo: The protocol info (Section 5.1) for this message is REQUIRED. The "messageType" parameter MUST be "SPECTRUM_USE_RESP"

responseInfo: The response info (Section 5.2) is REQUIRED and contains the response code, timestamp, etc.

4.6. Device Validation

Typically, a slave device needs a Master Device to ask the Database on its behalf for available spectrum. Depending on the regulatory domain, the Master Device also must validate with the Database that

the slave device is permitted to operate. When regulatory rules allow a Master Device to "cache" the available spectrum for a period of time, the Master Device MAY use the simpler Device Validation component, instead of the full Available Spectrum Query component, to validate a slave device.

When validating one or more slave devices, the Master Device sends the Database a request that includes the device identifier -- and any other parameters required by the regulatory rules -- for each slave device. The database returns a response that indicates whether each device is permitted to use the spectrum.

A typical sequence for using the Device Validation request is illustrated in Figure 5, where the Master Device already has a valid set of available spectrum for slave devices. Note that the communication and protocol between the slave device and Master Device is outside the scope of this document.

- o DEV_VALID_REQ (Section 4.6.1) is the device-validation request message
- o DEV_VALID_RESP (Section 4.6.2) is the device-validation response message

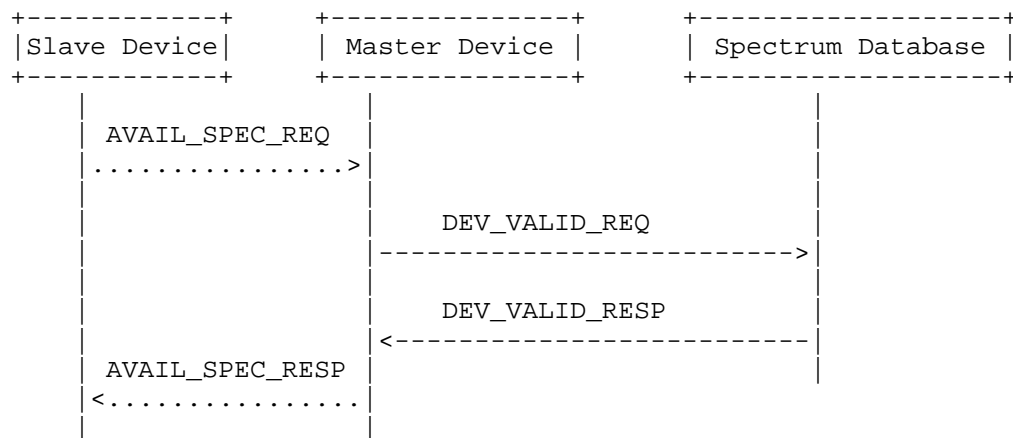
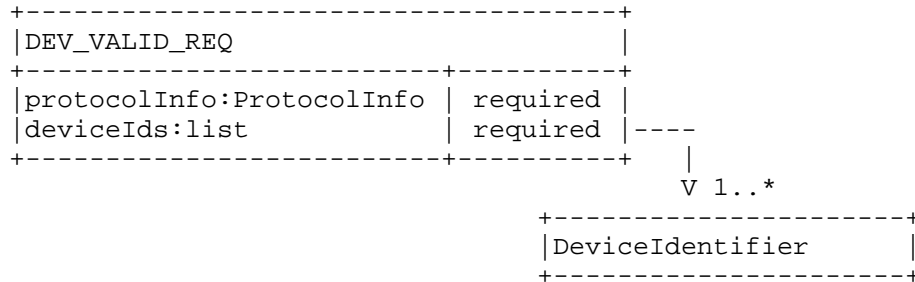


Figure 5

4.6.1. DEV_VALID_REQ

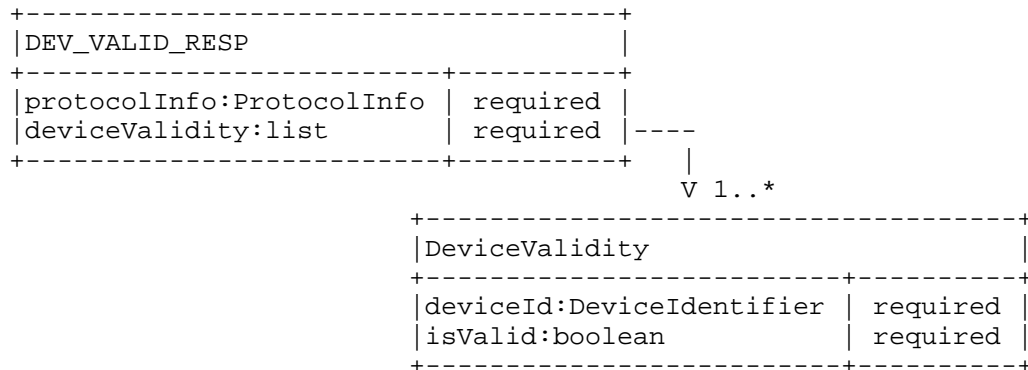


Parameters:

protocolInfo: The protocol info (Section 5.1) for this message is REQUIRED. The "messageType" parameter MUST be "DEV_VALID_REQ".

deviceIds: A list of device identifiers Section 5.4 is REQUIRED to specify the list of slave devices that must be validated.

4.6.2. DEV_VALID_RESP



Parameters:

protocolInfo: The protocol info (Section 5.1) for this message is REQUIRED. The "messageType" parameter MUST be "DEV_VALID_RESP".

deviceValidity: A list of device validity elements Section 5.14 is REQUIRED to report the list of slave devices and corresponding code of whether the device is valid. The number of entries MUST match the number of device IDs specified in the DEV_VALID_REQ message.

5. Protocol Parameters

This section presents the more details of parameters that make up the PAWS request and response messages. It also includes a sub-section defining response codes.

5.1. ProtocolInfo

All PAWS request and response messages MUST include the ProtocolInfo parameter:

+-----+		
ProtocolInfo		
+-----+		
version:string		required
messageType:string		required
+-----+		

Parameters:

version: Version of the PAWS protocol is REQUIRED. It MUST be the string, "1.0". If the data receives a request message containing a version it does not support, it MUST respond with an error message.

messageType: Name of the message type is REQUIRED. It specifies the name of its containing message.

5.2. ResponseInfo

All PAWS response messages MUST include the ResponseInfo parameter:

+-----+		
ResponseInfo		
+-----+		
code:string		required
message:string		optional
timestamp:string		optional
responseId:string		optional
.....		
*other:any		optional
+-----+		

Parameters:

code: The result code is REQUIRED. If the Database needs to respond with an error, it MUST set this to a defined error code. Valid values for result and error codes are TBD.

message: The message is OPTIONAL. When the result code is an error code, the Database SHOULD include a message that provides more details. The message MAY be in any language.

timestamp: The database MAY include the timestamp of the response. When provided, it MUST be in the form, YYYY-MM-DDThh:mm:ssZ, as defined by [RFC3339]. It MUST be expressed in UTC.

responseId: The database MAY include a unique ID for the response.

other: The database MAY include additional error details. The device MUST ignore any parameters it does not understand.

NOTE: When there is an error, the Database MUST include ResponseInfo in the response message, but MAY omit otherwise required portions of the response message.

5.3. GeoLocation

This parameter is used to specify the geo-location of the device.

+-----+ GeoLocation +-----+	
latitude:float	required
longitude:float	required
uncertainty:float	depends on regulatory domain
confidence:int	depends on regulatory domain
+-----+	

Parameters:

latitude, longitude: Floating-point numbers that express the latitude and longitude in degrees using the WGS84 datum. REQUIRED.

uncertainty: The uncertainty of the location in meters MAY be required, depending on the regulatory domain. When this parameter is optional, its default value is 0.

confidence: The location confidence level as an integer percentage MAY be required, depending on the regulatory domain. When the parameter is optional, its default value is 100.

5.3.1. Regulatory Specifics

For UK / Ofcom UHF TV-band devices:

- o The "uncertainty" parameter is REQUIRED if the uncertainty is greater than 50 meters.

5.4. DeviceIdentifier

The device identifier contains parameters that identify the specific device, such as its manufacturer serial number, and regulatory-specific ID (e.g., FCC ID), and any other regulatory-specific information, such as device-type classification.

DeviceIdentifier	
authority:string	required
serialNumber:string	required
identity:string	required
.....
*deviceType:string	depends on regulatory domain
*RAT:string	depends on regulatory domain
*other:any	

Parameters:

authority: A string that indicates the regulatory domain to which the device identifier applies is REQUIRED. It MUST use the 2-letter country codes defined by [ISO3166-1].

serialNumber: The manufacturer's device serial number is REQUIRED.

identity: The device's regulatory domain ID is REQUIRED.

Additional parameters in the DeviceIdentifier depend on each regulatory domain, and must be defined on a per-domain basis.

5.4.1. Regulatory Specifics

For the US / FCC TV-Band devices:

- o The authority value MUST be "US"
- o The identity value is the device's FCC ID
- o The "deviceType" parameter is REQUIRED to indicate the device type. Valid values are FIXED, MODE_1, MODE_2

For UK / Ofcom TV-Band devices:

- o The authority value MUST be "UK"
- o The "RAT" parameter is required to specify the Radio Access Technology. Valid values are TBD.
- o A "deviceClass" parameter is required to identify, among other things, the emission mask of the device. Valid values are TBD.

5.5. AntennaCharacteristics

Antenna characteristics provide additional information, such as the antenna height, antenna type, etc. Whether antenna characteristics must be provided in a request depends on the device type and regulatory domain.

AntennaCharacteristics	
height:float	depends on regulatory domain
heightType:enum	optional
heightUncertainty:float	depends on regulatory domain
.....
*characteristics: various	depends on regulatory domain

Parameters:

height: The antenna height in meters. Whether the antenna height is required depends on the device type and the regulatory domain.

heightType: If the height is required, then heightType is also REQUIRED. Valid values are:

- AGL Above ground level (default)
- AMSL Above mean sea level

heightUncertainty: The height uncertainty in meters. Whether this is required depends on the regulatory domain.

Depending on the regulatory authority, additional antenna characteristics may be required, such as:

- o antenna direction
- o antenna radiation pattern
- o antenna gain
- o antenna polarization

5.5.1. Regulatory Specifics

For the US / FCC TV-Band devices:

- o The height and heightType parameters are REQUIRED for FIXED device types.

5.6. DeviceCapabilities

Device capabilities provide additional information that MAY be used by the device provide additional information to the Database they may help it to determine available spectrum. If a database does not support device capabilities it MUST ignore the parameter altogether.

+-----+ DeviceCapabilities +-----+	
frequencyRange:list	optional +-----+

Parameters:

frequencyRange: Optional list of frequency ranges (Section 5.10)--- start and stop frequencies --- in which the device can operate. When specified, the Database SHOULD NOT return available spectrum that falls outside these ranges.

5.7. DeviceOwner

This parameter contains device-owner information required as part of device registration. Regulatory domains MAY require additional parameters. The minimum set of parameters are described below.

+-----+ DeviceOwner +-----+	
owner:string	required
operator:string	required
address:string	required
email:string	required
phone:string	required +-----+

Parameters:

owner: Name of the individual or business that owns the device is REQUIRED.
operator: Name of the device operator is REQUIRED.
address: Civic address of the device owner or operator of the device is REQUIRED.
email: Email address of the device owner or operator of the device is REQUIRED.
phone: Phone number of the device owner or operator of the device is REQUIRED.

NOTE: Whether the contact information must be that of the device owner or operator depends on the regulatory domain. Depending on the regulatory domain, the Database MAY be required to validate the device-owner information. In these cases, the Database MUST respond with an error message if validation fails.

5.8. RulesetInfo

This contains parameters for the rule set of a regulatory domain that is communicated using the Initialization component (Section 4.3).

+-----+ RulesetInfo +-----+		
authority:string		required
maxLocationChange:float		required
maxPollingSecs:int		required
maxValiditySecs:int		required
.....		
*other:any		depends
+-----+		

Parameters:

authority: A string that indicates the regulatory domain to which the ruleset applies is REQUIRED. It MUST use the 2-letter country codes defined by [ISO3166-1].

maxLocationChange: The maximum location change in meters is REQUIRED. When a device changes location by more than this specified distance, it MUST contact the Database to get the available spectrum for the new location. If the device is using spectrum that is no longer available, it MUST stop operation in those frequencies immediately.

maxPollingSecs: The maximum duration, in seconds, between requests for available spectrum is REQUIRED. The device MUST contact the Database to get available spectrum no less frequently than this duration. If the new spectrum information indicates that the device is using spectrum that is no longer available, it MUST stop operation in those frequencies immediately.

maxValiditySecs: The maximum duration that the available-spectrum information may be considered valid is REQUIRED. When a device is unable to contact the Database, it MAY continue to use the latest available- spectrum information at its location until its validity expires. The expiration is determined by adding maxValiditySecs to the timestamp of the AVAIL_SPECTRUM_RESP that provided the latest available-spectrum information.

other: This message is intended to be extensible with other regulatory-specific parameters. Devices MUST ignore all parameters in the message it does not understand.

5.8.1. RegulatorySpecifics

For the US / FCC TV-band rules:

- o "authority" MUST be the string, "US"
- o "maxLocationChange" MUST be 50 meters
- o "maxPollingSecs" MUST be 86400 seconds, corresponding to 24 hours
- o "maxValiditySecs" MUST be 172800 seconds, corresponding to 48 hours

5.9. Spectrum

Available spectrum can logically be characterized by a list of frequency ranges and permissible power levels for each range.

+-----+ Spectrum +-----+			
bandwidth:float		required	+-----+ FrequencyRange +-----+
frequencyRanges:list		required	
+-----+		1..*	+-----+ startHz:float required stopHz:float required maxPowerDBm:float optional channelId:string optional +-----+

Parameters:

bandwidth: This parameter is REQUIRED to define the operating bandwidth for which permissible power levels is to be specified. For example, FCC regulation would require only one spectrum specification at 6MHz bandwidth, but Ofcom regulation would require 2 specifications, at 0.1MHz and 8MHz.

frequencyRanges: A list of FrequencyRange (Section 5.10) objects is REQUIRED to specify frequency ranges and permissible power levels.

5.10. FrequencyRange

The FrequencyRange parameter specifies the maximum permissible power levels within a frequency range.

startHz: The inclusive start of the frequency range is REQUIRED

stopHz: The exclusive end of the frequency range is REQUIRED

maxPowerDBm: The maximum total power level (EIRP) -- computed over the corresponding operating bandwidth -- that is permitted within the frequency range. Depending on the context in which the FrequencyRange element appears, maxPowerDBm may be REQUIRED. For example, it is REQUIRED in the AVAIL_SPECTRUM_RESP (Section 4.5.2) and SPECTRUM_USE_NOTIFY (Section 4.5.5) messages, but it would not be used to describe Device Capabilities (Section 5.6).

channelId: The server MAY include a channel identifier, when applicable. When it is included, the Master Device SHOULD treat it as informative.

NOTE: (maxPowerDBm / bandwidth) defines the maximum permitted EIRP spectral density.

5.11. EventTime

The EventTime element specifies the start and stop times of an "event". This is used to indicate the time period for which a Spectrum (Section 5.9) is valid.

```
+-----+
|EventTime|
+-----+
|startTime:string|required|
|stopTime:string|required|
+-----+
```

Parameters:

startTime: The inclusive start of the event is REQUIRED.

stopTime: The exclusive end of the event is REQUIRED.

Both times are expressed using the format, YYYY-MM-DDThh:mm:ssZ, as defined by [[RFC3339]]. The times MUST be expressed using UTC.

5.12. SpectrumSchedule

The SpectrumSchedule element combines EventTime with Spectrum to define a time period in which the spectrum is valid.

```
+-----+
|SpectrumSchedule|
+-----+
|eventTime:EventTime|required|
|spectrum:list|required|----->+-----+
+-----+1..*+-----+
|bandwidth:float|
|frequencyRange:list|
+-----+
```

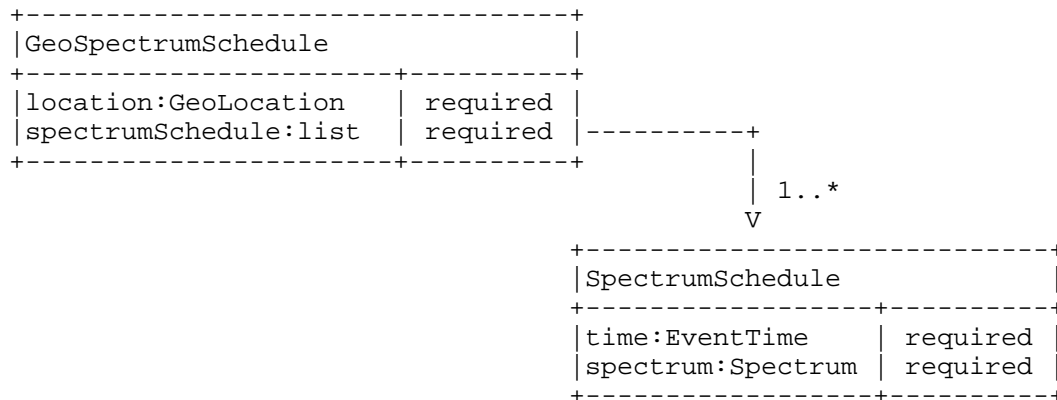
Parameters:

eventTime: The time period (Section 5.11) is REQUIRED to express "when" this specification is valid.

spectrum: List of Spectrum (Section 5.9) elements is REQUIRED to specify the available spectrum and permissible power levels, one per bandwidth.

5.13. GeoSpectrumSchedule

The GeoSpectrumSchedule element encapsulates the schedule of available spectrum at a location.



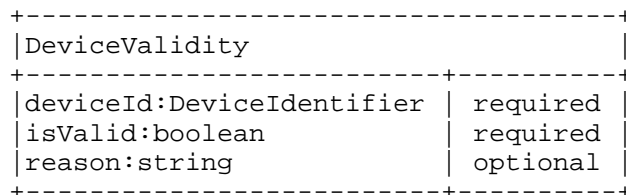
Parameters:

location: The location (Section 5.3) is REQUIRED to identify the location at which the spectrum schedule applies

location: The list of spectrum schedules (Section 5.12) is REQUIRED. At least one schedule MUST be included. More than one schedule MAY be included to represent future changes to the available spectrum.

5.14. DeviceValidity

The DeviceValidity element is used to indicate whether a device is valid. See Section 4.6.2.



Parameters:

deviceId: The device identifier (Section 5.4) that was used to check for validity. This is REQUIRED.

isValid: A REQUIRED boolean value that indicates whether the device is valid.

reason: If the device identifier is not valid, the Database MAY include a reason. The reason MAY be in any language.

5.15. Response Codes

TBD

6. Message Encoding

TBD

7. HTTPS Binding

This section describes the use of HTTP over TLS (HTTPS) [RFC2818] as the transport mechanism for the PAWS protocol. TLS provides message integrity and confidentiality between the Master Device and the Database. The Master Device MUST implement server authentication, as described in Section 3.1 of [RFC2818]. The device uses the URI determined (either statically configured or dynamically discovered) to authenticate the server. The device SHOULD fail a request if server authentication fails.

Depending on prior relationship between a database and device, the server MAY require client authentication, as described in The TLS Protocol [RFC5246], to authenticate the device.

To enable databases to handle large numbers of requests from large numbers of devices, the Database MAY support and devices SHOULD support Stateless TLS Session Resumption [RFC5077].

A PAWS request message is carried in the body of an HTTP POST request. A PAWS response message is carried in the body of an HTTP response. A PAWS response SHOULD include a Content-Length header.

The POST method is the only method REQUIRED for PAWS. If a database chooses to support GET, it MUST be an escaped URL, but the encoding of the URL is outside the scope of this document. The database MAY refuse to support the GET request by returning an HTTP error code, such as 404 (not found).

The Database MAY redirect a PAWS request. The Master Device MUST handle redirects by using the Location header provided by the server

in a 3xx response. When redirecting, the Master Device MUST observe the delay indicated by the Retry-After header. The Master Device MUST authenticate the Database that returns the redirect response before following the redirect. The Master Device MUST authenticate the Database indicated in the redirect.

8. Example Messages

TBD

9. IANA Considerations

TBD

10. Security Considerations

PAWS is a protocol whereby a Master Device requests a schedule of available spectrum at its location (or location of its slave devices) before it (they) can operate using those frequencies. Whereas the information provided by the Database must be accurate and conform to applicable regulatory rules, the Database cannot enforce, through the protocol, that a client device uses only the spectrum it provided. Specific requirements and security considerations for the PAWS protocol are described in [I-D.ietf-paws-problem-stmt-usecases-rqmts].

By using the PAWS protocol, the Master Device and the Database expose themselves to the following risks:

- o Accuracy: The Master Device receives incorrect spectrum-availability information.
- o Privacy: An unauthorized entity intercepts identifying data for the Master Device, such as serial number and location.

Protection from these risks depends on the success of the following steps:

1. The Master Device must determine a proper database.
2. The Master Device must connect to the proper database.
3. The database must determine or compute accurate spectrum-availability information.
4. PAWS messages must be transmitted unmodified between the Database and the Master Device.
5. PAWS messages must be encrypted to between the Database and the Master Device to prevent exposing private information.

6. For a slave device, the spectrum-availability information also must be transmitted unmodified and secure between the Master Device and the slave device, but that is outside the scope of the PAWS protocol.

Of these, only steps 2, 4, and 5 are within the scope of this document. [Editor's note: It is still open whether Step 1 is within the scope of this document]. Step 3 dependent on specific database implementations and regulatory rules and is outside the scope of this document. Step 6 requires a protocol between master and slave devices and is thus outside the scope of this document.

10.1. Assurance of Proper Database

This document assumes that the Database is contacted using a domain name or an IP address. Using HTTP over TLS [RFC2818], the Database authenticates its identity, either as a domain name or IP address, to the Master Device by presenting a certificate containing that identifier as a "subjectAltName" (i.e., as a dNSName or IP address). If the Master Device has external information as to the expected identity or credentials of the proper database (e.g., a certificate fingerprint), these checks MAY be omitted. Note that in order for the presented certificate to be valid at the client, the client must be able to validate the certificate. In particular, the validation path of the certificate must end in one of the client's trust anchors, even if that trust anchor is the Database certificate itself. [Editor's note: certificates can change certificate authorities (CAs) over time. Should there be a recommendation about not relying on a single, statically configured CA certificate in the Master Device?]

10.2. Protection Against Modification

To prevent a PAWS response message from being modified en route, messages must be transmitted over an integrity-protected channel. Using HTTP over TLS, the channel will be protected by appropriate cyphersuites.

10.3. Protection Against Eavesdropping

Using HTTP over TLS, messages protected by appropriate cyphersuites are also protected from eavesdropping or otherwise access by unauthorized parties en route

10.4. Client Authentication Considerations

Although the Database can inform a device of available spectrum it can use, the Database cannot enforce that the device uses any/only those frequencies. Indeed, a malicious device can operate without

ever contacting a database. Consequently, client authentication is not required for the PAWS protocol. Depending on prior relationship between a database and device, the Database may require client authentication. TLS provides client authentication, but there are some considerations:

- o As indicated in Section 3.2 of [RFC2818], the TLS client authentication procedure only determines that the device has a certificate chain rooted in an appropriate CA. The database would not know what the client identity ought to be, unless it has some external source of information. Distribution and management of such information, including revocation lists, are outside the scope of this document.
- o Authentication schemes are secure only to the extent that secrets or certificates are kept secure. When there are a vast number of devices in the world using PAWS, the possibility that device keys will not leak becomes small. Implementations should consider how to manage the system in the eventuality that there is a leak.

11. Contributors

This document draws heavily from the following Internet Draft documents, [I-D.das-paws-protocol] and [I-D.wei-paws-framework]. The editor would like to specifically call out and thank the contributing authors of these two documents.

Donald Joslyn
Spectrum Bridge Inc.
1064 Greenwood Blvd.
Lake Mary, FL 32746
U.S.A.
Email: d.joslyn at spectrumbridge dot com

Xinpeng Wei
Huawei
Phone: +86 13436822355
Email: weixinpeng@huawei.com

12. Acknowledgments

The authors gratefully acknowledge the contributions of: Gabor Bajko, Teco Boot, Nancy Bravin, Rex Buddenberg, Gerald Chouinard, Stephen Farrell, Michael Fitch, Joel M. Halpern, Donald Joslyn, Jussi Kahtava, Warren Kumari, Paul Lambert, Andy Lee, Anthony Mancuso,

Peter McCann, Basavaraj Patil, Scott Probasco, Brian Rosen, Andy Sago, Peter Stanforth, John Stine, and Juan Carlos Zuniga.

13. References

13.1. Normative References

- [ISO3166-1] "Country Codes",
<http://www.iso.org/iso/country_codes.htm>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3339] Klyne, G., Ed. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, July 2002.
- [RFC5077] Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State", RFC 5077, January 2008.
- [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

13.2. Informative References

- [I-D.das-paws-protocol] Das, S., Malyar, J., and D. Joslyn, "Device to Database Protocol for White Space", draft-das-paws-protocol-02 (work in progress), July 2012.
- [I-D.ietf-paws-problem-stmt-usecases-rqmts] Probasco, S. and B. Patil, "Protocol to Access White Space database: PS, use cases and rqmts", draft-ietf-paws-problem-stmt-usecases-rqmts-08 (work in progress), August 2012.
- [I-D.wei-paws-framework] Wei, X., Zhu, L., and P. McCann, "PAWS Framework", draft-wei-paws-framework-00 (work in progress), July 2012.
- [RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

Appendix A. Changes / Author Notes.

Notes:

- o For date-time format this is referencing RFC3339, instead of ISO8601 as discussed on the list, since it is more precise in its definition and is a real RFC. Is that acceptable?
- o Change needed: maxValidityTime in RulesetInfo doesn't work for US/FCC, since the rule indicates 11:59 of following day (no timezone specified), which cannot be expressed as a duration

Authors' Addresses

Vincent Chen (editor)
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

Email: vchen@google.com

Subir Das
Applied Communication Sciences
444 Hoes Lane
Piscataway, NJ 08854
U.S.A.

Phone:
Fax:
Email: sdas at appcomsci dot com
URI:

Zhu Lei
Huawei

Phone: +86 13910157020
Fax:
Email: lei.zhu@huawei.com
URI:

John Malyar
Telcordia Technologies Inc.
1 Ericsson Drive
Piscataway, NJ 08854
U.S.A.

Phone:
Fax:
Email: jmalyar at telcordia dot com
URI:

Peter J. McCann
Huawei
400 Crossing Blvd, 2nd Floor
Bridgewater, NJ 08807
USA

Phone: +1 908 541 3563
Fax:
Email: peter.mccann@huawei.com
URI:

PAWS
Internet-Draft
Intended status: Informational
Expires: January 10, 2013

Y. Wu
Y. Cui
Huawei
July 9, 2012

Protocol to Access White Space database: security considerations
draft-wu-paws-secutity-00.txt

Abstract

PAWS is an access protocol between the Master device and the White Space (WS) Database. Master Devices connect to the white space database directly using WS interface, but only authorized devices can get the service from database. If an attacker can have full access to the network medium between the master device and the database, the attacker may deploy varieties of attacks on the network if there is lack of security mechanism.

The present document describes the security threats to the current framework of PAWS, and meanwhile proposes the corresponding countermeasures.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 10, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction	4
2. Conventions and terminology	4
2.1. Conventions used in this Document	4
2.2. Terminology	4
3. Overview of Security threats and Requirements	5
3.1. Fundamental system architecture of PAWS	5
3.2. Security threats	5
3.2.1. Impersonation of a master device	6
3.2.2. Impersonation of database	6
3.2.3. MitM on the interface between master device and database	6
3.2.4. Attacks on the link of interface between master device and database	6
3.2.5. Attacks on the master device itself	7
3.2.6. Other potential attacks(To be added)	7
3.3. Security countermeasures	7
4. Security schemes	8
4.1. Overview	8
4.2. Analysis of security schemes	8
4.2.1. Databases deployed by third-party	8
4.2.2. Databases deployed by regulatory body of white space	12
4.3. TLS protocol	13
4.3.1. Brief introduction of TLS protocol	13
4.3.2. Security establishment procedure between master device and database	13
4.3.3. Drawbacks of TLS protocol	15
5. Security Considerations	15
6. IANA Considerations	15
7. Acknowledgments	15
8. Normative Reference	16
Authors' Addresses	16

1. Introduction

Portions of the radio spectrums that are allocated to a licensed, primary user but are unused or unoccupied at specific locations and times are defined as "white space". The concept of allowing secondary transmissions (licensed or unlicensed) in white space is a technique to "unlock" existing spectrum. Currently, the widely accepted scheme of utilizing white space is by querying the database and the related protocol "Protocol to Access White Space database (PAWS)" is proposed.

Entities of master device and Database, the interface between the two entities would have been defined in PAWS. There are much sensitive information, such as location and identity of master devices, which MAY be transmitted between the interface of the master device and the white space database when the PAWS is used. Attackers are able to make various types of attack by using the sensitive information if there is lack of security mechanism. Therefore, the messaging interface between the master device and the database needs to be secured. Meanwhile, the two entities SHALL be mutually authenticated and they both MUST be authorized by authority of white space management institution.

In this document, the security threats, the security features and the security mechanism(TLS) are discussed in details.

2. Conventions and terminology

2.1. Conventions used in this Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMEND", "MAY", and "OPTIONAL" that appear in this document are to be interpreted as described in [RFC2119].

2.2. Terminology

The Terminology Section of the latest version of [I-D.ietf-paws-problem-stmt-usecases-rqmts] shall be included by reference.

WS interface

The interface between master device and Database specifies data model and process of PAWS in this document.

3. Overview of Security threats and Requirements

3.1. Fundamental system architecture of PAWS

Figure 1 shows a common system model of PAWS, the master device is connected to internet by any means other than using the white space radio. More details of PAWS are described using the following steps:

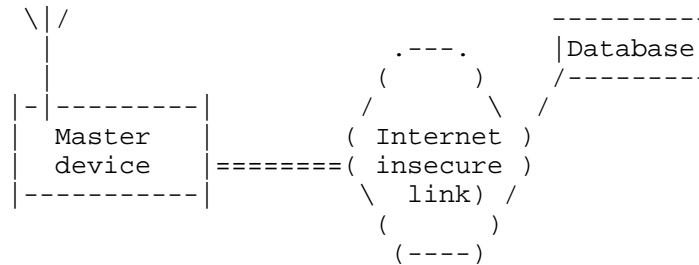


Figure 1: system architecture of PAWS

Description of system architecture:

- 1) The master device needs to discover white space database in the relevant regulatory domain by connecting to the internet by any means other than using the white space radio.
- 2) The master device will connect to the white space database, the link between master device and the white space database can be wired or wireless and provide IP connectivity, which may be insecure.
- 3) The master device may register with the white space database before the white space database provides information on available white space radio channels according to regulatory domain requirements. The information used in registration may include, but is not limited to, the device ID, the device's location, serial number assigned by the manufacturer and so on.
- 4) The master device queries the white space database for available white space channel lists.

3.2. Security threats

If there is lack of security mechanism in above PAWS architecture, various threats detailed in "ietf-paws-problem-stmt-use-cases-rqmts" may exist, and the corresponding attacks can be deployed. It can be summarized as follows from a security point of view:

3.2.1. Impersonation of a master device

If there is no authentication of the master device, the white space database cannot detect the rogue master device, and the available white space channel list will be passed to the Rogue master device. This enables a rogue master device to use the available channels. Besides, the rogue master device can connect to the white space database by using the registration exchanges, the DoS type attacks may be initiated. This shows that it is essential to perform some type of authentication of master device.

3.2.2. Impersonation of database

If there is no authentication of the database, an attacker may attempt to spoof a white space database and provide responses to a master device which are malicious and result in the master device causing interference to the primary user of the spectrum. At the same time, the attacker also can retrieve an available white space channel list from a legal database using the registration exchanges, which received from the master device.

3.2.3. MitM on the interface between master device and database

A man in the middle (MitM) node is inserted in between the master device and database, it can be considered to be a variant of the above attacks. The real master device will connect to the MitM node and the MitM node can connect to the real database. The MitM node can transparently transmit, receive, view, and modify the traffic between the real master device and the database without either of those nodes being aware of it. The important security point illustrated by this attack is that not only is it essential to perform mutual authentication of the master device and the white space database, it is important to ensure that all security tunnels from the master device terminate in the trusted white space database instead of in a MitM node.

3.2.4. Attacks on the link of interface between master device and database

The link between the master device and the white space database can be wired or wireless. An attacker may listen to the communication between a valid master device and database. The threats of this are as follows:

- 1) Steal the confidentiality of data transmitted in the packet payload, such as utilize the information about available channels by utilizing those channels. The result of such an attack is unauthorized use of channels by an unauthorized device.

2) The location/identity information can be gleaned by an eavesdropper and be used for tracking purposes.

3) An attacker could modify the communication between the master device and the database. The channel information and some other type parameters could be modified by an attacker which may result in interference to the primary user of that channel. Alternatively the attacker may indicate no channel availability at a location resulting in a denial of service to the master device.

3.2.5. Attacks on the master device itself

The master device may be deployed in vulnerable locations, and the less trusted types of transmission links will be used to interconnect that equipment to the database. Breaking the master device to get sensitive data is theoretically possible. The attacker may dig out the master device-database shared secret or a long term certificate from the master device and tries to add another master device.

3.2.6. Other potential attacks(To be added)

3.3. Security countermeasures

To mitigate the above threats, the security countermeasures below should be used. Namely:

1) The master device shall be authenticated by database based on a globally unique and permanent master device identity when it wants to establish connection with the database.

2) The master device shall authenticate the identity of database.

3) The master device and the white space database shall check that both of them are authorized by the regulator body of white space.

4) Sensitive data including authentication credentials, user information, cryptographic keys shall not be transmitted between the master device and the white space database in plaintext in unauthorized access. It means that the transport of data over the interface between the master device and the database shall be integrity, confidentially, and replay protected from unauthorized.

5) The master device should have a secure module to store long term key or certificate. The identity of master device could be stored in a trusted physical module and/or a possible non-removable smartcard.

4. Security schemes

4.1. Overview

According to the previous analysis, the security mechanism shall be able to provide the following security features:

1) Mutual authentication

Mutual authentication between the master device and the database shall be performed using certificates or pre-shared keys and so on. Besides, the master device and the database shall further be authenticated by the authority of regulatory body of white space to ensure that they are both authorized by regulatory body of white space due to the fact that the database may not be deployed by regulatory body of white space. The credentials and critical security functions for authentication shall be protected inside physically secure environment, such as Trusted Environment(TrE).

2) The protection mechanisms of the data

The data over the interface between the master device and the database shall be protected for integrity, confidentiality and anti-replay from unauthorized parties.

3) Trusted environment

The TrE shall be a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive data. All data produced through execution of functions within the TrE shall be unknowable to unauthorized external entities.

4.2. Analysis of security schemes

For business reasons or ease of management, databases may be deployed by different third-party that is authorized by regulatory body of white space. It means that there are two possible deployment cases: one is that the databases deployed by the third-party which are authorized by regulatory body of white space; the other is that the databases are directly deployed by regulatory body of white space.

4.2.1. Databases deployed by third-party

In this scene, when the master device wants to query the database for an available white space list, it shall be able to connect to the database and also be authorized by regulatory body of white space to use white space. It means that twice authentications shall be implemented, two suits of credentials are stored in master device and

white space database which are provided by different trusted authorities. There are two possible authentication models which are showed as follow:

Model 1

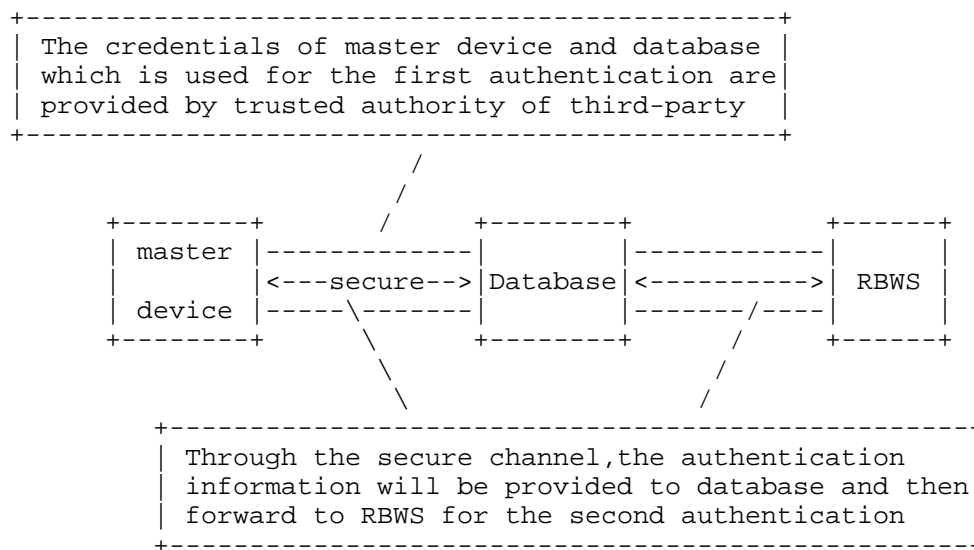


Figure 2: authentication model 1

In this model, the credentials of the master device and the database for second authentication both shall be checked by authority of RBWS after the master device successfully access to the white space database whenever the master device query the database, but what the database needs to do is able to establish connection with authority of regulatory body of white space (RBWS).

Under this circumstance, the whole querying procedure of white space channels can be showed as followed:

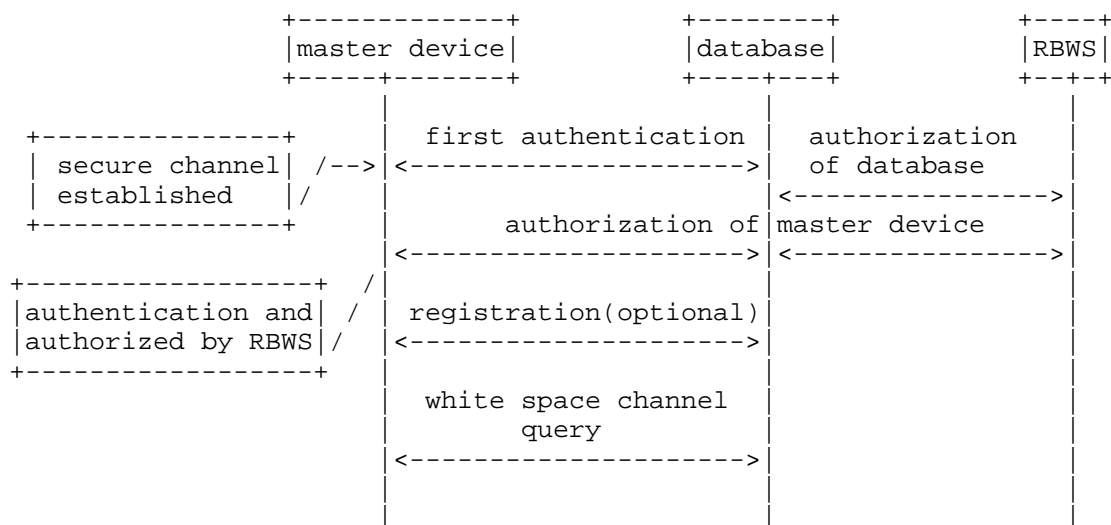


Figure 3: procedure of querying database

Firstly, the mutual authentication between the master device and the database shall be supported based on the credentials which are provided by an authority trusted by the third-party, e.g. the authority of third-party or by another party trusted by the third-party. Only the master device which has credentials with the third-party that deployed the database can connect to the database. And the master device also shall evaluate the connected database if it is a trusted database where the master device is able to register and receive service from the database. Namely the secure connectivity between the master device and the database shall be established first before the master device can query the available white space from the database.

Secondly, following the above successful mutual authentication between the master device and the database, they both shall also be authenticated and authorized by regulatory body of white space. The master device provides the information for authentication to database through the WS interface and then forward to regulatory body of white space by database. The credentials used for secondary authentication shall be provided by authority trusted by regulatory body of white space, e.g. the authority of regulatory body of white space or by another party trusted by the regulatory body of white space.

Finally, only when the twice mutual authentications are both passed,

the master device can query the database for available white space channels.

In addition, the information which is used for second authentication or for registration may be transmitted between master device and database after the first successful authentication, these information may contain sensitive data which shall not be known by others. So the secure channel shall be established after the first authentication which is used to provide security protection. The master device and the database shall not engage in any communication prior to the completion of the establishment of the secure channel other than messages for establishing the secure channel.

Model 2

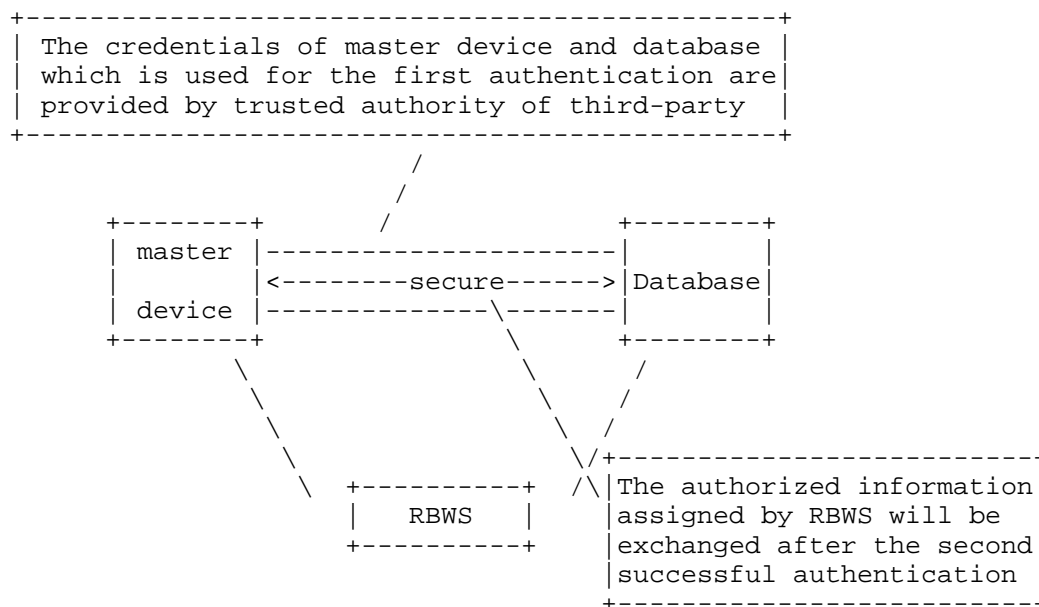


Figure 4: authentication model 2

In this model, the master device and database both can connect to regulatory body of white space.

On this occasion, the credentials provided by trusted authority of third-party are used to mutual authentication between the master device and the database first. The master device and the white space database must establish connection with RSWB respectively and authenticated by the authority of RBWS when the previous mutual

authentication is successful. Then the master device and database shall check whether the authorized information assigned by regulatory body of white space will be exchanged through the WS interface is legal. Only the two authentication procedures are both successful, the master device is able to query the database for available white space channel.

4.2.2. Databases deployed by regulatory body of white space

In this scenario, the master device can directly query the connected database for available white space lists when it is able to connect to the trusted database due to the fact that the databases are deployed by regulatory body of white space and the management of white space is also by regulatory body of white space. Only one credentials are needed, the credentials used to mutual authentication between master device and database can be assigned by trusted authority of regulatory body of white space, e.g. the authority of regulatory body of white space or by another party trusted by the regulatory body of white space. The security model can be showed as followed:

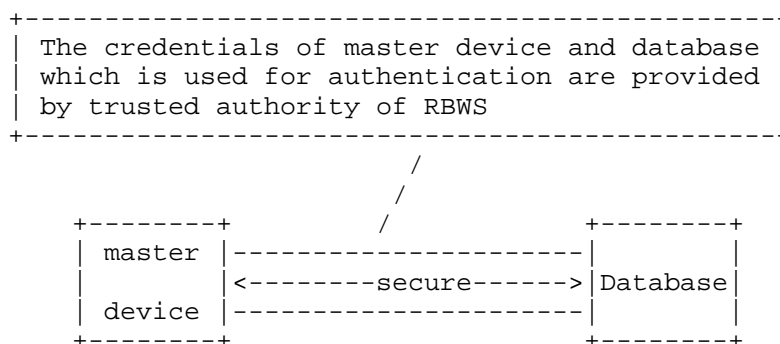


Figure 5: authentication model 3

After the successful mutual authentication, the secure channel shall be established to protect the communication between the master device and the database. The master device and the database shall not engage in any communication prior to the completion of the establishment of the secure channel other than messages for establishing the secure channel.

The TLS protocol depicted in section 4.3 can be considered to establish the secure channel according to the above analysis. The alternative security scheme IPsec can also be used in PAWS. But since TCP and HTTP protocol are recommended to use for PAWS, only the

TLS is introduced in this document.

4.3. TLS protocol

4.3.1. Brief introduction of TLS protocol

TLS protocol provides the communications privacy over the internet which is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol.

1) The TLS Handshake Protocol is responsible for negotiating a session, which is used to allow peers to agree upon security parameters for the record layer, authenticate themselves, instantiate negotiated security parameters, and report error conditions to each other.

a) The peer's identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA, DSA, etc). X509 certificate is recommended. When the certificate is used to authenticate the identity of the entity, each party shall verify the other's certificate whether it is valid and has not expired or revoked.

b) According the [RFC5246], RSA or Diffie-Hellman can be used for authentication and key exchange.

c) A `pre_master_secret` is created by key exchange process in TLS handshake protocol, which will be used to generate the `master_secret`. The master secret is required to generate the encryption keys and integrity keys.

2) The TLS Record Protocol takes messages to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, and transmits the result. Received data is decrypted, verified, decompressed, and reassembled, then delivered to higher level clients. Two basic security properties are as follows:

a) Confidentiality: symmetric cryptography is used for data encryption (e.g., AES, etc). The derivation of encryption keys are based on a secret negotiated by the TLS handshake protocol.

b) Integrity: A keyed MAC is used to message integrity check. Secure hash functions (e.g., SHA-1, etc) are used for MAC generated.

4.3.2. Security establishment procedure between master device and database

In related reference of PAWS, TCP and HTTP are recommended to be used

to load the messages in the interface between the master device and the database.

When the TLS protocol is used, all HTTP data between master device and the white space database must be sent as TLS "application data". Normal HTTP behavior should be followed. It means that security association shall be set up by using TLS protocol before establishment of the HTTP connection, and the mutual authentication shall be implemented in TLS protocol.

The following procedures shall be implemented first before the master device contacts to the database using a well-defined access method when it has determined the relevant white space database.

The master device acting as the HTTP client should also act as the TLS client. It should initiate a connection to the white space database on the appropriate port and then sent the TLS ClientHello to begin the TLS handshake.

1) The procedure of TLS handshake protocol can be described as follows which is based on the [RFC5246]GBP[not]it contains four stages:

a) The first stage: security capabilities including protocol version, session ID, cipher suite, compression method, and initial random numbers are established

b) The second stage: certificate of the database, key exchange, and request certificate shall be sent by database

c) The third phase: master device sends certificate if requested. Key exchange and certificate verification may be sent by master device

d) The last phase: change cipher suite and finish handshake protocol

2) Authentication methods

In above establishment procedure of TLS secure channel, Public key certificates or symmetric keys (namely pre-shared keys or PSKs) can be used for the mutual authentication between master device and database. In the PSK case, the shared key needs to be pre-configured in the master device and in the database by manual operation; When the PSK authentication is selected, the certificate and Certificate Request payloads are omitted from the response. The detailed procedure can reference the RFC4279. In the certificate case, the master device and database can obtain an operator certificate through the enrolment procedure.

The use of certificates has advantage that there is a standardized procedure for enrolling the private key corresponding to the certificate while the use of the PSK requires manual operation for establishing the PSK. On the other hand, the use of PSK has advantage that no PKI is required and the procedure after pre-establishment of PSK is simple. When using certificate for mutual authentication, a part of the usual certificate handling is replaced by subscription handling.

3) Security protection

For the completion of the TLS handshake protocol, the integrity, confidentiality and replay protected are all activated, all communications between the master device and the database shall be protected by the secure channel. The further authentication of the master device and the white space database should be protected by the secure channel if it needed.

4.3.3. Drawbacks of TLS protocol

Because the TLS runs over TCP, it is susceptible to a number of denial-of-service (DoS) attacks. An attacker who initiates a large number of TCP connections can cause a server to consume large amounts of CPU for doing RSA decryption. Besides, attackers can forge RSTs, thereby terminating connections, or forge partial TLS records, thereby causing the connection to stall. In this situation, implementers or users who are concerned with this class of attack should use IPsec.

5. Security Considerations

All contents of this document are dealing with security.

6. IANA Considerations

There have been no IANA considerations so far in this document.

7. Acknowledgments

Thanks to my colleagues for their sincerely help and comments when drafting this document.

8. Normative Reference

- [I-D.ietf-paws-problem-stmt-usecases-rqmts]
Probasco, S. and B. Patil, "Protocol to Access White Space
database: PS, use cases and rqmts",
draft-ietf-paws-problem-stmt-usecases-rqmts-03 (work in
progress), February 2012.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
Requirement Levels", BCP 14, RFC 2119, March 1997.

Authors' Addresses

Yizhuang Wu
Huawei Technologies

Email: wuyizhuang@huawei.com

Yang Cui
Huawei Technologies

Email: cuiyang@huawei.com

