

PAWS Working Group
Internet-Draft
Intended status: Informational
Expires: April 18, 2012

JC. Zuniga
InterDigital Communications, LLC
A. Sago
M. Fitch
BT

October 16, 2011

UK Use Cases and Requirements
draft-zuniga-paws-uk-use-cases-and-requirements-00

Abstract

This document proposes a simplification of the PAWS database discovery use case, two new use cases for indoor networking and machine to machine communications, and a set of requirements that drop out of all the use cases included so far in the working document. These use cases and requirements especially address the TV White Spaces needs in the United Kingdom, as currently known.

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 18, 2012.

Copyright Notice

Copyright (c) 2011 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	3
2.	Conventions and Terminology	3
2.1.	Conventions Used in This Document	3
2.2.	Terminology	3
3.	Use-Cases	3
3.1.	TVWS Database Discovery (proposed modifications to WG document)	3
3.2.	Indoor Networking	4
3.3.	Machine to Machine (M2M)	5
4.	Requirements	7
4.1.	Master	7
4.2.	Database	8
4.3.	Security	8
5.	Security Considerations	8
6.	IANA Considerations	9
7.	Acknowledgements	9
8.	Informative References	9
	Authors' Addresses	9

[1.](#) Introduction

This document proposes some modifications to the TV White Spaces use cases and requirements described in [\[I-D.ietf-paws-problem-stmt-usecases-rqmts\]](#). Similarly, some additional ones are presented. These use cases and requirements are meant to address specifically the regulatory needs of the UK, as currently known.

[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 [RFC 2119](#) [[RFC2119](#)].

[2.2.](#) Terminology

Model ID

A unique number for each master device and slave device that identifies the manufacturer, model number and serial number.

[3.](#) Use-Cases

[3.1.](#) TVWS Database Discovery (proposed modifications to WG document)

This use case is preliminary to creating a radio network using TV white space; it is a prerequisite to other use cases. The radio network is created by a master device. Before the master device can transmit in TV white space spectrum, it must contact a trusted database where the device can learn which channels are available for it to use. The master device will need to discover a trusted database in the relevant regulatory environment, using the following

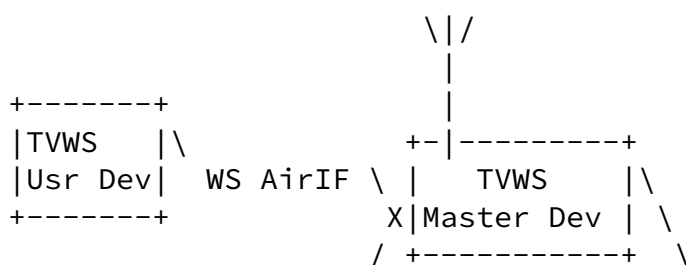
steps:

1. The master device is connected to the internet by any means other than using the TV white space radio.
2. The master device constructs and sends a service request over the Internet to discover availability of trusted databases in the local domain and waits for responses.
3. If no acceptable response is received within a pre-configured time limit, the master device concludes that no trusted database is available. If at least one response is received, the master device evaluates the response(s) to determine if a trusted database can be identified where the device is able to register and receive service from the database.

Optionally the initial query will be made to a listing approved by the national regulator for the domain of operation (e.g. a website either hosted by or under control of the national regulator) which maintains a list of TVWS databases and their internet addresses. The query results in the list of databases and their internet addresses being sent to the master, which then evaluates the response to determine if a trusted database can be identified where the master device is able to register and receive service from the database.

[3.2.](#) Indoor Networking

In this use case, the users are inside a house or office. The users want to have connectivity to the internet or to equipment in the same or other houses / offices. This deployment scenario is typically characterized by master devices within buildings, that are connected to the Internet using a method that does not utilise TV whitespace. The master devices can establish TV whitespace links between themselves, or between themselves and one or more user devices. Figure 1 is an illustration of the arrangement.



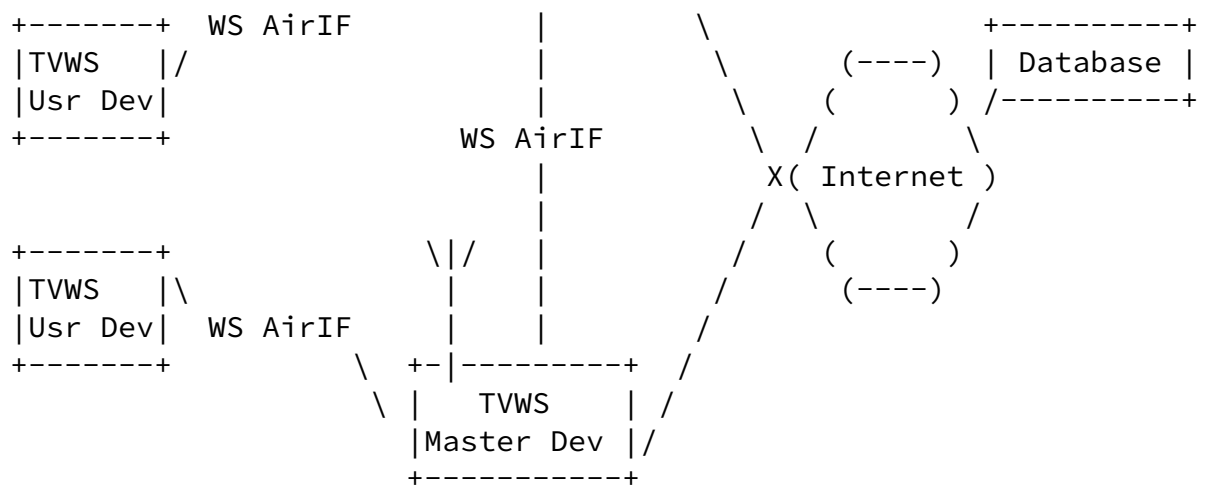


Figure 1: Example illustration of indoor TV Whitespace use-case

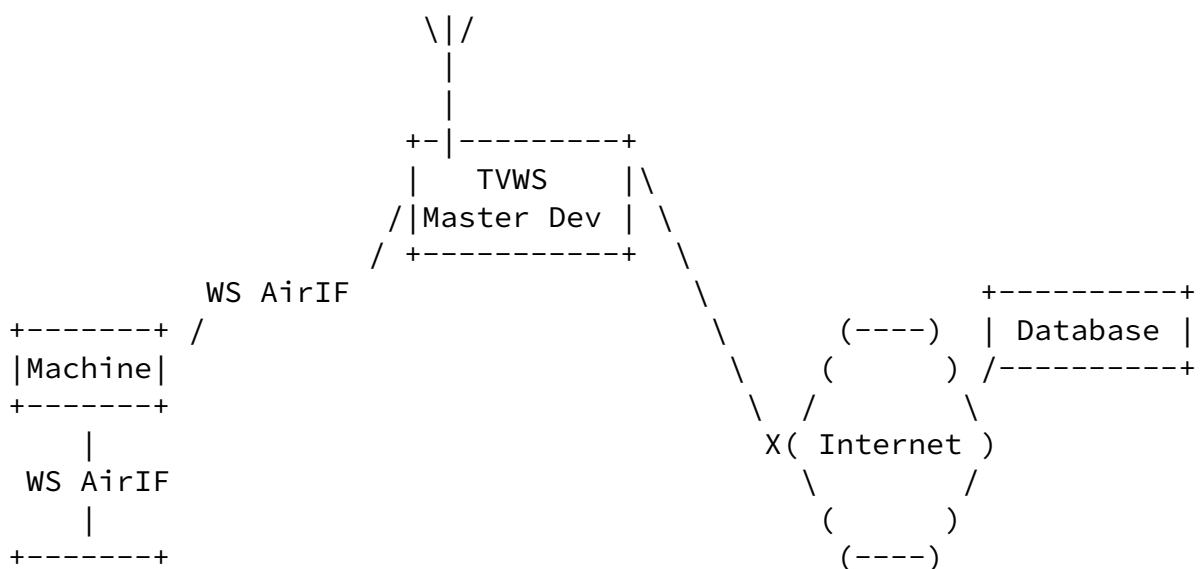
A simplified operational scenario utilizing TV whitespace to provide indoor networking consists of the following steps:

1. The master device powers up with its whitespace radio in idle or listen mode only (no active transmission on the whitespace frequency band).
2. The master device has internet connectivity and establishes a connection to a trusted white space database (see [Section 3.1](#) above).
3. The master device sends its geolocation and location uncertainty information, and optionally additional information which may include (1) device ID and (2) antenna characteristics, to a trusted database, requesting a list of available whitespace channels based upon this information.
4. The database responds with a list of available white space channels that the master device may use, and optional information which may include inter alia (1) a duration of time for the use of each channel (channel validity time) (2) a maximum radiated power for each channel, (3) an indication of the quality of the spectrum for each channel and (4) directivity and other antenna information.
5. Once the master device authenticates the whitespace channel list response message from the database, the master device selects one or more available whitespace channels from the list.
6. The user device(s) scan(s) the TV white space bands to locate the

- master device transmissions, and associates with the master.
7. The master device acknowledges to the database which of the available whitespace channels it has selected for its operation, and optionally other information, such as maximum transmit power and antenna characteristics. The database is updated with the information provided by the master device, in order to inform the channel quality information provided to other masters in subsequent requests.

3.3. Machine to Machine (M2M)

In this use case, machines include a whitespace device and can be located anywhere, fixed or on the move. The machines want to have connectivity to the internet or to other machines in the vicinity. All machines are slave devices, and machine communication over a TVWS channel, whether to a master device or to another machine, is under the control of the master device. This deployment scenario is typically characterized by a master device with internet connectivity by some connection that does not utilize TV white space. Figure 2 is an illustration of the arrangement.



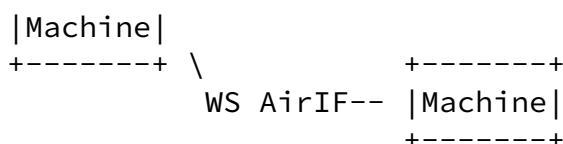


Figure 2: Example illustration of M2M TV Whitespace use-case

A simplified operational scenario utilizing TV white space to provide indoor networking consists of the following steps:

1. The master device powers up with its whitespace radio in idle or listen mode only (no active transmission on the whitespace frequency band).
2. The master device has internet connectivity and establishes a connection to a trusted white space database (see [Section 3.1](#) above).
3. The master device sends its geolocation and location uncertainty information, and optionally additional information which may include (1) device ID and (2) antenna characteristics, to a trusted database, requesting a list of available whitespace channels based upon this information.
4. The database responds with a list of available white space channels that the master device may use, and optional information which may include inter alia (1) a duration of time for the use of each channel (channel validity time) (2) a maximum radiated power for each channel, (3) an indication of the quality of the spectrum for each channel and (4) directivity and other antenna information.
5. Once the master device authenticates the whitespace channel list response message from the database, the master device selects one or more available whitespace channels from the list.

6. The devices fitted to the machines scan the TV bands to locate the master transmissions, and associate with the master device. Further signalling can then take place to establish direct links among those machines that have associated with the master device.
7. The master device acknowledges to the database which of the available whitespace channels it has selected for its operation, and optionally other information, such as channel resource information (e.g. duty cycle), maximum radiated power and antenna

characteristics. The database is updated with the information provided by the master device, in order to inform the channel quality information provided to other masters in subsequent requests.

4. Requirements

4.1. Master

1. A master device **MUST** include a mechanism to locate a trusted whitespace database.
2. A master device **MAY** register with a trusted white space database.
3. A master device **MUST** be able to determine its location using latitude-longitude coordinates.
4. A master device **MUST** determine its location with at least $\pm x$ meters accuracy, where the value of x is defined by the regulator for each regulatory domain and is well known.
5. A master device **MUST** place its location into the query it makes to the whitespace database.
6. A master device **MUST** be able to query the whitespace database for channel availability information for a specific expected coverage area around its current location.
7. A master device **MUST** be able to pass the accuracy of its determined location in the query it makes to the whitespace database.
8. A master device **MAY** send additional information in the query it makes to the database such as antenna height above ground level, device ID or antenna characteristics.
9. A master device **MUST** make a fresh query of the whitespace database for the available channels within a particular time interval, using a parameter sent by the database in response to the previous query. On expiry of the time interval then a master device **MUST** cease transmission in the TVWS band if no successful query attempt has been made or a query has been made but the database has not responded.
10. If slave devices change their location during operation, the master device **MUST** query the whitespace database for available operating channels each time a slave device moves outside the

11. Before transmitting in the TVWS band, a master device MAY send back to the whitespace database the start and stop frequencies it has chosen for operation and MAY send back additional optional information such as actual radiated power, antenna characteristics or channel resource information.
12. A master device MAY be able to indicate to slave devices the start and stop frequencies it has available for operation and the maximum permitted powers for the slave devices, and MAY be able to send additional optional information.

[4.2.](#) Database

1. The whitespace database MUST provide the available channel list on receipt of a query from a master device as start and stop frequencies for each channel.
2. The whitespace database MAY also provide allowable power limits for each channel.
3. The whitespace database MAY also provide time validity constraints for each channel.
4. The whitespace database MAY also provide other parameters to the master device.
5. The whitespace database MAY be able to accept optional messaging sent back from master devices indicating the start and stop frequencies the master device has chosen for operation and MAY be able to accept additional information such as actual radiated power, antenna characteristics or channel resource information.

[4.3.](#) Security

1. The protocol between the master device and the WS Database MUST support mutual authentication and authorization.
2. The protocol between the master device and the WS Database MUST support integrity and confidentiality protection.
3. The WS Database MUST support both username/password and digital certificates based authentication of the master device.
4. A master device MUST be capable of validating the digital certificate of the WS Database.
5. A master device MUST be capable of checking the validity of the WS Database certificate and whether it has been revoked or not.

[5.](#) Security Considerations

The messaging interface between the white space device and the database needs to be secured. Security requirements are listed in [Section 4.3](#).

[6.](#) IANA Considerations

This document has no requests to IANA.

[7.](#) Acknowledgements

The authors would like to acknowledge Martino Freda for all the fruitful discussions on this topic.

[8.](#) Informative References

[I-D.ietf-paws-problem-stmt-usecases-rqmts]
Probasco, S., Bajko, G., Patil, B., and B. Rosen,
"Protocol to Access White Space database: PS, use cases
and rqmts", [draft-ietf-paws-problem-stmt-usecases-rqmts-00](#)
(work in progress), September 2011.

Authors' Addresses

Juan Carlos Zuniga
InterDigital Communications, LLC
Montreal, Quebec
Canada

Email: juancarlos.zuniga@interdigital.com

Andy Sago
BT
Martlesham Heath, Suffolk
United Kingdom

Email: andy.sago@bt.com

Michael Fitch
BT
Martlesham Heath, Suffolk
United Kingdom

Email: michael.fitch@bt.com

