Working Group Draft
Internet-Draft
Intended status: Informational
Expires: January 3, 2013

S. Probasco, Ed.
B. Patil
Nokia

July 2, 2012

Protocol to Access White Space database: PS, use cases and rqmts
draft-ietf-paws-problem-stmt-usecases-rqmts-06

Abstract

Portions of the radio spectrum that are assigned to a particular use but are unused or unoccupied at specific locations and times are defined as "white space". The concept of allowing additional transmissions (which may or may not be licensed) in white space is a technique to "unlock" existing spectrum for new use. An obvious requirement is that these additional transmissions do not interfere with the assigned use of the spectrum. One approach to using the white space spectrum at a given time and location is to verify with a database for available channels.

This document describes a number of possible use cases of white space spectrum and technology as well as a set of requirements for the database query protocol. The concept of TV white spaces is described including the problems that need to be addressed to enable white space spectrum for additional uses without causing interference to currently assigned use. Use of white space is enabled by querying a database which stores information about the channel availability at any given location and time.

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 3, 2013.

Copyright Notice

Table of Contents

1. Introduction

1.1. Introduction to white space

Wireless spectrum is a commodity that is regulated by governments. The spectrum is used for various purposes, which include but are not limited to entertainment (e.g. radio and television), communication (e.g. telephony and Internet access), military (e.g. radars etc.) and, navigation (e.g. satellite communication, GPS). Portions of the radio spectrum that are assigned to a licensed user but are unused or unoccupied at specific locations and times are defined as "white space". The concept of allowing additional transmissions (which may or may not be licensed) in white space is a technique to "unlock" existing spectrum for new use. An obvious requirement is that these additional transmissions do not interfere with the assigned use of the spectrum. One interesting observation is that often, in a given physical location, the assigned user(s) may not be using the entire band assigned to them. The available spectrum for additional transmissions would then depend on the location of the additional user. The fundamental issue is how to determine for a specific location and specific time, if any of the assigned spectrum is available for additional use. Academia and Industry have studied multiple cognitive radio mechanisms for use in such a scenario. One simple mechanism is to use a geospatial database that records the assigned users occupation, and require the additional users to check the database prior to selecting what part of the spectrum they use. Such databases could be available on the Internet for query by additional users.

Spectrum useable for data communications, especially wireless Internet communications, is scarce. One area which has received much attention globally is the TV white space: portions of the TV band that are not used by broadcasters in a given area. In 2008 the United States regulator (the FCC) took initial steps when they published their first ruling on the use of TV white space, and then followed it up with a ruling in 2010 [FCC Ruling] that established the basic foundation for TV white space service in the US. In May 2012 the FCC issued minor updates further refining the previous ruling [3MOO]. Finland passed an Act in 2009 enabling testing of cognitive radio systems in the TV white space. The ECC has completed Report 159 [ECC Report 159] containing requirements for operation of cognitive radio systems in the TV white space. Ofcom published in 2004 their Spectrum Framework Review [Spectrum Framework Review] and their Digital Dividend Review [DDR] in 2005, with proposals from 2009 onwards to access TV white space, leading to the 2011 Ofcom Statement Implementing Geolocation [Ofcom Implementing] which has been followed by draft requirements for TV white space devices [Ofcom Requirements]. More countries are expected to provide access to

their TV spectrum in similar ways. Any entity that is assigned spectrum that is not densely used may be asked to give it up in one way or another for more intensive use. Providing a mechanism by which additional users share the spectrum with the assigned user is attractive in many bands in many countries.

Television transmission until now has primarily been analog. The switch to digital transmission has begun. As a result the spectrum assigned for television transmission can now be more effectively used. Unused channels and bands between channels can be used by additional users as long as they do not interfere with the service for which that channel is assigned. While urban areas tend to have dense usage of spectrum and a number of TV channels, the same is not true in semi-rural, rural and remote areas. There can be a number of unused TV channels in such areas that can be used for other services. Figure 1 shows TV white space within the lower UHF band:

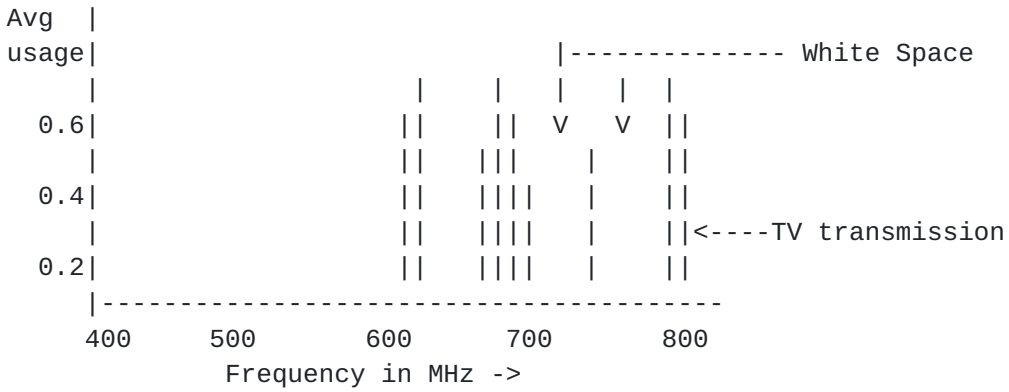

Figure 1: High level view of TV White Space

The fundamental issue is how to determine for a specific location and specific time if any of the spectrum is available for additional use. There are two dimensions of use that may be interesting: space (the area in which an additional user would not interfere with the assigned use), and time: when the additional transmission would not interfere with the assigned use. In this discussion, we consider the time element to be relatively long term (e.g. hours in a day) rather than short term (e.g. fractions of a second). Location in this discussion is geolocation: where the transmitters (and sometimes receivers) are located relative to one another. In operation, the database records the assigned user's transmitter (and some times receiver) locations along with basic transmission characteristics such as antenna height, and power. Using rules established by the local regulator, the database calculates an exclusion zone for each

assigned user, and attaches a time schedule to that use. The additional user queries the database with its location. The database intersects the exclusion zones with the queried location, and returns the portion of the spectrum not in any exclusion zone. Such methods of geospatial database query to avoid interference have been shown to achieve favorable results, and are thus the basis for rulings by the FCC and reports from ECC and Ofcom. In any country, the rules for which assigned entities are entitled to protection, how the exclusion zones are calculated, and what the limits of use are by additional users may vary. However, the fundamental notion of recording assigned users, calculating exclusion zones, querying by location and returning available spectrum (and the schedule for that spectrum) are common.

This document includes the problem statement, use cases and requirements associated with the use of white space spectrum by secondary users via a database query protocol.

1.2. Scope

1.2.1. In Scope

This document applies only to communications required for basic service in TV white spaces. The protocol will enable a white space radio device to complete the following tasks:

1. Determine the relevant white space database to query.

2. Connect to the database using a well-defined access method.

3. Register with the database using a well-defined protocol.

4. Provide its geolocation and perhaps other data to the database using a well-defined format for querying the database.

5. Receive in response to the query a list of currently available white space channels or frequencies using a well-defined format for the information.

6. Send an acknowledgment to the database with information containing channels selected for use by the device.

1.2.2. Out of Scope

The following topics are out of scope for this specification:

Co-existence and interference avoidance of white space devices within the same spectrum

Provisioning (releasing new spectrum for white space use)

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

Database

In the context of white space and cognitive radio technologies, the database is an entity which contains, but is not limited to, current information as required by by the regulatory policies about available spectrum at any given location and time, and other types of related (to the white space spectrum) or relevant information.

Device Class

Identifies classes of devices defined by Regional Regulators, including fixed, mobile, portable, etc... May also indicate if the device is indoor or outdoor.

Device ID

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

Location Based Service

An application or device which provides data, information or service to a user based on their location.

Master Device

A device which queries the WS Database to find out the available operating channels.

Protected Entity

An assigned user of white space spectrum which is afforded protection against interference by additional users (white space devices) for its use in a given area and time.

Protected Contour

The exclusion area for a Protected Entity, held in the database and expressed as a polygon with geospatial points as the vertices.

Slave Device

A device which uses the spectrum made available by a master device, and cannot query the database directly.

TV White Space

TV white space refers specifically to radio spectrum which has been allocated for TV broadcast, but is not occupied by a TV broadcast, or other assigned user (such as a wireless microphone), at a specific location and time.

TV White Space Device (TVWSD)

A White Space Device that operates in the TV bands.

White Space (WS)

Radio spectrum which is not fully occupied at a specific location and time.

White Space Device (WSD)

A device which opportunistically uses some part of white space spectrum. A white space device can be an access point, base station, a portable device or similar. A white space device may be required by local regulations to query a database with its location to obtain information about available spectrum.

3. Prior Work

3.1. The concept of Cognitive Radio

A cognitive radio uses knowledge of the local radio environment to dynamically adapt its own configuration and function properly in a changing radio environment. Knowledge of the local radio environment can come from various technology mechanisms including sensing (attempting to ascertain primary users by listening for them within the spectrum), location determination and Internet connectivity to a database to learn the details of the local radio environment. White Space is one implementation of cognitive radio. Because a cognitive radio adapts itself to the available spectrum in a manner that

prevents the creation of harmful interference, the spectrum can be shared among different radio users.

3.2. Background information on white space in the US

Television transmission in the United States has moved to the use of digital signals as of June 12, 2009. Since June 13, 2009, all full-power U.S. television stations have broadcast over-the-air signals in digital only. An important benefit of the switch to all-digital broadcasting is that it freed up parts of the valuable broadcast spectrum. More information about the switch to digital transmission is at [DTV].

Besides the switch to digital transmission for TV, the guard bands that exist to protect the signals between stations can be used for other purposes. The FCC has made this spectrum available for unlicensed use and this is generally referred to as white space. Please see the details of the FCC ruling and regulations in [FCC Ruling]. The spectrum can be used to provide wireless broadband as an example.

3.3. Background information on white space in the UK

Background information on white space in UK Since its launch in 2005, Ofcom's Digital Dividend Review [DDR] has considered how to make the spectrum freed up by digital switchover available for new uses, including the capacity available within the spectrum that is retained to carry the digital terrestrial television service. Similarly to the US, this interleaved or guard spectrum occurs because not all the spectrum in any particular location will be used for terrestrial television and so is available for other services, as long as they can interleave their usage around the existing users.

In its September 2011 Statement [Ofcom Implementing] Ofcom says that a key element in enabling white space usage in the TV bands is the definition and provision of a database which, given a device's location, can tell the device which frequency channels and power levels it is able to use without causing harmful interference to other licensed users in the vicinity. Ofcom will specify requirements to be met by such geolocation databases. It also says that the technology has the possibility of being usefully applied elsewhere in the radio spectrum to ensure it is used to maximum benefit. For example, it may have potential in making spectrum available for new uses following any switch to digital radio services. Alternatively it may be helpful in exploiting some of the public sector spectrum holdings. Ofcom will continue to consider other areas of the radio spectrum where white space usage may be of benefit.

3.4. Air Interfaces

Efforts are ongoing to specify air-interfaces for use in white space spectrum. IEEE 802.11af, IEEE 802.15.4m and IEEE 802.22 are all examples. Other air interfaces could be specified in the future such as LTE.

4. Use cases and protocol services

There are many potential use cases that could be considered for the TV white space spectrum. Providing broadband Internet access in urban and densely populated hotspots, rural and underserved areas are examples. Available channels may also be used to provide Internet 'backhaul' for traditional Wi-Fi hotspots, or by towns and cities to monitor/control traffic lights or read utility meters. Still other use cases include the ability to offload data traffic from another Internet access network (e.g. 3G cellular network) or to deliver location based services. Some of these use cases are described in the following sections.

4.1. Protocol services

A complete protocol solution must provide all services that are essential to enable the white space paradigm. Before a white space device can begin operating it needs to know what channels are available by sending a query to a white space database for a list of available channels, the white space device must have the capability to first locate or "discover" a suitable database. Additionally, some regulatory authorities require the white space device to register with the database as a first step. This section describes the features required from the protocol.

4.1.1. White space database discovery

White space database discovery is preliminary to creating a radio network using white space; it is a prerequisite to the use cases below. The radio network is created by a master device. Before the master device can transmit in white space spectrum, it must contact a trusted database where the device can learn if any channels are available for it to use. The master device will need to discover a trusted database in the relevant regulatory domain, using the following steps:

1. The master device is connected to the Internet by any means other than using the white space radio. A local regulator may identify exception cases where a master may initialize over white space (e.g. the FCC allows a master to initialize over the TV white

space in certain conditions).

2. The master device constructs and sends a service request over the Internet to discover availability of trusted databases in the local regulatory 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 master device is able to receive service from the database.

Optionally the radio device is pre-programmed with the Internet address of at least one trusted database. The device can establish contact with a trusted database using one of the pre-programmed Internet addresses and establish a white space network (as described in one of the following use cases).

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 WS 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.

4.1.2. Device registration with trusted Database

Registration may be preliminary to creating a radio network using white space; in some regulatory domains, for some device types, it is a prerequisite to the use cases below. The radio network is created by a master device. Before the master device can transmit in white space spectrum, it must contact a trusted database where the device can learn if any channels are available for it to use. Before the database will provide information on available radio channels, the master device must register with the trusted database. Specific requirements for registration come from individual regulatory domains and may be different.

Figure 2 shows an example deployment of this scenario.

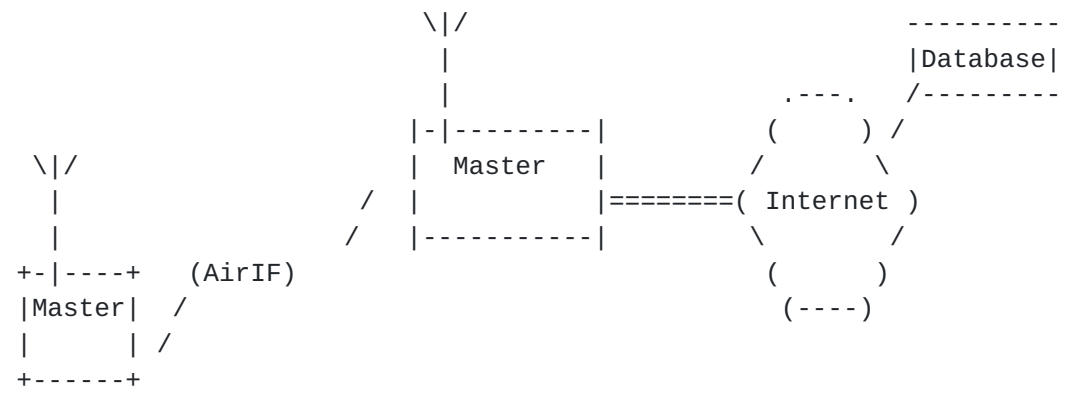

Figure 2: Example illustration of registration requirement in white space use-case

A simplified operational scenario showing registration consists of the following steps:

1. The master device must register with its most current and up-to-date information. Typically the master device will register prior to operating in white space for the first time after power up, after changing location by a predetermined distance, and after regular time intervals.

2. The master device shall provide to the database during registration all information required according to local regulatory requirements. This information may include, but is not limited to, the Device ID, serial number assigned by the manufacturer the device's location, device antenna height above ground, name of the individual or business that owns the device, name of a contact person responsible for the device's operation address for the contact person, email address for the contact person and phone number of the contact person.

3. The database shall respond to the registration request with an acknowledgement code to indicate the success or failure of the registration request. Additional information may be provided according to local regulator requirements.

4.2. Use cases

4.2.1. Hotspot: urban Internet connectivity service

In this use case Internet connectivity service is provided in a "hotspot" to local users. Typical deployment scenarios include urban areas where Internet connectivity is provided to local businesses and residents, and campus environments where Internet connectivity is provided to local buildings and relatively small outdoor areas. This

deployment scenario is typically characterized by multiple masters (APs or hotspots) in close proximity, with low antenna height, cells with relatively small radius (a few kilometers or less), and limited numbers of available radio channels. Many of the masters/APs are assumed to be individually deployed and operated, i.e. there is no coordination between many of the masters/APs. The masters/APs in this scenario use a TDD radio technology. Each master/AP has a connection to the Internet and may provide Internet connectivity to other master and slave devices.

Figure 3 shows an example deployment of this scenario.

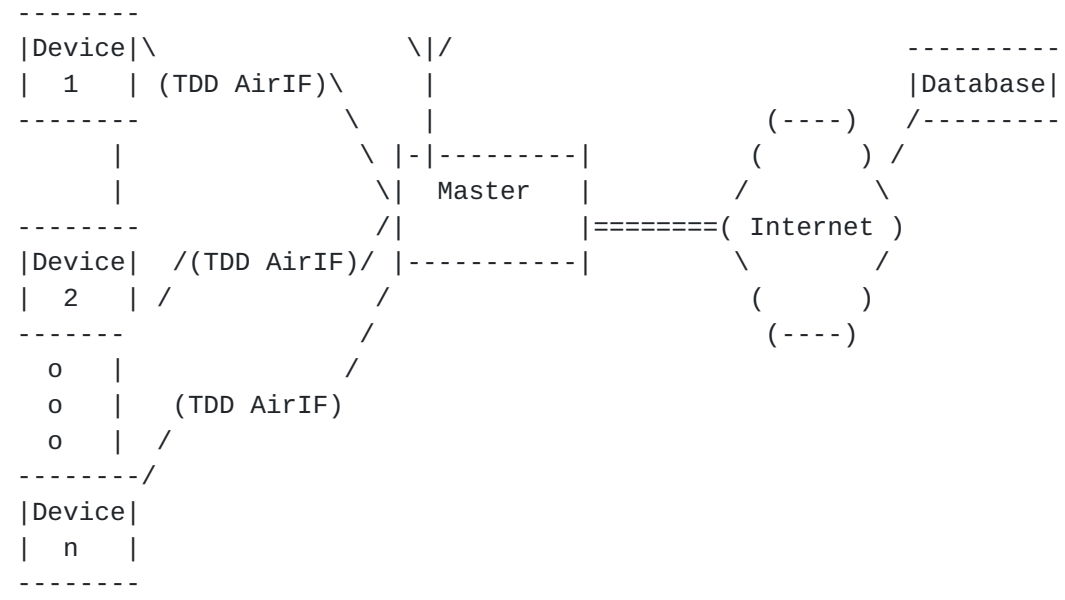

Figure 3: Hotspot service using TV white space spectrum

Once a master/AP has been correctly installed and configured, a simplified power up and operation scenario utilizing TV White Space to provide Internet connectivity service to slave devices, including the ability to clear WSDs from select channels, is described. This scenario consists of the following steps:

1. The master/AP powers up; however its WS radio and all other WS capable devices will power up in idle/listen only mode (no active transmissions on the WS frequency band). A local regulator may identify exception cases where a master may initialize over white space (e.g. the FCC allows a master to initialize over TV white space in certain conditions).

2. The master/AP has Internet connectivity, determines its location (either from location determination capability or from saved value that was set during installation), and establishes a connection to a trusted white space database (see Section 4.1.1).

3. The master/AP registers with the trusted database according to regulatory domain requirements (see Section 4.1.2).

4. Following the successful registration process (if registration is required), the master/AP will send a query to the trusted database requesting a list of available WS channels based upon its geolocation. The complete set of parameters to be provided from the master to the database is specified by the local regulator. Parameters may include WSD location, accuracy of that location, device antenna height, device identifier of a slave device requesting channel information.

5. If the master/AP has met all regulatory domain requirements (e.g. been previously authenticated, etc), the database responds with a list of available white space channels that the master may use, and optionally a duration of time for their use, associated maximum power levels or a notification of any additional requirements for sensing.

6. Once the master/AP has met all regulatory domain requirements (e.g. authenticated the WS channel list response message from the database, etc), the AP selects one or more available WS channels from the list. Prior to initiating transmission, if required by local regulation, the master/AP informs the database of the frequencies and power level it has chosen. This reporting of the frequencies and power levels to the database is repeated for each slave device that associated with the master.

7. The slave or user device scans the TV bands to locate a master/AP transmission, and associates with the AP.

8. The slave/user device queries the master for a channel list. In the query the slave/user device provides attributes that are defined by local regulations. These may include the slaves' Device ID and its geolocation.

9. Once the master/AP has met all regulatory domain requirements (e.g. validating the Device ID with the trusted database, etc) the master provides the list of channels locally available to the slave/user device. Prior to initiating transmission, if required by local regulation, the slave device informs the master/AP of the frequencies and power level it has chosen, and

the master/AP relays this information to the database.

10. The master sends an enabling signal to establish that the slave/user device is still within reception range of the master. This signal shall be encoded to ensure that the signal originates from the master that provided the available list of channels.

11. Periodically, at an interval established by the local regulator, the slave/user device must receive an enabling signal from the master that provided the available list of channels or contact a master to re-verify or re-establish the list of available channels.

12. The master/AP must periodically repeat the process to request a channel list from the database, steps 4 through 6 above. The frequency to repeat the process is determined by the local regulator. If the response from the database indicates a channel being used by the master/AP is not available, the master/AP must stop transmitting on that channel immediately. In addition or optionally, the database may send a message to the master/AP to rescind the availability of one or more channels. The master/AP must stop transmitting on that channel immediately.

13. The slave or user device must periodically repeat the process to request a channel list from the master/AP, steps 8 and 9 above. The frequency to repeat the process is determined by the local regulator. If the response from the master/AP indicates that a channel being used by the slave or user device is not available, the slave or user device must stop transmitting on that channel immediately. In addition or optionally, the database may send a message to the master/AP to rescind the availability of one or more channels. The master/AP must then notify the slave or user device of the rescinded channels. The slave or user device must stop transmitting on that channel immediately.

4.2.2. Wide-Area or Rural Internet broadband access

In this use case, Internet broadband access is provided as a Wide-Area Network (WAN) or Wireless Regional Area Network (WRAN). A typical deployment scenario is a wide area or rural area, where Internet broadband access is provided to local businesses and residents from a master (i.e., BS) connected to the Internet. This deployment scenario is typically characterized by one or more fixed master(s)/BS(s), cells with relatively large radius (tens of kilometers, up to 100 km), and a number of available radio channels. Some of the masters/BSs may be deployed and operated by a single entity, i.e., there can be centralized coordination between these

masters/BSs, whereas other masters/BSs may be deployed and operated by operators competing for the radio channels where decentralized coordination using the air-interface would be required. The BS in this scenario uses a TDD radio technology and transmits at or below a transmit power (EIRP) limit established by the local regulator. Each base station has a connection to the Internet and may provide Internet connectivity to multiple slaves/user devices. End-user terminals or devices may be fixed or portable.

Figure 4 shows an example deployment of this scenario.

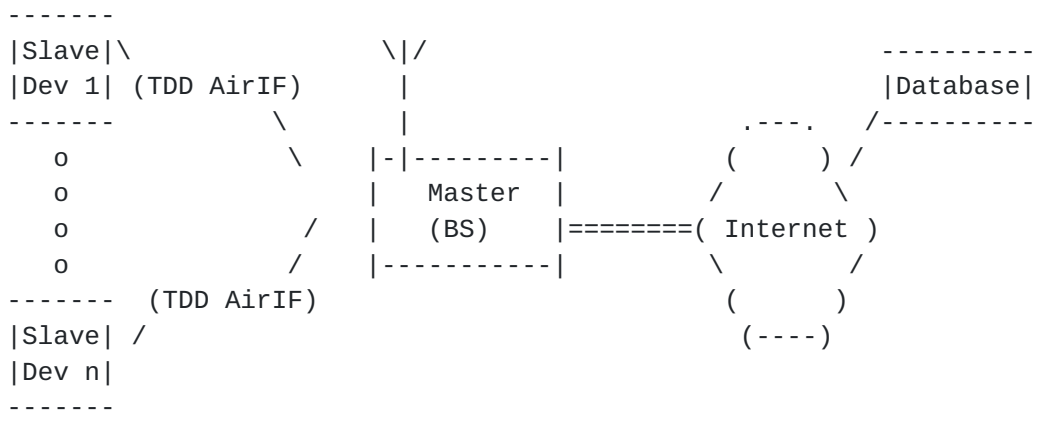

Figure 4: Rural Internet broadband access using TV white space spectrum

Once the master/BS has been professionally installed and configured, a simplified power up and operation scenario utilizing TV White Space to provide rural Internet broadband access consists of the following steps:

1. The master/BS powers up; however its WS radio and all other WS capable devices will power up in idle/listen-only mode (no active transmissions on the WS frequency band).

2. The master/BS has Internet connectivity, determines its location (either from location determination capability or from a saved value that was set during installation), and establishes a connection to a trusted white space database (see Section 4.1.1).

3. The master/BS registers with the trusted database service (see Section 4.1.2). Meanwhile the DB administrator may be required to store and forward the registration information to the

regulatory authority. If a trusted white space database service is not discovered, further operation of the WRAN may be allowed according to local regulator policy (in this case operation of the WRAN is outside the scope of the PAWS protocol).

4. Following the successful registration process (if registration is required), the master/BS will send a query to the trusted database requesting a list of available WS channels based upon its geolocation. The complete set of parameters to be provided from the master to the database is specified by the local regulator. Parameters may include WSD identifier, location, accuracy of that location, device antenna height, etc...

5. If the master/BS has been previously authenticated, the database responds with a list of available white space channels that may be used by the master/BS and optionally a maximum transmit power (EIRP) for each channel, a duration of time the channel may be used or a notification of any additional requirement for sensing.

6. Once the master/BS authenticates the WS channel list response message from the database, the master/BS selects an available WS channel(s) from the list. Such selection may be improved based on a set of queries to the DB involving a number of hypothetical slave or user devices located at various locations over the expected service area so that the final intersection of these resulting WS channel lists allows the selection of a channel that is likely available over the entire service area to avoid potential interference at the time of slave/user terminal association. The operator may also disallow some channels from the list to suit local needs if required.

7. The slave or user device scans the TV bands to locate a WRAN transmission, and associates with the master/BS.

8. In some regulatory domains, before a master device sends a channel list, the slave/user device provides its geolocation to the BS which, in turn, queries the database for a list of channels available at the slave's geolocation.

9. Once this list of available channels is received from the database by the master, the latter will decide, based on this list of available channels and on the lists for all its other associated slaves/user devices whether it should: a) continue operation on its current channel if this channel is available to all slaves/user devices, b) continue operation on its current channel and not allow association with the new slave/user device in case this channel is not available at its location or c)

change channel to accommodate the new slave. In the latter case, the master will notify all its associated slaves/user devices of the new channel to which they have to move.

10. The master/BS must periodically repeat the process to request a list of available channels from the database for itself and for all its associated slaves/user devices. If the response from the database indicates that the channel being used by the master/BS is no longer available for its use, the master/BS must indicate the new operating channel to all its slave/user terminals, stop transmitting on the current channel and move to the new operating channel immediately. If the channel that a slave/user terminal is currently using is no longer included in the list of locally available channels, the master may either drop its association with the slave/user device so that this device ceases all operation on its current channel or the master may decide to move the entire cell to another channel to accommodate the slave/user terminal and indicate the new operating channel to all its slave/user devices before dropping the link. The slave/user devices may then move to the identified new operating channel or scan for another WRAN transmission on a different channel. The frequency to repeat the process is determined by the local regulator.

11. The slave/user device must transmit its new geographic location every time it changes so that the repeated process described under item 10 can rely on the most up-to-date geolocation of the slave/user device.

4.2.3. Offloading: moving traffic to a white space network

In this use case internet connectivity service is provided over TV white space as a supplemental or alternative datapath to a 3G or other internet connection. In a typical deployment scenario an end user has a primary internet connection such as a 3G cellular packet data subscription. The user wants to use a widget or application to stream video from an online service (e.g. youtube) to their device. Before the widget starts the streaming connection it checks connectivity options available at the current time and location. Both 3G cellular data is available as well as TVWS connectivity (the user is within coverage of a TVWS master -- hotspot, WAN, WRAN or similar). The user may decide for many and various reasons such as cost, RF coverage, data caps, etc. to prefer the TVWS connection over the 3G cellular data connection. Either by user selection, preconfigured preferences, or other algorithm, the streaming session is started over the TVWS internet connection instead of the 3G cellular connection. This deployment scenario is typically characterized by a TVWS master/AP providing local coverage in the

same geographical area as a 3G cellular system. The master/AP is assumed to be individually deployed and operated, i.e. the master/AP is deployed and operated by the user at his home or perhaps by a small business such as a coffee shop. The master/AP has a connection to the internet and provides internet connectivity to the slave/ end-user's device.

The figure below shows an example deployment of this scenario.

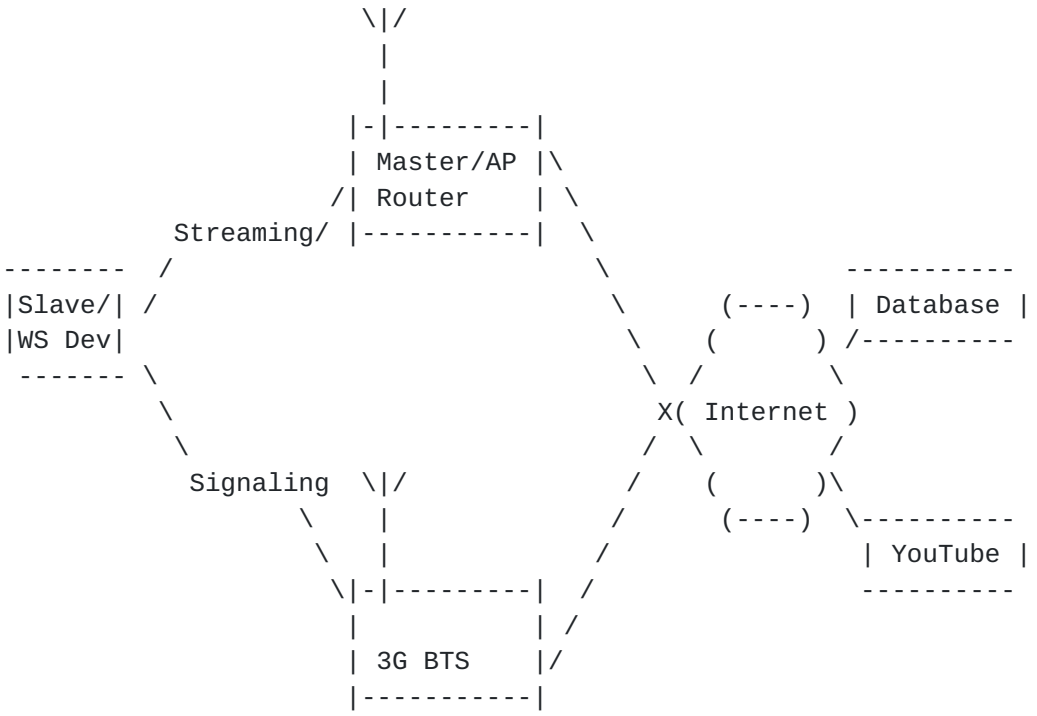

Figure 5: Offloading: moving traffic to a white space network

Once a dual or multi mode device (3G + TVWS) is connected to a 3G network, a simplified operation scenario of offloading selected content such as video stream from the 3G connection to the TWVS connection consists of the following steps:

1. The dual mode (or multi mode) device (3G + TVWS) is connected to a 3G network. The device has located a TVWS master/AP operating on an available channel and has associated or connected with the TVWS master/AP.

2. The user activates a widget or application that streams video from YouTube. The widget connects to YouTube over 3G cellular data. The user browses content and searches for video selections.

3. The user selects a video for streaming using the widget's controls. Before the widget initiates a streaming session, the widget checks the available connections in the dual mode device and finds a TVWS master/AP is connected.

4. Using either input from the user or pre-defined profile preferences, the widget selects the TVWS master/AP as the connection to stream the video.

4.2.4. White space serving as backhaul

In this use case Internet connectivity service is provided to users over a more common wireless standard such as Wi-Fi with white space entities providing backhaul connectivity to the Internet. In a typical deployment scenario an end user has a device with a radio such as Wi-Fi. An Internet service provider or a small business owner wants to provide Wi-Fi Internet connectivity service to their customers. The location where Internet connectivity service via Wi-Fi is to be provided is within the coverage area of a white space master (e.g. Hotspot or Wide-Area/Rural network). The service provider installs a white space slave device and connects it to the Wi-Fi access point(s). Wi-Fi access points with an integrated white space slave component may also be used. This deployment scenario is typically characterized by a WS master/AP/BS providing local coverage. The master/AP has a connection to the Internet and provides Internet connectivity to slave devices that are within its coverage area. The WS slave device is 'bridged' to a Wi-Fi network thereby enabling Internet connectivity service to Wi-Fi devices. The WS Master/AP/BS which has some form of Internet connectivity (wired or wireless) queries the database and obtains available channel information. It then provides service using those channels to slave devices which are within its coverage area.

Figure 6 shows an example deployment of this scenario.

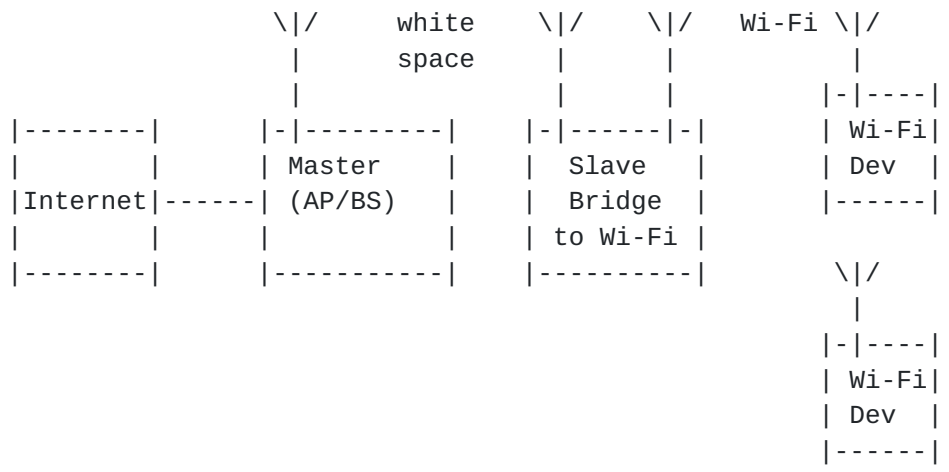

Figure 6: WS for backhaul

Once the bridged device (WS + Wi-Fi) is connected to a master and WS network, a simplified operation scenario of backhaul for Wi-Fi consists of the following steps:

1. A bridged device (WS + Wi-Fi) is connected to a master device operating in the WS spectrum. The bridged device operates as a slave device in either Hotspot or Wide-Area/Rural Internet use cases described above.

2. Once the slave device is connected to the master, the Wi-Fi access point has Internet connectivity as well.

3. End users attach to the Wi-Fi network via their Wi-Fi enabled devices and receive Internet connectivity.

4.2.5. Rapid deployed network for emergency scenario

Organizations involved in handling emergency operations often have a fully owned and controlled infrastructure, with dedicated spectrum, for day to day operation. However, lessons learned from recent disasters show such infrastructures are often highly affected by the disaster itself. To set up a replacement quickly, there is a need for fast reallocation of spectrum, where in certain cases spectrum can be cleared for disaster relief. To utilize unused or cleared spectrum quickly and reliably, automation of allocation, assignment and configuration is needed. A preferred option is to make use of a robust protocol, already adopted by radio manufacturers. This approach does in no way imply such organizations for disaster relief must compete on spectrum allocation with other white spaces users, but they can. A typical network topology would include wireless access links to the public Internet or private network, wireless ad hoc network radios working independent of a fixed infrastructure and

satellite links for backup where lack of coverage, overload or outage of wireless access links occur.

Figure 7 shows an example deployment of this scenario.

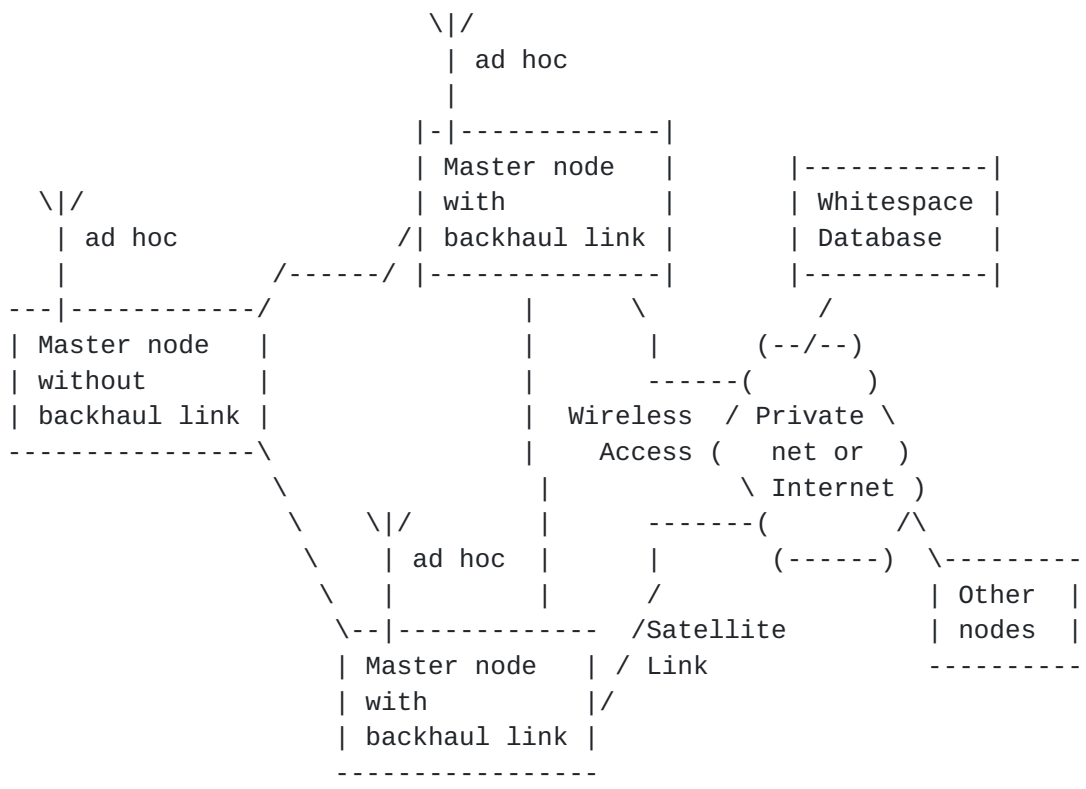

Figure 7: Rapid deployed network with partly connected nodes

In the ad hoc network, all nodes are master nodes in a way that they allocate RF channels from the white space database. However, the backhaul link may not be available to all nodes, such as depicted for the left node in Figure 7. To handle RF channel allocation for such nodes, a master node with a backhaul link relays or proxies the database query for them. So master nodes without a backhaul link follow the procedure as defined for clients. The ad hoc network radios utilize the provided RF channels. Details on forming and maintenance of the ad hoc network, including repair of segmented networks caused by segments operating on different RF channels, is out of scope of spectrum allocation.

4.2.6. Mobility

In this use case, the user has a non-fixed (portable or mobile) device and is riding in a vehicle. The user wants to have connectivity to another device which is also moving. Typical

deployment scenarios include urban areas and rural areas where the user may connect to other users while moving. This deployment scenario is typically characterized by a master device with low antenna height, Internet connectivity by some connection that does not utilize TV white space, and some means to predict its path of mobility. This knowledge of mobility could be simple (GPS plus accelerometer), sophisticated (GPS plus routing and mapping function) or completely specified by the user via user-interface.

Figure 8 shows an example deployment of this scenario.

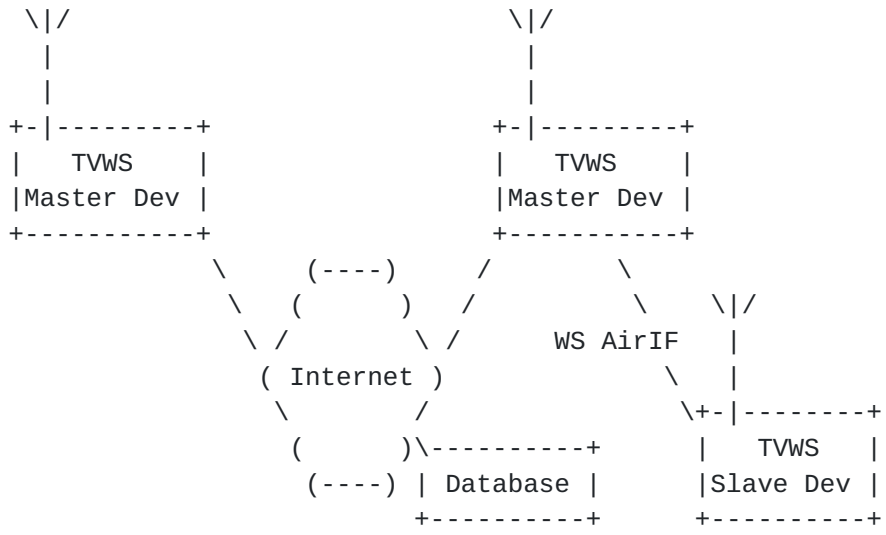

Figure 8: Example illustration of mobility in TV white space use-case

A simplified operational scenario utilizing TV whitespace to provide connectivity service in a mobility environment consists of the following steps:

1. The mobile master device powers up with its WS radio in idle or listen mode only (no active transmission on the WS frequency band).

2. The mobile master has Internet connectivity, determines its location, and establishes a connection to a trusted white space database (see Section 4.1.1).

3. The mobile master registers with the trusted database according to regulatory domain requirements (see Section 4.1.2).

4. Following the successful registration process (if registration is required), the mobile master will send a query to the trusted database requesting a list of available WS channels based upon

its current location, other parameters required by the local regulator (see Section 4.2.1, step 4) and a prediction of its future location. The current location is specified in latitude and longitude. The method to specify the future location is TBD, potential methods include movement vector (direction and velocity), a set of latitude/longitude points which specify a closed polygon where the future location is within the polygon, or similar.

5. If the mobile master has met all regulatory domain requirements (e.g. been previously authenticated, etc), the database responds with a list of available white space channels that the mobile master may use, and optional information which may include (1) a duration of time for the use of each channel (2) a maximum transmit power for each channel and (3) notification of any additional requirement for sensing.

6. Once the mobile master has met all regulatory domain requirements (e.g. authenticated the WS channel list response message from the database, etc), the master selects one or more available WS channel(s) from the list for use. At this point the mobile master may begin direct communication with another mobile master using methods outside the scope of PAWS.

7. The slave/user device scans to locate a mobile master transmission, and associates with the mobile master.

8. The slave/user device queries the master for a channel list, providing to the master the slave's device identification, and optionally its geolocation and a prediction of its future location.

9. Once the mobile master has met all regulatory domain requirements (e.g. the slave's device identification is verified by the database), the mobile master provides the list of channels locally available to the slave/user device.

10. If the mobile master moves outside the predicted range of future positions in step 4, it must repeat the process to request a channel list from the database, steps 4 through 6 above. If the response from the database indicates a channel being used by the mobile master is not available, the master/AP must stop transmitting on that channel immediately.

11. The slave or user device must periodically repeat the process to request a channel list from the master/AP, steps 8 and 9 above. The frequency to repeat the process is determined by the local regulator. If the response from the master/AP indicates that a

channel being used by the slave or user device is not available, the slave or user device must stop transmitting on that channel immediately. In addition or optionally, the database may send a message to the master/AP to rescind the availability of one or more channels. The master/AP must then notify the slave or user device of the rescinded channels. The slave or user device must stop transmitting on that channel immediately.

4.2.7. 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 utilize whitespace. The master devices can establish whitespace links between themselves, or between themselves and one or more user devices.

Figure 9 shows an example deployment of this scenario.

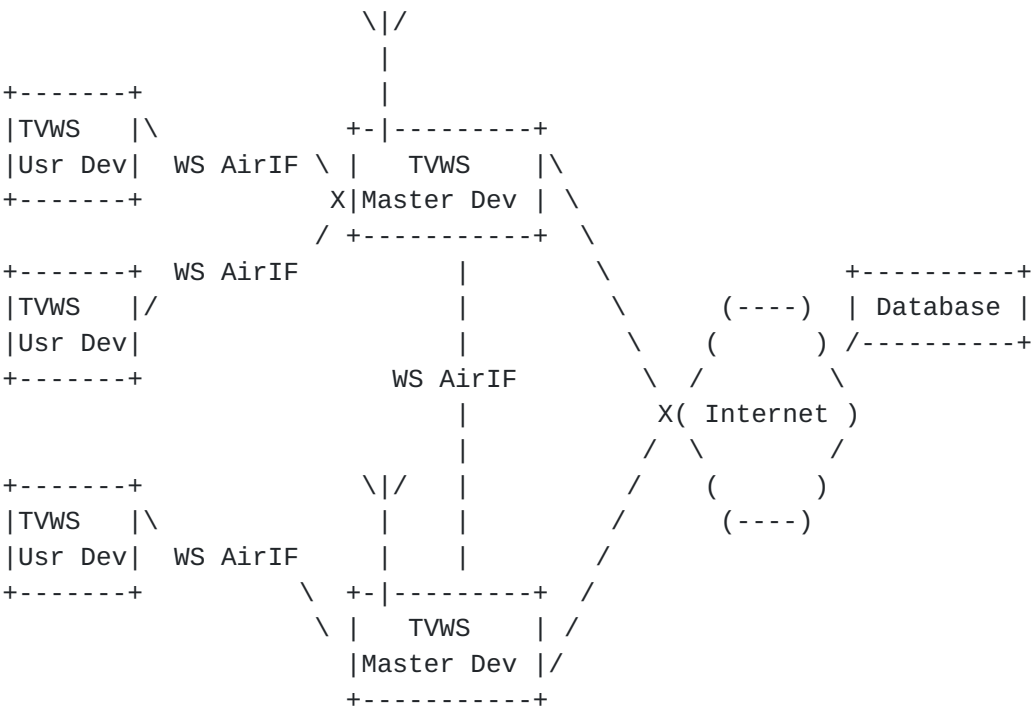

Figure 9: Example illustration of indoor TV white space use-case

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, determines its location (either from location determination capability or from a saved value that was set during installation), and establishes a connection to a trusted white space database (see Section 4.1.1).

3. The master device registers with the trusted database according to regulatory domain requirements (see Section 4.1.2).

4. Following the successful registration process (if registration is required), the master device sends a query to the trusted database requesting a list of available WS channels based upon its geolocation. The complete set of parameters to be provided from the master to the database is specified by the local regulator. Parameters may include WSD location, accuracy of that location, device antenna height, device identifier of a slave device requesting channel information.

5. If the master has met all regulatory requirements, 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, and (3) directivity and other antenna information.

6. 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. At this point the mobile master may begin direct communication with another mobile master using methods outside the scope of PAWS.

7. The user device(s) scan(s) the white space bands to locate the master device transmissions, and associates with the master.

4.2.8. Machine to Machine (M2M)

In this use case, each "machine" includes a white space slave device and can be located anywhere, fixed or on the move. Each machine needs to have connectivity to the Internet and or to other machines in the vicinity. Machine communication over a TVWS channel, whether to a master device or to another machine (slave device), is under the control of a 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 10 shows an example deployment of this scenario.

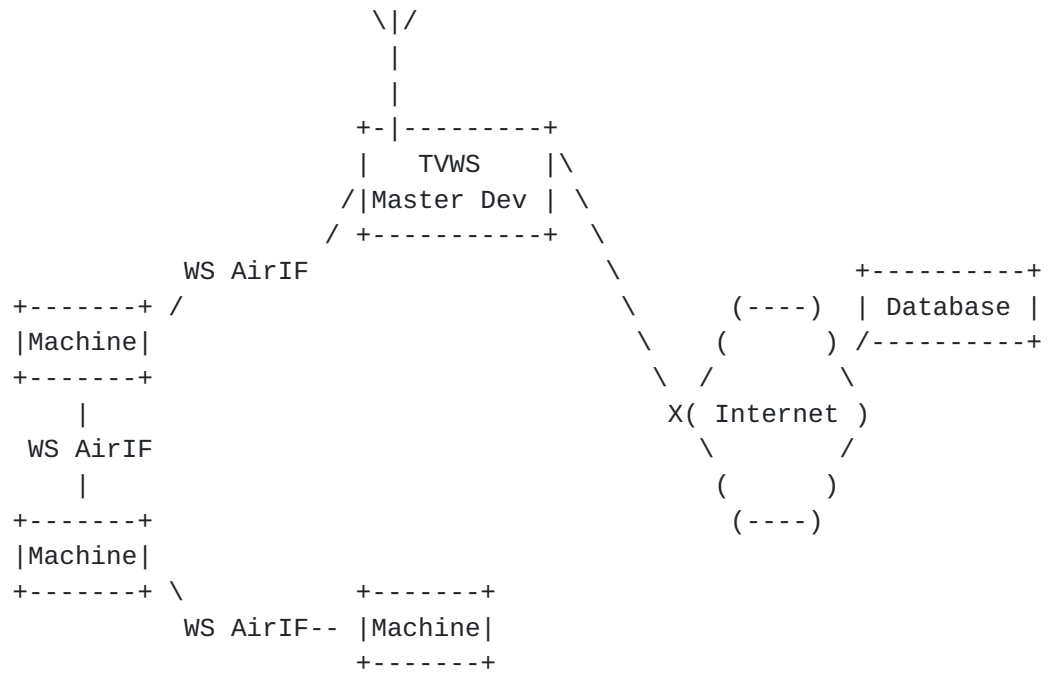

Figure 10: Example illustration of M2M TV white space use-case

A simplified operational scenario utilizing TV whitespace to provide machine to machine connectivity 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, determines its location (either from location determination capability or from saved value that was set during installation), and establishes a connection to a trusted white space database (see Section 4.1.1).

3. The master/AP registers with the trusted database according to regulatory domain requirements (see Section 4.1.2).

4. Following successful registration (if registration is required), 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.

5. If the master has met all regulatory domain requirements, 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 or a notification of any additional requirements for sensing.

6. 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.

7. The slave devices fitted to the machines scan the TV bands to locate the master transmissions, and associate with the master device.

8. Further signaling can take place outside scope of PAWS to establish direct links among those slave devices that have associated with the same master device. At all times these direct links are under the control of the master device. For example, common to all use cases, there may be a regulatory requirement for transmissions from slave to master to cease immediately if so requested by the master, or if connection to the master is lost for more than a specified period of time. When one of these conditions occurs, transmissions from slave to slave would also cease. Various mechanisms could be used to detect loss of signal from the master, for example by requiring masters to transmit regular beacons if they allow slave to slave communications. Direct slave to slave transmissions could only restart if each slave subsequently restores its connection to the same master, or each slave joins the network of another master.

5. Problem Statement

The use of white space spectrum is enabled via the capability of a device to query a database and obtain information about the availability of spectrum for use at a given location. The databases are reachable via the Internet and the devices querying these databases are expected to have some form of Internet connectivity, directly or indirectly. The databases may be country specific since the available spectrum and regulations may vary, but the fundamental operation of the protocol should be country independent.

An example high-level architecture of the devices and white space databases is shown in Figure 11:

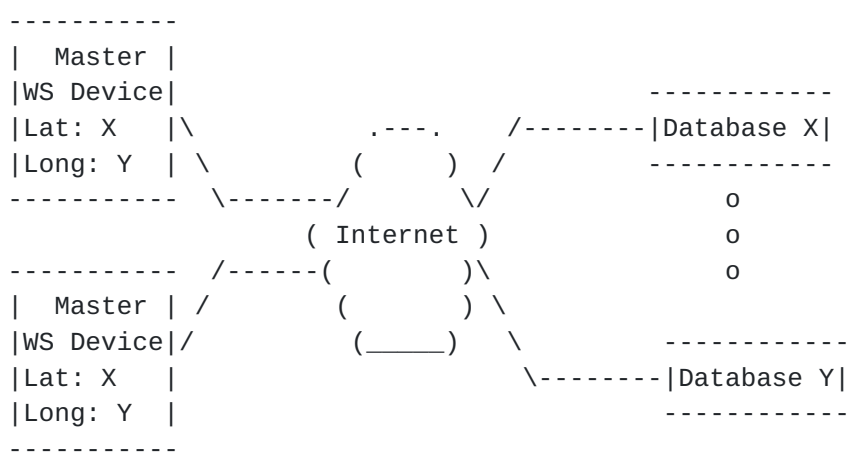

Figure 11: High level view of the White space database architecture

In Figure 11, note that there could be multiple databases serving white space devices. The databases are country specific since the regulations and available spectrum may vary. In some countries, for example, the U.S., the regulator has determined that multiple, competing databases may provide service to White Space Devices.

A messaging interface between the white space devices and the database is required for operating a network using the white space spectrum. The following sections discuss various aspects of such an interface and the need for a standard. Other aspects of a solution including provisioning the database, and calculating protected contours are considered out of scope of the initial effort, as there are significant differences between countries and spectrum bands.

5.1. Global applicability

The use of TV white space spectrum is currently approved by the FCC in the United States. However regulatory bodies in other countries are also considering similar use of available spectrum. The principles of cognitive radio usage for such spectrum is generally the same. Some of the regulatory details may vary on a country specific basis. However the need for devices that intend to use the spectrum to communicate with a database remains a common feature. The database provides a known, specifiable Protection Contour for the primary user, not dependent on the characteristics of the White Space Device or its ability to sense the primary use. It also provides a way to specify a schedule of use, because some primary users (for example, wireless microphones) only operate in limited time slots.

Devices need to be able to query a database, directly or indirectly over the public Internet and/or private IP networks prior to

operating in available spectrum. Information about available spectrum, schedule, power, etc. are provided by the database as a response to the query from a device. The messaging interface needs to be:

1. Radio/air interface agnostic - The radio/air interface technology used by the white space device in available spectrum can be IEEE 802.11af, IEEE 802.15.4m, IEEE 802.16, IEEE 802.22, LTE etc. However the messaging interface between the white space device and the database should be agnostic to the air interface while being cognizant of the characteristics of various air-interface technologies and the need to include relevant attributes in the query to the database.

2. Spectrum agnostic - the spectrum used by primary and secondary users varies by country. Some spectrum has an explicit notion of a "channel" a defined swath of spectrum within a band that has some assigned identifier. Other spectrum bands may be subject to white space sharing, but only have actual frequency low/high parameters to define protected entity use. The protocol should be able to be used in any spectrum band where white space sharing is permitted.

3. Globally applicable - A common messaging interface between white space devices and databases will enable the use of such spectrum for various purposes on a global basis. Devices can operate in any country where such spectrum is available and a common interface ensures uniformity in implementations and deployment. Since the White Space Device must know its geospatial location to do a query, it is possible to determine which database, and which rules, are applicable, even though they are country specific.

4. Address regulatory requirements - Each country is likely to have regulations that are unique to that country. The messaging interface needs to be flexible to accommodate the specific needs of a regulatory body in the country where the white space device is operating and connecting to the relevant database.

5.2. Database discovery

Another aspect of the problem space is the need to discover the database. A white space device needs to find the relevant database to query, based on its current location or for another location. Since the spectrum and databases are country specific, the device will need to discover the relevant database. The device needs to obtain the IP address of the specific database to which it can send queries in addition to registering itself for operation and using the available spectrum.

5.3. Protocol

A protocol that enables a white space device to query a database to obtain information about available channels is needed. A device may be required to register with the database with some credentials prior to being allowed to query. The requirements for such a protocol are specified in this document.

5.4. Data model definition

The contents of the queries and response need to be specified. A data model is required which enables the white space device to query the database while including all the relevant information such as geolocation, radio technology, power characteristics, etc. which may be country and spectrum and regulatory dependent. All databases are able to interpret the data model and respond to the queries using the same data model that is understood by all devices.

Use of XML for specifying a data model is an attractive option. The intent is to evaluate the best option that meets the need for use between white space devices and databases.

6. Requirements

6.1. Normative Requirements

D. Data Model Requirements:

D.1: The Data Model MUST support specifying the location of the WSD, the uncertainty in meters, the height & its uncertainty, and confidence in percentage of the location determination. The Data Model MUST support both North American Datum of 1983 and WGS84.

D.2: The Data Model MUST support specifying the regulatory domain and its corresponding data requirements.

D.3: The Data Model MUST support specifying an ID of the transmitter device. This ID would contain the ID of the transmitter device that has been certified by a regulatory body for its regulatory domain. The Data Model MUST support a device class. The Data Model MUST support specifying information about the type of RAT of the transmitter device.

D.4: The Data Model MUST support specifying a manufacturer's serial number for a white space device.

D.5: The Data Model MUST support specifying the antenna and radiation related parameters of the subject, such as:

antenna height

antenna gain

maximum output power, EIRP (dBm)

antenna radiation pattern (directional dependence of the strength of the radio signal from the antenna)

spectrum mask with lowest and highest possible frequency

spectrum mask in dBr from peak transmit power in EIRP, with specific power limit at any frequency linearly interpolated between adjacent points of the spectrum mask

measurement resolution bandwidth for EIRP measurements

D.6: The Data Model MUST support specifying owner and operator contact information for a transmitter. This includes the name of the transmitter owner, name of transmitter operator, postal address, email address and phone number of the transmitter operator.

D.7: The Data Model MUST support specifying a list of available channels. The Data Model MUST support specification of this information by channel numbers and by start and stop frequencies. The Data Model MUST support a channel availability schedule and maximum power level for each channel in the list.

D.8: The Data Model MUST support specifying channel availability information for a single location and an area (e.g. a polygon defined by multiple location points or a geometric shape such as a circle).

D.9: The Data Model MUST support specifying the frequencies and power levels selected for use by a device in the acknowledgement message.

P. Protocol Requirements:

P.1: The protocol MUST provide a mechanism to enable WSD discovery. In some environments, a listing of the approved white space databases is maintained by the national regulator. The protocol MUST support discovery of a database using a listing approved by a national regulator.

P.2: The address of a database (e.g. in form of a URI) can be preconfigured in a master device. The master device MUST be able to contact a database using a pre-configured database address.

P.3: The protocol MUST support determination of regulatory domain governing its current location.

P.4: The protocol MUST provide the ability for the database to authenticate the master device.

P.5: The protocol MUST provide the ability for the master device to verify the authenticity of the database with which it is interacting.

P.6: The messages sent by the master device to the database and the messages sent by the database to the master device MUST support integrity protection.

P.7: The protocol MUST provide the capability for messages sent by the master device and database to be encrypted.

P.8: The protocol MUST support the master device registering with the database.

P.9: The protocol MUST support a registration acknowledgement including appropriate result codes.

P.10: The protocol MUST support a channel query request from the master device to the database. The channel query request message MUST include parameters as required by local regulatory requirement. These parameters MAY include any of the parameters and attributes required to be supported in the Data Model Requirements.

P.11: The protocol MUST support a channel query response from the database to the master device. The channel query response message MUST include parameters as required by local regulatory requirement. These parameters MAY include any of the parameters and attributes required to be supported in the Data Model Requirements.

P.12: The protocol MUST support a channel usage message from the master device to the database. The channel usage message MUST include parameters as required by local regulatory requirement for the master and its associated slaves. These parameters MAY include any of the parameters and attributes required to be supported in the Data Model Requirements.

P.13: The protocol MUST support a channel usage message acknowledgement.

P.14: The protocol MUST support a validation request from the master to the database to validate a slave device. The validation request MUST include the slave device ID.

P.15: The protocol MUST support a validation response from the database to the master to indicate if the slave device is validated by the WSDB. The validation response MUST include a response code.

P.16: The protocol between the master device and the database MUST support the capability to change channel availability information on short notice.

P.17: The protocol between the master device and the database MUST support a channel availability request which specifies a geographic location as an area as well as a point.

6.2. Non-normative requirements

O. Operational Requirements:

O.1: The database and the master device MUST be connected to the Internet.

O.2: A master device MUST be able to determine its location including uncertainty and confidence level. A fixed master device MAY use a location programmed at installation or have the capability to determine its location to the required accuracy. A mobile master device MUST have the capability to determine its location to the required accuracy.

O.3: The master device MUST identify a database to which it will register, make channel requests, etc... The master device MAY select a database for service by discovery at runtime or the master device MAY select a database for service by means of a pre-programmed URI address.

O.4: The master device MUST implement at least one connection method to access the database. The master device MAY contact a database directly for service (e.g. as defined by FCC) or the master device MAY contact a listing server first followed by contact to a database (e.g. as defined by Ofcom).

O.5: The master device MUST obtain an indication about the regulatory domain governing operation at its current location, i.e. the master device MUST know if it operates under regulations from FCC, Ofcom, etc...

O.6: The master device MAY register with the database according to local regulatory policy. Not all master devices will be required to register. Specific events will initiate registration, these events are determined by regulator policy (e.g. at power up, after movement, etc...). When local regulatory policy requires registration, the master device MUST register with its most current and up-to-date information, and MUST include all variables mandated by local regulator policy.

O.7: A master device MUST query the database for the available channels based on its current location before starting radio transmission in white space. Parameters provided to the database MAY include device location, accuracy of the location, antenna characteristic information, device identifier of any slave device requesting channel information, etc...

O.8: The database MUST respond to an available channel list request from an authenticated and authorized device and MAY also provide time constraints, maximum output power, start and stop frequencies for each channel in the list and any additional requirements for sensing.

O.9: According to local regulator policy, a master device MAY inform the database of the actual frequency usage of the master and its slaves. The master MUST include parameters required by local regulatory policy, e.g. device ID, manufacturer's serial number, channel usage and power level information of the master and its slaves.

O.10: After connecting to a master device's radio network a slave device MUST query the master device for a list of available channels. The slave MUST include parameters required by local regulatory policy, e.g. device ID, device location.

O.11: According to local regulatory policy, the master device MAY query the database with parameters received from the slave device.

O.12: The database MUST respond to a query from the master device containing parameters from a slave device.

O.13: A master device MUST repeat the query to the database for the available channels as often as required by the regulation (e.g., FCC requires once per day) to verify that the operating channels continue to remain available.

O.14: A master device which changes its location more than a threshold distance (specified by local regulatory policy) during its operation, MUST query the database for available operating channels each time it moves more than the threshold distance (e.g., FCC specifies 100m) from the location it previously made the query.

O.15: According to local regulator policy, a master device may contact a database via proxy service of another master device.

O.16: 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.

O.17: A Master device MUST include its unique identity in all message exchanges with the database.

6.3. Guidelines

The current scope of the working group is limited and is reflected in the requirements captured in Section 6.1. However white space technology itself is expected to evolve and address other aspects such as co-existence and interference avoidance, spectrum brokering, alternative spectrum bands, etc. The design of the data model and protocol should be cognizant of the evolving nature of white space technology and consider the following set of guidelines in the development of the data model and protocol:

1. The data model SHOULD provide a modular design separating out messaging specific, administrative specific, and spectrum specific parts into separate modules.

2. The protocol SHOULD support determination of which administrative specific and spectrum specific modules are used.

7. IANA Considerations

This document has no requests to IANA.

8. Security Considerations

Threat model for the PAWS protocol

Assumptions:

It is assumed that an attacker has full access to the network medium between the master device and the white space database. The attacker may be able to eavesdrop on any communications between these entities. The link between the master device and the white space database can be wired or wireless and provides IP connectivity.

It is assumed that both the master device and the white space database have NOT been compromised from a security standpoint.

Threat 1: User modifies a device to masquerade as another valid certified device

> Regulatory environments require that devices be certified and register in ways that accurately reflect their certification. Without suitable protection mechanisms, devices could simply listen to registration exchanges, and later registering claiming to be those other devices. Such replays would allow false registration, violating regulatory regimes. A white space database may be operated by a commercial entity which restricts access only to authorized users. A master device MAY need to identify itself to the database and be authorized to obtain information about available channels.

Threat 2: Spoofed white space database

> A master device discovers a white space database(s) through which it can query for channel information. The master device needs to ensure that the white space database with which it communicates with is an authentic entity. The white space database needs to provide its identity to the master device which can confirm the validity/authenticity 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.

Threat 3: Modifying a query request

An attacker may modify the query request sent by a master device to a white space database. The attacker may change the location of the device or the capabilities in terms of its transmit power or antenna height etc. which could result in the database responding with incorrect information about available channels or max transmit power allowed. The result of such an attack is that the master device would cause interference to the primary user of the spectrum. It could also result in a denial of service to the master device by indicating that no channels are available.

Threat 4: Modifying a query response

An attacker could modify the query response sent by the white space database to a master device. The channel information or transmit power allowed type of parameters carried in the response could be modified by the attacker resulting in the master device using channels that are not available at a location or transmitting at a greater power level than allowed resulting in interference to the primary user of that spectrum. Alternatively the attacker may indicate no channel availability at a location resulting in a denial of service to the master device.

Threat 5: Unauthorized use of channels by an uncertified device

An attacker may be a master device which is not certified for use by the relevant regulatory body. The attacker may listen to the communication between a valid master device and white space database and utilize the information about available channels in the response message by utilizing those channels. The result of such an attack is unauthorized use of channels by a master device which is not certified to operate. The master device querying the white space database may be operated by a law-enforcement agency and the communications between the device and the database are intended to be kept private. A malicious device should not be able to eavesdrop on such communications.

Threat 6: Third party tracking of white space device location and identity

A white space database in a regulatory domain may require a master device to provide its identity in addition to its location in the query request. Such location/identity information can be gleaned by an eavesdropper and used for tracking purposes. A master device may prefer to keep the location/identity information hidden from eavesdroppers, hence the protocol should provide a means to protect the location and identity information of the master device

and prevent tracking of locations associated with a white space database query. When the master device sends both its identity and location to the DB, the DB is able to track it. If a regulatory domain does not require the master device to provide its identity to the white space database, the master device may decide not to send its identity, to prevent being tracked by the DB.

Threat 7: Malicious individual acts as a PAWS entity (spoofing DB or as MiM) to terminate or unfairly limit spectrum access of devices for reasons other than incumbent protection

A white space database MAY include a mechanism by which service and channels allocated to a master device can be revoked by sending an unsolicited message. A malicious node can pretend to be the white space database with which a master device has registered or obtained channel information from and send a revoke message to that device. This results in denial of service to the master device.

Threat 8: Natural disaster resulting in inability to obtain authorization for white space spectrum use by emergency responders

In the case of a sizable natural disaster a lot of Internet infrastructure ceases to function. Emergency services users need to reconstitute quickly and will rely on establishing radio WANs. The potential for lot of radio WAN gear that has been unused suddenly needs to be pressed into action. And the radio WANs need frequency authorizations to function. Regulatory entities may also authorize usage of additional spectrum in the affected areas. The white space radio entities may need to establish communication with a database and obtain authorizations. In cases where communication with the white space database fails, the white space devices cannot utilize white space spectrum. Emergency services, which require more spectrum precisely at locations where network infrastructure is malfunctioning or overloaded, backup communication channels and distributed white space databases are needed to overcome such circumstances. Alternatively there may be other mechanisms which allow the use of spectrum by emergency service equipment without strict authorization or with liberal interpretation of the regulatory policy for white space usage.

The security requirements arising from the above threats are captured in the requirements of section 6.1.

9. Summary and Conclusion

Wireless spectrum is a scarce resource. As the demand for spectrum grows, there is a need to more efficiently utilize the available and allocated spectrum. Cognitive radio technologies enable the efficient usage of spectrum via means such as sensing or by querying a database to determine available spectrum at a given location for opportunistic use. White space is the general term used to refer to the bands within the spectrum which is available for secondary use at a given location. In order to use this spectrum a device needs to query a database which maintains information about the available channels within a band. A protocol is necessary for communication between the devices and databases which would be globally applicable.

The document describes some examples of the role of the white space database in the operation of a radio network and also shows examples of services provided to the user of a TVWS device. From these use cases, requirements are determined. These requirements are to be used as input to the definition of a Protocol to Access White Space database (PAWS).

10. Acknowledgements

The authors acknowledge Gabor Bajko, Teco Boot, Nancy Bravin, Rex Buddenberg, Gerald Chouinard, Stephen Farrell, Michael Fitch, Joel M. Halpern, Jussi Kahtava, Paul Lambert, Brian Rosen, Andy Sago, Peter Stanforth, John Stine and, Juan Carlos Zuniga for their contributions to this document.

11. References

11.1. Normative References

[802.11p] IEEE, "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements; Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications; Amendment 6: Wireless Access in Vehicular Environments; http://standards.ieee.org/getieee802/download/802.11p-2010.pdf", July 2010.

[802.22] IEEE, "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Wireless Regional Area Networks (WRAN) - Specific requirements; Part 22: Cognitive Wireless RAN

Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV bands", July 2011.

[FCC47CFR90.210]
FCC, "Title 47 Telecommunication CFR Chapter I - Federal Communication Commission Part 90 - Private Land Mobile Radio Services - Section 210 Emission masks; http://edocket.access.gpo.gov/cfr_2010/octqtr/pdf/47cfr90.210.pdf", October 2010.

[PAWS-PS] IETF, "Protocol to Access White Space database: Problem statement; https://datatracker.ietf.org/doc/draft-patil-paws-problem-stmt/", July 2011.

[RFC2119] IETF, "Key words for use in RFCs to Indicate Requirement Levels; http://www.rfc-editor.org/rfc/pdfrfc/rfc2119.txt.pdf", March 1997.

11.2. Informative References

[3MOO] FCC, "Federal Communications Commission, Third Memorandum Opinion and Order", April 2012.

[DDR] Ofcom - Independent regulator and competition authority for the UK communications industries, "Digital Dividend Review; http://stakeholders.ofcom.org.uk/spectrum/project-pages/ddr/".

[DTV] "Digital TV Transition; http://www.dtv.gov".

[ECC Report 159]
Electronic Communications Committee (ECC) within the European Conference of Postal and Telecommunications Administrations (CEPT), "TECHNICAL AND OPERATIONAL REQUIREMENTS FOR THE POSSIBLE OPERATION OF COGNITIVE RADIO SYSTEMS IN THE 'WHITE SPACES' OF THE FREQUENCY BAND 470-590 MHZ; http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP159.PDF", January 2011.

[FCC Ruling]
FCC, "Federal Communications Commission, "Unlicensed Operation in the TV Broadcast Bands; http://edocket.access.gpo.gov/2010/pdf/2010-30184.pdf"", December 2010.

[Ofcom Implementing]

Ofcom, "Ofcom, "Implementing Geolocation; http://stakeholders.ofcom.org.uk/consultations/geolocation/statement/"", September 2011.

[Ofcom Requirements]
Ofcom, "Ofcom, Draft final regulatory requirements for white space devices in the UHF TV band", June 2012.

[RFC5222] IETF, Hardie, T., Netwon, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol;http://www.rfc-editor.org/rfc/pdfrfc/rfc5222.txt.pdf", August 2008.

[Spectrum Framework Review]
Ofcom - Independent regulator and competition authority for the UK communications industries, "Spectrum Framework Review; http://stakeholders.ofcom.org.uk/consultations/sfr/", February 2005.

[TV Whitespace Tutorial Intro]
IEEE 802 Executive Committee Study Group on TV White Spaces, "TV Whitespace Tutorial Intro; http://grouper.ieee.org/groups/802/802_tutorials/2009-03/2009-03-10%20TV%20Whitespace%20Tutorial%20r0.pdf", March 2009.

Authors' Addresses

Scott Probasco (editor)
Nokia
6021 Connection drive
Irving, TX 75039
USA

Email: scott.probasco@nokia.com

Basavaraj Patil
Nokia
6021 Connection drive
Irving, TX 75039
USA

Email: basavaraj.patil@nokia.com