

PAWS
Internet-Draft
Intended status: Informational
Expires: August 18, 2013

Mancuso, Ed.
Google
Probasco
Patil
February 14, 2013

Protocol to Access White Space (PAWS) Database: Use Cases and
Requirements

draft-ietf-paws-problem-stmt-usecases-rqmts-13

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. This document includes the problem statement for the development of a protocol to access a database of whitespace information followed by use cases and requirements for that protocol. Finally, requirements associated with the protocol are presented.

Requirements Language

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].

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 August 18, 2013.

Copyright Notice

Copyright (c) 2013 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
 - 1.1. Introduction to White Space 3
 - 1.2. Scope 4
 - 1.2.1. In Scope 4
 - 1.2.2. Out of Scope 4
- 2. Terminology Used in this Document 4
- 3. Problem Statement 5
 - 3.1. Global Applicability 6
 - 3.2. Database Discovery 7
 - 3.3. Device Registration 8
 - 3.4. Protocol 8
 - 3.5. Data Model Definition 8
- 4. Use Cases 9
 - 4.1. Master-slave White Space Networks 9
 - 4.2. Offloading: Moving Traffic to a White Space Network . . . 11
 - 4.3. White Space Serving as Backhaul 13
 - 4.4. Rapid Network Deployment During Emergencies 14
 - 4.5. White Space Used for Local TV Broadcaster 15
- 5. Requirements 16
 - 5.1. Data Model Requirements 16
 - 5.2. Protocol Requirements 17
 - 5.3. Operational Requirements 18
 - 5.4. Guidelines 19
- 6. IANA Considerations 19

7. Security Considerations 20
8. Acknowledgements 21
9. References 22
9.1. Normative References 22
9.2. Informational References 22
Authors' Addresses 22

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 (primary) user but are unused or unoccupied at specific locations and times are defined as "white space." The concept of allowing additional (secondary) 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 secondary transmissions do not interfere with the assigned use of the spectrum. One interesting observation is that often, in a given physical location, the primary user(s) may not be using the entire band assigned to them. The available spectrum for secondary transmissions would then depend on the location of the secondary user. The fundamental issue is how to determine, for a specific location and specific time, if any of the assigned spectrum is available for secondary use.

Academia and Industry have studied multiple cognitive radio [1] mechanisms for use in such a scenario. One simple mechanism is to use a geospatial database that contains the spatial and temporal profile of all primary licensees' spectrum usage, and require secondary users to query the database for available spectrum that they can use at their location. Such databases can be accessible and queryable by secondary users on the Internet.

Any entity that is assigned spectrum that is not densely used may be asked by a governmental regulatory agency to share it to allow for more intensive use of the spectrum. Providing a mechanism by which secondary users share the spectrum with the primary user is attractive in many bands in many countries.

This document includes the problem statement followed by use cases and requirements associated with the use of white-space spectrum by secondary users via a database query protocol. The final sections include the requirements associated with such a protocol. Note that the IETF has undertaken to develop a white-space database query protocol (see [I-D.ietf-paws-protocol]).

Mancuso, et al.

Expires August 18, 2013

[Page 3]

Internet-Draft

paws-use-cases-and-reqmts

February 2013

1.2. Scope

1.2.1. In Scope

This document covers the requirements for a protocol to allow a device to access a database to obtain spectrum availability information. Such a protocol should allow a device to perform the following actions:

1. Determine the relevant white-space database to query.
2. Connect to and optionally register with the database using a well-defined protocol.
3. Provide its geolocation and perhaps other data to the database using a well-defined format for querying the database.
4. Receive in response to the query a list of available white-space frequencies using a well-defined format for the information.
5. Send an acknowledgment to the database with information containing channels selected for use by the device and other device operation parameters.

Note. The above protocol actions should explicitly or implicitly support the ability of devices to re-register and/or re-query the database when it changes its location or operating parameters, to receive permission to operate in its new location and/or with its new operating parameters, and send an acknowledgment to the database that includes information on its new operating parameters.

1.2.2. Out of Scope

The following topics are out of scope for this specification:

1. Co-existence and interference avoidance of white space devices within the same spectrum.
2. Provisioning (releasing new spectrum for white space use).

2. Terminology Used in this Document

Database A database is an entity that contains current information about available spectrum at a given location and time as well as other types of information related to spectrum availability and usage.

Mancuso, et al. Expires August 18, 2013 [Page 4]

Internet-Draft paws-use-cases-and-reqmts February 2013

Device Class Identifies classes of devices including fixed, mobile, portable, etc... May also indicate if the device is indoor or outdoor.

Device ID An identifier for each master device.

Master Device A device that queries the database, on its own behalf and/or on behalf of a slave device, to obtain available spectrum information.

Slave Device A device that queries the database through a master device.

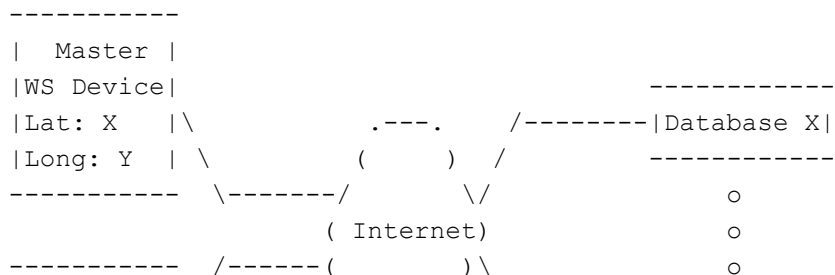
White Space (WS) Radio spectrum that is available for secondary use at a specific location and time.

White Space Device (WSD) A device that uses white-space spectrum as a secondary user. A white space device can be a fixed or portable device such as an access point, base station, or cell phone.

3. 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. While databases are expected to support the rule set(s) of one or more regulatory domains, and the regulations and available spectrum associated with each rule set may vary, the fundamental operation of the protocol should be regulatory independent.

An example high-level architecture of the devices and white-space databases is shown in Figure 1.



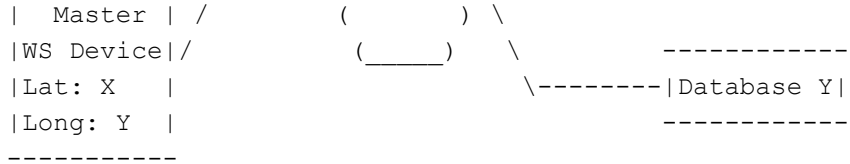


Figure 1: High-level View of White Space Database Architecture

Note that there could be multiple databases serving white space devices. In some countries, such as the U.S., the regulator has determined that multiple 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.

3.1. Global Applicability

The use of white-space spectrum is currently approved or being considered in multiple regulatory domains, whose rules may differ. However, the need for devices that intend to use the spectrum to communicate with a database remains a common feature. The database implements rules that protect all primary users, independent of the characteristics of the white space devices. It also provides a way to specify a schedule of use, since 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. Interface agnostic - An interface between a master white space device and database can be wired or unwired (e.g., a radio/air interface technology such as IEEE 802.11af, IEEE 802.15.4m, IEEE 802.16, IEEE 802.22, LTE etc.) However, the messaging interface

between a master white space device and the database should be agnostic to the interface used for such messaging while being cognizant of the characteristics of the interface technology and the need to include any 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 primary and secondary 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 location where such spectrum is available and a common interface ensures uniformity in implementations and deployment. To allow the global use of white space devices in different countries (whatever the regulatory domain), the protocol should support the database communicating applicable regulatory rule set information to the white space device.
4. Flexible and extensible data structures - Different databases are likely to have different requirements for the kinds of data required for registration (different regulatory rule sets that apply to the registration of devices) and other messages sent by the device to the database. For instance, different regulators might require different device-characteristic information to be passed to the database.

3.2. Database Discovery

The master device must obtain the address of a trusted white-space database, which it will query for available white-space spectrum. If the master device uses a discovery service to locate a trusted white-space database, it performs the following steps:

1. The master device constructs and sends a request (e.g., over the Internet) to a trusted discovery service.
2. 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. If so, it establishes contact with the trusted database.

3. The master device establishes a white space network as described in Section 4.

Optionally, and in place of steps 1 - 3 above, the master device can be pre-programmed with the location (e.g., Internet address) of one or more one trusted databases. The master device can establish contact with one of these trusted databases.

3.3. Device Registration

The master device may register with the database before it queries the database for available spectrum. A registration process may consist of the following steps:

1. The master device sends registration information to the database. This information may include the Device ID, serial number assigned by the manufacturer, device location, device antenna height above ground, name of the individual or business that owns the device, and the name, street and email address, and telephone number of a contact person responsible for the device's operation.
2. The database responds to the registration request with an acknowledgement to indicate the success of the registration request or with an error if the registration was unsuccessful. Additional information may be provided by the database in its response to the master device.

3.4. Protocol

A protocol that enables a white space device to query a database to obtain information about available spectrum 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.

3.5. 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.

Mancuso, et al.

Expires August 18, 2013

[Page 8]

Internet-Draft

paws-use-cases-and-reqmts

February 2013

4. Use Cases

There are many potential use cases for white-space spectrum - for example, providing broadband Internet access in urban and densely-populated hotspots as well as rural and remote, underserved areas. Available white-space spectrum may also be used to provide Internet 'backhaul' for traditional Wi-Fi hotspots or for use by towns and cities to monitor/control traffic lights, read utility meters, and the like. Still other use cases include the ability to offload data traffic from another Internet access network (e.g., 3G cellular network) or to deliver data, information, or a service to a user based on the user's location. Some of these use cases are described in the following sections.

4.1. Master-slave White Space Networks

There are a number of common scenarios in which a master white space device will act as proxy or mediator for one or more slave devices using its connection to the Internet to query the database for available spectrum for itself and for one or more slave devices. These slave devices may be fixed or mobile, in close proximity with each other (indoor network or urban hotspot), or at a distance (rural or remote WAN). Once slave devices switch to white-space spectrum for their communications, they may connect through the master to the Internet or use white-space spectrum for intra-network communications only. The master device can continue to arbitrate and control white space communications by slave devices, and may notify them when they are required to change white-space frequencies or cease white space communications.

Figure 2 depicts the general architecture of such a simple master-slave network, in which the master device communicates on its own

behalf and on behalf of slave devices with a white-space database.

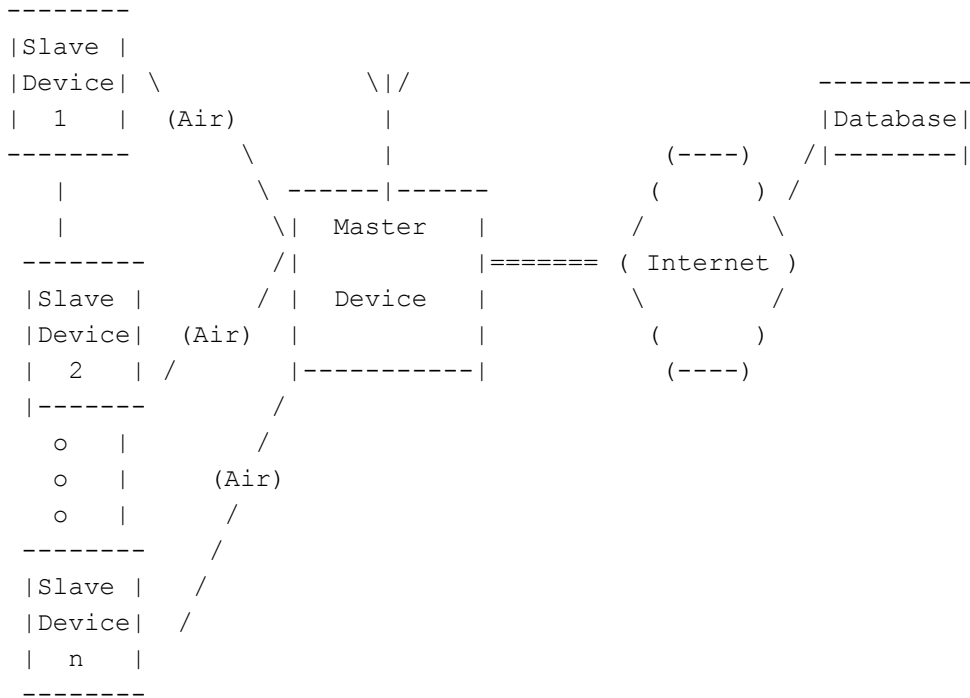


Figure 2: Master-Slave White Space Network

The protocol requirements for these master-slave device and other

similar scenarios is essentially the same: the protocol must support the ability of a master device to make available-spectrum query requests on behalf of slave devices, passing device identification, geolocation, and other slave device parameters to the database as required to obtain a list of white-space spectrum available for use by one or more slave devices. Of course, different use cases will use this spectrum information in different ways, and the details of master/slave communications may be different for different use cases.

Common steps may occur in master-slave networks include the following:

1. The master device powers up.
2. Slave devices power up and associate with the master device via Wi-Fi or some other over-the-air non-white-space spectrum. Until the slave device is allocated white-space spectrum, any master-slave or slave-slave communications occurs over such non-white-space spectrum.
3. The master has Internet connectivity, determines (or knows) its location, and establishes a connection to a trusted white-space database (see Section 3.2).

4. The master may register with the trusted database (see Section 3.3).
5. The master sends a query to the trusted database requesting a list of available white-space spectrum based upon its geolocation. Query parameters may include the master's location, device identifier, and antenna height. The master may send available-spectrum requests to the database on behalf of slave devices.
6. The database responds to the master's query with a list of available white-space spectrum, associated maximum power levels, and a durations of time for spectrum use. If the master made requests on behalf of slave devices, the master may transmit the obtained available-spectrum lists to the slaves (or the master may allocate spectrum to slaves from the obtained spectrum

lists).

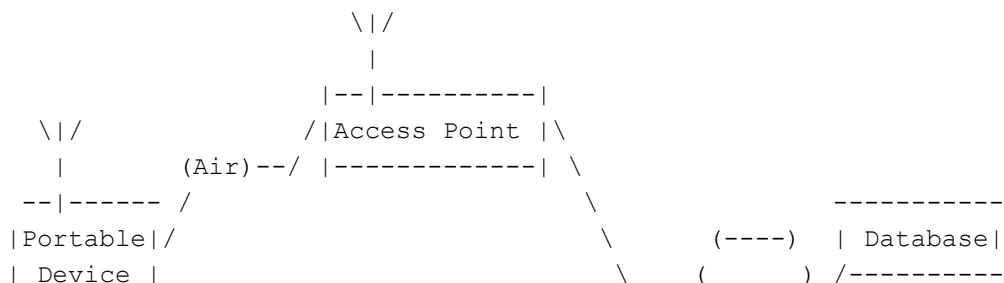
7. The master may inform the database of the spectrum and power level it selects from the available spectrum list. If a slave device has been allocated available white-space spectrum, the slave may inform the master of the spectrum and power level it has chosen, and the master may, in turn, relay such slave device usage to the database.
8. Further communication among masters and slaves over the white space network may occur via the selected/allocated white-space spectrum frequencies.

Note: Steps 5 through 7 may be repeated by the master device when it (or a slave device that uses the master as a proxy to communicate with the database) changes its location or operating parameters -- for example, after a master changes location, it may query the database for available spectrum at its new location, then acknowledge the subsequent response received from the database with information on the spectrum and power levels it is using at the new location.

4.2. Offloading: Moving Traffic to a White Space Network

This scenario is a variant of the master-slave network described in the previous use case. In this scenario, an access point (AP) offers a white space service that offloads Internet traffic as an alternative datapath to a more congested or costly Internet wire, wireless, or satellite service.

Figure 3 shows an example deployment of this scenario.



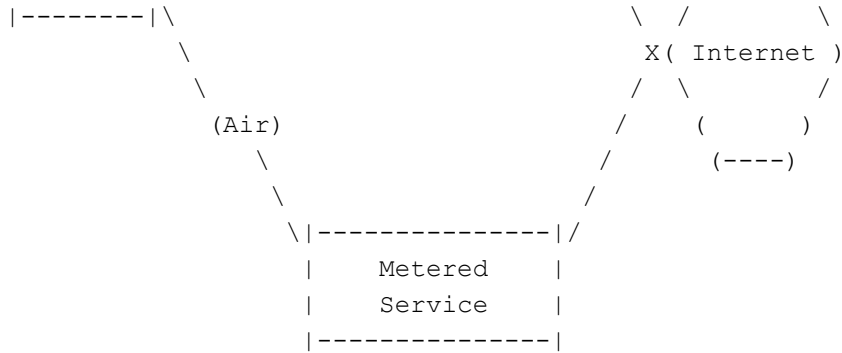


Figure 3: Offloading Traffic to a White Space Network

A simplified operation scenario of offloading content, such as video stream, from the a congested or costly Internet connection to a white space service provided by an AP consists of the following steps:

1. The AP contacts the database to determine channels it can use.
2. The portable device connects to a paid Internet service and selects a video for streaming.
3. The portable device determines if it can offload to a white space access point:
 - A. If the portable device knows its location, it
 1. asks the database (using the paid service) for available white-space spectrum;
 2. listens for and connects to the AP over the permitted white-space spectrum.
 - B. If the portable device does not have GPS or other means to determine its position, it
 1. uses non-white-space spectrum to listen for and connect to the AP;

2. asks the AP to query the database for permitted white-space spectrum on its behalf;
 3. uses the permitted white-space spectrum to connect to the AP.
4. The portable device accesses the Internet through the AP to stream the selected video.

4.3. White Space Serving as Backhaul

In this use case, an Internet connectivity service is provided to users over a common wireless standard, such as Wi-Fi, with a white space master/slave network providing backhaul connectivity to the Internet. Note that Wi-Fi is referenced in Figure 4 and the following discussion, but any other technology can be substituted in its place.

Figure 4 shows an example deployment of this scenario.

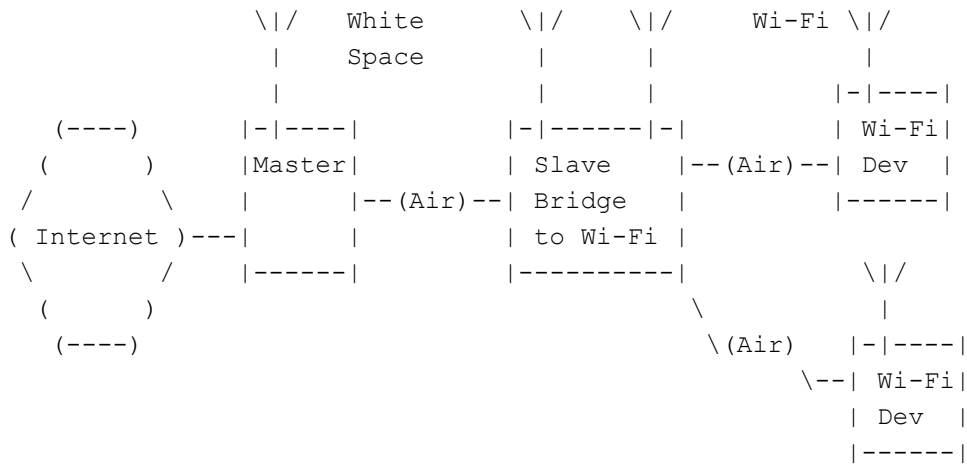


Figure 4: White Space Network Used for Backhaul

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:

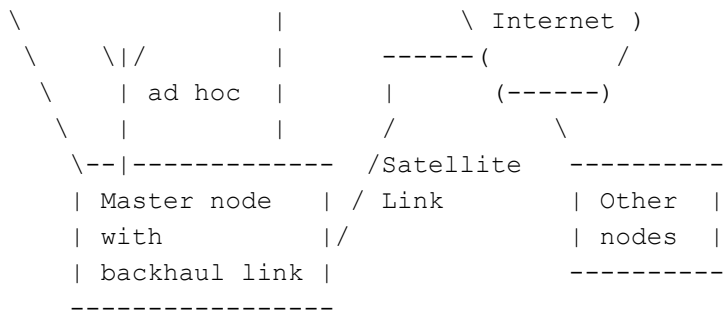


Figure 5: Rapid-deployed Network with Partly-connected Nodes

In the ad-hoc network, all nodes are master nodes that allocate RF channels from the white-space database (as described in Section 4.1). However, the backhaul link may not be available to all nodes, such as depicted for the left node in the above figure. 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.

4.5. White Space Used for Local TV Broadcaster

Available white-space spectrum can be deployed in novel ways to leverage the public use of hand-held and portable devices. One such use is white-space spectrum used for local TV transmission of audio-video content to portable devices used by individuals in attendance at an event. In this use case, audience members at a seminar, entertainment event, or other venue plug a miniature TV receiver fob into their laptop, computer tablet, cell phone, or other portable device. A master device obtains a list of available white-space spectrum (as described in , (Section 4.1), then broadcasts audio-video content locally to the audience over one of the available frequencies. Audience members receive the content through their miniature TV receivers tuned to the appropriate white space band for display on their portable device monitors.

Figure 6 shows an example deployment of this scenario.

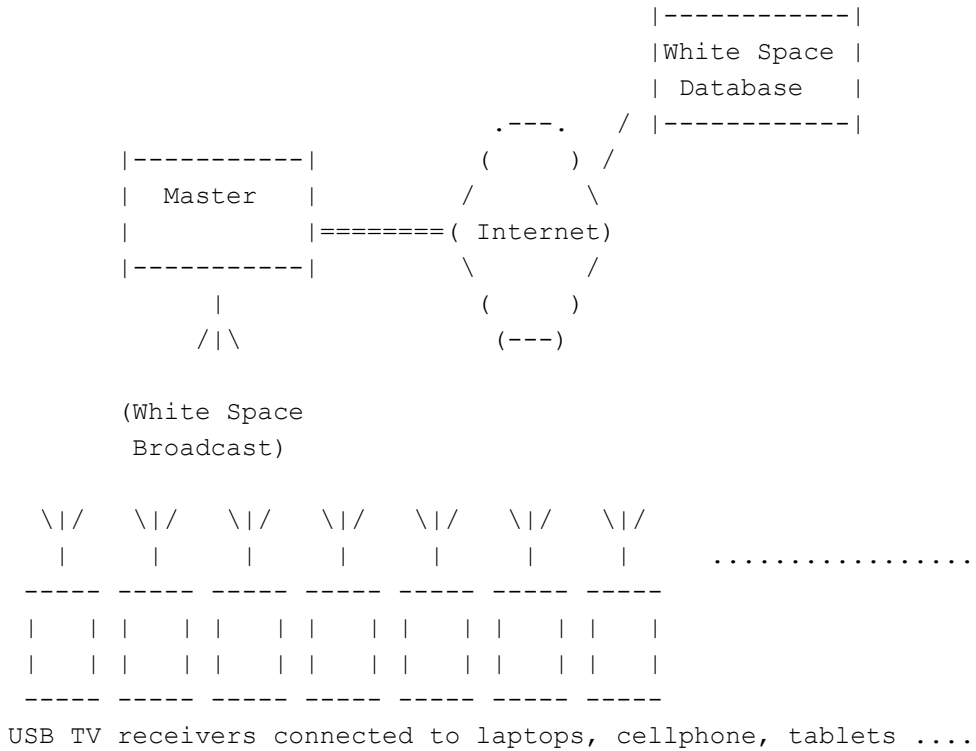


Figure 6: White Space Used for Local TV Broadcast

5. Requirements

5.1. Data Model Requirements

D.1 The Data Model MUST support specifying the geolocation of the white-space device, the uncertainty in meters, the height & its uncertainty, and confidence in percentage of the location determination. The Data Model MUST support [WGS84].

D.2 The Data Model MUST support specifying the data and other applicable requirements of the rule set that applies to the white space device at its current location.

D.3 The Data Model MUST support device description data that identifies a white-space device (serial number, certification IDs, etc.) and describes device characteristics, such as device class (fixed, mobile, portable, indoor, outdoor, etc.), Radio Access Technology (RAT), etc.

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 white-space device, 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 spectrum availability. Spectrum units are specified by low and high frequencies and may have an optional channel identifier. The Data Model MUST support a schedule including start time and stop time for spectrum unit availability. The Data Model MUST support maximum power level for each spectrum unit.
- D.8 The Data Model MUST support specifying spectrum 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 white-space device in the acknowledgement message.

5.2. Protocol Requirements

- P.1 The master device identifies a database to which it can register, make spectrum availability requests, etc. The protocol must support the discovery of an appropriate database given a location provided by the master device. The master device may select a database by discovery at run time or by means of a pre-programmed URI address. The master device may validate discovered or configured database addresses against a list of known databases (e.g., a list of databases approved by a regulatory body).
- P.2 The protocol must support the database informing the master of the regulatory rules (rule set) that applies to the master device (or any slave devices on whose behalf the master is contacting the database) at the current location or the master (or slave) device(s).
- P.3 The protocol MUST provide the ability for the database to authenticate the master device.
- P.4 The protocol MUST provide the ability for the master device to verify the authenticity of the database with which it is interacting.

- P.5 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.6 The protocol MUST provide the capability for messages sent by the master device and database to be encrypted.
- P.7 The protocol MUST support the master device registering with the database (see Device Registration (Section 3.3)).
- P.8 The protocol MUST support a registration acknowledgement indicating the success or failure of the master device registration.
- P.9 The protocol MUST support an available spectrum request from the master device to the database, which may include one or more of the data items listed in Data Model Requirements (Section 5.1).
- P.10 The protocol MUST support an available spectrum response from the database to the master device, which may include one or more of the data items listed in Data Model Requirements (Section 5.1).
- P.11 The protocol MUST support a spectrum usage message from the master device to the database, which may include one or more of the data items listed in Data Model Requirements (Section 5.1).
- P.12 The protocol MUST support a spectrum usage message acknowledgement.
- P.13 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.14 The protocol MUST support a validation response from the database to the master to indicate if the slave device is validated by the database. The validation response MUST indicate the success or failure of the validation request.
- P.15 The protocol MUST support the capability for the database to inform master devices of changes to spectrum availability information in a timely manner.

5.3. Operational Requirements

This section contains operational requirements of a white-space database-device system, independent of the requirements of the

protocol for communication between the white-space database and devices.

Mancuso, et al. Expires August 18, 2013 [Page 18]
Internet-Draft paws-use-cases-and-reqmts February 2013

- 0.1 The database and the master device MUST be connected (e.g., through the Internet).
- 0.2 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.
- 0.3 The master device MUST be configured to understand and comply with the requirements of the rule set of the regulatory body that apply to its operation at its location.
- 0.4 A master device MUST query the database for the available spectrum based on its current location before starting radio transmission in white space.
- 0.5 The database MUST respond to an available spectrum list request.
- 0.6 After connecting to a master device, a slave device MUST query the master device for a list of available spectrum. The master device then queries the database on behalf of the slave device for an available spectrum list, using parameters received from the slave device. After the master device receives a response to its request for an available spectrum list on behalf of a slave device, the master device MUST relay the response to the slave device.

5.4. Guidelines

White space technology itself is expected to evolve and include attributes 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.

6. IANA Considerations

This document makes no request of IANA.

Mancuso, et al. Expires August 18, 2013 [Page 19]
Internet-Draft paws-use-cases-and-reqmts February 2013

7. Security Considerations

PAWS is a protocol whereby a Master Device requests a schedule of available spectrum at its location (or location of its Slave Devices) before it (they) can operate using those frequencies. Whereas the information provided by the Database must be accurate and conform to applicable regulatory rules, the Database cannot enforce, through the protocol, that a client device uses only the spectrum it provided. In other words, devices can put energy in the air and cause interference without asking the Database. Hence, PAWS security considerations do not include protection against malicious use of the white-space spectrum.

Threat model for the PAWS protocol:

Assumptions:

The link between the master device and the white-space database can be wired or wireless and provides IP connectivity. 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.

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

A master device identifies itself to the database in order to obtain information about available spectrum. Without suitable protection mechanisms, devices can listen to registration

exchanges, and later register with the database by claiming the identity of another device.

Threat 2: Spoofed white-space database

A master device attempts to discover a white-space database(s) that it can query for available spectrum information. An attacker may attempt to spoof a white-space database and provide responses to a master device that 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 its capabilities (transmit power, antenna height etc.), and, as a result, the database responds

Mancuso, et al.

Expires August 18, 2013

[Page 20]

Internet-Draft

paws-use-cases-and-reqmts

February 2013

with incorrect information about available spectrum or maximum transmit power allowed. The result of such an attack is that the master device can cause interference to the primary user of the spectrum. It may also result in a denial of service to the master device if the modified database response indicates that no channels are available to the master device.

Threat 4: Modifying a query response

An attacker may modify the query response sent by the white-space database to a master device. For example, an attacker may modify the available spectrum or power level information carried in the database response. As a result, a master device may use spectrum that is not available at a location or may transmit at a greater power level than allowed. Such unauthorized use can result in interference to the primary user of that spectrum. Alternatively, an attacker may modify a database response to indicate that no spectrum is available at a location, resulting in a denial of service to the master device.

Threat 5: Third party tracking of white space device location and

identity

A master device may 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 unauthorized tracking purposes.

Threat 6: Malicious individual acts as a white space database to terminate or unfairly limit spectrum access of devices

A white-space database may include a mechanism by which service and spectrum allocated to a master device can be revoked by sending a revoke message to a master device. A malicious user can pretend to be a white-space database and send a revoke message to that device. This results in denial of service to the master device.

The security requirements arising from the above threats are captured in the requirements of Section 5.2.

8. Acknowledgements

The authors acknowledge Gabor Bajko, Teco Boot, Nancy Bravin, Rex Buddenberg, Vincent Chen, Gerald Chouinard, Stephen Farrell, Michael Fitch, Joel M. Halpern, Jussi Kahtava, Paul Lambert, Barry Leiba,

Mancuso, et al. Expires August 18, 2013 [Page 21]

Internet-Draft paws-use-cases-and-reqmts February 2013

Subramanian Moonesamy, Pete Resnick, Brian Rosen, Andy Sago, Peter Stanforth, John Stine, and Juan Carlos Zuniga for their contributions to this document.

9. References

9.1. Normative References

[I-D.ietf-paws-protocol]

Chen, V., Das, S., Zhu, L., Malyar, J., and P. McCann,
"Protocol to Access Spectrum Database",
draft-ietf-paws-protocol-03 (work in progress),
February 2013.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[WGS84] National Imagery and Mapping Agency, "Department of Defense World Geodetic System 1984, Its Definition and Relationships with Local Geodetic Systems, NIMA TR8350.2 Third Edition Amendment 1", January 2000, <http://earth-info.nga.mil/GandG/publications/tr8350.2/tr8350_2.html>.

9.2. Informational References

URIs

[1] <<http://fcc.gov/oet/cognitiveradio/>>

Authors' Addresses

Anthony Mancuso (editor)
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

Phone:
Fax:
Email: amancuso@google.com
URI:

Mancuso, et al. Expires August 18, 2013 [Page 22]

Internet-Draft paws-use-cases-and-reqmts February 2013

Scott Probasco

Phone:
Fax:
Email: scott@probasco.me

URI:

Basavaraj Patil

Phone:

Fax:

Email: bpatil@ovi.com

URI:

