

Internet Engineering Task Force  
Internet-Draft  
Intended status: Informational  
Expires: July 5, 2014

X. Wei  
L. Zhu  
Huawei  
Jan 2014

PAWS Database Discovery  
draft-wei-paws-database-discovery-03

Abstract

This document provides a Database Discovery mechanism for PAWS. By this mechanism the master device gets the available WSDBs it can communicate.

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 July 5, 2014.

Copyright Notice

Copyright (c) 2014 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. Motivations . . . . .	3
2. Terminology and Conventions . . . . .	5
3. Solutions . . . . .	6
3.1. Solution 1 . . . . .	6
3.2. Solution 2 . . . . .	7
3.3. Solution 3 . . . . .	10
3.4. Solution 4 . . . . .	11
4. Security Considerations . . . . .	11
5. IANA Consideration . . . . .	11
6. Acknowledgements . . . . .	11
7. References . . . . .	11
7.1. Normative references . . . . .	11
7.2. Informative References . . . . .	12
Authors' Addresses . . . . .	12

## 1. Introduction

### 1.1. Motivations

In the PAWS protocol, the master device queries the database for available spectrum, but it MUST determine the URL for the database before it can send any PAWS messages. Brief discussions of database discovery can be found in [RFC6953] and [PAWS PROTOCOL].

Different regulatory domains might deploy their own WSDB and several WSDBs might be deployed in the same regulatory domain, so before querying the WSDB master device should find out which WSDB can provide service for it. And there are some WSDB discovery scenarios.

S1: Master device locates in its own regulatory domain, master device needs to know the available WSDBs that can provide service for it in the regulatory domain.

S2: In the regulatory domain, when some WSDBs are not available any more or some new WSDBs are setup, master device should accommodate to the change of available WSDBs.

S3: A portable master device could move from its home regulatory domain to a different regulatory domain, and it should find available WSDB in target regulatory domain. For example, when a person, named Bob, travels and takes a Wi-Fi AP (could be integrated with laptop PC) with him, if there is a port of wired network, it is easy for him to setup a wireless network for use. But if Bob takes an AP using white space spectrum, it must find an available WSDB in that regulatory domain before setup the wireless network.

Several different methods could be used for master device to determine the appropriate URL(s) for connection. Here we list some possible methods for this purpose (not all methods are included here):

M1: The manufacture or the user of master device can manually pre-configure statically the URL(s) of one or more WSDBs that is available for master device to query white space spectrum (e.g. master device and WSDB have agreements with each other.). For example, if master device is to be used in U.S., it will be configured with the WSDB of U.S., and then it directly connects to the WSDB in U.S., or if master device is to be used in several countries it can be configured with different WSDBs for each country.

M2: Master device might be configured by certain provisioning process after attaching to operator's network. The provisioning process might be DHCP process, OSS process etc.

M3: An entity of Listing server [PAWS PROTOCOL], providing the URLs for one or more WSDBs, could be deployed in a regulatory domain, then master device queries and checks available WSDBs from the Listing server.

M4: When WSDB, which master device currently connects to, cannot provide service any more, it can redirects the master device to another WSDB that can provide service [PAWS PROTOCOL].

But in some scenarios the methods above may not work very well:

(1) To pre-configure master device, the user has to know the available WSDB (s) that can be used in the regulatory domain, it may be inconvenient especially when master device is moved to a different regulatory domain.

(2) It is possible that some WSDBs are not available any more or some new WSDBs are setup, the pre-configuring and provisioning method may not cope with it very well.

(3) In pre-configuring method, it is possible for master device to be pre-configured with available WSDB of several regulatory domains. But master device must decide which regulatory domain it locates in before choosing the available WSDB.

(4) The network provision method might work well only in case of WSDBs are maintained by network operators or there should be some agreement relationship between network operator and WSDB maintainer.

(5) In the method that WSDB provides redirecting to the master device, some security related issues have to be considered. It might be feasible for a WSDB to provide master device with URL of another WSDB in the same regulatory domain. But in case when master device moves from regulatory domain A to regulatory domain B, it might seem not right for WSDB of A to provide regulatory domain information and available WSDBs or Listing server of B to the master device, because WSDB and master devices are each certified to operate in certain regulatory domains.

At power-up master device does not reliably know the regulatory domain corresponding to its current location, and therefore does not reliably know with which WSDB(s) it can communicate to. Furthermore it is essential that master device connects with a trusted WSDB for proper operation and indeed regulatory compliance.

So a dynamic WSDB discovery mechanism is provided here, the mechanism can be used independently or cooperate with other methods, e.g. master device could first connect to the configured or provisioned

WSDB, if that fails then the master device can use the dynamic mechanism described in this document to find out available WSDB.

The dynamic WSDB discovery mechanism is used by master device to discover available WSDBs for its current location and related regulatory domain information. After master device gets the information about available WSDB and regulatory domain information, it then chooses the proper WSDB for querying white space spectrum using PAWS procedures.

The discovery mechanism discussed here will provide master device with two kinds of information: the regulatory domain where the device currently locates and the available list of WSDBs or a Listing server in current domain.

The mechanism discussed in this memo will be provided as an OPTIONAL method as described in [PAWS PROTOCOL].

## 2. Terminology and Conventions

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

The terminology from PAWS: problem statement, use cases and requirements RFC6953 [RFC6953] is applicable to this document.

### 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.

### White Space Database (WSDB)

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 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.

### White Space Database Discovery Server (WSDB DS)

A server function provided to a white space device, the client. The white space device contacts a WSDB DS to receive the service of discovering or identifying one or more white space databases.

### RB\_server

Master device can query its current regulatory body domain information from RB\_server. RB\_server setup by vendor or by third party. Besides regulatory domain information, RB\_server might provide additional information (TBD).

#### LoST

LoST (Location-to-Service Translation Protocol) RFC5222 [RFC5222] is an XML-based protocol for mapping service identifiers and geodetic or civic location information to service contact URIs and associated information.

### 3. Solutions

Considering of different business models, regulations in different regulatory domain and some existing deployments, in this version of draft, several possible solutions are discussed.

[NOTE1: Although several solutions are discussed here, but finally we may only choose the best one.]

#### 3.1. Solution 1

It's reasonable for the regulatory body to know all the WSDBs deployed in its domain, because when a WSDB is deployed it must get the permission of regulatory body. So it is suitable for each regulatory body to deploy a WSDB DS.

In this solution, each regulatory body maintains its own WSDB DS, which records all the WSDBs for the regulatory domain. When master device operates in certain regulatory domain, it gets available WSDB from regulatory domain's WSDB DS.

Besides WSDB DS deployed by each regulator body, an entity named RB\_Server is also deployed. RB\_Server is a server which provides WSDB DS information to master device according to geo-location provided by master device. The DNS domain name or IP address of RB\_Server should pre-configured in master device. There are two considerations on how to deploy RB\_Server.

(a) RB\_Server(s) could be setup according to international agreement among various spectrum regulators. In this case a query protocol between master device and RB\_Server is needed, and LoST protocol would be an appropriate candidate. RB\_Server and WSDB DS act as LoST server and master device acts as LoST client.

(b) Absent such an international agreement, each radio vendor would

be responsible (under its certification agreement with each regulator) to ensure that its devices operate properly when they are in the geographic territory for which they have been certified, RB\_Server could be setup by the vendor of master device, and each vendor's RB\_Server provides service to its own master device.

An example of deployment is shown in Figure 1. There are three regulatory domains, named A, B and C; one or more WSDBs and one WSDB DS are deployed in each domain.

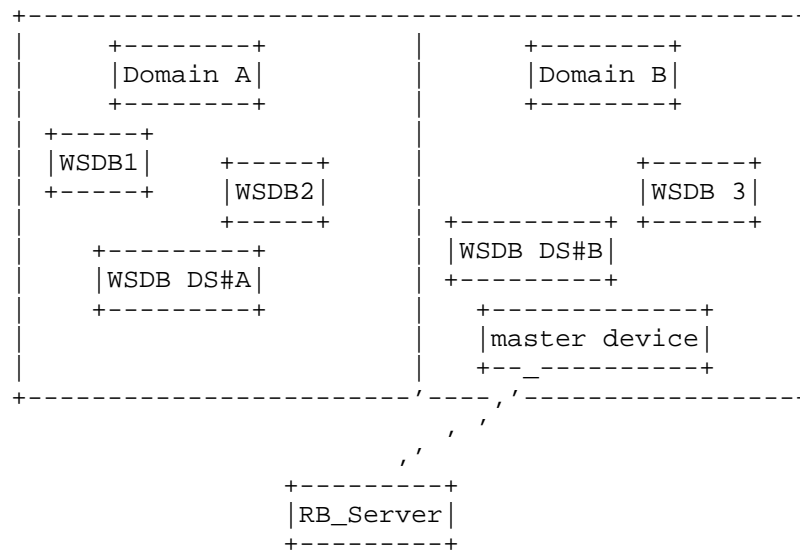


Figure 1: Solution 1: Framework of WSDB discovery

### 3.2. Solution 2

This solution provides a more flexible WSDB discovery method. In this solution, RB\_Server and DNS system are used.

It is possible that regulatory bodies get an agreement each one deploys its own WSDB DS, and under such an agreement solution1 would be a good choice for WSDB discovery. But if regulatory bodies cannot reach such an agreement, i.e. not all regulatory bodies would deploy WSDB DS, then solution2 would be a good choice. The framework of WSDB discovery for solution 2 is shown in Figure 2.

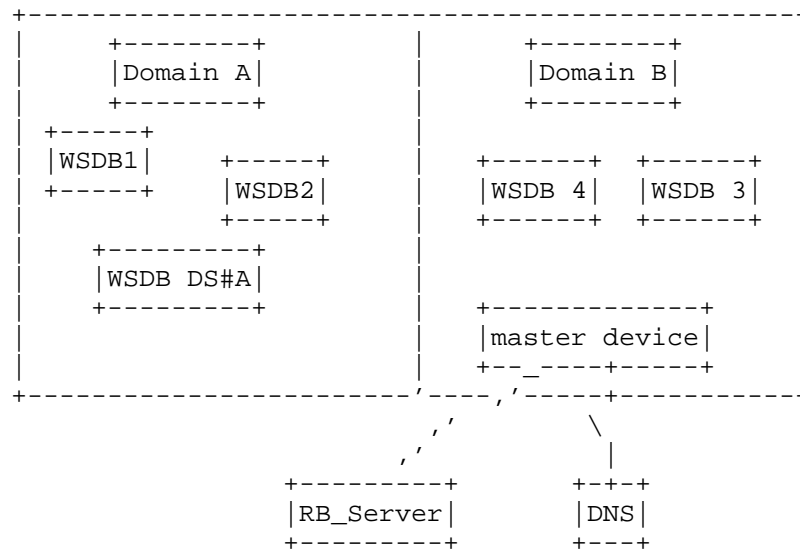


Figure 2: Solution 2: Framework of WSDB discovery

The basic WSDB discovery procedure is shown in Figure 3.



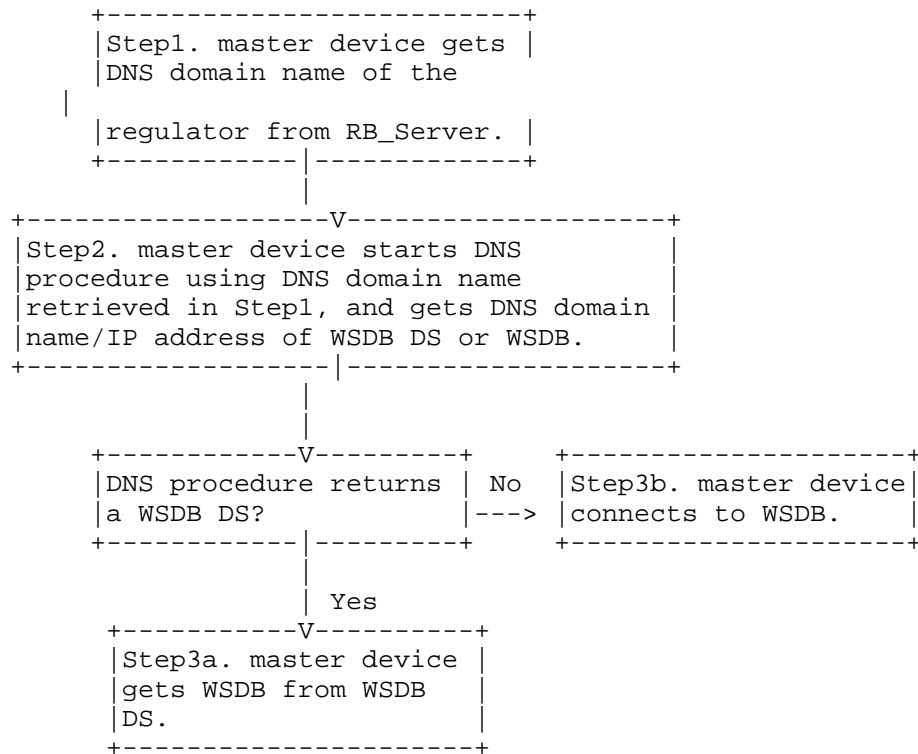


Figure 3: Solution2: Basic WSDB discovery procedure

In this solution, NAPTR DNS Resource Record (RR) RFC3403 [RFC3403] is used. Each regulator maintains NAPTR RRs by itself, and every WSDB or WSDB DS has a related NAPTR RR. The service field of NAPTR RR is used to indicate whether the RR is for WSDB or WSDB DS. An example of NAPTR RRs is shown as follows. [NOTE2: If NAPTR RR for WSDB DS exists, then there might be no NAPTR RRs for WSDBs.]

A simple NAPTR example:

paws.fcc.gov

IN NAPTR 100 100 A paws-db '' exam1.company1.com ; DB returned

IN NAPTR 100 100 A paws-ds '' exam2.company2.com ; WSDB DS returned

IN NAPTR 100 100 A paws-db '' exam3.company3.com ; DB returned

There is a bit of difference between RB\_Servers in solution 2 and

solution 1, in solution 2 RB\_Server returns DNS domain name for the regulatory domain, which will be used in the following DNS procedure.

### 3.3. Solution 3

In this solution, WSDB DS is deployed independently from regulatory domain (but we don't except regulatory body from deploying their own WSDB DS). WSDB DS maintains WSDBs for regulatory domains or only maintains WSDB DS in case regulator deploys WSDB DS by itself and needs master device get WSDB from its own WSDB DS. The DNS domain name or IP address of such an independent WSDB DS should be pre-configured in master device. An example of deployment is shown in Figure 4.

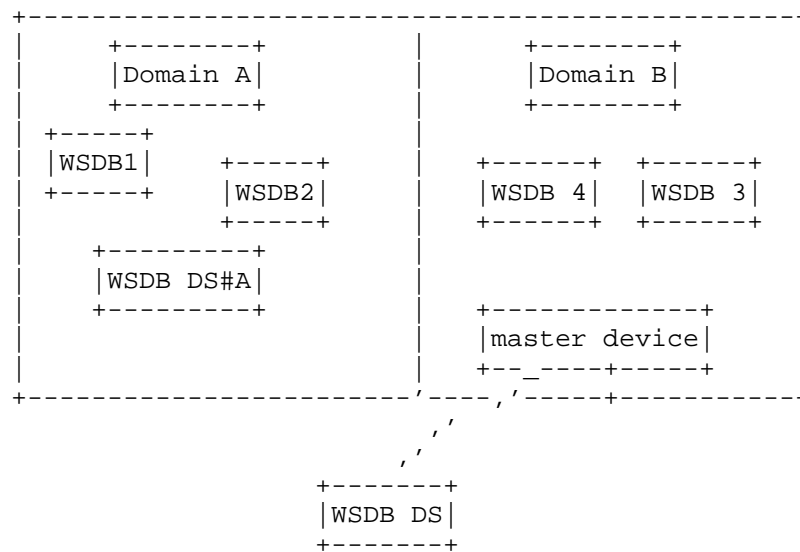


Figure 4: Solution 3: Framework of WSDB discovery

There are two considerations on how to deploy independent WSDB DS.

(a) WSDB DS could be setup according to international agreement among various spectrum regulators. In this case a query protocol between master device and WSDB DS is needed, and LoST protocol would be an appropriate candidate. Both independent WSDB DS and WSDB DS deployed by regulatory body act as LoST server and master device acts as LoST client.

(b) Absent such an international agreement, each radio vendor would be responsible (under its certification agreement with each regulator) to ensure that its devices operate properly when they are

in the geographic territory for which they have been certified, WSDB DS could be setup by the vendor of master device, and each vendor's WSDB DS provides service to its own master device.

### 3.4. Solution 4

Like solution1, in this solution each regulatory body deploys its own WSDB DS. A LoST service wsdb is defined, which is used to get URL of WSDB, and WSDB DS acts as a server that can provide wsdb service. Master device acts as LoST client.

One DHCP extension has been defined in RFC5223 for discovering LoST server, so when master device attaches to operator's network, master device could be provisioned with IP address of an LoST server through DHCP procedure. The LoST server provisioned here might not be the address of WSDB DS, but according to LoST architecture, master device can finally connect to WSDB DS after iterative or recursive procedures.

## 4. Security Considerations

TBD.

## 5. IANA Consideration

TBD.

## 6. Acknowledgements

## 7. References

### 7.1. Normative references

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3403] Mealling, M., "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database", RFC 3403, October 2002.
- [RFC5222] Hardie, T., Newton, A., Schulzrinne, H., and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol", RFC 5222, August 2008.

## 7.2. Informative References

## [PAWS PROTOCOL]

Chen, V., Das, S., Zhu, L., McCann, P., and J. Malyar,  
"Protocol to Access Spectrum Database",  
draft-ietf-paws-protocol-07 (work in progress), Dec 2013.

[RFC6953] Mancuso, A., Probasco, S., and B. Patil, "Protocol to  
Access White-Space (PAWS) Databases: Use Cases and  
Requirements", RFC 6953, May 2013.

## Authors' Addresses

Xinpeng Wei  
Huawei

Phone: +86 134 3682 2355  
Email: weixinpeng@huawei.com

Lei Zhu  
Huawei

Phone: +86 139 1015 7020  
Email: lei.zhu@huawei.com

