IEEE Standard for Information Technology—

Telecommunications and information exchange between systems

Wireless Regional Area Networks (WRAN)—

Specific requirements

Part 22.3: Spectrum Characterization and Occupancy Sensing

Sponsor

**LAN/MAN Standards Committee**of the  
**IEEE Computer Society**

Approved Date XX

**IEEE-SA Standards Board**

Abstract: This standard specifies the architecture, abstraction layers, interfaces and metadata requirements for Spectrum Characterization and Occupancy Sensing (SCOS) system, a defines performance parameters, units and measures. This SCOS system comprises one or more semi-autonomous Spectrum Sensing Devices which scan electromagnetic spectrum, digitize it and perform processing, transmitting the resultant data with appropriate metadata to a central storage and processing system, according to rules, policies or instructions imposed on the Spectrum Sensing Devices by a management system.

Keywords: radio spectrum sensing, spectrum monitoring, signal characterization, cognitive radio, IEEE 802.22.3, WRAN standards

[[1]](#footnote-1)•

**IEEE Standards** documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied “**AS IS**.”

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required. Comments and recommendations on standards, and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board

445 Hoes Lane

Piscataway, NJ 08854

USA

Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

This standard specifies the functional elements, system architecture, abstraction layers, interfaces and metadata requirements for Spectrum Characterization and Occupancy Sensing (SCOS) system, with some limited definition of performance parameters, units and measures. It is intended to incorporate elements of existing standards and technology components to make it fast to implement using “off the shelf” hardware and software modules. The standard is intended to be flexible to make it forward-compatible as both radio sensing hardware and software technology develops, with an emphasis on using shared, virtualized, Internet-connected computing resources. The reference architecture describes one or more semi-autonomous Spectrum Sensing Devices which scan electromagnetic spectrum, digitize it and perform some level of processing, transmitting the resultant data with appropriate metadata to a Spectrum Sensing Management System. This command and control system manages scan requests from users, manages and advertises to users the scanning resources available to it from its connected Sensing Devices, and packages and forwards scan data to specified destinations according to rules, policies or instructions imposed by operator of the SCOS system.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association web site at <http://ieeexplore.ieee.org/xpl/standards.jsp>, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA web site at <http://standards.ieee.org>.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL:   
<http://standards.ieee.org/reading/ieee/updates/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: [http://standards.ieee.org/reading/ieee/interp/  
index.html](http://standards.ieee.org/reading/ieee/interp/index.html).

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. A patent holder or patent applicant has filed a statement of assurance that it will grant licenses under these rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses. Other Essential Patent Claims may exist for which a statement of assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this standard was submitted to the IEEE-SA for approval, the following voting members had participated in the IEEE P802.22.3 Task Group:

**TBC**

Major contributions to this standard were made by the following individuals:

**TBC**

The following members of the balloting committee voted on this **TBC**. Balloters may have voted for approval, disapproval, or abstention.

When the IEEE-SA Standards Board approved this on TBC, it had the following membership:

**Richard H. Hulett,** *Chair*

**John Kulick,** *Vice Chair*

**Robert M. Grow,** *Past Chair*

**Judith Gorman,** *Secretary*

\*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish Aggarwal, *NRC Representative*

Richard DeBlasio, *DOE Representative*

Michael Janezic, *NIST Representative*

Patricia Gerdon

*IEEE Standards Program Manager, Document Development*

Catherine Berger

*IEEE Standards Project Editor*

**Contents**

1. Overview 11

1.1 Scope 11

1.2 Purpose 12

1.3 Reference Applications 12

2. Normative References 14

3. Abbreviations and acronyms 14

4. Functional Requirements 14

4.1 Introduction 14

4.2 Managed objects 15

4.3 Regulatory requirements 15

4.4 Device classes and complexity 16

4.5 Number of devices 16

4.6 Network Topology 16

4.7 Real-time applications 16

4.8 Security 17

4.9 Security of Spectrum Databases and Cognitive Radio Systems 17

4.10 Security of sensed data 18

4.11 Channelization 18

4.12 Reporting to the Spectrum Sensing Management System 18

4.13 Sensor Location 18

5. System architecture 18

5.1 Reference architecture 18

5.2 Management Reference Architecture 23

6. Architecture System Requirements 28

7. System Definitions and Interfaces 32

7.1 System Units and Parameters 33

7.2 Metadata Formats 34

8. Security Systems 35

Annex A Informative: Regulatory Technical requirements 37

Annex B Device and System Security Recommendations 38

Annex C 63

Annex D (normative) IEEE 802.22 regulatory domains and regulatory classes requirements 64

D.1 Regulatory domains, regulatory classes, and professional installation 64

D.2 Radio performance requirements 65

Annex E (informative) Sensing 66

E.1 References 66

Annex F (informative) Bibliography 67

IEEE Standard for Information Technology—

Telecommunications and information exchange between systems

Wireless Regional Area Networks (WRAN)—

Specific requirements

Part 22.3: Standard for Spectrum Characterization and Occupancy Sensing

***IMPORTANT NOTICE: This standard is not intended to ensure safety, security, health, or environmental protection. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.***

***This IEEE document is made available for use subject to important notices and legal disclaimers.   
These notices and disclaimers appear in all publications containing this document and may   
be found under the heading “Important Notice” or “Important Notices and Disclaimers   
Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at*** [***http://standards.ieee.org/IPR/disclaimers.html***](http://standards.ieee.org/IPR/disclaimers.html)***.***

1. Overview
   1. Scope

The purpose of the Spectrum Characterization and Occupancy Sensing (SCOS) system is to acquire and make available data from networks of sensors. It is intended to establish a platform that enables “spectrum sensing as a service” and collective measurement efforts.

The standard leverages interfaces and primitives that are derived from IEEE Std. 802.22-2011, and uses commonly used network transport mechanisms to achieve the control and management of the system. Interfaces and primitives are provided for conveying value-added sensing information to various spectrum sharing database services. This standard specifies a device operating in the bands below 1 GHz and a second device operating from 2.7 GHz to 3.7 GHz, but is not inherently limited to these bands.

* 1. Purpose

The purpose is to specify operating characteristics of the components of the Spectrum Characterization and Occupancy Sensing System. The intent of this standard is to create an open platform where elements of the architecture are characterised in terms of the capabilities they offer to other elements, defined through abstractions and interfaces with standardised metadata sets attached to scan data, allowing users of the data to manipulate it in independent systems according to their requirements.

The SCOS system is defined around “Actors” which use the platform to query the “Sensing Manager” for the capabilities of “Sensing Devices” associated with it, request for tasks to be placed in the scan scheduler, and once the scan is complete for the spectrum data and associated metadata to be sent back to the Sensing Manager for transmission to one ore more Data Stores. There is no mandate around hardware standards or sensing techniques, instead each sensing task has metadata describing the sensing device’s parameters (e.g. antenna gain, amplifier/SDR noise floor, software libraries used), the sensing task and environmental parameters (device location, operating conditions). This moves the requirement to understand and correctly process the sensing data to the user of the system.

The Sensing Manager allows the operator of the SCOS system to apply policies in terms of what the sensing device may do (e.g. not allow hi-res raw scans in sensitive military bands, prioritise resources for particular users, etc). These policies could be imposed by the SCOS operator, a national regulator or law enforcement agency in a very granular way.

Although spectrum database design and visualization are critical element to spectrum management, we limit the scope of this standards to details required to establish machine to machine communications between user (Actor), Sensing Manager, Sensing Device and Data Store to which the scan data is transmitted. User data management and visualization is left for users to meet business and/or organizational goals. This standard does, however, define a number of elements to permit the subjective user to assess data quality at reception.

* 1. Reference Applications
     1. White Space device radio operator (possibly edge case – assumes a CR can use 802.22.3 as SCOS device)

Either the network operator or device operator using spectrum sensing to identify primary or other secondary users of particular channels. Spectrum sensing either built into the radio devices or standalone sensing units.

* + 1. National regulators

National radio regulators would use a system comprising spectrum sensing devices to feed into a national spectrum utilization database for assignment management and planning purposes, and generating historical records for compliance monitoring and enforcement.

Devices deployed in various scenarios:

* Fixed devices at key locations and high sites
* Mobile devices on vehicles that travel widely and can create a sample set of spectrum utilization through snapshots at time or location intervals
* Devices either at fixed locations or periodically moved to create location-based spectrum utilization datasets
* Nationally deployed in a swarm of a given device density to create real-time national spectrum utilization maps and for validation of Spectrum Geolocation databases.
  + 1. Scientific community:

Scientists using sensitive radio frequency systems (e.g. radio-telescopes) struggle with RF interference. SCOS devices can let them identify RFI and the location of their sources.

* + 1. Law enforcement and public order

Law enforcement and other authorities are increasingly dealing with problems stemming from radio-controlled or radio-connected systems.

**Illegal drone use:**  These include people flying radio-controlled unmanned aerial vehicles (drones) in prohibited places. SCOS systems can be used to detect characteristic transmissions of drone operation in areas such as in the airfield flight traffic area.

**Detecting jamming devices:** A problem area for security staff and law enforcement is the use of radio jammers to interfere with remote control devices like vehicle keyless entry systems or radio links for alarm systems. SCOS devices can be used to identify and locate jamming systems.

**Detecting unauthorized mobile phone use:** Controlled and high security areas such as prisons will frequently prohibit the use of cellular phones in certain areas, but may not jam operating frequencies because of other regulations. Identifying and locating transmissions allows direct action to be taken on equipment users.

* + 1. Network Operator

Radio planning for fixed radio deployment.

Spectrum forensics for identifying sources of interference.

1. Normative References

Sections of the IEEE P1900.6 standard defining the M-SAPs.

To be completed…

1. Abbreviations and acronyms

Actor – A human or machine entity that interacts with the SSM to query scan resources or request scans to be scheduled

RF – Radio Frequency

RFI – Radio Frequency Interference

SCOS – Spectrum Characterization and Occupancy Sensing

SD or SSD – Spectrum Sensing Device

SM or SSM – Spectrum Sensing Manager

1. Functional Requirements
   1. Introduction

Various national regulators and government authorities are developing regulatory and policy frameworks to allow cooperative spectrum sharing approaches in order to optimize spectrum utilization. There is emphasis on greater spectrum efficiencies, spectrum sharing and spectrum utilization, which requires not only database-driven configuration of the radios, but systems that can provide spectrum occupancy at a particular location and at a particular time.

The IEEE 802.22.3 standard described in this document will help fulfil this need by creating a Spectrum Characterization and Occupancy Sensing (SCOS) system. This will improve knowledge of spectrum utilization and support shared spectrum applications, hence benefitting the regulators and users alike.

The Spectrum Occupancy Sensing (SCOS) System has many applications which include:

1. On-demand spectrum survey and report

2. Collaborative spectrum measurement and calibration

3. Labelling of systems using the spectrum

4. Spectrum planning

5. Spectrum mapping

6. Coverage analysis for wireless deployment

7. Terrain and topology - shadowing and fading analysis

8. Quantification of the available spectrum through spectrum observatories [2, 13],

9. Complement the database access for spectrum sharing by adding in-situ awareness and faster decision making.

10. Space-Time-Frequency spectrum hole identification and prediction where non-time-sensitive tasks can be performed at certain times and at certain locations, when the spectrum use is sparse or non-existent

11. Identification and geolocation of interference sources.

The Spectrum Characterization Occupancy Sensing (SCOS) systems may be deployed to characterize many bands such as VHF/UHF, L, S, C and X bands.

* 1. Managed objects

Anything here?

* 1. Regulatory requirements

This standard should provide mechanisms to meet the regulatory requirements of national operators that have defined parameters or requirements for spectrum sensing in various applications. These regulatory requirements would take two forms: the first is technical requirements for sensitivity, resolution, etc. The second is limitations on how and where sensing might be done where there are sensitivities around privacy, military use and other national policies and regulations.

* + 1. Technical Requirements

(is this a requirement if metadata describes sensing data well enough for end user to make a call)

* + 1. Policy Requirements

To allow for granularity in what the SCOS systems can do, but also ensure spectrum occupancy or utilization data is not exposed in contravention of national policy or regulation, it is proposed that the SSM would be able to apply policies to allow or disallow certain functionality in the SSDs, or disallow transmission of the data to third party systems.

These policies would be determined by the SSM operator (e.g. a national regulator or network operator), and cascaded down to any connected SSDs. These policies would allow sensing only according to allowed metrics (e.g. no hi-resolution raw scans in military radar bands), and limit sensing data transmission to certain classes of third party systems.

* 1. Device classes and complexity

The following sensing device categories may be considered:

* **Energy Efficient Sensing Devices**: This standard should provide mechanisms of energy efficient operations, eg. solar powered or battery operated spectrum sensors for monitoring applications.
* **Small form factor devices**: Devices that can fit the spectrum sensing function within a small form factor (e. g. a USB dongle, cell phone etc.)
* **Advanced Spectrum Sensing Devices**: Advanced Spectrum Sensing Devices with capable Radio Frequency Front Ends (RFFE) and dedicated resources for spectrum sensing may be considered.
* **Non-dedicated Devices with Sensing Capability:** A number of consumer and professional radio devices contain radio receivers that can be used as sensing devices, including mobile phone handsets, Wi-Fi access points (from 802.11ac) and Dynamic Spectrum Access radio systems (including 802.22).
  1. Number of devices

This standard shall support at least one Spectrum Sensing Device to cover a location or area, communicating with a back-end Spectrum Sensing Management System (SSM), but will extend to describing an architecture and interfaces for multiple SSDs potentially communicating with multiple SSM instances.

* 1. System Architecture
     1. Network Topology

The SCOS system consists of a single SSM, which communicates over any standard network transport with one or more SSDs. The SSDs shall not communicate with each other, or directly with the user of the SCOS system (Actor). One or more Actors may communicate directly with one or more SSMs, but each communication is independent of the others.

The topology is hence N:1:N for Actor:SSM:SSD.

Provision has been made for an SSM Proxy, where an SSM can communicate with other SSMs as if they were associated SSDs.

Provision has also been made for an SSD Proxy, which allows a non 802.22.3 compliant SSD to associate with and be controlled by an SSM.

* + 1. Functional Components

Figure 1. Architecture Block Diagram illustrates the functional components within the SCOS system. Note that all arrows in this diagram refer to connections made over a standard network transport (the choice of which is up to the implementer of the SCOS system).

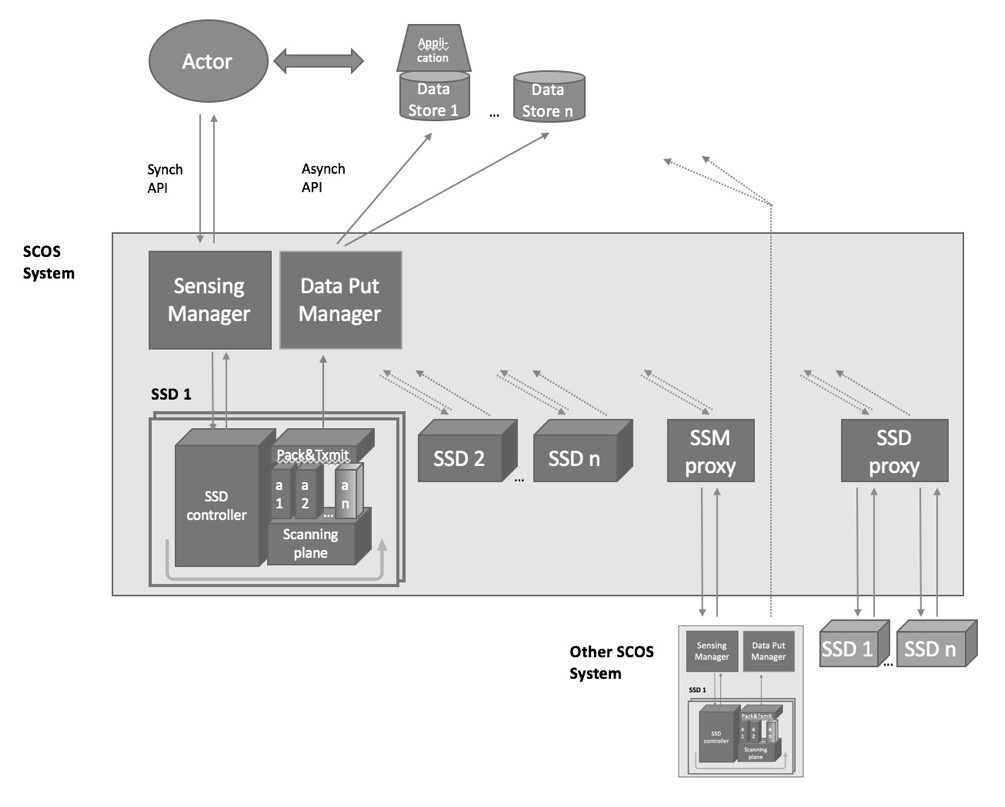


Figure 1. Architecture Block Diagram

* An Actor (user of the SCOS system) and SSM (Sensing Manager) communicate by REST API to ask for available resources, and request a scan.
* The SSM is associated with SSDs (Sensing Devices) through a synchronous interface, where the SSM enumerates and holds a list of available resources for each SSD.
* The SSM stores and manages a schedule of scans against the sensing resources, and synchronizes this schedule with all SSDs both on a change being made and periodically to ensure correct state.
* An SSD performs the scans in the schedule, and transmits the data and associated metadata through an asynchronous interface (message queue, or real time stream) to a “Data Put Manager” that performs system data validation (i.e. that a transmission is received completely, partial scans are consolidated, etc).
* The “Data Put Manager” applies any policies and then handles the Store & Forward to one or more data stores.

Typically (but not necessarily) the SSM and Data Put Manager would be running on the same physical server.

Note: Potentially examine “resource discovery” model akin to the IEEE P1903 Next Gen Service Oriented Networks.

* 1. Real-time applications

The sensing devices will be performing spectrum sensing functions according to its scheduler (which is managed by its SSM), which can be updated in near-real time (dependant on speed of communication between Actor, SSM and SSD), or perform scans at scheduled intervals based on pre-configured schedules. However, the spectrum sensing reporting of data is out on a Best Effort basis, since the SCOS System uses the chosen available transport mechanism (e. g. 802.11, 802.22, Ethernet, Cable, Cellular etc.).

The SCOS system will benefit if sensing reports from various sensors are provided on a reasonable time-scales (e. g. minutes) so that the information is not stale. However, this is not a mandatory requirement. Also, the messaging format may be defined such that it does not produce excessive overhead penalty on the transport layer being used.

It is envisioned that real-time streaming will be provided for in future drafts of 802.22.3.

* 1. Security
  2. Security of Spectrum Databases and Cognitive Radio Systems

This standard mandates secure authentication and authorisation between Actor and SSM, SSD and SSM, SSM and Data Put Manager, and Data Put Manager and Data Store. Traffic between these components must also be encrypted. The specific security technology to be used is not mandated in this standard, but recommended best practices are described in Annex B. Note that the security model does not extend past transmission to the Data Store. Responsibility for securing the spectrum data at destination remains the responsibility of the operator of that store.

The technology model is designed to ensure that data derived from SCOS devices and SSM are not used as an attack vector against White Space Databases, regulator spectrum management databases, etc. It is also designed to ensure that only authorised Actors can make use of the SCOS resources, and that they are correctly identified to enable correct application of the relevant system policies.

* + 1. Inter-layer security
       1. Intra-device Layers (physical interfaces)

This standard defines security mechanisms to ensure integrity of sensing chain from antenna to data store.

* Antenna to amplifier/filters: physical security of device in terms of cable/connectors (tampering such as substituting antenna, physical such as connector corrosion)
* Amplifier to SDR: cable connectors or PCB connections
* SDR to processing unit: cable connectors or PCB connections
* Enclosure for active elements: Protection against moisture, dust ingress. Screening against RFI from external sources. Screening to protect antenna elements against RFI from active elements.

(NOTE – this section needs considerable attention)

* + - 1. Network Layer

Since this standard uses any available transport mechanism for data transmission, it will not recommend its own security mechanisms, but will use the existing security mechanisms of the transport mechanism being used (e.g. network 802.11 using Transport Layer Security,

* + 1. Application Layer

Data transmissions should be secured on the application layer using mechanisms to guarantee the integrity and confidentiality of sensing and control data transmissions. This standard does not specify the technology used, but recommended implementation practices are noted in Annex B: Device and System Security Recommendations.

* 1. Security of sensed data

This Standard shall not support mechanisms that expose user data modulated onto signals. For example, any kind of demodulation of the signals that may interfere with the privacy of the users shall not be not be supported. However, the SCOS system shall support sophisticated spectrum sensing methods such as cyclostationary processing that can detect signals and characterize their modulation type.

* 1. Channelization

This standard may specify a Spectrum Manager entity that can command various sensors to go and sense in certain bands, or it may even specify the spectrum sensors to ignore certain bands from sensing.

This standard may provide one primary channelization map for all the spectrum sensors (e. g. 5 MHz).

* 1. Reporting to the Spectrum Sensing Manager

This standard defines interfaces to and from each SSD to the SSM service to provide value added information back to the database on spectrum sensing device health, capabilities and configuration, and its scheduled activities.

* 1. Sensor Location

The SCOS device can convey the location of the sensors to the aggregation entity such as the SSM. The instruction to use available location capabilities on the SSD (e.g. GPS location) will be part of the scan schedule instruction from the Actor requiring the scan. This feature allows the SSM or the aggregation entity to localize the proximity of the signal source location allowing more efficient spectrum management.

1. System architecture
   1. Conceptual Architecture: Entities

The entities shown in Figure 1. Architecture Block Diagram are described as:

* Actor is the entity that initiates a spectrum monitoring request to one or more Spectrum Sensing Managers (SSM). Actors can be human or machine, and have various levels of privileges regarding what spectrum information collection can be initiated. Actors would determine where sensing data is to be transmitted, and authorization to access that data would rest with the owner of that data storage entity. and what spectrum information can be accessed from a Data Store.
* Data Store is a data base for storing spectrum information collected from the sensing network. There can be multiple Data Stores that sensing data is transmitted to by the Data Put Manager, and these can be, but not necessarily, associated with a specific Actor.
* Data Put Manager receives transmissions of packaged scan data from SSDs, and retransmits it to one or more destinations, as defined by the policies associated with each Actor (source of scan requests)
* Spectrum Sensing Manager manages a collection of Spectrum Sensing Devices (SSD). Requests for spectrum measurements from Actors are inserted into a scan schedule on the SSM for all its attached SSDs, as far as possible under a set of slot availability rules. This schedule is synched to the appropriate SSDs associated with the SSM. Data from the SSDs are collected at the Data Put Manager for transmission to one or more Data Stores for long term storage and processing.
* Spectrum Sensing Device is the sensing hardware that collects the spectrum data requested by the SSM on behalf of each Actor. The SSDs may exist with various levels of sophistication. The less sophisticated might be capable of measuring only one band, at only one resolution with little on-board processing. Other sensors may incorporate sophisticated antenna techniques, multiple bands, calibration processes, on-board data processing and/or storage and/or be capable of mobile operation.
* SSM Proxy lets one SSM talk to another, with the downstream SSM appearing as if it were an SSD with a set of resources it provides. This downstream SCOS system would need to be 802.22.3 compliant.
* SSD Proxy lets an SSM talk to any other proprietary sensing hardware, acting as a software translation mechanism that translates between commands/metrics/etc. It would need to be custom written for the particular device it talks to.
  1. Interaction of Entities

Figure 2 illustrates the basic SCOS interface structure.

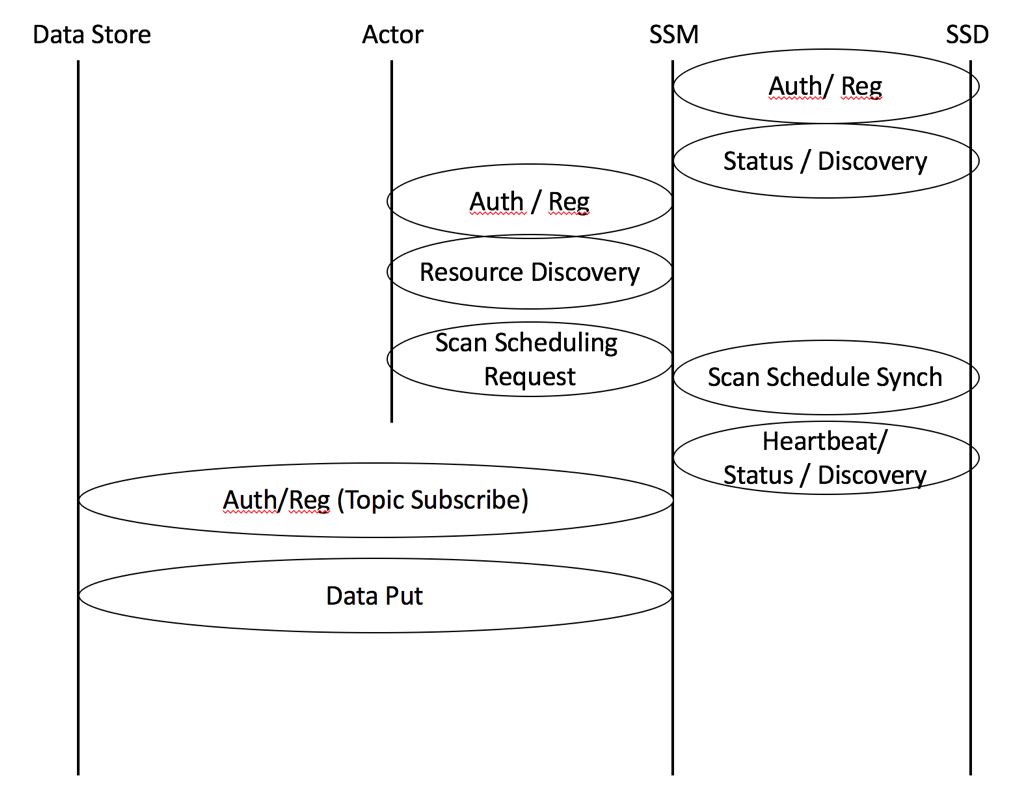


Figure 2. Basic Interface Structure

* 1. Reference architecture

The proposed architecture is composed of four key elements: an Actor (s), a spectrum sensing device (SSD), a spectrum sensing management system (SSM), a Data Put Manager and a Data Store(s). The flow of instructions and data is described in Figure 3: SCOS Functional Block Diagram.

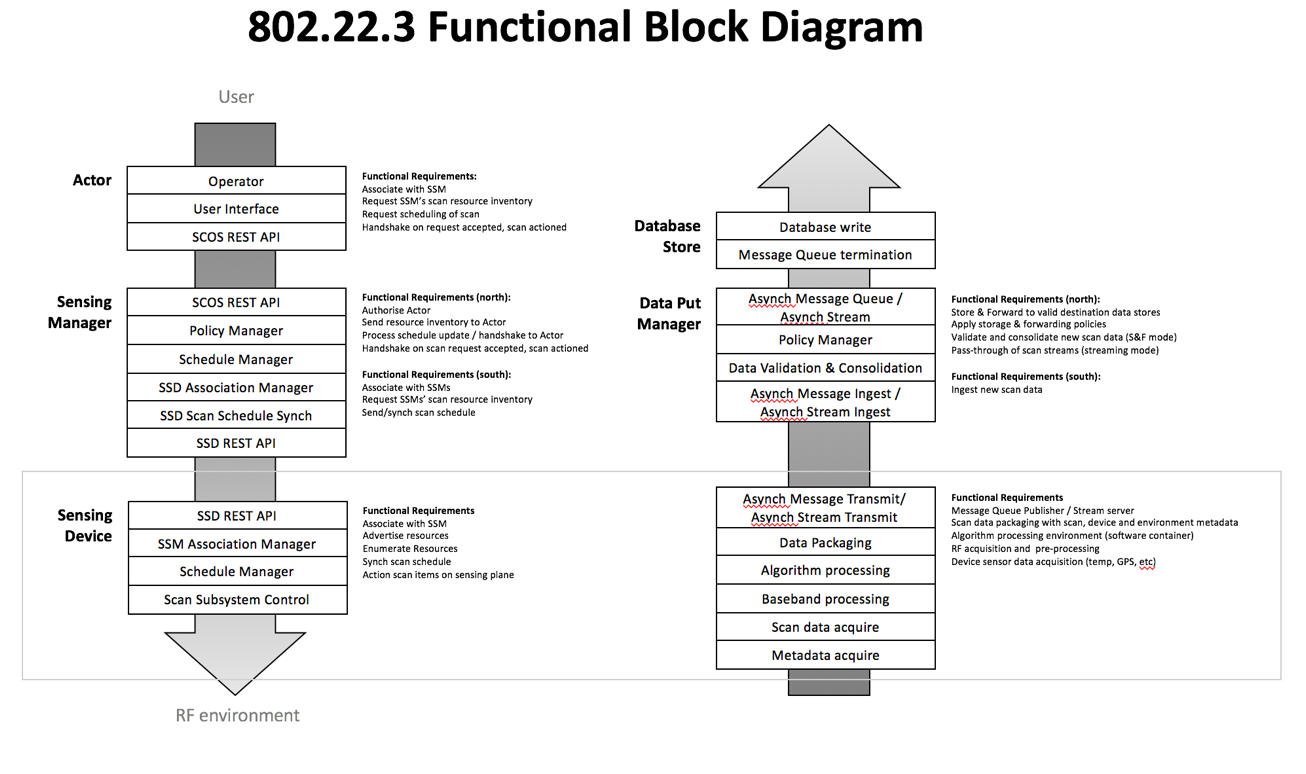


Figure 3: SCOS Functional Block Diagram

This diagram can be extended with the concept of proxying to allow SCOS systems to be cascaded, or the use of non 802.22.3 compliant sensing devices.

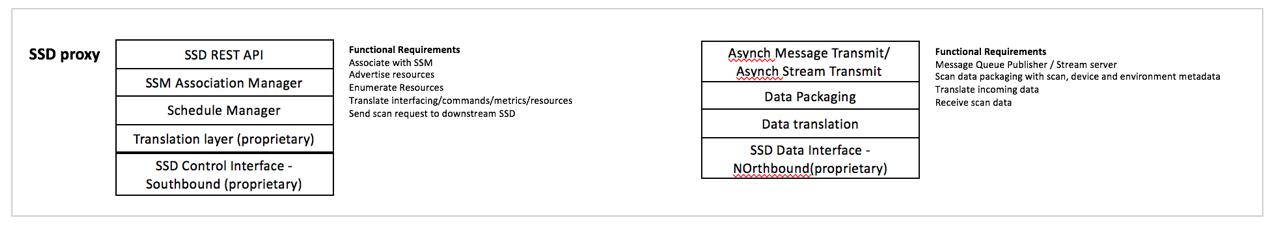


Figure 4: SSD Proxy

****

Figure 5: SSM Proxy

* + 1. System Interface Functions

The communication between each of the entities defined above can be grouped and defined within the Interface Categories shown in Figure 6. Message Sequence and described below.

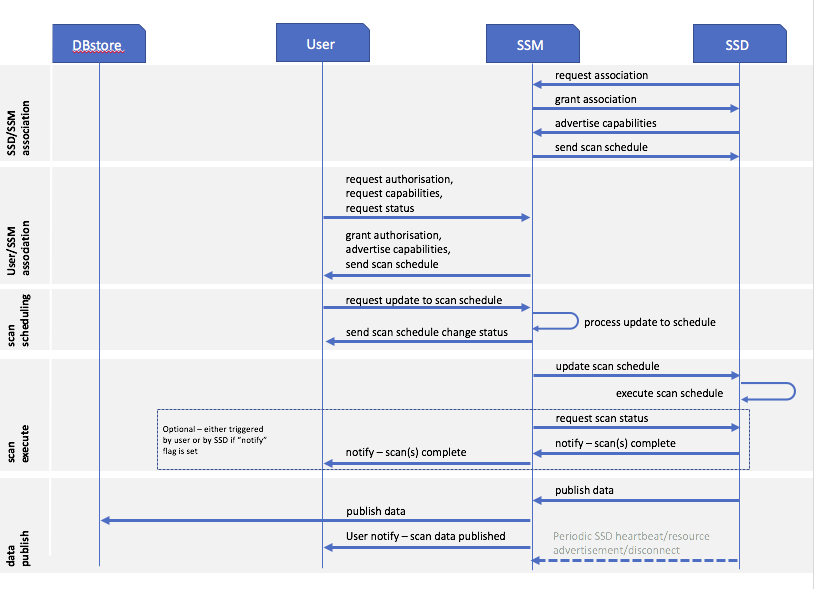


Figure 6. Message Sequence

* + - 1. USER <−> SSM
         1. Authentication and Registration

These procedures define the association and authentication process for an SSM and USER entity to connect and communicate. They include facilities to prevent spoofing based on shared key exchange. Once an SSM is authenticated and registered to a USER, the USER can then discover the capabilities of the SSM and its associated SSD’s. The USER may then define and make sensing requests to the SSM, which include a designation of the DBstore(s) to which the data is to be sent. The SSM will notify the USER when measurements are successfully completed (or not) and available at the DBstore.

* + - * 1. Resource Discovery

Resource Discovery is the process of informing the USER of what capabilities that the SSM has with regard to what types of measurements, what bands can be measured and associated measurement parameters that can be specified and controlled and over what locations. This takes the form of a resource/capability descriptor and the current scan schedule per SSD.

* + - * 1. Scan Request

The Scan Request message from the USER to the SSM includes the parameters of the desired spectrum measurement to be made and any associated processing to be performed by either the SSD or the SSM. This scan request is wrapped in a scheduling task description, defining the time the scan is to be made, the repetition rate (if applicable), the locations, etc. When the scan parameters in their scheduling wrapper are received by the SSM it will be validated as possible to be executed (i.e. the resources requested meet the SSMs schedule of resources available), and either acknowledged as being queue, or a refusal is returned to the USER. If a scan schedule is upated for a particular SSD, it is then replicated down to that SSD.

* + - 1. SSM <−> SSD
         1. Authentication and Registration

These procedures define the association and authentication process for an SSD and SSM entity to connect and communicate. They include facilities to prevent spoofing based on shared key exchange. Once an SSD is authenticated and registered to a SSM, the SSM can then discover the capabilities of the SSD. An SSM will have associated with it at least one SSD. The SSM may then assign sensing requests to the appropriate set of SSDs in order to fulfill the sensing request of the USER.

* + - * 1. Status and Discovery

The Status and Discovery process serves two functions. The first is to inform the SSM of what capabilities that the SSD has with regard to what types of measurements, what bands can be measured and associated measurement facilities (such calibration, antenna control, mobility, storage, processing) that can be specified and controlled and over what locations. The SSD will transmit a package describing its capabilities and available resources at time of authentication/discovery, and if there is any change in its configuration. The second function is to maintain association with the SSM. It will transmit a period heartbeat to indicate it is still associated with the SSM. If it is to disconnect, it will transmit a disassociation message (e.g. if it is rebooting or about to go into an offline mode).

* + - * 1. Scan Request

The Scan Request message originating from the SSM is sent to the appropriate SSDs for execution as a scan schedule. It includes the parameters of the desired spectrum measurement to be made based on knowledge of the SSD’s capabilities. This request will include the time to make the measurement, the repetition rate (if applicable), the locations, etc. and the format of the measured data. In the case of a single, once-off scan, the schedule will indicate no repitition.

* + - 1. Data Store <−> USER
         1. Authentication and Registration

These procedures define the association and authentication process for a Data Store and Actor entity to connect and communicate. They include facilities to prevent spoofing based on shared key exchange. Once a Data Store is authenticated and registered to an Actor, the Actor is then authorized to cause data to be delivered to the Data Store, and read that data.

* + - * 1. Resource Discovery

Resource Discovery is the process of informing the Actor of what capabilities that the Data Store has with regard to what types of data can be stored, at what rate, at what access level, and in what quantity can be specified. It may also initiate that association of a particular Data Store with a specific SSM that will be providing the data.

* + - 1. SSM <−> Data Store
         1. Authentication and Registration

These procedures define the association and authentication process for a Data Store and SSM entity to connect and communicate. They include facilities to prevent spoofing based on shared key exchange. Once a Data Store is authenticated and registered with a SSM, the SSM is then authorized to cause data to be delivered to the Data Store based on the privileges of the Data Store and the SSM. The Data Stores can be grouped into Data Store Groups, where a transmission of data from the SSM is delivered to multiple Data Stores.

* + - * 1. Data PUT

These procedures define and enable the storage of data from the SSM to the DBstore. The successful reception of this data initiates a notification of the initiating USER that requested that data.

* + 1. Spectrum Sensing Device (SSD)

SSDs convert radiative electromagnetic energy into a voltage, which is then sampled. The samples can then be processed in various ways to provide information on the immediate RF environment, e.g., amplitude statistics versus frequency, amplitude and phase versus time at a given frequency, occupancy statistics, angle of arrival.

* + - 1. Hardware Model

Figure 6: Hardware Model Block Diagram provides a simplified hardware block diagram of a general SSD model. SSD hardware designs are not required to have each component shown in the block diagram. Specifics for each component (e.g., presence, model, operational parameters), however, is required metadata when SSD capabilities are queried by the SSM. This SSD definition metadata will also accompany the output data messages.

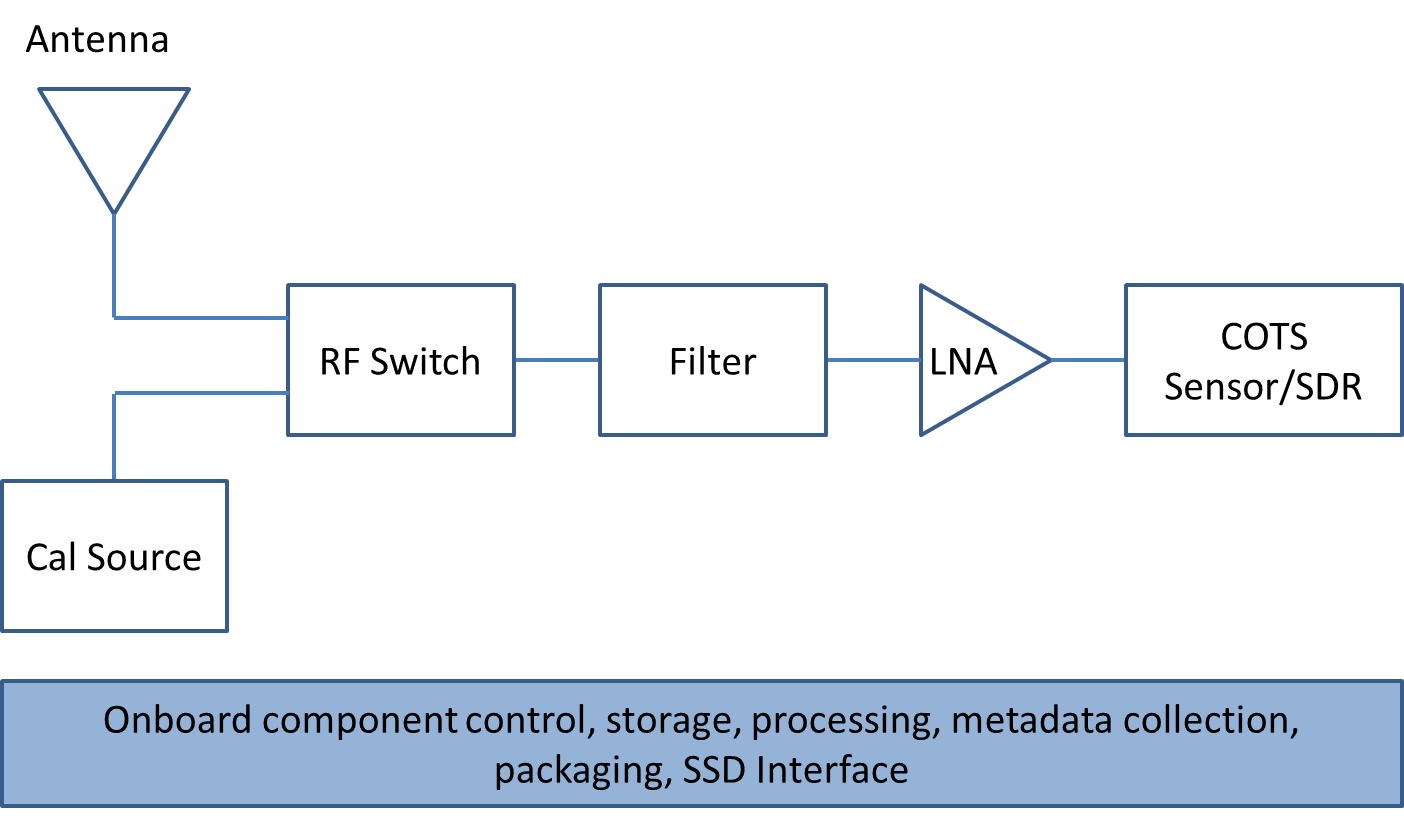


Figure 7: Simplified Hardware Model Block Diagram

The SSD is composed of the following functional elements, as follows:

* Section 1: An antenna used to detect RF energy. This is fed to Section 2 over a hardware interface (cable)
* Section 2: A sensing unit consisting of an RF switch (optional), filter, Low Noise Amplifier (with the option of being able to accept a calibration signal). This sends the conditioned signal to Section 3 over an analogue hardware interface (interconnect).
* Section 3: A detecting unit consisting of (all or some of) an Analogue Digital Converter, spectrum analyser or Software Defined Radio to act as a baseband processor, performing a quadrature demodulation of the conditioned signal and acquires the baseband signal. This sends digitised signal over a digital interface (interconnect)
* Section 4: A signal processing unit that runs a signal detection and/or classification algorithm. It sends detection/classification data to Section 5 over a software interface.
* Section 5: A metadata consolidation and data packaging unit that combines sensing data with hardware, operating and system-configured metadata. It sends data packages to the transmission system over a software interface.
* Section 6: A transmission unit that transmits scan data to the destination system over a best-effort IP connection.

Typically Section 4 (signal processing), Section 5 (metadata and data packaging) and Section 6 (data transmission) are software components running in the host controller.

In all cases the Host Controller sends command and control signals to Section 2 (sensing) and Section 3 (detecting), and polls these, and any sensor input devices such as GPS, for necessary metadata items.

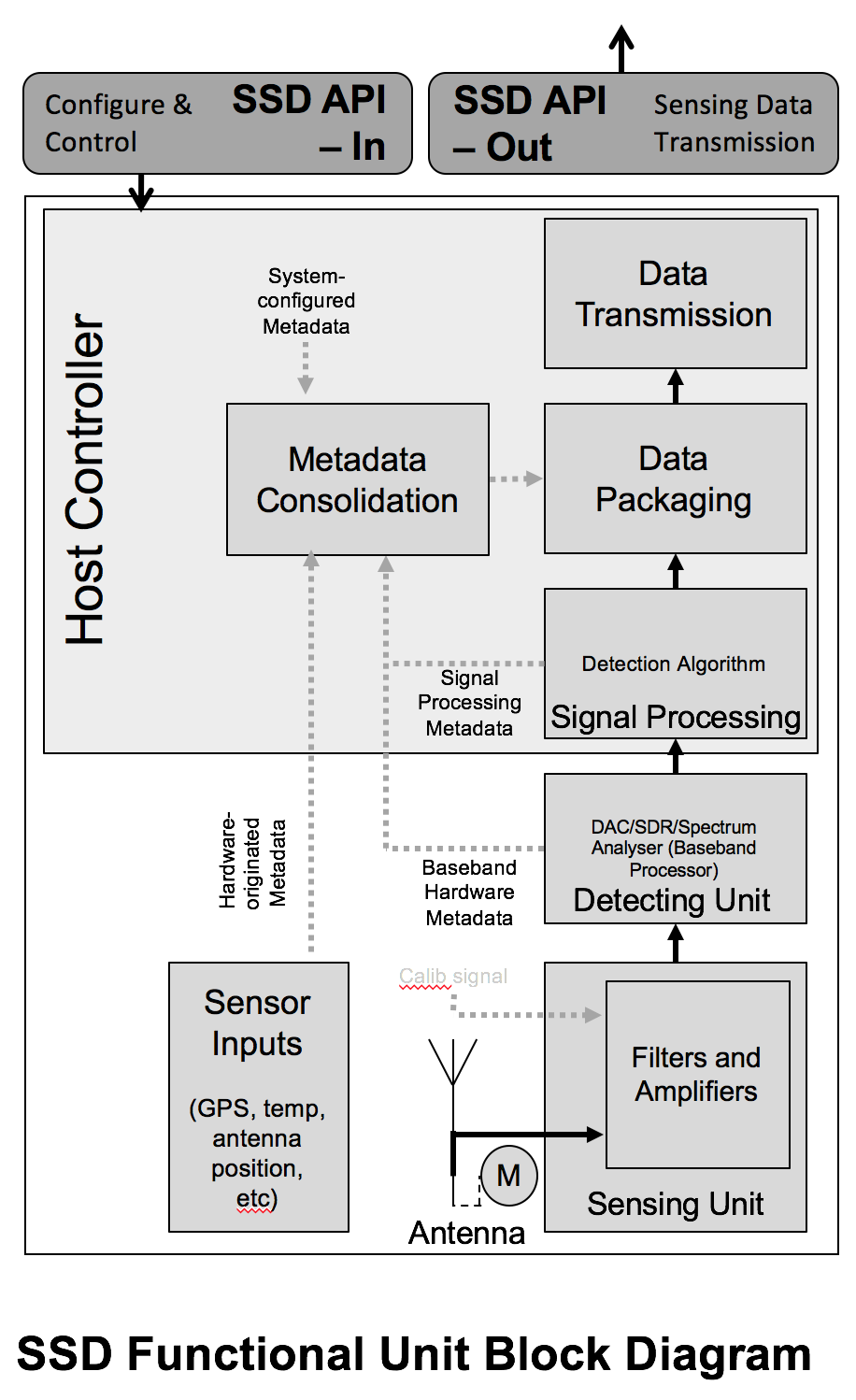


Figure 7: SSD Functional Elements

This block diagram can be split into the hardware layer and the software processes that run alongside. These hardware blocks or software services can/will generate metadata that is associated with each item.

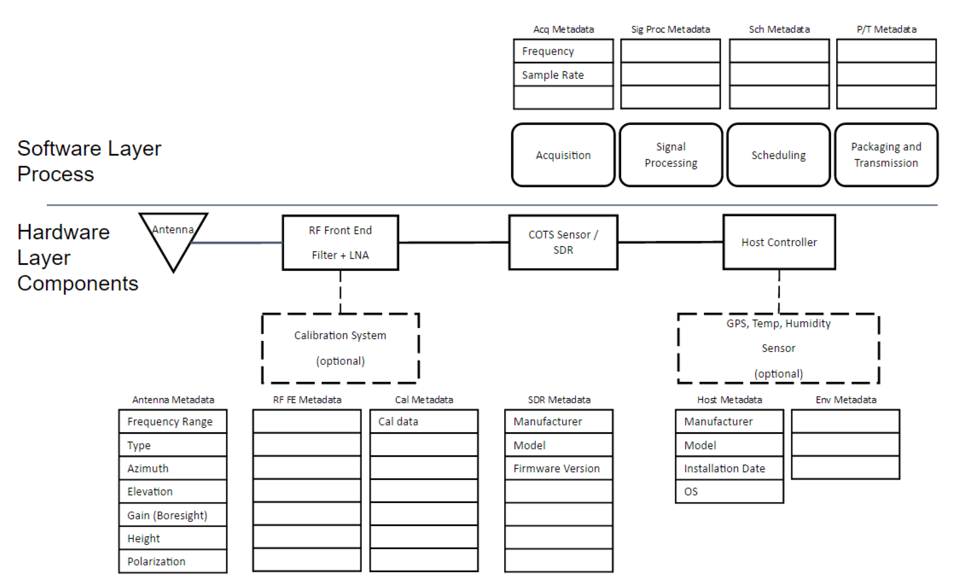


Figure 7: Hardware model - components and processes

* + - 1. Calibration Model

<Mike to send calibration method details.>

A calibration can be done in the lab at build/commissioning time, and stored as a calibration file on the SSD.

Further, an SSD with a self-calibration capability can be instructed through an administrative interface (not USER request) to perform a calibration using a local calibration source.

* + - 1. Algorithm Model

The Algorithm models shall be described in terms of inputs into black box: the identity of the USER and SSM requesting the scan, the measurement parameters, which algorithm is to be used; and outputs from the black box: the identity of the USER and SSM requesting the scan, the requested scan parameters, the identification of the algorithm model, and the processed results.

<Define use cases>

Normative model: general energy detection algortithm

At least one algorithm model is defined – a general energy detection algorithm.

<Trigger event algorithm>

<DF algorithm>

<Cyclostationary>

It is the responsibility of the SSM operator to publish algorithm definitions externally. Code does not need to be publicly accessible.

Allow for the development of advanced algorithms, e.g., DF.

* + - 1. SSD Hardware specification
         1. Top level metadata

|  |  |  |
| --- | --- | --- |
| Parameter | Values | Description |
| Antenna | 0 | Number of antennas |
| Calibration source |  | Present/absent |
| RF switch |  | Present/absent |
| RFFilter |  | Present/absent |
| LNA |  |  |
| Sensor |  | COTS/SDR |

* Antenna Metadata
* Calibration Source Metadata
* RF-Filter Metadata
* LNA Metadata
* Sensor Capability Metadata
  + - 1. SSD Software specification
         1. Algorithm specification

|  |  |  |
| --- | --- | --- |
| Algorithm | Value | Notes |
| Unspecified | 0 |  |
| Energy Detection | 1 | Default |
| Direction Finding | 2 |  |
| Cyclostationary | 3 |  |
| Wideband | 4 |  |

* + - 1. SSD Control
         1. Scheduler Specification

|  |  |  |
| --- | --- | --- |
| Algorithm | Value | Notes |
| Unspecified | 0 |  |
| Host Controller | 1 |  |
| Embedded Job Controller | 2 |  |
| Multilevel | 3 |  |
|  |  |  |

* + - * 1. SSD Output Specification

|  |  |  |
| --- | --- | --- |
| Algorithm | Value | Notes |
| Unspecified | 0 | Invalid |
| Time domain IQ | 1 | Default |
| Freq domain IQ | 2 |  |
| Time domain Amp, Phase | 3 |  |
| Freq domain Amp, Phase | 4 |  |

* + 1. Spectrum Sensor Manager (SSM)

<Roger’s input>

* + - 1. Scheduling

<Mike’s input>

Scheduling is defined in terms of scan intervals that take up slots in a calendar schedule. These slots will include slots for long scans; and slots for very short scans to ensure fair allocation of scan resources.

Scheduling requests from a USER will be defined in terms of duration, time, repetition, etc, as well as a flag to inducate whether the desired scan slots are “Exact Time” slots or “Nearest Time” slots. The scheduler on the SSM will use this to try meet the USER request (and either confirm the scan schedule is accepted or refused).

* + 1. Data Distribution

<William’s input>

* + - 1. Messaging Format

SSD and SSM messages will be in JavaScript Object Notation (JSON). JSON is a language-independent data-interchange format that is easy for humans to read and write. There are code and functions readily available in C, C++, C#, Java, JavaScript, MATLAB, Perl, and Python for parsing and generating JSON. It is a lightweight alternative to XML, commonly used to transmit data between server and browser applications.

The data fields in the JSON message descriptions below are required fields. If an attribute is not relevant to the sensor implementation, then the value is set to NaN or "NaN". Each message (in general) will begin with a header comprised of attribute-value pairs in ASCII characters. The first five fields are the same for all messages; they are:

1. Ver = Schema/data transfer version with the major.minor.revision syntax (string)

2. Type = Type of JSON message (string) {“Sys”, ”Loc”, or “Data”}

3. SensorID = Unique identifier of sensor (string of URL unreserved characters)

4. SensorKey = Authentication key given out by MSOD (integer)

5. t = Time [seconds since Jan 1, 1970 UTC] (long integer)

The following are specific formatting rules to be followed to avoid problems when messages are ingested into MSOD: (1) All timestamps, i.e., t (defined above)and t1 (to be defined in Data message description) will be reported as seconds since 1/1/1970 midnight UTC in the UTC time zone. (2) String values must only contain URL unreserved characters (i.e., uppercase and lowercase letters, decimal digits, hyphen, period, underscore, and tilde), and (3) Field names cannot start with an underscore because that convention is reserved for MSOD internal use.

* + - * 1. SSD Messages

<Apurva’s input>

* + - * 1. SSM Messages

<Roger’s input>

* + 1. Actor definition
       1. Usage Models

There are at least three main classes of consumers of spectrum data:

**Type A Consumers:** are specifically looking for current sensing information, and request specific scans to obtain specific data (e.g. law enforcement).

**Type B Consumers:** have a requirement to keep spectrum information up to date (e.g. spectrum occupancy database operators), and will need to request periodic scans to achieve this.

**Type C Consumer:** those that want to read spectrum information from a data store that is already populated with their required data. These users are not contemplated in this standard.

In general it should be assumed that a Type A consumer would have higher priority in terms of scan resources, as governed by a Policy expanded on below.

* + - 1. Data Ownership

The entity that builds/owns the SCOS owns the data it acquires. It can sell this data. Once that transaction takes place. The client has ownership, which is not necessarily exclusive - i.e., SCOS can sell it to other clients.

* + 1. SSM Policy

<Nilesh input>

A policy layer in the SSM at the northbound and southbound API will ensure that the SSM is operated within requirements of a local authority (national regulator, law enforcement, military, etc).

The policy on the southbound interface will determine, based on the USER type, (e.g. how a central authority can define what kinds of sensing can be done in what bands, what data governance rules there are, etc

-- resource allocation – what kinds of users are authorized to request resources from the sensor network and in which priority (i.e. if a sensing network is resource constrained, who gets first dibs on the sensors)

Policy on the northbound interface (SSM>DBstore) will have rules for how sensing data may be distibuted, and data storage policies. This would include which scan data takes priority if local storage in the store&forward buffer is running out due to a failed transmission link, and how long certain USER data is allowed to be stored in the local store&forward buffer.

Policy file: It is envisioned in the first version of this standard that the SSM stores a policy file which is installed manually by Sensing Operator (through mechanism such as SSH and update pull, or remote SCP).

Security Considerations

<Nilesh input>

* + 1. SSM Administration

Administrative functions on the SSDs and SSMs are largely assumed to be implementor-specific, and out of scope for the standard.

Requirements in an Informative Annex would include that there is:

* + - 1. Administrator interface:

An administrator interface that has a secure mechanism to administer the system, allowing:

* performing of calibrations
* updating firmware
* changing configuration of SSD, and making associated changes to the SSD configuration file
* triggering reboots

The administration interface must be a secure interface with key exchange, and these keys must not be the same as keys used for USER<>SSM<>SSD authentication.

* 1. SCOS Metadata Specification
     1. Metadata Classes

Metadata is defined into Classes to allow granularity in which metadata is stored or transmitted to reduce traffic and storage requirements.

* Class A metadata is for hard/fixed parameters that should not change (e.g. device ID, hardware config, antenna type, etc)
* Class B is for parameters configured per device (antenna orientation, sweep range, etc)
* Class C are scan/user dependent (swept freq, sensing algorithm, location, user info, etc).
  + 1. Reference architecture for SSM

SSM receives different messages from several SSDs, puts these messages in a queue and starts to unpack and process the received packets according to the time of arrival. The relevant data is locally stored until it is sent to an authorised third party system, such as a geographical database.

The “southbound” interfaces between the SSD(s) and the SSM(s) are:

* SSM Control/SSD Interface: allows the SSM to request SSD capability information, and to push sensing requests to the SSD, either as a single task or as a schedule of tasks.
* SSD/SSM Ingest Interface: allows an SSD to transmit a package of sensing data to the SSM.

The “northbound” interfaces between the SSM and other systems are:

* Platform Control Interface: Allows an authorised user to request that the SSM queries the capabilities of particular sensing devices, and to request scans, or to request a scan schedule be transmitted to devices.
* Spectrum Occupancy Database Interface: Transmits sensing data to specified external systems.

The SSM has to distinct operating fucntions:

* Sensing Platfrom Control: Authenticates and authorises users to perform functions on the SSM, according to policies or other rules imposed on it.
* Sensing Platform Data Processing: Receives sensing data packages from SSDs, unpacks and performs validation, stores in local data store and manages transmission of data on to authorised consumers of sensing data.
  + 1. Interface – Sensing

Physical interface:

Input: N/A

Output: Interconnect from filter/amp to SDR

API: Controller to antenna motor

Metadata: Antenna gain

Antenna type

Antenna orientation and polarization (if non omnidirectional antenna is used)

Antenna bandwidth

Antenna impedance

Insertion loss (into amp)

Return loss

Amplifier gain

Filter parameters

Noise metric

* + 1. Interface – Detecting

Physical interfaces

Input: Interconnect from filter/amp to SDR

Output: N/A

API: Scan request and parameters

Sensing-to-Packaging transfer

Input parameters:

Channel to be sensed

Max Scan time

Sensing method to be adopted

Resolution bandwidth setting (RBW)

Metadata: Scan parameters (channel, scan time, sensing method, resolution bandwidth)

SSD hardware ID/key

Battery level (if the SSD is battery powered)

Temperature/humidity (in order to evaluate if the SSD hardware is working in normal operating condition)

Sensor location coordinates

(Management System metadata)

(Detecting Metadata)

(Management System metadata)

(Capture Metadata)

* + 1. Interface – Packaging

Physical interface:

Input: N/A

Output: N/A

API: Packaging-to-MQ

SCOS-as-a-Service Request

Metadata: Packaging information (time, certificates, etc)

Network information (media, connection)

(Sensing Metadata)

(Detecting Metadata)

* + 1. Interface – Transmission

Physical interface:

Input: N/A

Output: Best effort IP transport

SSL encryption

Transmission Control

API: MQ-to-Ingest

Ingest-to-Data Store

Metadata: Package audit information

(Packaging Metadata)

(Sensing Metadata)

(Detecting Metadata)

* + 1. Interfaces – Management

Physical interface:

Input: Best effort IP transport

Output: Best effort IP transport

SSL encryption

Transmission Control

API: Management-to-MQ

SCOS-as-a-Service Request

Metadata: Management system certs

* 1. Management Reference Architecture
     1. Spectrum Sensing Platform – Sensing Service Control
        1. Spectrum sensing API

The spectrum sensing platform provides spectrum sensing as a service using Spectrum sensing API. This is the northbound interface from the block diagram.

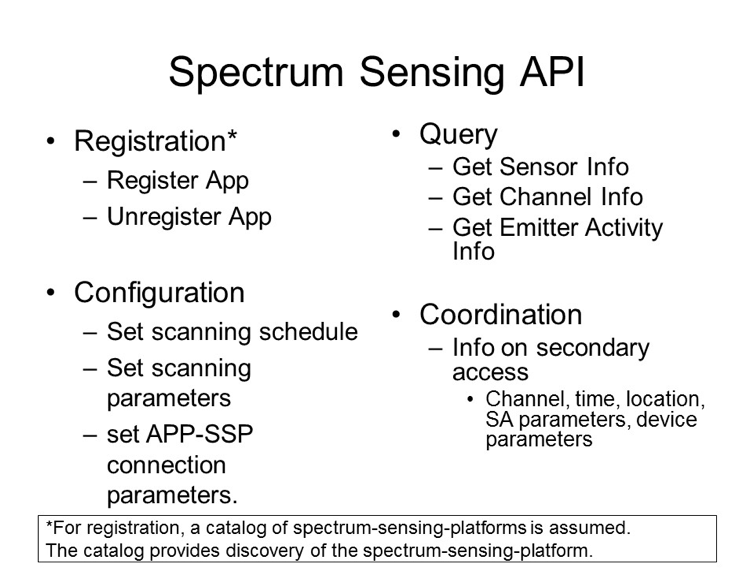
We identify following four types of API

1. Registration (ID, key exchange, authorisation)
2. Query (sensor model, signal processing capability (occupancy, characterisation, calibration, df), health, availability, location)
3. Configuration (sensing config, scheduling config, calibration, [operational])
4. Notification of Change (reverse Query)
5. Notification of Busy (TBC?)

With the Registration API, an SSA can enable/disable usage of the API. Configuration API enables an SSA to configure the SSP for desired purpose. Using Query API, an SSA can request real-time data or past data. (*Inference regarding secondary spectrum-access is purposefully excluded from the SSP API. For example, Is it safe to transmit? This spectrum-access inference logic is considered to be in the apps that are using the spectrum-sensing platform*.)

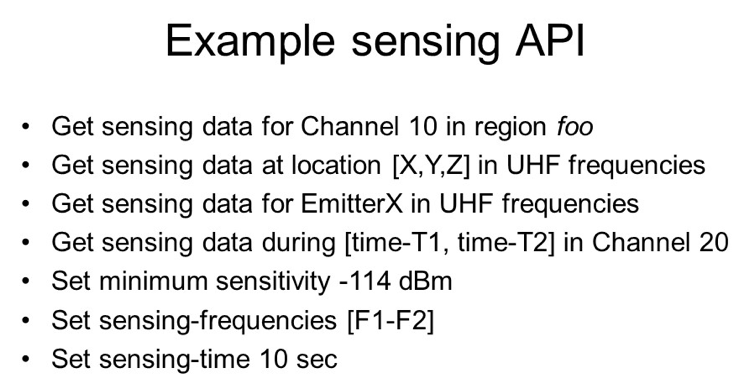
The coordination API is optional. It can be used in circumstances wherein the Apps wants to provide information about secondary spectrum-access. For example, an SSA may use the real-time sensing data and infer feasibility of secondary spectrum-access. This SSA would grant spectrum-access parameters to secondary user radios and use the coordination API to notify the secondary spectrum access to SSP.

Following diagram captures the high-level summary of the SSP API.



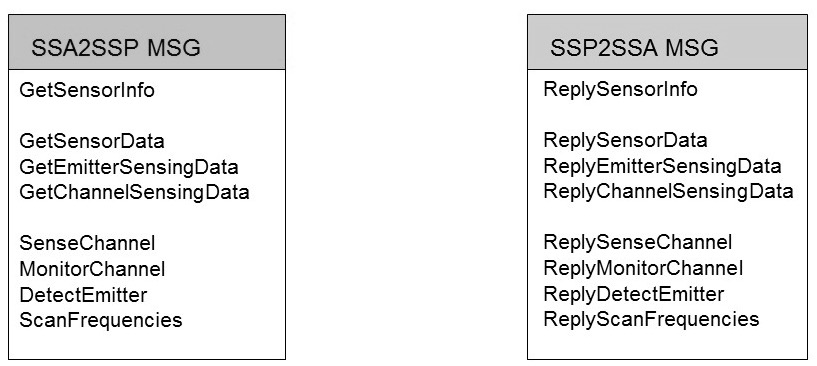
* + - 1. Example spectrum sensing API design

The spectrum sensing requirements vary significantly in terms of geographies (different countries have different regulations) and they have been evolving over time. The requirements also vary depending on frequency-bands. Thus, there is a need for configurability and extensibility for SSP API. In this regard, policy-based interface is very much appealing. Furthermore, we may consider developing semantics for sensing-data and ontology-driven sensing policy (OWL). Following diagram shows some examples of possible SSP API.

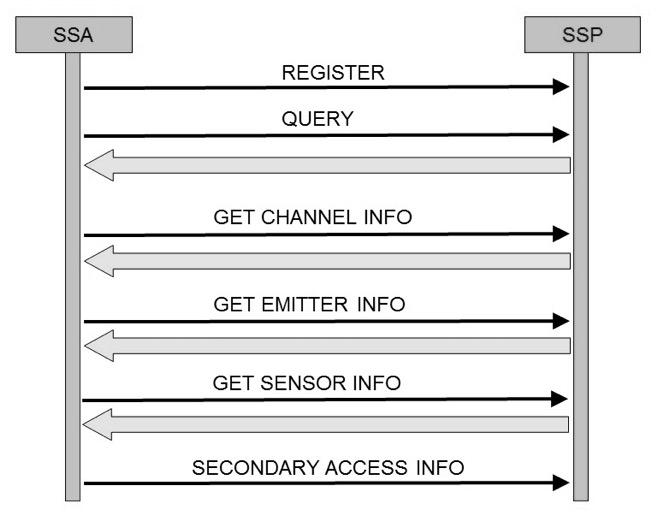


* + - 1. Message Exchange

SSA API requests and SSP API response are encapsulated in messages. Each message has a message-ID, message-Type, and the message body. Following diagram identifies various message types.



Following sequence diagram illustrates message exchange between SSA and SSP.



* + 1. Spectrum Sensing Control

The spectrum sensing platform provides spectrum sensing service by controlling the spectrum sensing devices (SSD) with southbound interface. There are following 3 types of API

1. Registration: Allows to add/remove an SSD to SSP
2. Control: Controlling the sensing function and schedule of an SSD
3. Query: Requesting sensing data from an SSD

* + - 1. Sensing Functions

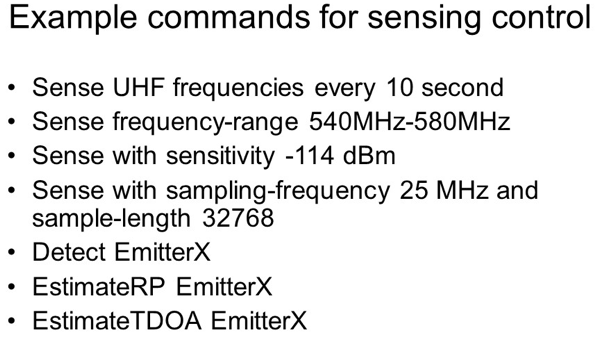
There exist multiple sensing techniques/algorithms from energy detection to exploiting cyclostationarity and signal statistics. Some sensors may be able to report occupancy in terms of aggregate RF-power received at the sensor location while higher end sensors may be able to estimate location and received power (RP) in the presence of cochannel interface and noise.

* + - 1. Sensing Schedule

The SSP may need to scan a wide range of frequencies at a specific periodicity. Thus, SSP may in tur define a sensing schedule for each of SSDs. The schedule may be adapted in response to certain events or policies from the SSAs.

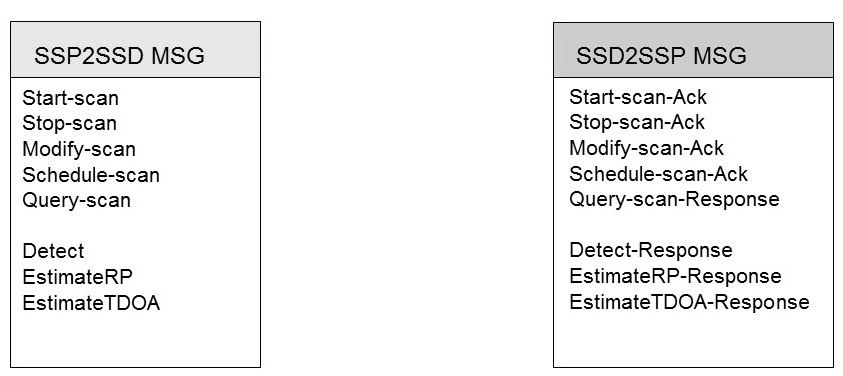
Examples

Following are a few examples of the interface between the SSP and SSD.

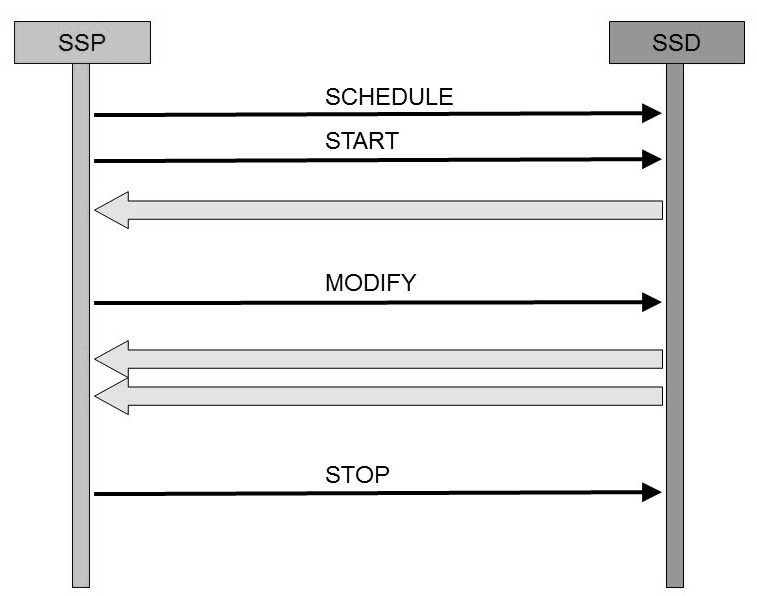


* + - 1. Message Exchange

The message from SSP to SSD is formatted in the similar way (has message-ID, message-type, and actual message). Following diagram shows some of the message types.

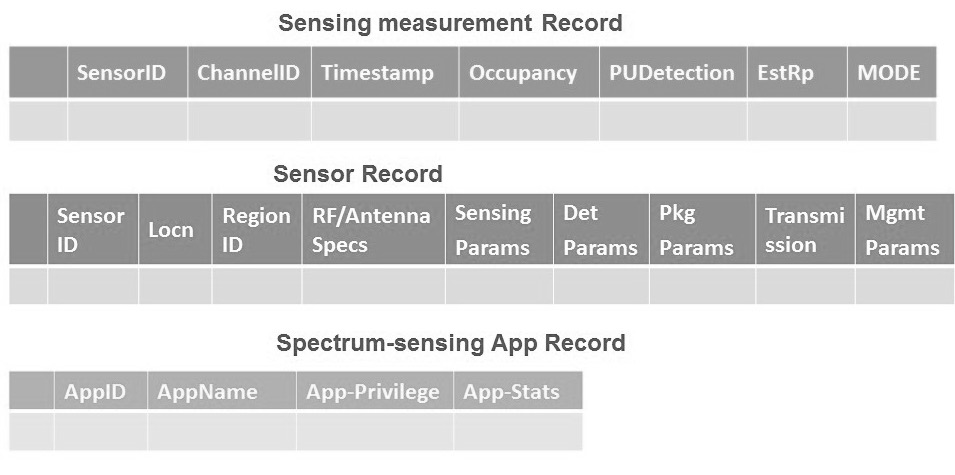


Following sequence diagram illustrates the message exchange between SSP and SSD.



* + - 1. Data Store

SSP collects and stores the sensing data to provide the services defined under the SSP APi. One of the popular approaches is to use relational database. Following diagram illustrates records for (a) sensing measurement, (b) SSD (c) SSA.



Alternate approach could be to develop spectrum sensing semantics based data-store.

1. Architecture System Requirements

* Radio energy is detected up by an antenna on Spectrum Sensing Device and transferred through an interconnect to a signal pre-conditioner containing mixers/filters/amplifier segments, according to pre-determined hardware parameters
* Signal is transferred to the SSD’s SDR to produce baseband signal, quantised by ADC and passed in digital form to be processed by a sensing technique, the nature of which is stored in metadata, with method described in informative section of Annex [to be listed?]
* This sensing data is packaged along with key metadata within the SSD and stored locally for transmission. Metadata includes:  
  – scan time, scan duration, scan location, device identifiers…  
  – hardware parameters of antenna and radio front end
* The package is (a) transmitted to a remote system that (b) ingests and validates data, and (c) stores for further processing
* The back-end management system exchanges control information with SSDs
* e.g. device management, operation validation, integrity of information chain verification, maintenance tasks
  + 1. Detecting

Radio energy is detected up by an antenna on Spectrum Sensing Device and transferred through an interconnect to a signal pre-conditioner containing mixers/filters/amplifier segments, according to pre-determined hardware parameters

Sensing information should consist of:

* Calibrated Power Spectral Density (PSD)
* Energy Detection Results
* Presence of Known and Unknown Signals.
  + List of Detected Signals
  + List of Frequency where there are Unknown Signals
  + List of Frequencies where there are Known Signals

TV Band Signals - ATSC, DVB-T, ISDB-T

Wireless Microphone Signals

Radar Signals – Detection and Identification – e. g. SPN-43

Wi-Fi Signals, LTE, CDMA, WCDMA, GSM Signals

Un-authorized signal alarms

Interference Alarms

Update on the Protecton Contour based on Sensing

* + 1. Sensing

Signal is transferred to the SSD’s SDR to produce baseband signal, quantised by ADC and passed in digital form to be processed by an accepted sensing technique

* + 1. Packaging

This sensing activity is packaged along with key metadata

* + 1. Transmission – from SSD to WSME / from Platform Control tp WSME

Northbound (SSD to platform): The package is transmitted to a remote system that ingests and validates data, and stores for further processing, with ACK back to SSD that packages were received.

Southbound (platform to SSD): Control messages are transmitted to SDD for execution by SSD, with ACK that control messages was received, and response code that instruction was accepted/rejected.

* + - 1. Message queues

The SSM devices use MQTT to speak to a MQ server instance (e.g. RabbitMQ). The MQ server instance maps the MQTT topics from the SSM into queues which the SSM ingest layer monitors and processes messages out of.

All traffic from the SSM to the SSM’s goes via AMQP queues into the MQ server instance which maps it out to the appropriate MQTT topics. The SSM pick up messages on any topics to which they have subscribed.

* + - 1. Message Queue security

The MQTT segment has security based on TLS with pre-generated certificates.

* + - 1. QOS

All messaging on the MQTT side makes use of QOS 1. When using QoS level 1, it is guaranteed that a message will be delivered at least once to the receiver. The message can also be delivered more than once. If a message is delivered more than once it should start a counter and a clock. If the clock/counter exceeds a threshold it should create an alert on the administration console that there is a comms or ingest fault.

The SSM’s use a non clean session when connecting which ensures that messages sent to the client when non connected will be queued and delivered on reconnection. On the RabbitMQ the messages are queued on a topic for a client for up to 30 minutes before being discarded (this threshold for discussion).

The MQ server must use persistent queues for all applicable queues. Messages should survive a restart.

* + 1. Ingest

Package must be reliably, securely and scaleably received and transmitted to data store

Messages are processed inside the SSM using an ESB application. The ESB application architecture allows for small discrete message handlers to be written to deal with each type of message. Using a load balanced and multiple instances of the servers the load can be shared out across multiple servers.

Handlers are written for each of the types of messages. These handle unpacking and persistence of the incoming data. In some circumstances messages may be forwarded on to a task processor for further processing or analysis. All messages are persisted in a database.

* + 1. Storage

Data moved into structured database

* + 1. Platform Control Messages

HTTP service endpoints are implemented in the ESB application to allow for the triggering of outbound control messages to the SSDs through a southbound interface.

A variety of task requests can be predefined by the SSM policy such as different scan modes of the SSM, defining different timeframes, scan parameters, etc:

- Test Mode: one ping and one raw scan every 15 minutes

- Mobile Mode: one ping and one raw scan every 10 minutes

- Static Mode: one ping and one TV channel scan every 15 minutes. one raw scan every ½ hour.

These messages can be used to trigger SSD scan activity, or for system management.

* + 1. Management and Maintenance

The back-end management system exchanges control information with SSDs

Manage them

* Device health reports – power, temperature, location, GPS health, OS/environment health, network health, storage health, scheduled and by query
* Manage by device, group, Class of device

Validate their operation

* Run test scans against known data points (e.g. from WSDB)

Verify integrity of information chain

* Software tools to validate process chain

Perform maintenance

* Push updates to devices (software, OS, firmware, certifications)
* Perform remote reboots, resets
* Shell into device to do diagnostics
  + 1. User Device Control

Ability for authorized user to instruct Sensing Devices to perform particular scans

**Messaging and Command and Control**



**Figure 1. SCOS Architecture**

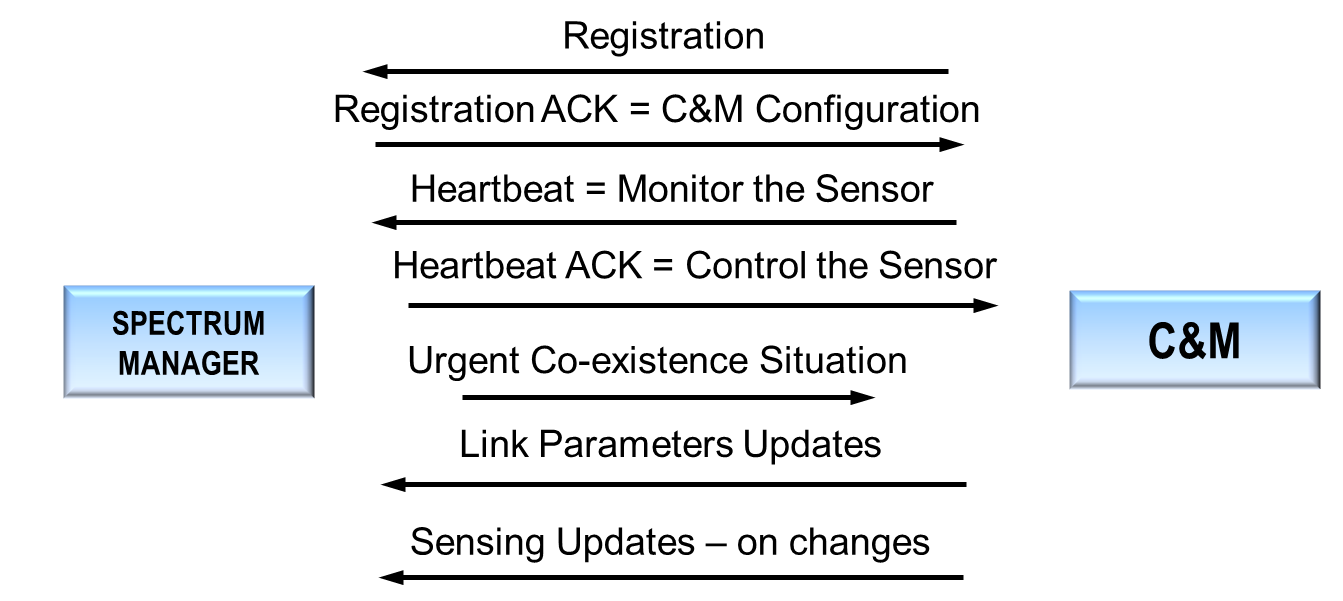


Figure 10: SCOS Messaging

* + 1. User Data Store Interrogation

Ability for authorized user to pull information from data store via API.

* + 1. Policy Management and Enforcement

Ability to cascade policies down from master server to SSD management servers and there to SSDs to determine:

* Possible sensing techniques
* Scan parameters
* Data upload qualities from SSD to data store

1. System Definitions and Interfaces

Definitions of units, measurements for each defined parameter in the standard

The parameters defined in the previous section need a detailed definition. In the following, they will be defined in detail, a priority grid (paradigm MoSCoW adopted) will be provided and canonical measurement units will be given.

According to MoSCoW paradigm, used in software engineering requisite classification, a parameter can belong to the following categories:

M (MUST HAVE): very high priority parameter, it cannot be missed in the data exchange process;

S (SHOULD HAVE): medium priority parameter, it is requested to be present but in rarely cases he could be skipped.

C (COULD HAVE): low priority parameter, it could be useful if present but its absence would not affect negatively the system;

W (WISH LIST): optional parameter, to be used if room: not actually needed.

* 1. System Units and Parameters

**Stage 1 parameters:**

**Antenna gain (M):** the ratio of the power received by the antenna and the power received by a hypothetical lossless isotropic antenna.

**Antenna type (M):** according to its shape and radiation pattern, different antenna types can be used for SCOS purposes, if they can provide requested accuracy results.

**Antenna bandwidth (M):** the frequency range over which an antenna can work well.

**Amplifier gain (M):** it is the difference (in dB) or the ratio between the power at the exit stage and that one at the input stage of the amplifier.

**Antenna orientation and polarization (if non omnidirectional antenna is used) (S):** The polarization of an antenna is intended the orientation of the electric field (E-plane) of the radio wave wrt the Earth's surface. It depends of the physical structure of the antenna and its orientation.

**Insertion loss (into amp) (S):** it refers to the attenuation the received field experiences passing through the wire connecting the antenna to the amplifier.

**Return loss (S):** it is defined as the power loss of the signal due to the reflections in correspondence with impedance discontinuity along the transmission line.

Analytically, it is defined as: , where *Pi* is the incident power, *Pr* the reflected power.

**Noise figure (S):** noise level estimation through the analysis of a surely vacant channel.

**Filter parameters (C):** filter defined by typology (LPF, HPF, BPF, RBF) and cut-off frequencies.

**Antenna impedance (C):** the output impedance of the antenna.

**Stage 2 parameters:**

Input parameters:

**Channel to be sensed (M)**: frequency interval to be scanned, it can be provided through starting and stop frequency, or by using a LUT (look-up table), where a correspondence between a unique code and channel features is provided, in order to minimize data exchange communication overhead.

**Max Scan time (S)**: it is the amount of time a SSD must spend in order to acquire the signal and perform sensing. No data packaging time included.

**Resolution bandwidth setting (S):** it is actually defined as the ratio between the frequency interval under analysis and the number of frequency bins of the FFT process. Higher the RBW, higher the probability to detect very narrowband signals, such as wireless microphones.

**Sensing method to be adopted (C):** if more than one sensing method is loaded into SSD, the SSM could send a code corresponding to one of those methods, especially if different performance is ensured by different sensing methods.

Output Metadata:

**SSD hardware ID/key (M):** alphanumeric code indicating the specific SSD, for fixed stations it could be related to the sensor position.

**Scan parameters (S)** (channel, scan time, sensing method, resolution bandwidth): definition corresponds to input parameters but they are provided back to the SSM in order to ack the system that requested parameters have been correctly set and used.

**Temperature/humidity (S)** (in order to evaluate if the SSD hardware is working in normal operating condition): in some atypical conditions (extremely hot or extremely cold) the SSD hardware may provide inaccurate results or they could be corrected by a correcting factor depending on the temperature/humidity pair.

**Battery level (C)** (if the SSD is battery powered): indicated as the percentage wrt the full charge value, under a threshold sensing could be considered not reliable and recharging could be enabled by SSM.

**Sensor location coordinates (M for mobile devices, C for fixed stations):** latitude and longitude or distance from a reference point or node. Values can be provided by a GPS sensor embedded in SSD.

* + 1. Key minimum sensing parameters

In order to be compliant with SCOS framework, every SSDs must show, on testing scenario, performance in terms of two figures of merit:

1. Detection Probability (Pd):
2. False Alarm Probability (Pfa):

Where *Bo,i , Bo,tot , Bf,i* and *Bf,tot* represent the *ith* detected occupied bandwidth inside the actually occupied frequency interval, the total occupied bandwidth, the *ith* detected occupied bandwidth inside the free frequency interval, the total free frequency bandwidth, respectively.

According to SCOS purposes, Pd must be greater than 90% and Pfa less than 10% for every operating conditions, down to the minimum sensitivity level, defined in Section **Error! Reference source not found.**.

* + 1. Standard system units

|  |  |
| --- | --- |
| Parameter | Unit of measurement |
| Antenna gain | dBi |
| Antenna bandwidth | MHz |
| Antenna Impedance | Ω |
| Insertion loss | dB/m |
| Return loss | dB |
| Amplifier gain | dB |
| Scan time | ms |
| Resolution bandwidth | kHz |
| Temperature | K |
| Humidity | %rh |
| Battery level | % |
| Sensor Location coordinates | DD°MM’SS’’ N/S (latitude)  DD°MM’SS’’ W/E (longitude) |

* 1. Metadata Formats

Definition of metadata to be captured at each layer

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Data type** | **Format** |
| Antenna gain | Numerical | integer |
| Antenna type | enumerator | 1. Dipole antenna 2. Half-wave dipole antenna 3. Monopole antenna 4. Etc. |
| Antenna bandwidth | Numerical | Double (two digits after decimal mark) |
| Antenna impedance | Numerical | Integer |
| Antenna orientation | Numerical | Roll |
| Antenna polarization | Enumerator | 1. Horizontal 2. Vertical 3. Circular 4. Elliptical   Etc. |
| Insertion loss | Numerical | Double (two digits after decimal mark) |
| Return loss | Numerical | Double (two digits after decimal mark) |
| Amplifier gain | Numerical | Double (two digits after decimal mark) |
| Filter parameter: |  |  |
| Filter type | Enumerator | 1. LPF 2. HPF 3. BPF 4. Etc |
| Cut-off frequencies | Numerical | Double (two digits after decimal mark) |
| Channel to be sensed | Numerical | Double (two digits after decimal mark) |
| Channel to be sensed | Enumerator | List of channel |
| Max scan time | Numerical | Integer |
| Sensing method to be adopted | Enumerator | 1. Energy detection 2. cyclostationarity 3. matched filter 4. Etc |
| Resolution bandwidth setting | Numerical | Integer |
| SSD hardware ID/key | Alphanumeric |  |
| Battery level | Numerical | integer |
| Temperature | numerical | Double (one digit after decimal mark) |
| Humidity | Numerical | Integer |
| Sensor Location coordinates | alphanumeric | DD°MM’SS’’ N/S (latitude)  DD°MM’SS’’ W/E (longitude) |

1. Security Systems
   * + 1. Threat overview
       2. Authorisation, authentication, identity
       3. Security design between each architecture layer
          1. Physical security
          2. Data transmission security
       4. Security and redundancy model for data stores

# Informative: Regulatory Technical requirements

Various countries will have differing requirements here, but a few countries already have definitions in place that should be observed. For example, in the FCC rules for the VHF/UHF TV bands, the FCC requires a spectrum sensing detection accuracy as specified by the Table 1: FCC Sensing sensitivity requirements.

Table 1: FCC Sensing sensitivity requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Regulatory domain** | **Type of signal** | **Sensing detection threshold**  **(in dBm)** | **Data fusion rule for distributed sensinga** | **Monitoring requirements** |
| USA | ATSC | –114  (averaged over 6 MHz) | “OR” rule | Detection threshold referenced to an omni-directional receive antenna with a gain of 0 dBi |
| USA | NTSC | –114  (averaged over 100 kHz) | “OR” rule | Detection threshold referenced to an omni-directional receive antenna with a gain of 0 dBi |
| USA | Wireless microphone | –107  (averaged over 200 kHz) | “OR” rule | Detection threshold referenced to an omni-directional receive antenna with a gain of 0 dBi |

aThe value “1” indicates detection.

Other requirements for the 2.7 GHz to 3.7 GHz band shall be defined based on the evolving regulations. For example, the spectrum sensing devices in the 2.7 GHz to 3.7 GHz can sense for Radar Signals and provide that information to the Spectrum Access System (SAS) that is being defined in these bands.

# Device and System Security Recommendations

\* Remote access to SSD hardware through remote secure shell (SSH) and similar technologies must not use the same keys as SSM/SSD interface keys

\* Devices’ physical characteristics must be evaluated and enumerated at build validation and testing, with hardware and configuration parameters written to file /DEVICEHARDWAREPARAMETERS.CONFIGFILE (placeholder) and stored in non-writable file

\* Any changes to hardware configuration (e.g. change of antenna) must be recorded in DEVICEHARDWARECONFIGCHANGES.LOGILE and changes made to relevant parameters in D..H...P...CONFIGFILE, either through manual editing of config file or through a secure remote update mechanism (e.g. scripted SCP file revision).

# Implementation Guidelines/Notes

<Currently this section contains miscellaneous notes>

Tasking API, Mission API and Data Request API: The Mission API would be the equivalent of the SCOS API (i.e. where the Actor requests a scan schedule); the Task API would be the SSD API (i.e. the SSM sending an schedule update to a specific SSD). The Data Request API would not be included in the current design, as the retrieval of scan data would be between the Actor and the Data Store, which is implementation dependent.

# Review of 802.22 sections

**Areas of 802.22 that are potentially directly relevant/usable in 802.22.3**

* + 5.1.3.2 Spectrum Sensing Automation
  + 5.1.3.3 Security sublayer 2
  + 7 Management messages, esp

7.2 Addressing and connections

Each A-BS and CPE in an A-WRAN shall have a 48-bits universal MAC address, as defined in

IEEE Std 802® . This address uniquely defines the A-BS and CPE from within the set of all possible

vendors and equipment types. It is used as part of the authentication process by which the A-BS and CPE

each verifies the identity of the other at the time of network association. The A-BS MAC address is

broadcast by the A-BS on superframe control header (SCH) on PHY Operation Mode 1 (Clause 9) or

frame control header (FCH) on PHY Operation Mode 2 (Clause 9a) and is present in every CBP burst.

Each A-WRAN device regularly broadcasts a CBP burst containing its Device ID and Serial Number.

This is done as part of the device’s self-identification process that helps identify potential interference

sources to incumbent services and for coexistence purposes.

Connections are identified by two items, a 913-bit station ID (SID) and a 3-bit flow ID (FID). The SID

uniquely identifies a station that is under the control of the BS, the A-BS, or the distributed scheduling ACPE. A SID can be for a unicast station, when referencing a single CPE, or for a multicast station, when

referencing a multicast group (of CPEs). A FID identifies a particular traffic flow assigned to a CPE. The

tuple of SID and FID (SID | FID) forms a connection identifier (CID) that identifies a connection for the

CPE. The SID is signaled in the DS/US-MAP allocation, and the FID is signaled in the generic MAC

header (GMH) of a MAC PDU. This allows for a total of up to 8192 stations, each with a maximum of

eight flows that can be supported within each downstream and upstream channel.

At CPE initialization, three flows shall be dedicated for management connections (see 12.2) for the purpose

of carrying MAC management messages and data between a CPE and the BS/A-BS or the distributed

scheduling A-CPE. The three flows reflect the fact that there are inherently three different levels of QoS for

traffic sent on management connections between a CPE and the BS/A-BS or the distributed scheduling ACPE.

The basic flow is used by the BS/A-BS MAC or the distributed scheduling A-CPE MAC and CPE MAC to exchange short, time-urgent MAC management messages; whereas, the primary management flow is used by the BS/A-BS or the distributed scheduling A-CPE MAC and CPE MAC to exchange longer, more delay-tolerant MAC management messages (Table 19 specifies which MAC management messages are transferred on which type of connections). Finally, the secondary management flow is used by the BS/A-BS or the distributed scheduling A-CPE and CPE to transfer more delay-tolerant, standards-based (e.g., DHCP, TFTP, and SNMP) messages that are carried in IP datagrams. The secondary management flow may be packed and/or fragmented, similarly to the primary management except that no ARQ should be used for the latter since it is more time critical. The FIDs for these connections shall be assigned according to the specification in 12.2. The same FID value is assigned to both upstream and downstream members of each connection.

The CID, which is a tuple of SID | FID, can be considered a connection identifier even for nominally

connectionless traffic like IP, since it serves as a pointer to destination and context information.

7.7 Management messages

As can be seen in 281HTable 19, the MAC defines a collection of management messages to support and

implement its basic functions. All these messages are carried in the payload of a MAC PDU, and share the

same message structure as depicted in 282HFigure 15. Management messages begin with a Type field that

uniquely identifies the message in question, while its payload varies according to the message type. As for

transmission, management messages can only be transmitted in Initial Ranging, Basic, Primary, Multicast

Management, or Broadcast type of FIDs (see 283H Table 279, 284H Table 280, and 285H Table 281). No other types of FIDs shall carry management messages.

7.7.7 REG-REQ/RSP

CPEs shall register with a BS before receiving or being provided any type of service. In the following

subclauses, the registration process incorporated in the MAC as well as a series of IEs that may be carried

by these messages are presented.

7.7.7.1 REG-REQ

The format of a REG-REQ message is shown in 406HTable 45. This message shall be transmitted by CPEs at

initialization phase.

The FID field carried in the MAC header of the PDU where this message is transmitted shall be the primary

management FID for this CPE, which is assigned during the RNG-CMD message.

7.7.7.2 REG-RSP

The format of an REG-RSP message is shown in 408HTable 46. This message shall be transmitted by the BS in

response to a REG-REQ.

The FID field carried in the MAC header of the PDU where this message is transmitted shall be the primary

management FID of the CPE for which this message is intended.

7.7.7.3 REG-REQ/RSP information elements

REG-REQ and REG-RSP management messages may carry a number of IEs that support the registration

process. The REG-REQ message shall include the CPE NMEA Location String IE. These IEs are described

in detail in the following subclauses.

7.7.7.3.1 CPE NMEA Location String

This is the location data string pertaining to the CPE’s location. It shall be in the NMEA 0183 ASCII

format. This IE shall be added to the REG-REQ message during initial registration during network entry, as

well as in the transmission of a REG-REQ that is in response to a RNG-CMD sent with ranging status set

to “Re-range and Re-register” (see 41H7.14.2.11).

~~7.7.7.3.2 Convergence sublayer configuration~~

~~The Convergence sublayer configuration parameter dictates how the provider intends to operate the CPE on~~

~~an ongoing basis. If the IE= 0, the CPE shall use the Ethernet CS. This allows the CPE to either act as a~~

~~bridge or other Ethernet device. If IE = 1, the CPE shall use the IP CS. This allows the CPE to either act as~~

~~a router, or other IP-based device.~~

7.7.7.3.3 IP Version

This field indicates the version of Internet Protocol used on the Secondary Management Connection. IPv6

is not mandatory. The omission of the IP Version parameter in the REG-REQ message shall be interpreted

as IPv4 support only.

7.7.7.3.4 CPE capability

Through the registration process a BS shall become aware of the capabilities of the registering CPEs. The

following subclauses describe the IEs that convey the CPE capability information to the BS.

7.7.7.3.4.1 IP ROHC support

This IE indicates the ability of the CPE to support IP Robust Header Compression (ROHC).

7.7.7.3.4.2 ARQ support

This field indicates the availability of CPE support for ARQ. If ARQ is enabled for Secondary

Management flow, the IEs that are defined in 412H7.7.8.9.17.2 to 413H7.7.8.9.17.8 shall be added to the REG-REQ or REG-RSP to facilitate configuration of ARQ that is to be applied on PDUs traversing the Secondary

Management flow.

7.7.7.3.4.3 ARQ parameters

This field provides the fragmentation and ARQ parameters applied during the establishment of the

secondary management connection. This field is related to the ARQ parameters described in 414H7.7.8.9.17.

7.7.7.3.4.4 DSx Flow Control

This field specifies the maximum number of concurrent DSA, DSC, or DSD transactions that may be outstanding.

7.7.7.3.4.5 MCA Flow Control

This field specifies the maximum number of concurrent MCA transactions that may be outstanding.

7.7.7.3.4.6 Maximum number of Multicast Groups supported

This field indicates the maximum number of simultaneous Multicast Groups to which the CPE is capable of

belonging.

7.7.7.3.4.7 Measurement support

The CPE adds this IE in the REG-REQ to indicate to the BS what sensing capabilities the CPE supports, as

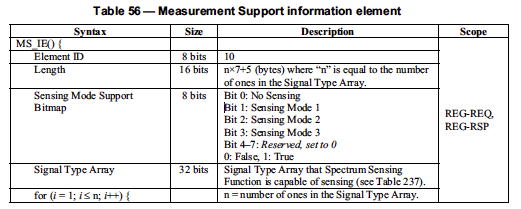
well as how well the CPE can sense for particular signals. In the REG-RSP, the BS sets this IE to configure

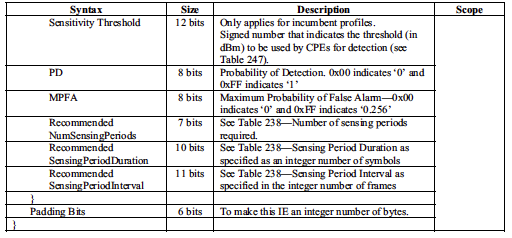
what sensing capabilities the CPE will make use of and how sensing for particular signals is to be executed.

Note that if the “No Sensing” bit (Bit 0) in the Sensing Mode Support Bitmap is set to True, Bits 1, 2, and 3

shall be set to False. When the BS configures the IE for transmission in a REG-RSP, then sensing would be

disabled at the CPE.





7.7.7.3.4.8 Manufacturer-specific Antenna Model

7.7.7.3.4.9 CPE Antenna Gain

This information provided by the CPE at registration can be used by the BS to prioritize its list of

backup/candidate channels based on the receiving performance of its CPE.

7.7.7.3.4.10 CPE residual delay

This residual delay shall be measured by the manufacturer when the CPE is co-located with the BS (i.e., BS

and CPE antennas are co-located or the BS and CPE are connected through the proper lengths of feed

cables) and the Timing Advance (see 420HTable 44) is set to zero. The manufacturer shall record this residual

delay in the CPE, which shall be reported to the BS at the time of registration on the network.

(perhaps this can store ping time form Management System to SSD to store latency on scan request/response?)

7.7.7.3.4.12 Permanent Station ID

This field specifies the permanent SID assigned to a CPE. This IE is included if the CPE Privacy (see

Clause 421H8) during network entry is supported by the operator.

7.7.7.3.4.13 CPE Operational Capability

This field allows the CPE to signal to the BS that it is to be operated as a Fixed or Portable terminal.

7.7.7.3.5 CPE Registration Timer

This timer is used to govern how long a CPE and BS maintain context of each other after registration has

been completed. This value is set based on the type of CPE, either portable or fixed, that is currently

attempting registration. This value is used to set T30.

7.7.8.9 Service Flow encodings

43HTable 72 and the subsequent subclauses define the parameters associated with upstream/downstream

scheduling for a service flow. The encapsulated upstream and downstream flow classification configuration

setting strings share the same subtype field numbering plan because many of the subtype fields defined are

valid for both types of configuration settings except service flow encodings. One major parameter of the

service flow definition is the direction of the service flow (see 4H7.7.8.9.1). This parameter determines if

subsequent service flow parameters are applied in the downstream (BS to CPE) or upstream (CPE to BS)

service flow. Classification rule parameterization (see 45H7.7.8.9.18) is made of a compound set of IEs defined

in 46H7.7.8.9.18.1 through 47H7.7.8.9.18.3.14.

(this can potentially be used to store parameters defining Management back end to SSD’s network/response characteristics)

7.7.8.9.1 Service Flow Direction

This parameter is used to indicate the direction of the service flow. Service flows are unidirectional and are

DS (BS to CPE) or US (CPE to BS).

7.7.8.9.2 SFID

The format of the Service Flow Identifier (SFID) is defined in 48HTable 74.

7.7.8.9.3 Service Class Name

The format of the Service Class Name is defined in 49HTable 75.

7.7.8.9.4 QoS Parameter Set Type

The format of the QoS Parameter Set Type is defined in 450HTable 76 as the three first bits of the octet, and

451HTable 77 enumerates all the combinations for these 3 bits that define controls for how QoS parameter sets

are applied to the service flow that is being configured.

7.7.8.9.5 Maximum Sustained Traffic Rate

The format of the Maximum Sustained Traffic Rate is defined in 452HTable 78.

(Good to provide metrics for “real time” scan capabilities)

7.7.8.9.6 Maximum Traffic Burst

The format of the Maximum Traffic Burst is defined in 453HTable 79.

7.7.8.9.7 Minimum Reserved Traffic Rate

The format of the Minimum Reserved Traffic Rate is defined in 454HTable 80.

7.7.8.9.8 Minimum Tolerable Traffic Rate

The format of the Minimum Tolerable Traffic Rate is defined in 45HTable 81.

7.7.8.9.9 Service Flow Scheduling Type

The format of the Service Flow Scheduling Type is defined in 456HTable 82.

7.7.8.9.10 Request/Transmission Policy

The format of the Request/Transmission Policy is defined in 457HTable 83.

7.7.8.9.11 Tolerated Jitter

The format of the Tolerated Jitter is defined in 458HTable 84.

7.7.8.9.12 Maximum Latency

The format of the Maximum Latency is defined in 459HTable 85.

7.7.8.9.13 Fixed-length vs. Variable-length SDU Indicator

The format of the Fixed-length vs Variable-length SDU Indicator is defined in 460HTable 86.

7.7.8.9.16 Maximum Tolerable Packet Loss Rate

The format of the Maximum Tolerable Packet Loss Rate is defined in 463HTable 89.

7.7.8.9.13 Fixed-length vs. Variable-length SDU Indicator

The format of the Fixed-length vs Variable-length SDU Indicator is defined in 460HTable 86.

7.7.8.9.14 SDU Size

The format of the SDU Size is defined in 461HTable 87.

7.7.8.9.15 Target SAID

The format of the Target SAID is defined in 462HTable 88.

7.7.8.9.16 Maximum Tolerable Packet Loss Rate

The format of the Maximum Tolerable Packet Loss Rate is defined in 463HTable 89.

7.7.8.9.17 ARQ parameter IEs for ARQ-enabled connections

Parameters related to ARQ configuration are encoded in a compound attribute (Element ID = 17) as shown

in 464HTable 90, made up of subattributes described in 465H7.7.8.9.17.1 through 46H7.7.8.9.17.8.

7.7.8.9.17.1 ARQ Enable

7.7.8.9.17.2 ARQ\_WINDOW\_SIZE

7.7.8.9.17.3 ARQ\_RETRY\_TIMEOUT

7.7.8.9.17.4 ARQ\_BLOCK\_LIFETIME

7.7.8.9.17.5 ARQ\_SYNC\_LOSS\_TIMEOUT

7.7.8.9.17.6 ARQ\_DELIVER\_IN\_ORDER

7.7.8.9.17.7 ARQ\_RX\_PURGE\_TIMEOUT

7.7.8.9.17.8 ARQ\_BLOCK\_SIZE

7.7.11 CPE Basic Capability Request/Response (CBC-REQ/RSP)

The motivation of basic capability negotiation is to facilitate effective communication between the BS and

the CPE during the reminder of the initialization protocols, e.g., key exchange, registration. The following

shows the CBC-REQ and CBC-RSP message formats, along with their information elements and the

physical parameters involved.

7.7.11.1 CBC-REQ

The CPE CBC-REQ shall be transmitted by the CPE during initialization. A CPE shall generate CBC-REQ

messages in the form shown in 490HTable 105. Basic Capability Requests contain those CPE capabilities IEs

that are necessary for effective communication with the CPE during the remainder of the initialization

protocols. Only the following parameters shall be included in the Basic Capabilities Request (see 491H7.14.2.9),

namely the Physical Parameters Supported and the Bandwidth Allocation Supported. Capabilities for

Construction and Transmission of MAC PDUs may be supported if needed.

7.7.11.2 CBC-RSP

The CPE CBC-RSP shall be transmitted by the BS in response to a received CBC-REQ. The following

parameters shall be included in the CBC-RSP if found in the CPE CBC-REQ, namely the Physical

Parameters Supported (494H7.7.11.3.2) and the Capabilities for Construction and Transmission of MAC PDUs

(495H7.7.11.3.1). In addition, the BS responds to the subset of CPE capabilities present in the CBC-REQ

message. The BS responds to the CPE capabilities to indicate whether they may be used. If the BS does not

recognize a CPE capability, it may return this as “off” in the CBC-RSP. Only capabilities set to “on” in the

CBC-REQ may be set “on” in the CBC-RSP, as this is the handshake indicating that they have been

successfully negotiated.

7.7.11.3 CBC-REQ/RSP information elements

The information elements include the following:

1) Capabilities for construction and transmission of MAC PDUs (see 49HTable 107)

2) Physical parameters supported (see 50HTable 108 , 501HTable 109, and 502HTable 110)

7.7.12 De/Re-Register Command (DREG-CMD)

The DREG-CMD message shall be transmitted by the BS on a CPE’s Basic or Primary Management FID to

force the CPE to change its access state. The BS may transmit the DREG-CMD unsolicited or in response

to a CPE DREG-REQ message. Upon receiving a DREG-CMD, the CPE shall take the action indicated by

the action code.

7.7.13 CPE De-Registration Request (DREG-REQ)

A CPE may send a DREG-REQ message to a BS in order to notify the BS of CPE de-registration from

Normal Operation service from the BS. The MAC Management Message Type for this message is given in

512HTable 19. The format of the message is shown in 513HTable 116.

7.7.11.3 CBC-REQ/RSP information elements

The information elements include the following:

1) Capabilities for construction and transmission of MAC PDUs (see 49HTable 107)

2) Physical parameters supported (see 50HTable 108 , 501HTable 109, and 502HTable 110)

7.7.11.3.1 Capabilities for of MAC PDUs

Bit 0: Ability to receive requests piggybacked

7.7.11.3.2 Physical parameters supported

7.7.11.3.2.1 Maximum CPE Transmit EIRP

The Maximum CPE Transmit EIRP information element indicates the maximum EIRP achievable at the

CPE for the transmission of a full multiplex (60 subchannels) while still meeting the required RF mask (see

503H9.13) or other performance limits set by the manufacturer. The maximum EIRP parameters are reported in

dBm and quantized in 0.5 dB steps ranging from –64 dBm (encoded 0x00) to 63.5 dBm (encoded 0xFF).

Values outside this range shall be assigned the closest extreme. The EIRP accuracy shall be Å}1.5 dB when

the level is at least 10 dB below the maximum regulatory power limit and Å}0.5 dB elsewhere.

7.7.12 De/Re-Register Command (DREG-CMD)

The DREG-CMD message shall be transmitted by the BS on a CPE’s Basic or Primary Management FID to

force the CPE to change its access state. The BS may transmit the DREG-CMD unsolicited or in response

to a CPE DREG-REQ message. Upon receiving a DREG-CMD, the CPE shall take the action indicated by

the action code.

7.7.13 CPE De-Registration Request (DREG-REQ)

A CPE may send a DREG-REQ message to a BS in order to notify the BS of CPE de-registration from

Normal Operation service from the BS. The MAC Management Message Type for this message is given in

7.7.18 Measurements management

This subclause presents the mandatory measurements management component of the MAC, which is a

critical component for many features of the protocol including incumbent system protection.11

The BS can transmit the Bulk Measurement request (BLM-REQ) management message (see 530H7.7.18.1) via

unicast, multicast, or broadcast to one or multiple CPEs. This message contains instructions on the type of

measurements to be performed, when to perform it, the measurement duration, which channels to be

measured, and so on. Since the correct receipt of these management messages may be critical to the correct

system behavior (especially for in-band measurements—see 531H7.19.1), the BS may require CPEs to

acknowledge the receipt of BLM-REQ messages. This is done through Bulk Measurement response (BLMRSP) messages, and these are covered in 532H7.7.18.2. Next, 7.7.18.353H deals with Bulk Measurement report (BLM-REP) messages that, as the name suggests, allows CPEs to report back to the BS all the

measurement data they have collected as per requested by the BS in the corresponding BLM-REQ

message.

7.7.18.1 Bulk Measurement request (BLM-REQ)

534HTable 125 illustrates the format of a BLM-REQ message. BLM-REQ messages can contain a multitude of

single measurement messages (see 535HTable 127). Each of these single measurement requests can be

associated with a different type of measurement.

7.7.18.1.1 Single measurement request

538HTable 127 gives the format of single measurement requests, which are carried in the body of BLM-REQ

management messages. These single measurement requests shall be of various types as shown in 539HTable

131. Also, as seen from 540HTable 127, various timing parameters are associated with measurement requests.

541HFigure 16 depicts how these parameters are related to a measurement activity (the Randomization Interval

and Duration parameters are introduced in the next subclauses).

~~7.7.18.1.1.2 Beacon Measurement Request~~

7.7.18.1.1.1 Signal-Specific Measurement Request

This refers to a particular incumbent signal specific measurement. Incumbent detection thresholds are

specified during the registration procedure (see 57H7.7.7.3.4.7).

7.7.18.1.1.3 Measurement Stop Request

7.7.18.1.1.4 Status of CPE out-of-band sensing results

7.7.18.1.1.5 Location Configuration Measurement Request

~~7.7.18.1.1.6 Measurement request for frequency response of active OFDM subcarriers at the CPE~~

7.7.18.1.1.7 Silent period channel FFT output measurement request

7.7.18.2 Bulk Measurement response (BLM-RSP)

A BLM-RSP management message (shown in 567HTable 140) is sent in response to a BLM-REQ and serves to

confirm the receipt of the BLM-REQ message by the CPE. The need to send a BLM-RSP message is

indicated by the BS in the corresponding BLM-REQ message, through the use of the Confirmation Needed

field.

7.7.18.3 Bulk Measurement report (BLM-REP)

A BLM-REP management message (see 569HTable 141) is sent from a CPE to a BS, and contains the

measurement data collected by the CPE as per requested by the BS in a preceding BLM-REQ message.

Unsolicited BLM-REP management messages can also be sent from a CPE to a BS for the purpose of

signaling backup channels that are no longer available.

7.7.18.3.1 Single Measurement Report

7.7.18.3.1.1 Signal-Specific Measurement Report

~~7.7.18.3.1.2 Beacon Measurement report~~

~~A Beacon Measurement report (see 594HTable 146) is sent from a CPE to its corresponding BS, and conveys~~

~~information about one single overhead SCH (transmitted by other BSs) and/or CBP packet (transmitted by~~

~~other CPEs).~~

~~7.7.18.3.1.3 Unavailable Backup Channel~~

7.7.18.3.1.4 Backup channel list clearance depth

7.7.18.3.1.5 Backup/candidate channel list clearance depth

7.7.18.3.1.6 Status of CPE out-of-band sensing results

7.7.18.3.1.7 Location Data report

A Location Data report (see 610H Table 151), includes a string of location data that the CPE has obtained from

satellite. The report format shall be as described in NMEA 0183, and the length shall be the length of the

NMEA 0183 ASCII string plus 3 octets.

7.7.18.3.1.9 Consolidated Spectrum Occupancy Measurement report

A Consolidated Spectrum Occupancy Measurement report (see 618HTable 153) is sent from a CPE to its

corresponding BS, and conveys a brief summary about the overall spectrum occupancy from the viewpoint

of the CPE.

7.7.18.3.1.11 Silent period FFT output measurement report

A channel FFT output measurement report for the OFDM subcarriers during a silent period (see 62HTable 155)

is sent from a CPE to its corresponding BS, and conveys the I&Q values of each subcarrier representing the

state of interference and noise in the transmission channel from the viewpoint of the CPE. These values

represent the raw output of the FFT process done over one selected symbol at the CPE.

(can be used for raw I/Q scan reports)

7.7.18.4 Bulk Measurement Acknowledgement (BLM-ACK)

A BLM-ACK management message (shown in 624HTable 156) shall be sent from the BS to the CPE in response to a received BLM-REP. It serves to confirm to the CPE the reception of the BLM-REP message by the BS.

7.7.19 Config File TFTP Complete (TFTP-CPLT)

The Config File TFTP-CPLT message shall be generated by the CPE whenever it has successfully retrieved

its configuration file from the provisioning server (see 626H7.14). If the CPE does not need a config file, it shall

send the TFTP-CPLT message to the BS anyway to indicate that it has completed secondary management

connection initialization and is ready to accept services. The format of the TFTP-CPLT shall be as shown

in 627HTable 157.

7.7.20 Config File TFTP Complete Response (TFTP-RSP)

The Config File TFTP-RSP message shall be generated by the BS in response to a TFTP-CPLT message

from the CPE (see 628H7.14). The format of the TFTP-RSP shall be as shown in 629HTable 158.

7.7.21 Security Control Management (SCM) messages (SCM-REQ/RSP)

SCM employs two MAC message types: SCM Request (SCM-REQ) and SCM Response (SCM-RSP), as

described in 630HTable 159.

These MAC management message types distinguish between SCM requests (CPE-to-BS) and SCM

responses (BS-to-CPE). Each message encapsulates one SCM message in the Management Message

Payload.

SCM protocol messages transmitted from the CPE to the BS shall use the form shown in Table 160. They

are transmitted on the CPEs Primary Management Connection.

7.7.21.1 SCM EAP Start

SCM EAP Start shall be used during network entry to initiate an EAP session. The BS shall be capable of

initiating an EAP session with EAP Start if the network authenticator does not. The “Key Sequence

Number” attribute shall only be present in EAP Start messages transmitted during reauthentication. Note

that during reauthentication, the EAP Start message shall be protected by the MMP key.

7.7.21.2 SCM EAP Transfer

EAP Transfer shall be used when an EAP payload has to be transferred between the CPE and the network

authenticator (through the BS). The EAP Payload attribute shall be present in all EAP Transfer messages.

The “Key Sequence Number” attribute shall only be present in EAP Transfer messages during

reauthentication. Note that during reauthentication, the EAP Start message shall be protected by the MMP

key.

7.7.21.3 SCM Key-Request

A CPE sends a SCM Key-Request message to the BS to request new TEK and TEK-related parameters or

GTEK and GTEK-related parameters for the multicast or broadcast service.

Once a CPE has completed authentication, it has keying material (MMP\_KEY) that can be used to sign

and/or encrypt further MAC management messages. If SCM Key-Request is only to be signed, then CPE

will use MMP\_KEY derived from the AK identified by AK Sequence Number in Key-Request will be used

to generate the Ciphertext ICV (see 637H 8.4.2.1.2). If SCM Key-Request is to be encrypted, then CPE will use

the MMP\_KEY derived from the most current of its AKs to generate the Ciphertext ICV and encrypt the

message (see 638H 8.4.2.1.3).

7.7.21.4 SCM Key-Reply

The BS responds to a CPE’s SCM Key -Request message with a SCM Key-Reply message.

The GKEK-Parameters attribute is a compound attribute containing all of the GKEK-related parameters

corresponding to a GSAID. This would include the GKEK, the GKEK’s remaining key lifetime, and the

GKEK’s key sequence number.

Once the AAA has completed authentication with a particular CPE, both the CPE and BS have keying

material (MMP\_KEY) that can be used to sign and/or encrypt further MAC management messages. If SCM

Key-Reply is only to be signed, then BS will use MMP\_KEY derived from the AK identified by AK

Sequence Number in Key-Reply will be used to generate the Ciphertext ICV (see 639H 8.4.2.1.2). If SCM Key-

Reply is to be encrypted, then BS will use the MMP\_KEY derived from the most current of its AK’ s to

generate the Ciphertext ICV and encrypt the message (see 640H 8.4.2.1.3).

GKEK parameters shall only be included in Key-Reply message, when responding to Key-Request that is

conducted immediately after completion of Authentication exchange. To update GKEK parameters for an

existing GSA, the BS shall add new GKEK parameters to the list of SA descriptors in an SA Add message.

7.7.21.5 SCM Key-Reject

The BS responds to a CPE’s SCM Key -Request message with a SCM Key-Reject message if the BS rejects the CPE’s traffic keying material request.

Confirmation code is set to 0x0E when the Key Request was made for a SA for which the CPE is not

currently authorized. Confirmation code is set to 0x0B when the Key Request message cannot be properly

authenticated and decrypted.

Once a BS has completed authorization with a particular CPE, both have keying material (MMP\_KEY) that

can be used to sign and/or encrypt further MAC management messages. If SCM Key-Reject is only to be

signed, then BS will use MMP\_KEY derived from the AK identified by AK Sequence Number in Key-

Reject will be used to generate the Ciphertext ICV (see 642H 8.4.2.1.2). If SCM Key-Reject is to be encrypted,

then BS will use the MMP\_KEY derived from the most current of its AK’ s to generate the Ciphertext ICV

and encrypt the message (see 643H 8.4.2.1.3).

7.7.21.6 SCM GSA-Add

This message is sent by the BS to the CPE to establish one or more additional GSAs, after completion of

the Authentication exchange. BS shall use this method to update material (e.g., GKEKs and associated

parameters) for existing GSAs.

Once the AAA has completed authentication with a particular CPE, both the CPE and BS have keying

material (MMP\_KEY) that can be used to sign and/or encrypt further MAC management messages. If SCM

GSA-Add is only to be signed, then BS will use MMP\_KEY derived from the AK identified by AK

Sequence Number in GSA-Add will be used to generate the Ciphertext ICV (see 646H 8.4.2.1.2). If SCM GSAAdd is to be encrypted, then BS will use the MMP\_KEY derived from the most current of its AKs to

generate the Ciphertext ICV and encrypt the message (see 647H 8.4.2.1.3). The format of the GSA Descriptor is

described in 8.2.7.

7.7.21.7 SCM GSA-Remove

This message is sent by the BS to the CPE to remove one or more additional GSAs. This message shall

only be transmitted to CPEs after the BS has removed those CPEs from the multicast group to which the

GSA was applied.

7.7.21.8 SCM TEK-Invalid

The BS sends a SCM TEK-Invalid message to a client CPE if the BS determines that the CPE encrypted an

upstream PDU with an invalid TEK (i.e., an SAID’s TEK key sequence number), contained within the

received packet’s MAC header, is out of the BS’s range of known, valid sequence numbers for that SAID.

Message Response Code is set to 0x02 when sending TEK Invalid message.

Once the AAA has completed authentication with a particular CPE, both the CPE and BS have keying

material (MMP\_KEY) that is used to sign and encrypt further MAC management messages. The SCM

TEK-Invalid is to be encrypted, so the BS shall use the MMP\_KEY derived from the most current of its

AKs to generate the Ciphertext ICV and encrypt the message (see 650H 8.4.2.1.3).

7.21 Quiet periods and sensing

In order to meet the Channel Detection Time for detecting the presence of incumbents in the operating

channel, an IEEE 802.22 network shall schedule network-wide quiet periods for sensing. During these quiet

periods, all network traffic is suspended and base stations and CPEs shall perform in-band sensing. This

process is coordinated by the BS, which is responsible for scheduling the quiet periods….etc.etc

Probably not relevant as it mostly describes inter-frame and quiet time sensing characteristics for .22.

7.23 Synchronization of the IEEE 802.22 base stations

The BSs shall synchronize the absolute local start time of their superframe period, to the start of every

minute referenced to UTC to a tolerance of less than or equal to Å}2 μs.

All base stations shall use a common clock derived from a global navigational systems such as GPS to

synchronize their MAC frames. Every BS upon activation will, as a first step, derive its system clock based

on this common clock.

Every base station shall be equipped with a global navigational system receiver capable of receiving a UTC

synchronized 1 pps timing signal. The accuracy of the clock pulses derived from the global navigational

system are accurate to Å} 100 ns and the pulses that are derived typically have rise times within Å} 2.5 ns.

Although the IEEE 802.22 specification requires the presence of a GPS receiver, other techniques (e.g.,

IEEE Std 1588-2008 [B13]) may be considered as long as they meet the required tolerance.

(use for synchronizing Back end Management systems, SSDs)

9.12 Antenna

9.12.1.2 Sensing antenna reference pattern

The gain of the sensing antenna in the horizontal azimuthal plane shall be equivalent to an omni-directional

antenna. The deviation from this nominal gain shall be no worse than –1 dB. Such maximum deviation

from this nominal gain should be kept over Å}20 degrees in the vertical pattern in all azimuths.

9.12.2 Antenna interface

9.12.2.1 TRU/AU physical interface

The IEEE 802.22 BS and CPE may be implemented as separate TRUs and AUs or integrated into a single

unit. In the case where they are separate units, the TRU and the AU shall have a coaxial interface to convey

the radio signals to be transmitted and received by the antenna as well as ancillary signals to be transferred

between the TRU and AU such as data, clock and power supply.

An integrated unit is defined as one where removal or disconnection of the RF antenna or GPS antenna

shall only be possible through tampering with the unit in such a way as to trigger the tamper proof

mechanisms (see Clause 1426H11). Any other implementation will result in separate CPE and AUs to which the

following specification shall apply.

~~When implemented as separate units, interfaces shall exist on both the AU and the TRU. The transceiver~~

~~unit shall be connected to the AU via a 50-ohm coaxial cable. The AU shall consist of the antenna and,~~

~~where required, the integrated GPS receiver. The TRU interface shall be a female “N” type connector. The~~

~~AU interface shall be a female “N” type connector. The coaxial cable shall have a male Standard or~~

~~Corrugated type “N” connector at both the TRU and the AU ends. The length of the coaxial cable shall be~~

~~less than 50 meters for cables fitted with Standard type “N” connectors and be less than 250 meters for~~

~~cables fitted with corrugated type “N” connectors. These connectors shall comply with MIL-PRF-39012E~~

~~with Amendment 1 and MIL-STD-348. 1427HTable 229 summarizes the technical requirements for the “N”~~

~~connectors and 1428HFigure 159 illustrates typical TRU and AU interfaces and the coaxial cable linking them.~~

Would make things very complicated to have separate TRU/AU units.

9.12.2.3 AU antenna information mapping

1432HTable 230 presents the mapping of the information to be stored at the AU. It is defined by segments that

contain the type of information (3 octets), the length of the segment (1 octet), and the information, followed

by a CRC-16 to protect the information contained in the segment during transmission.

Each data segment shall begin with a 3 ASCII characters long code contained in the following 3 octets:

\_ MDL: Antenna model segment. These 3 first octets are followed by one octet indicating the length of

data to follow before the closing 2 CRC octets. The data shall contain the antenna model and serial

number stored in a character string assigned by the AU manufacturer.

\_ USA, GBR, etc.: Regulatory domain ISO 3166 [B44] code included as the first 3 octets followed by

one octet indicating the length of data to follow before the closing 2 CRC octets. The data portion shall

contain one octet per channel indicating the on-axis gain of the antenna at the center frequency. The

channels correspond to those listed in 134H Annex A and are ordered the same way as shown in 1434H134H Annex A

(see Table A.171435H for the USA and Table A.18 1437H for European countries). Additional segments can be

added for further regulatory domains up to 2k octets.

\_ Gainn : Maximum on-axis antenna gain in the specific channel in 0.25 dB units ranging from – 22.0 dBi

(0x01) to 41.0 dBi (0xFD). Code 0x00 shall be assigned to channels for which the antenna is not

intended to be used. Code 0x01 shall also be used for antenna gain smaller than – 22.0 dBi. Code 0xFE

shall be used for antenna gain higher than 41.0 dBi. Code 0xFF is not allowed. (See 1439H Table 58,

140H 7.7.7.3.4.9).

9.14 Receiver requirements

9.14.1 Receiver minimum sensitivity

The receiver minimum sensitivity level, RSS, is defined as the minimum power, measured at the antenna

port, at which the bit error rate performance is equal to the required limit. The equation is given as follows:

RSS (dBm) = Reference Thermal Noise Density Level

+ Noise Figure

+ Effective Channel Bandwidth

+ Required Signal-to-Noise Ratio

+ Receiver Implementation Margin

+ Interference Allowance

where

Reference Thermal Noise Density Level = Boltzman Constant + 10Å~log(Reference Noise Temperature)

with Boltzman Constant = –138.6 dB(mW/(K Å~ MHz)) and Reference Noise Temperature = 290 K

(degrees Kelvin)

Noise Figure = 3 dB for the base station and 6 dB for the CPE

Effective Channel Bandwidth = 10 log (Signal Bandwidth (MHz) ) with Signal Bandwidth values as in

14HTable 201)

Required Signal-to-Noise Ratio = the Reference Normalized SNR as shown in 145HTable 228 for a BER

performance of 2Å~10–4 where the values include 1.1 dB, 1.3 dB, and 1.5 dB decoder implementation

margins for QPSK, 16-QAM, and 64-QAM modulations respectively

Receiver Implementation Margin = 1.9 dB and 2.1 dB for BS and CPE respectively, accounting for the

coupling loss, pre-amplification filter loss, assuming that a low-noise pre-amplifier is located at the

antenna

Interference Allowance = 1 dB for either BS or CPE to cover for the impact of local interference at the

receiver

The base station and CPE minimum receiver sensitivity for the three channel bandwidths shall at least meet

the values given in 146HTable 231.

9.14.2 Receiver selectivity

The receiver selectivity is a measure of the ability of the receiver to reject signals from adjacent channels,

while receiving a wanted signal on the selected frequency. It is defined as the ratio of the selected channel

signal power to the power of the signal in the adjacent channel, subject to the target BER of 2Å~10–4.

For IEEE 802.22 WRAN systems, the minimum receiver selectivity shall be

D/Uadj = 50.7 dB for the most robust modulation: QPSK, rate: 1/2

corresponding to the 55 dBr (72.5 dBc) rejection in the first adjacent channel of a transmitted WRAN

signal (consistent with what is specified in the FCC R&O 08-260).

9.14.3 Receiver tolerance to interference overload

The receiver tolerance to interference overload (also known as the receiver blocking level or maximum

input level) refers to the effect of strong RF signals in channels other than the channel of interest and its

two adjacent channels on the ability of the receiver to decode a wanted signal in the selected channel.

The receiver tolerance to interference overload (i.e., maximum input level) for both the base station and

CPE shall be – 8 dBm.

10. Cognitive radio capability

10.1 General

This clause describes the cognitive radio capabilities supported by IEEE Std 802.22, which are required to

meet regulatory requirements for protection of incumbents as well as to provide for efficient operation of

IEEE 802.22 networks. The cognitive radio capabilities include: BS’s SM, Spectrum Sensing Automaton

(SSA), Access to the database services, Channel set management, Policy (147HTable 234 and 141HAnnex A), CPE

Registration and Tracking, Spectrum Sensing services, and Geolocation services.

(most of this section is not strictly relevant as state machines, etc are used in the context of a CPE/BS configuration to determine allowed channels of operation)

10.4 Spectrum sensing

Spectrum sensing is the process of observing the RF spectrum of a television channel to determine its

occupancy (by either incumbents or other WRANs).

The base station and all CPEs shall implement the Spectrum Sensing Function (SSF).

The SSF shall be driven by the SSA. The SSF shall observe the RF spectrum of a television channel and

shall report the results of that observation to the SM (at the BS) via its associated SSA. The Spectrum

Sensing Function (SSF) is described in 1585H10.4.1. The primitives for the SSF are described in 1586H10.7.

10.4.1 Spectrum Sensing Function (SSF)

The Spectrum Sensing Function observes the RF spectrum of a television channel for a set of signal types

and reports the results of this observation. The spectrum sensing function is implemented in both the base

station and the CPEs. There are MAC management frames that allow the base station to control the

operation of the spectrum sensing function within each of the CPEs. 1587HFigure 183 illustrates the inputs and

outputs of the spectrum sensing function.

The inputs to the spectrum sensing function come from the SM via SSA. The inputs to the spectrum

sensing function are described in 10.4.1.1. The outputs from the spectrum sensing function are returned to

the SM via SSA. The outputs of the spectrum sensing function are described in 1589H10.4.1.2. The behavior of

the spectrum sensing function is described in 10.4.1.3.

Some of the possible sensing techniques that can be used to realize the spectrum sensing function are

described in 1591H141HAnnex C. The use of any specific sensing technique is optional, as long as the inputs, outputs and behavior meet the specification of this subclause.

10.4.1.1 SSF inputs

A summary of the spectrum sensing inputs is given in 1592HTable 236.

The RF input is connected via an RF stage to the WRAN sensing antenna.

The ISO 3166 country code defines the regulatory domain of operation. For example, the ISO 3166 country

code ‘US A’ corresponds to the regulatory domain of the United States of America.

The channel number is the relative television channel number that the SSF is to sense. The center frequency

for each channel number and the exact mapping between the relative channel number and the absolute

channel number are given in 1596H141H Annex A.

The channel bandwidth is the bandwidth of the television channel that the SSF is to sense.

The signal type array (STA) indicates which signal types that are to be sensed for by the SSF. The array is a

one-dimensional array of length STALength , indexed from 0 to STALength – 1. The STA is a binary array

whose elements are either zero or 1. The ith element in the array specifies whether the SSF is to sense for ith

signal type. The mapping of STA index to signal type is given in 1597H Table 237.

The value of STALength is 32 and can be represented using 4 octets.

A one in index zero of the STA indicates sensing for any signal type, with no distinction between signal

types. A one in index one of the STA indicates the SSF should sense for an IEEE 802.22 WRAN.

As an example, if the STA is given as follows:

STA= (0010111000000000…00)

Then the SSF shall sense for an IEEE 802.22.1 Sync Burst, an ATSC signal, and NTSC signal and a

wireless microphone. Table A.11 specifies that, depending upon the regulatory domain of operation, some

STA indices in the STA shall be set at all times.

The sensing window specification array (SWSA) is a two-dimensional array of length STA Length NÅ~32.

Each row of the SWSA is a sensing window specification (SWS). If the ith element of the STA is one (1)

then the ith row of the SWSA shall be set to a valid sensing window specification. If the ith row of the STA

is set to zero (0) then the ith row of the SWSA does not need to be set to a valid SWS since it will be

ignored by the SSF.

A sensing window specification (SWS) consists of three parameters. These three parameters specify the

window of time over which the SSF shall sense for specified signal type. 159H Figure 184 illustrates a sensing

window.

A sensing window consists of NumSensingPeriods number of sensing periods. The minimum number of

sensing periods is one and the maximum number is 255. This maximum number is based on the need to

avoid that a rogue BS could bring down other co-existing co-channel BSs in the area by excessive

scheduling of quiet periods.

Each sensing period is of duration SensingPeriodDuration symbols and adjacent sensing periods are

separated by SensingPeriodInterval symbols as shown in 160H Figure 184.

The parameters in a sensing window specification are given in 1601H Table 238. Such sensing window can

occupy a portion of a quiet period, an entire quiet period or multiple quiet periods.

The details on how quiet periods are scheduled are found in 1602H 7.5.1.

(a lot of this section is designed to detect free channels in a White Space implementation, and need to be broadened)

10.4.1.2 SSF outputs, etc

(Designed for classification of candidate channels in TVWS implementation)

10.5 Geolocation

Two modes of geolocation can be used with IEEE Std 802.22. Satellite-based geolocation is mandatory.

Terrestrial-based geolocation assisted by the CDMA ranging, superframe preamble, frame preamble and

the coexistence beacon protocol is also described in the paragraphs that follow. The geolocation technology

shall detect if any device in the network moves by a distance greater than the values specified in 1635HTable A.9

in 1636HAnnex A. In such case, the BS and CPE shall follow the local regulations and shall obtain the new list of

available channels from the database service based on the new location of the device.

10.5.1 Satellite-based Geolocation

The BS shall use its satellite-based geolocation capability to determine the latitude and longitude of its

transmitting antenna within a radius of 50 m. The BS may also use the altitude information derived from

the satellite-based geolocation capability.27

Each CPE shall use its satellite-based geolocation technology to determine the latitude and longitude of its

antenna within a radius of 50 m. Each CPE may also use its altitude above mean sea level. Each CPE shall

provide its geolocation coordinates using the NMEA strings to the BS during the registration process. The

WRAN system shall use the NMEA strings provided by each CPE’s satellite-based geolocation subsystem

to determine the location of the CPEs.

The satellite-based geolocation antenna shall be co-located (i.e., ≤ 1 m separation) with the transmit and

sensing antennas.

Lock to satellite-based geolocation system is not necessary to continue operation. However, the device

shall cease operation if T30 expires after losing the lock. If movement is detected, the CPE shall be deregistered via the DREG-CMD with code 0x01. CPE transmission can be re-enabled with the code 0x03 if new coordinates can be obtained. If new coordinates cannot be obtained, the CPE can be shut down by a

DREG-CMD with code 0x04 or be forced to reinitialize on the current operating channel via a DREGCMD

with code 0x05.

10.5.2 Terrestrial Geolocation

Allows for devices to define location in terms of previously located devices… may complicate SSD standard

10.6 Database service

10.6.1 System model for the database access

The system model that has been assumed all along in the development of IEEE Std 802.22 is a point-tomultipoint

model for extending broadband access to less populated rural areas where more available

channels can be found. In this model, the base station (BS) is assumed to control all RF parameters of its

associated customer premises equipment (CPE) (frequency, EIRP, modulation, etc.) in a “master-slave”

relationship so that the responsibility of protecting the TV broadcast incumbents is fully carried by the

Wireless Regional Area Network (WRAN) operator. When this model was applied to an interface to the database service proposed in the FCC R&O 08-260, the initial finding made by the IEEE 802.22 Working

Group was that this interface is to take place entirely between the database service and the BS rather than

with its individual CPEs. The system architecture and interface to the database services that the IEEE

802.22 Working Group has developed is depicted in 1678H Figure 185.

10.6.2 Database service access

The BS will initially enlist with the database service as a fixed device.29 It will also enlist all its associated

CPEs with their geographic location, device identification, etc. as obtained at association on a real time

basis since its association may depend on the response from the database service. On an ongoing basis, the

BS will then query the database (at least once every 24 hours) using the M-DB-AVAILABLE-CHANNELREQUEST message so that it can retrieve the channel information. Furthermore, the database service could send any update relevant to the BS operation through ‘push’ internet technology since the network address of the base station is provided as part of the messages. Such ‘push’ technology would allow for a better reaction time than the 24 hours minimum access time currently specified while keeping the database traffic to a minimum.

10.6.3 Security for these messages

Security on the messages exchanged between the base station and the database service will be critical for

the proper operation of the systems to allow authentication of the database service provider as well as the

WRAN system querying the service. Security will also be necessary to avoid the message exchange being

altered on the backhaul connection. The network will only support SSL on the link between the database

service and the BS to provide transport layer security. The IEEE 802.22 network shall use the same

authentication protocols for device and database service authentication and for interacting with the database

(i.e., EAP-TLS or EAP-TTLS, see 1679H8.4.3) as those specified for device authentication in Clause 1680H8. All

database service primitives are exchanged between the CPE/BS and the database service via Attribute

Value Pairs of EAP messaging. The formatting of said messages shall conform to the authentication service

(e.g., RADIUS/RFC 2865 [B26] or DIAMETER/RFC 3588 [B1]) that the database service employs.

10.7 Primitives for cognitive radio capabilities

10.7.1 Database service primitives

The following list of messages, present in IEEE Std 802.22, defines the necessary messaging to support

access to the database service by the BS. The format described in 10.7.1.1 to 10.7.1.8 shall be used for the

messages sent directly to the database service as well as those received directly from the database service.

Some parameters in the following primitives are variable-length character strings. The length of these

parameters is given in terms of the number of characters in those strings. The total size of those parameters

is the number of characters (the length) multiplied by the size of each character. For ASCII character sets,

each character is 1 octet. For Unicode character sets, each character is 2 octets. Note that all variable-length

character strings shall be null terminated.

10.7.1.1 M-DB-AVAILABLE-REQUEST

10.7.1.2 M-DB-AVAILABLE-CONFIRM

10.7.1.3 M-DEVICE-ENLISTMENT-REQUEST

10.7.1.4 M-DEVICE-ENLISTMENT-CONFIRM

10.7.1.8 M-DB-DELIST-CONFIRM

10.7.4 Spectrum Sensing Services

The IEEE 802.22 PHY layer shall provide local spectrum sensing services through its SSF accessed

through the SM-SSF-SAP. 170HTable 261 summarizes the spectrum sensing primitives supported through the

SM-SSF-SAP interface. The primitives are discussed in the subclauses referenced in the table.

10.7.4.1 SM-SSF-SAP-CHANNEL-SENSING.request

The SM-SSF-SAP-CHANNEL-SENSING.request primitive allows the SM to request the local PHY SSF

unit to perform spectrum sensing. 1704HTable 262 specifies the parameters for the SM-SSF-SAP-CHANNELSENSING.request primitive.

10.7.4.1.1 When generated

The SM-SSF-SAP-CHANNEL-SENSING.request primitive is generated by the SM and issued to the SSF

to request the local PHY SSF to perform spectrum sensing.

10.7.4.1.2 Effect on receipt

When the SSF receives the SM-SSF-SAP-CHANNEL-SENSING.request primitive, it requests the local

PHY SSF to perform spectrum sensing.

On receipt of the SM-SSF-SAP-CHANNEL-SENSING.request the SSF shall issue a SM-SSF-SAPCHANNEL-SENSING.confirm primitive to the SM with a status value.

10.7.4.2 SM-SSF-SAP-CHANNEL-SENSING.confirm

The SM-SSF-SAP-CHANNEL-SENSING.confirm primitive is used to inform the SM whether its request

to the local PHY SSF was successfully generated by the SM. 1713H Table 263 specifies the parameters for the

SM-SSF-SAP-CHANNEL-SENSING.confirm primitive.

10.7.4.2.1 When generated

The SM-SSF-SAP-CHANNEL-SENSING.confirm primitive is generated by the SSF and issued to its SM

to indicate whether the received SM-SSF-SAP-CHANNEL-SENSING.request was valid and whether the

SSF is able to perform sensing for the signal types as requested. If the SSF is able to perform the sensing in

the requested sensing mode and with the requested probability of false alarm for all types of signals

requested, the Status code shall be set to SUCCESS. If the SSF does not support the requested sensing

mode, the status value should be INVALID\_REQUEST. If one or more of the signal types in the request is

not valid or the SSF does not have the capability to sensing a requested signal type, the status code should

be set to INVALID\_SIGNAL\_TYPE and the corresponding invalid signal types shall be indicated in the

Invalid Signal Type Array.

10.7.4.2.2 Effect on receipt

When the SM receives the SM-SSF-SAP-CHANNEL-SENSING.confirm primitive, it will identify whether

its request to the local PHY SSF was successfully received by the SSF. The status parameter indicates the

appropriate error code from 1718H7.7.24 in case the request is invalid.

10.7.4.3 SM-SSF-SAP-SENSING-RESULTS.indication

The SM-SSF-SAP-SENSING-RESULTS.indication primitive is used to inform the SM when the results of

a previously issued request to the local PHY SSF were successfully generated by the SSF. 1719HTable 264

specifies the parameters for the SM-SSF-SAP-SENSING-RESULTS.indication primitive.

10.7.4.3.1 When generated

The SM-SSF-SAP-SENSING-RESULTS.indication primitive is generated by the SSF and issued to the SM

to indicate the results of a previously issued request to the local PHY SSF have been generated.

10.7.4.3.2 Effect on receipt

When the SM receives the SM-SSF-SAP-SENSING-RESULTS.indication it will obtain the sensing results

to its request to the local PHY SSF.

10.7.5 Geolocation services

The PHY layer provides local geolocation services through its satellite-based location acquisition unit to

the SM/SSA through the SM-GL-SAP. 1727HTable 265 summarizes the geolocation primitives supported through

the SM-GL-SAP interface. The primitives are discussed in the subclauses referenced in the table.

10.7.5.1 SM-GL-SAP-GEOLOCATION.request

The SM-GL-SAP-GEOLOCATION.request primitive allows the SM to request the local PHY geolocation

unit to perform geolocation. 1731HTable 266 specifies the parameters for the SM-GL-SAPGEOLOCATION.

request primitive.

10.7.5.1.1 When generated

The SM-GL-SAP-GEOLOCATION.request primitive is generated by the SM and issued to its SSF to

request the local PHY geolocation service to perform geolocation.

10.7.5.1.2 Effect on receipt

When the Geolocation receives the SM-GL-SAP-GEOLOCATION.request primitive, it requests the local

PHY geolocation service to perform geolocation.

On receipt of the SM-GL-SAP-GEOLOCATION.request the Geolocation shall issue a SM-GL-SAPGEOLOCATION.

confirm primitive to the SM with a status value.

10.7.5.2 SM-GL-SAP-GEOLOCATION.confirm

The SM-GL-SAP-GEOLOCATION.confirm primitive is used to inform the SM whether its request to the

local PHY geolocation service was successfully generated by the Geolocation. 1732HTable 267 specifies the

parameters for the SM-GL-SAP-GEOLOCATION.confirm primitive.

10.7.5.2.1 When generated

The SM-GL-SAP-GEOLOCATION.confirm primitive is generated by the Geolocation and issued to its SM

to indicate whether the received SM-GL-SAP-GEOLOCATION.request was valid, in which case the

Geolocation acquires the requested NMEA sentence from the local PHY geolocation service.

10.7.5.2.2 Effect on receipt

When the SM receives the SM-GL-SAP-GEOLOCATION.confirm primitive, it will identify whether its

request to the local PHY geolocation service was successfully received by the Geolocation. The status

parameter indicates the appropriate error code from 173H7.7.24 in case the local PHY geolocation service was

not available.

10.7.5.3 SM-GL-SAP-GEOLOCATION-RESULTS.indication

The SM-GL-SAP-GEOLOCATION-RESULTS.indication primitive is used to inform the SM when a

response to a previously issued request to the local PHY geolocation service was successfully received by

the Geolocation. 1734HTable 268 specifies the parameters for the SM-GL-SAP-GEOLOCATIONRESULTS.

indication primitive.

10.7.5.3.1 When generated

The SM-GL-SAP-GEOLOCATION-RESULTS.indication primitive shall be generated by the Geolocation

and issued to the SM to indicate the reception of a response to a query previously issued to the local PHY

geolocation service.

10.7.5.3.2 Effect on receipt

When the SM receives the SM-GL-SAP-GEOLOCATION-RESULTS.indication it shall identify whether

the response to its request to the local PHY service was successfully received by the Geolocation, in which

case, the SM will obtain NMEA string containing the latitude and longitude information. If the response is

not successful the SM may decide to issue another request.

10.7.6 Antenna primitives

Essential antenna information is provided to the MAC by the antenna through the M-SAP. The M-SAP is

an interface that provides a means of exchanging information between the SM at the BS MAC and the SSA

at the CPE MAC and their respective antenna. 1735HTable 269 summarizes the primitives supported by the MAC to access antenna information through the M-SAP interface. The primitives are discussed in the subclauses referenced in the table.

(can use this to store antenna information – perhaps mandated that antenna is integrated)

10.7.6.1 M-ANTENNA-INTEGRATED.request

The M-ANTENNA-INTEGRATED.request primitive allows the MAC to identify whether the device’s

antenna is integrated or non-integrated through the M-SAP in order to know whether it is required to get

antenna gain information for calculation of EIRP. The M-ANTENNA-INTEGRATED.request primitive

has no attributes.

10.7.6.1.1 When generated

The M-ANTENNA-INTEGRATED.request primitive shall be generated by the MAC and issued to its

antenna to identify the whether its antenna is integrated or non-integrated.

10.7.6.1.2 Effect on receipt

When the antenna receives the M-ANTENNA-INTEGRATED.request primitive, the antenna shall generate

an M-ANTENNA-INTEGRATED.confirm primitive to indicate whether the antenna is integrated or nonintegrated.

10.7.6.2 M-ANTENNA-INTEGRATED.confirm

The M-ANTENNA-INTEGRATED.confirm primitive allows the antenna to inform the MAC whether it is

integrated or non-integrated through the M-SAP. 1740HTable 270 specifies the parameters for the MANTENNA-

INTEGRATED.confirm primitive.

10.7.6.2.1 When generated

The M-ANTENNA-INTEGRATED.confirm primitive shall be generated by the antenna and issued to its

MAC when an M-ANTENNA-INTEGRATED.request primitive is received to indicate whether the

antenna is integrated or non-integrated through the M-SAP.

10.7.6.2.2 Effect on receipt

When the MAC receives the M-ANTENNA-INTEGRATED.confirm primitive, the SM at the BS and the

SSA at the CPE shall identify whether the antenna is integrated or non-integrated.

10.7.6.3 M-ANTENNA-INFORMATION.request

The M-ANTENNA-INFORMATION.request primitive allows the MAC to request antenna information

from the antenna. The M-ANTENNA-INFORMATION.request primitive has no attributes.

10.7.6.3.1 When generated

The M-ANTENNA-INFORMATION.request primitive shall be generated by the SM of a BS or the SSA of

the CPE and issued to their respective antenna for antenna information.

10.7.6.3.2 Effect on receipt

When the antenna receives the M-ANTENNA-INFORMATION.request primitive, the antenna shall

generate an M-ANTENNA-INFORMATION.response containing information that describes the attributes

of the antenna.

10.7.6.4 M-ANTENNA-INFORMATION.response

The M-ANTENNA-INFORMATION.response primitive is used to respond to the MAC request with

antenna information. 1741HTable 271 specifies the parameters for the M-ANTENNA-INFORMATION.response

primitive.

10.7.6.4.1 When generated

The M-ANTENNA-INFORMATION.response primitive shall be generated by the antenna and issued to

the MAC to respond with information about the antenna.

10.7.6.4.2 Effect on receipt

When the MAC receives the M-ANTENNA-INFORMATION.response, MAC shall store the maximum

gain (dBi) for each channel so that the device can convert from transmit power to EIRP.

(this requires extensive development … far too primitive for 22.3 purposes)

11. Configuration

Tamper-proof mechanisms shall be implemented to prevent unauthorized modification to firmware and/or

functionalities (e.g., MAC address, SM/SSA functionality, database service communication, RF sensing,

DFS, TPC, tuning) that would allow device or network operation to violate either the specifications of

IEEE Std 802.22 or the requirements of the local regulations. Any attempt to load unapproved firmware

into an IEEE 802.22 device shall render it inoperable. Measures for both local and remote attestation of

authorized and approved hardware and software running on an IEEE 802.22 device shall be implemented.

Implementation of the Trusting Computing Group’s Trusted Platform Module (TPM) Main Specification

Level 2 Version 1.2 (Revision 103) [see TPM references in Clause 1742H2] shall be used to bind the hardware

and software running on IEEE 802.22 devices to a cryptographic key.

When a CPE detects that the information on the antenna model and serial number has changed (see 1743H9.12.2)

after a request from the BS for this information (REG-REQ/RSP, see 174H7.7.7.3.4.9), the CPE shall reinitialize.

12. Parameters and connection management

12.1 Parameters, timers, message IEs

This subclause defines bounds for various parameters, timers, and message/IE fields that are specified

throughout the standard.

13. MIB structure

The definition of managed objects in this standard is expressed in Structure of Management Information

Version 2 (SMIv2). It supports a management protocol agnostic approach, including SNMP.

The basic MIB objects are the following:

\_ wranDevMib: Basic MIB for BS/CPE device management. Can be used to track software versioning of

BS/CPE HW/SW and what SNMP traps can be configured on those devices

\_ wranIfBsMib: Basic MIB for BS-related MIB objects related to providing fixed AND portable service.

\_wranIfBsSfMgmtMib: Basic MIB for managing items related to Service Flow

configuration, instantiation, and management\_ wranIfCpeMib: Basic MIB for CPE-related MIB objects related to operation of fixed AND portable

CPEs

\_ wranIfSmMib: Basic MIB for SM related MIB objects

\_ wranIfSsaMib: Basic MIB for Spectrum Automaton related MIB objects

\_ wranIfDatabaseServiceMib: Basic MIB for Database Service access related MIB objects

(it is probably necessary to include MIB in standard – for discussion)

14 Management plane interfaces and procedures

14.1 Primitive format

In this clause, the components that make up each primitive are defined.

14.1.1 Purpose

Text describing the function that this primitive services.

14.1.2 SAP type

Type of SAP, either M-SAP or C-SAP, over which this primitive operates.

14.1.3 Operation type

Specification of the operation type of the primitive, i.e., what kind of transaction the primitive is executing.

The operation type can be one of the following:

 Information Request (REQUEST)

 Event Indication

 Information Confirmation (CONFIRM)

14.1.4 Destination

Entity that is receiving the primitive, e.g., BS, CPE, NCMS/AAA.

14.1.5 Data

A set of one for more information elements that carry information that is pertinent to the servicing of the

primitive. For each information element, data type and size of data are provided.

14.1.5.1 Handling timestamp fields in primitives

Primitives with data fields that represent a time value or timestamp shall be defined in terms of UTC time.

The format of the string is pulled from IETF RFC 3339. The following format shall be used: “YYYY-MMDDThh:

mm:ssZ”; where YYYY is the 4-digit year, MM is the 2-digit month (1..12), DD is the 2-digit day

(01..31), hh is the 2-digit hour (00..23), mm is the 2-digit minute (00..59), and ss is the 2-digit minute

(00..59).

14.2 Primitive definitions

Primitives for both SAPs are defined in this subclause. Definitions for Management SAP (M-SAP) and

Control SAP (C-SAP) primitives are provided for in 14.2.1 and 14.2.2, respectively. M-SAP primitives

cover system configuration, monitoring statistics, notifications/triggers, sensing/geolocation reporting, and

communication with the database service. C-SAP primitives cover CPE management, session management,

security context management, radio resource management, and AAA service signaling.

(a huge amount that can be borrowed in device config (DHCP, etc)

14.2.1 Management SAP (M-SAP)

14.2.1.1 Accounting management primitives

Accounting management pertains to monitoring and managing information regarding CPE data

transmission usage. Accounting records are updated whenever a CPE starts registration (REG-REQ) upon

entry, is provisioned/configured for a new service flow (DSA-REQ/RSP), has a service flow configuration

altered (DSC-REQ/RSP), and/or requests de-registration (DREG-REQ).

There are three accounting management primitives: M-ACCOUNTING-REQUEST, M-ACCOUNTINGCONFIRMATION, and M-ACCOUNTING-INDICATION.

14.2.1.2 Internet Protocol (IP) management primitives

IP management pertains to executing primitives related to establishing IP connections using the secondary

management connection during CPE initialization (see 7.14.2.13).

There are four IP management primitives: M-DHCP-DISCOVER-REQUEST, M-DHCP-OFFERCONFIRMATION, M-DHCP-SETUP-REQUEST, and M-DHCP-SETUP-CONFIRMATION.

14.2.1.3 Database service primitives

The following list of messages, present in the IEEE Std 802.22, defines the necessary messaging to support

access to the database service by the BS. The format described in the following subclauses shall be used

for the messages sent directly to the database service as well as those received directly from the database

service. Some parameters in the following primitives are variable-length character strings. The length of

these parameters is given in terms of the number of characters in those strings. The total size of those

parameters is the number of characters (the length) multiplied by the size of each character. For ASCII

character sets, each character is 1 octet. For Unicode character sets, each character is 2 octets. Note that all

variable-length character strings shall be null terminated.

14.2.1.4 BS configuration and monitoring primitives

The BS SM occasionally sends the available channel list to its higher layers for additional channel

classification. The available channel list can be presented to its higher layers to have channels classified as

disallowed. The classification of an operating channel by the BS is also performed by its higher layers.

The M-SAP is an interface that provides a means of exchanging information between the SM and the

higher layers in the BS. Table 299 summarizes the primitives supported by the SM to pass the available

channel list and to receive disallowed channel classifications and the selected operating channel through the

M-SAP interface. The primitives are discussed in the subclauses referenced in the table.

(very TVWS centric… channel management primitives)

~~14.2.1.5.1 M-WRAN-SERVICE-REPORT-REQUEST~~

~~14.2.1.5.1.1 Purpose~~

~~The M-WRAN-SERVICE-REPORT-REQUEST primitive is sent by the CPE SA to request the higher~~

~~layers for a selection of a WRAN service based on the available WRAN service list information provided~~

~~this primitive. Table 305 specifies the parameters for the M-WRAN-SERVICE-REPORT-REQUEST~~

~~primitive.~~

14.2.1.6 Antenna primitives

Essential antenna information is provided to the MAC by the antenna through the M-SAP. The M-SAP is

an interface that provides a means of exchanging information between the SM at the BS MAC and the SSA

at the CPE MAC and their respective antenna. Table 308 summarizes the primitives supported by the MAC

to access antenna information through the M-SAP interface. The primitives are discussed in the subclauses

referenced in the table.

Table 308—Available WRAN services list primitives supported by the M-SAP

Name Request Indication Confirm

M-ANTENNA-INTEGRATED 14.2.1.6.1 14.2.1.6.2

M-ANTENNA-INFOMRATION 14.2.1.6.3 14.2.1.6.4

14.2.1.6.1 M-ANTENNA-INTEGRATED-REQUEST

14.2.1.6.1.1 Purpose

The M-ANTENNA-INTEGRATED-REQUEST primitive allows the MAC to identify whether the device’s

antenna is integrated or non-integrated through the M-SAP in order to know whether it is required to get

antenna gain information for calculation of EIRP. The M-ANTENNA-INTEGRATED-REQUEST

primitive has no attributes.

14.2.1.6.1.2 SAP type

M-SAP

14.2.1.6.1.3 Operation type

Information Request

14.2.1.6.1.4 Destination

Antenna Interface (see 9.12.2)

14.2.1.6.1.5 Data

There are no attributes for this primitive.

14.2.1.6.1.6 When generated

The M-ANTENNA-INTEGRATED-REQUEST primitive shall be generated by the MAC and issued to its

antenna to identify whether its antenna is integrated or non-integrated.

14.2.1.6.1.7 Effect of receipt

When the antenna receives the M-ANTENNA-INTEGRATED-REQUEST primitive, the antenna shall

generate an M-ANTENNA-INTEGRATED-CONFIRMATION primitive to indicate whether the antenna is

integrated or non-integrated.

14.2.1.6.2 M-ANTENNA-INTEGRATED-CONFIRMATION

14.2.1.6.2.1 Purpose

The M-ANTENNA-INTEGRATED-CONFIRMATION primitive allows the antenna to inform the MAC

whether it is integrated or non-integrated through the M-SAP. Table 309 specifies the parameters for the

M-ANTENNA-INTEGRATED-CONFIRMATION primitive.

14.2.1.6.2.2 SAP type

M-SAP

14.2.1.6.2.3 Operation type

Information Confirmation

14.2.1.6.2.4 Destination

CPE, BS

14.2.1.6.2.5 Data

14.2.1.6.2.6 When generated

The M-ANTENNA-INTEGRATED-CONFIRMATION primitive shall be generated by the antenna and

issued to its MAC when an M-ANTENNA-INTEGRATED-REQUEST primitive is received to indicate

whether the antenna is integrated or non-integrated through the M-SAP.

14.2.1.6.2.7 Effect of receipt

When the MAC receives the M-ANTENNA-INTEGRATED-CONFIRMATION primitive, the SM at the

BS and the SSA at the CPE shall identify whether the antenna is integrated or non-integrated.

14.2.1.6.3 M-ANTENNA-INFORMATION-REQUEST

14.2.1.6.3.1 Purpose

The M-ANTENNA-INFORMATION-REQUEST primitive allows the MAC to request antenna

information from the antenna. The M-ANTENNA-INFORMATION-REQUEST primitive has no

attributes.

14.2.1.6.3.2 SAP type

M-SAP

14.2.1.6.3.3 Operation type

Information Request

14.2.1.6.3.4 Destination

Antenna Interface (see 9.12.2)

14.2.1.6.3.5 Data

This primitive has no attributes.

14.2.1.6.3.6 When generated

The M-ANTENNA-INFORMATION-REQUEST primitive shall be generated by the SM of a BS or the

SSA of the CPE and issued to their respective antenna for antenna information.

14.2.1.6.3.7 Effect of receipt

When the antenna receives the M-ANTENNA-INFORMATION-REQUEST primitive, the antenna shall

generate an M-ANTENNA-INFORMATION-CONFIRMATION containing information that describes the

attributes of the antenna.

14.2.1.6.4 M-ANTENNA-INFORMATION-CONFIRMATION

14.2.1.6.4.1 Purpose

The M-ANTENNA-INFORMATION-CONFIRMATION primitive is used to respond to the MAC request

with antenna information. Table 310 specifies the parameters for the M-ANTENNA-INFORMATIONCONFIRMATION

primitive.

14.2.1.6.4.2 SAP type

M-SAP

14.2.1.6.4.3 Operation type

Information Confirmation

14.2.1.6.4.4 Destination

CPE, BS

14.2.1.6.4.5 Data

14.2.1.6.4.6 When generated

The M-ANTENNA-INFORMATION-CONFIRMATION primitive shall be generated by the antenna and

issued to the MAC to respond with information about the antenna.

14.2.1.6.4.7 Effect of receipt

When the MAC receives the M-ANTENNA-INFORMATION-CONFIRMATION, MAC shall store the

maximum gain (dBi) for each channel so that the device can convert from transmit power to EIRP.

14.2.2 Spectrum Manager-Spectrum Sensing Function SAP (SM-SSF-SAP)

14.2.2.1 Spectrum sensing function primitives

The IEEE 802.22 PHY layer shall provide local spectrum sensing services through its SSF accessed

through the SM-SSF-SAP. Table 311 summarizes the spectrum sensing primitives supported through the

SM-SSF-SAP interface. The primitives are discussed in the subclauses referenced in the table.

14.2.2.1.1 SM-SSF-SAP-CHANNEL-SENSING-REQUEST

14.2.2.1.1.1 Purpose

The SM-SSF-SAP-CHANNEL-SENSING-REQUEST primitive allows the SM to request the PHY SSF

unit (in either the local SSA or remote SSA at a CPE) to perform spectrum sensing. Table 312 specifies the

parameters for the SM-SSF-SAP-CHANNEL-SENSING-REQUEST primitive.

14.2.2.1.1.2 SAP type

SM-SSF-SAP

14.2.2.1.1.3 Operation type

Information Request

14.2.2.1.1.4 Destination

SSA SSF

14.2.2.1.1.5 Data

14.2.2.1.1.6 When generated

The SM-SSF-SAP-CHANNEL-SENSING-REQUEST primitive is generated by the SM and issued to the

SSF to request the SSF to perform spectrum sensing.

14.2.2.1.1.7 Effect of receipt

When the SSA receives the SM-SSF-SAP-CHANNEL-SENSING-REQUEST primitive, it requests the SSF

to perform spectrum sensing. If the sensing request can be serviced, the SSA replies by sending the SMSSF-

SAP-CHANNEL-SENSING-INDICATION to indicate to SM it can perform sensing, executes

sensing, and then sends sensing results back to SM in SM-SSF-SAP-SENSING-RESULTSCONFIRMATION.

If the sensing request cannot be serviced, the SSA will send back a failure code in the

SM-SSF-SAP-CHANNEL-SENSING-INDICATION.

14.2.2.1.2 SM-SSF-SAP-CHANNEL-SENSING-INDICATION

14.2.2.1.2.1 Purpose

The SM-SSF-SAP-CHANNEL-SENSING-INDICATION primitive is used to inform the SM whether its

request to the local PHY SSF or remote SSF at a CPE was successfully generated by the SM. Table 313

specifies the parameters for the SM-SSF-SAP-CHANNEL-SENSING-INDICATION primitive.

14.2.2.1.2.2 SAP type

SM-SSF-SAP

14.2.2.1.2.3 Operation type

Event Indication

14.2.2.1.2.4 Destination

SM

14.2.2.1.2.5 Data

14.2.2.1.2.6 When generated

The SM-SSF-SAP-CHANNEL-SENSING-INDICATION primitive is generated by the SSF and issued to

its SM to indicate whether the received SM-SSF-SAP-CHANNEL-SENSING-REQUEST was valid and

whether the SSF is able to perform sensing for the signal types as requested. If the SSF is able to perform

signals requested, the Status Code shall be set to SUCCESS. If the SSF does not support the requested

sensing mode, the Status Code value should be INVALID\_REQUEST. If one or more of the signal types in

the request are not valid or the SSF does not have the capability of sensing a requested signal type, the

status code should be set to INVALID\_SIGNAL\_TYPE, and the corresponding invalid signal types shall

be indicated in the Invalid Signal Type Array.

14.2.2.1.2.7 Effect of receipt

When the SM receives the SM-SSF-SAP-CHANNEL-SENSING-INDICATION primitive, it will identify

whether its request to the SSF was successfully received by the SSF. The status parameter indicates the

appropriate error code from 7.7.24 in case the request is invalid.

14.2.2.1.3 SM-SSF-SAP-SENSING-RESULTS-CONFIRMATION

14.2.2.1.3.1 Purpose

The SM-SSF-SAP-SENSING-RESULTS-CONFIRMATION primitive is used to inform the SM when the

results of a previously issued request to the SSF were successfully generated by the SSF. Table 314

specifies the parameters for the SM-SSF-SAP-SENSING-RESULTS-CONFIRMATION primitive.

14.2.2.1.3.2 SAP type

SM-SSF-SAP

14.2.2.1.3.3 Operation type

Information Confirmation

14.2.2.1.3.4 Destination

SM

14.2.2.1.3.5 Data

14.2.2.1.3.6 When generated

The SM-SSF-SAP-SENSING-RESULTS-CONFIRMATION primitive is generated by the SSF and issued

to the SM to indicate the results of a previously issued request to the SSF have been generated.

14.2.2.1.3.7 Effect of receipt

When the SM receives the SM-SSF-SAP-SENSING-RESULTS-CONFIRMATON, it will obtain the

sensing results to its request to the SSF.

14.2.3 Spectrum Manager-Geolocation SAP (SM-GL-SAP)

14.2.3.1 Geolocation primitives

The PHY layer provides local geolocation services through its satellite-based location acquisition unit to

the SM/SSA through the SM-GL-SAP. Table 315 summarizes the geolocation primitives supported through

the SM-GL-SAP interface. The primitives are discussed in the subclauses referenced in the table.

14.2.3.1.1 SM-GL-SAP-GEOLOCATION-REQUEST

14.2.3.1.1.1 Purpose

The SM-GL-SAP-GEOLOCATION-REQUEST primitive allows the SM to request the local PHY

geolocation unit or the one at a CPE to perform geolocation. Table 316 specifies the parameters for the

SM-GL-SAP-GEOLOCATION-REQUEST primitive.

14.2.3.1.1.2 SAP type

SM-GL-SAP

14.2.3.1.1.3 Operation type

Information Request

14.2.3.1.1.4 Destination

SSA GL

14.2.3.1.1.5 Data

14.2.3.1.1.6 When generated

The SM-GL-SAP-GEOLOCATION-REQUEST primitive is generated by the SM and issued to an SSA

(either its own or remote at a CPE) GL to request the geolocation service to perform geolocation.

14.2.3.1.1.7 Effect of receipt

When the SSA GL receives the SM-GL-SAP-GEOLOCATION-REQUEST primitive, it attempts execution

of the geolocation service to perform geolocation. If the geolocation request can be satisfied, it sends a SMGL-

SAP-GEOLOCATION-INDICATION with a successful status, executes the geolocation, and returns

the result in SM-GL-SAP-GEOLOCATION-RESULTS-CONFIRMATION. If the geolocation request

cannot be satisfied, it sends a SM-GL-SAP-GEOLOCATION-INDICATION with a failure status.

14.2.3.1.2 SM-GL-SAP-GEOLOCATON-INDICATION

14.2.3.1.2.1 Purpose

The SM-GL-SAP-GEOLOCATION-INDICATION primitive is used to inform the SM whether its request

to the PHY geolocation service was successfully generated by the Geolocation function of the SSA.

Table 317 specifies the parameters for the SM-GL-SAP-GEOLOCATION-INDICATION primitive.

14.2.3.1.2.2 SAP type

SM-GL-SAP

14.2.3.1.2.3 Operation type

Event Indication

14.2.3.1.2.4 Destination

SM

14.2.3.1.2.5 Data

14.2.3.1.2.6 When generated

The SM-GL-SAP-GEOLOCATION-INDICATION primitive is generated by the SSA GL and issued to its

SM to indicate whether the received SM-GL-SAP-GEOLOCATION-REQUEST was valid. If the request is

valid, the SSA GL acquires the requested NMEA sentence from the geolocation service.

14.2.3.1.2.7 Effect of receipt

When the SM receives the SM-GL-SAP-GEOLOCATION-INDICATION primitive, it will identify

whether its request to the geolocation service was successfully received by the SSA GL. The status

parameter indicates the appropriate error code from 7.7.24 in case the geolocation service was not

available.

14.2.3.1.3 SM-GL-SAP-RESULTS-CONFIRMATION

14.2.3.1.3.1 Purpose

The SM-GL-SAP-GEOLOCATION-RESULTS-CONFIRMATION primitive is used to inform the SM

when a response to a previously issued request to the geolocation service was successfully received by the

SSA GL. Table 318 specifies the parameters for the SM-GL-SAP-GEOLOCATION-RESULTSCONFIRMATION

primitive.

14.2.3.1.3.2 SAP type

SM-GL-SAP

14.2.3.1.3.3 Operation type

Information Confirmation

14.2.3.1.3.4 Destination

SM

14.2.3.1.3.5 Data

14.2.3.1.3.6 When generated

The SM-GL-SAP-GEOLOCATION-RESULTS-CONFIRMATION primitive shall be generated by the

SSA GL and issued to the SM to indicate the reception of a response to a query previously issued to the

geolocation service.

14.2.3.1.3.7 Effect of receipt

When the SM receives the SM-GL-SAP-GEOLOCATION-RESULTS-CONFIRMATION, it shall identify

whether the response to its request to the geolocation service was successfully received by the SSA GL. If

the response was successful, the SM will obtain NMEA string containing the latitude and longitude

information. If the response is not successful, the SM may decide to issue another request.

# 

# (normative) IEEE 802.22 regulatory domains and regulatory classes requirements

This annex describes the various technical parameters and specifications required by the various regulatory domains for operation of the IEEE Std 802.22 in the TV bands.

## Regulatory domains, regulatory classes, and professional installation

Table A.1 specifies the regulatory domains and licensing regime where the IEEE 802.22 systems are planned to be authorized to operate in the TV bands.

Table A.1—Regulatory domains

|  |  |  |  |
| --- | --- | --- | --- |
| **Geographic**  **area** | **Regulatory domain ISO 3166 (3 Bytes)** | **Licensing regime** | **Approval**  **authority** |
| United States | USA | Unlicensed | FCC |
| Canada | CAN | Licensed | IC |
| United Kingdom | GBR | — | OFCOM |
| — | — | — | — |

1921HTable A.2 specifies the authorized regulatory classes under their respective regulatory domains.

Table A.2—Regulatory classes

|  |  |  |
| --- | --- | --- |
| **Regulatory domain** | **Regulatory class and profile** | |
| **Fixed** | **Personal portable** |
| USA | Stationary fixed | Mode I & IIa |
| CAN | Stationary fixed | N/A |
| — | — | — |

aThe behavioral limits sets for Modes I and II are defined in the FCC Report and Order. However, IEEE Std 802.22 will only operate in portable nomadic Mode II.

Table A.3 specifies the requirement for professional installation of the WRAN BS and CPEs.

Table A.3—Professional installation requirement

|  |  |  |  |
| --- | --- | --- | --- |
| **Regulatory domain** | **Type of terminal** | | **Definition of professional installer** |
| **BS** | **CPE** |
| USA | Professionally installed | Professionally installed | A professional installer is a competent individual or team of individuals with experience in installing radio communications equipment and who normally provides service on a fee basis—such an individual or team can generally be expected to be capable of ascertaining the geographic coordinates of a site and entering them into the device for communication to a database. |
| CAN | Professionally installed | N/A | Same as for USA. |
| — | — | — | — |

## Radio performance requirements

### Sensitivity and Noise

# (informative) Sensing

This annex contains descriptions of a number of sensing techniques. A sensing technique is an implementation of the spectrum sensing function.

…

## References

# (informative) Bibliography

At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the references listed below.

1. The Institute of Electrical and Electronics Engineers, Inc.

   3 Park Avenue, New York, NY 10016-5997, USA

   Copyright © 2011 by the Institute of Electrical and Electronics Engineers, Inc.

   All rights reserved. Published 1 July 2011. Printed in the United States of America.

   IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics   
   Engineers, Incorporated.

   **PDF: ISBN 978-0-7381-6723-7 STD97146**

   **Print: ISBN 978-0-7381-6724-4 STDPD97146**

   *IEEE prohibits discrimination, harassment and bullying. For more information, visit* [*http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html*](http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html)*.*

   *No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.*  [↑](#footnote-ref-1)