The IEEE 802.22 WRAN Standard and its interface to the White Space Database

REQUIREMENTS FOR PAWS

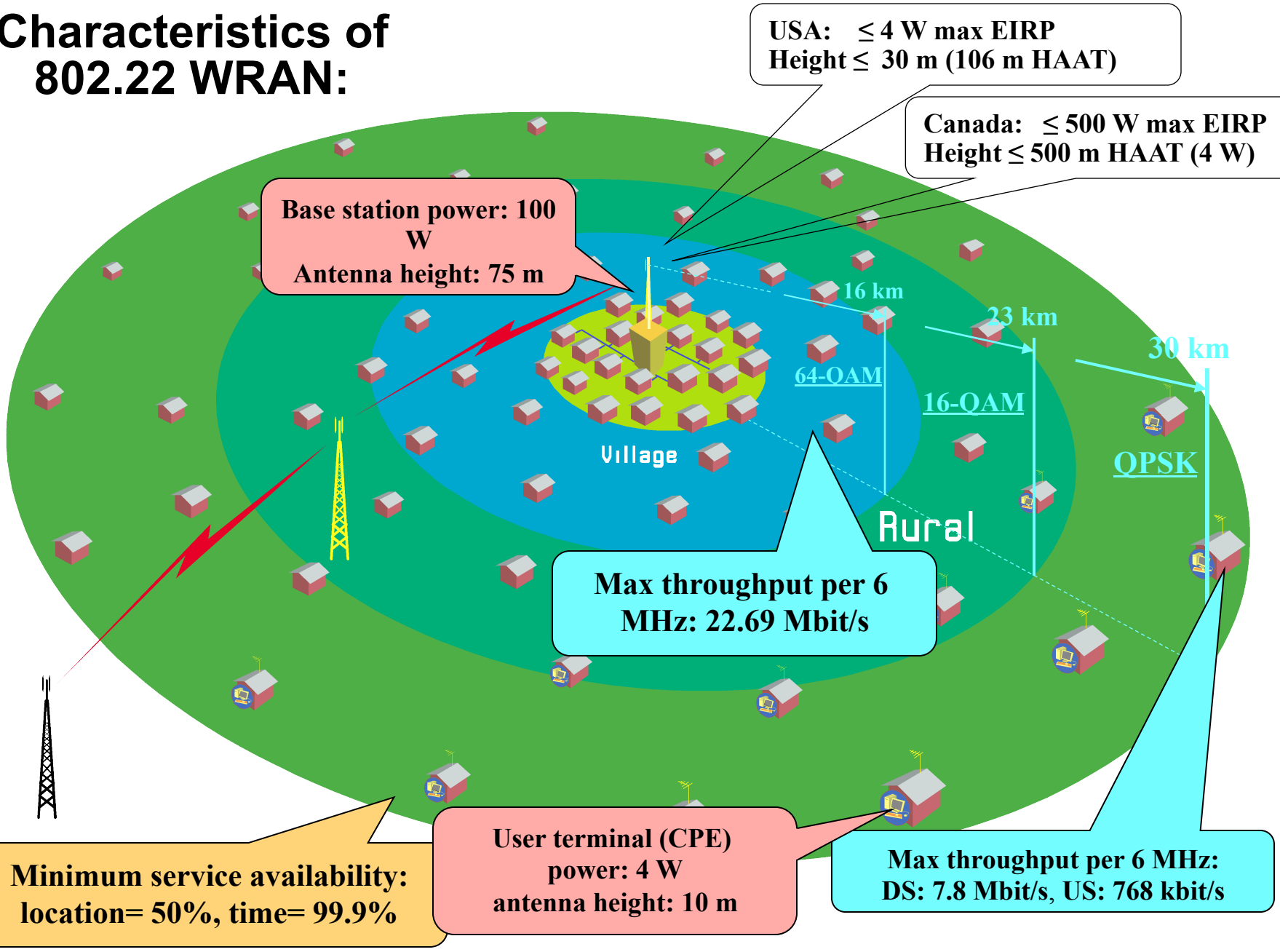
IETF PAWS
Working Group Meeting

Apurva N. Mody, apurva.mody@ieee.org
Chair, IEEE 802.22 Working Group (www.ieee802.org/22)

Gérald Chouinard, gerald.chouinard@crc.ca
IEEE 802.22 Working Group Vice-chair and lead editor

Jerome Kalke, (CBS), Ranga Reddy, Nancy Bravin

Characteristics of 802.22 WRAN:



IEEE 802.22 WRAN Standard
Key features

- WRAN: Wireless Regional Area Network
  - Aimed at bringing broadband access to hard-to-reach, low population density areas, typical of rural environments and developing countries
- Operate in vacant channels in TV broadcast bands to take advantage of better signal propagation at lower frequencies
- Operate as license-exempt equipment although the base station (BS) and possibly the customer premise equipment (CPE) have to be professionally installed
- Point-to-multipoint network topology
  - Base station connected to the Internet through a backhaul
  - Base station provides service to up to 512 CPEs (fixed or portable) and controls all their RF characteristics ("master-slave")
- Use cognitive radio capabilities to avoid interference to broadcast incumbents and other WRAN systems
  - Access to databases
  - RF sensing

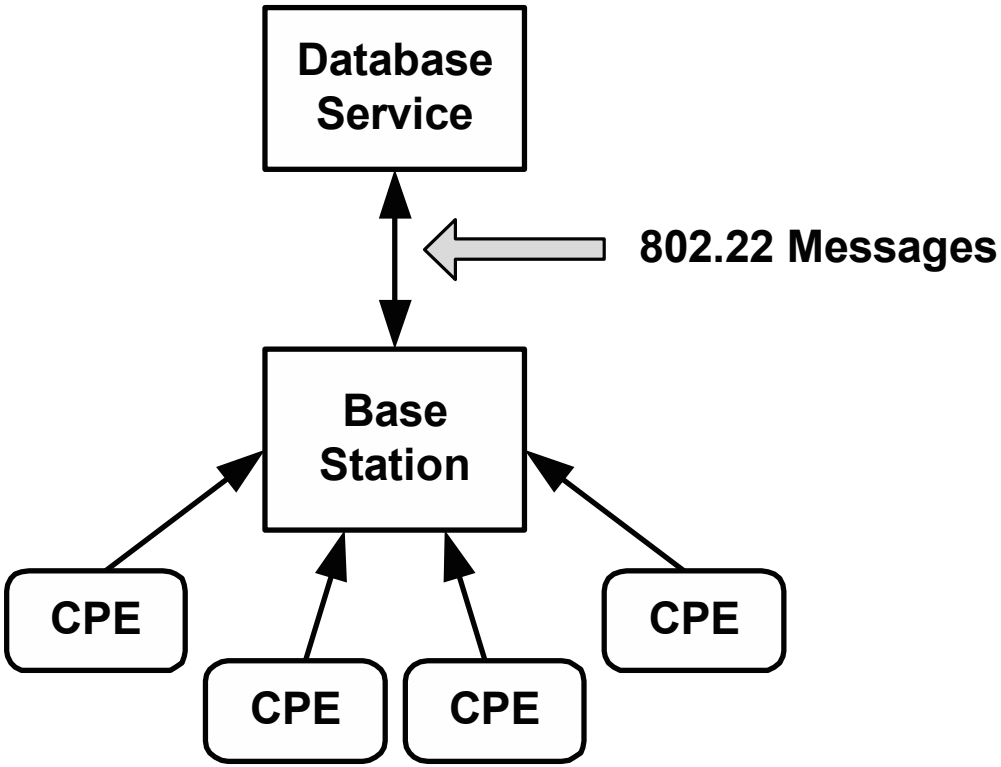
802.22 Unique Proposition

- *First* IEEE 802 Standard for operation in Television Whitespaces
- *First* IEEE Standard that is specifically designed for rural and regional area broadband access aimed at removing the digital divide
- *First* IEEE Standard that has all the Cognitive Radio featur
- Recipient of the IEEE SA *Emerging Technology Award*

REQUIREMENTS

802.22 database interface model

To comply with the FCC R&O 08-260, the IEEE 802.22 interface to the database will take place entirely between the **database service and the Base Station (BS)** rather than with its individual CPEs (BS has to find the channel that is common to all its CPEs rather than the CPEs doing it individually (MO&O 10-174: 15.711(e)). **In other words, BS acts as a proxy to all the CPEs**



DATA MODEL REQUIREMENTS (1)

[AMENDED] D.1: The Data Model MUST support specifying the Following Parameters~~antenna height parameter of the subject~~

Antenna Parameters (Master WSD => database)

Height Parameters

AGL in meters: Unsigned INT, 2 Bytes (0 – 65,535 cm)

Example: 802.22 primitive:

Antenna height	Integer	1 byte	Antenna height above ground level in meters.

[Note: our assumption is that the database will compute the HAAT in meters from the antenna AGL and ground elevation at the specified location (lat, long) obtained from a topographic database by the database server.]
[Note: portable antenna height may be 1.5 m. Base stations in Canada can be at up to 500 m HAAT which could be completely contributed by the antenna AGL (e.g., mounted on a broadcast tower). Two bytes are therefore necessary.]

DATA MODEL REQUIREMENTS (2)

Gain Parameters

Antenna directionality information in dB: relative to the main lobe maximum gain for every 5 degree azimuth clockwise starting from the direction of the maximum antenna gain expressed in unit of 0.25 dB over the range –63.75 dB (encoded 0x00) to 0 dB (0xFF):
Character String of 72 bytes

Antenna azimuth in degrees, clockwise from true North: 2 bytes INT

Example: 802.22 primitive:

Antenna information	Character String	72 bytes	Antenna directionality information of the device in dB relative to the main lobe maximum gain for every 5 degree azimuth clockwise starting from the direction of the maximum antenna gain expressed in unit of 0.25 dB over the range –63.75 dB (encoded 0x00) to 0 dB (0xFF). (to allow the database calculation of the channel availability and the maximum allowed EIRP values at the registering location19)
Antenna azimuth	Integer	2 bytes	Antenna azimuth in degrees, clockwise from true North

(Continued)

DATA MODEL REQUIREMENTS (3)

Gain Parameters (Continued)

Note:
Antenna directionality will represent the antenna gain pattern in the horizontal plane in dB referred to the gain of its main lobe and it is assumed that the database service will use its knowledge of the geolocation of the base station and the device being enlisted to calculate the azimuth of the device antenna main lobe for interference calculations in the case of base station and CPE operation. Omni-directional antennas shall be assumed as the default.

DATA MODEL REQUIREMENTS (4)

RF Mask Parameters (Master WSD => database)

Regulatory Domain (3 ASCII Letters), Device Type (Regulatory Class: e. g., Fixed, Personal/Portable, Mobile, etc.) (1 byte INT), Mask Number Index (2 byte INT) (where Mask Number Index corresponds to a particular RF Mask of an equipment that is stored in the database and that has passed the regulatory certification).

Example: 802.22 primitive:

Device Type	Integer	1 byte	The value identifies the type of device at the geolocation registering 0x00 = Fixed base station 0x01 = Fixed CPE 0x02 = Personal/portable mode 0x03–0xFF = *Reserved*

DATA MODEL REQUIREMENTS (5)

[AMENDED] D.2: The data model MUST support specifying an ID of the subject. This ID would ~~be~~contain the ID of the device used ~~to be~~that has been certified by a regulatory body for ~~a~~ its regulatory domain as well as an identification of the technology that is being used. (Master WSD => database)

Example: 802.22 primitives:

Name	Type	Length	Description
Device Type	Integer	1 byte	The value identifies the type of device at the geo-location registering 0x00 = Fixed base station 0x01 = Fixed CPE 0x02 = Personal/portable mode 0x03-0xFF = *Reserved*
Device-ID Length	Integer	2 bytes	Length of Device-ID field (# of characters)
Device-ID	Character String	Variable	In US, this is FCC-ID
Serial Number Length	Integer	2 bytes	Length of Serial Number field (# of characters)
Serial Number	Character String	Variable	

Note: The device-ID and Serial Number could be replaced by a universal identifier made of one or many parts . The master WSD must also specify, as part of its registration process with the database, the technology that it uses (e.g., IEEE 802.22, IEEE 802.11af, etc.) (see requirement O.7).

DATA MODEL REQUIREMENTS (6)

[AMENDED] D.3: The Data Model MUST support specifying the location of the ~~subject~~WSD, the uncertainty in meters and confidence in percentage ~~and accuracy of~~ for the location determination. (Master WSD => database)

Example: 802.22 primitives:

Name	Type	Length	Description
Location Data String Length	Integer	2 bytes	Length of Location Data String field (# of characters)
Location Data String	Character String	NMEA 0183 Character String	The value identifies the location of the device (latitude, longitude).[20]

Note: NMEA 0183 $GPGGA or $GPGLL String can carry latitude and longitude information. In the work of the IEEE 802.22 Working Group, it was assumed that the altitude of a geographic point would be derived at the database based on the latitude and longitude of the location of the WSD (see the note related to HAAT in D.1 above for which ground elevation information would need to be known). In 802.22 networks, the CPEs acquire their geolocation and transmit their latitude and longitude to the base station at the time of association. The base station would augment the location information defined in the NMEA string format with uncertainty (m) and confidence level (%) as the local regulator may want to define it. These uncertainty and confidence values would be generated at the base station based, for example, on the technology used by the WSDs to acquire their geolocation. The uncertainty could also be artificially increased to take into account the size of the area around a WSD where other WSD's not requiring geolocation (e.g., Mode I devices in the USA) would operate.

DATA MODEL REQUIREMENTS (7)

[AMENDED] D.4: The Data Model MUST support specifying a list of available channel along with the maximum EIRP (dBm) that can be accommodated ~~list~~ and time constraints for the channel list availability. (Database => Master WSD)

Example: 802.22 primitives:

Name	Type	Length	Description
Number of Channels Available	Integer	1 byte	
{ If(Number of Channels Available > 0)			If the number of channels is equal to 0, this means that the device cannot operate.

For (i=1; i≤ Number of Channels Available; i++) {
Channel_Number
Max_Allowed_EIRP (dBm)
Availability schedule
}
	Vector of 2xN bytes and a number of pairs of NMEA 0183 $ZDA strings	Variable	List of available channel numbers and corresponding maximum allowed EIRP expressed in dBm over the range –64 dBm (encoded 0x00) to +63.5 dBm (encoded 0xFF) as well as the availability schedule (start and stop date/time) for each channel in Universal date and time system.

}			

(See D.4 above. Also, specifying the "maximum output power" is not sufficient since it may or may not include the antenna gain. Specifying the EIRP is needed. D.5 should be deleted since it is proposed to be covered in D.4.)

DATA MODEL REQUIREMENTS (8)

[AMENDED] D.6: The Data Model MUST support specifying channel availability information for single and multiple locations. The database MUST also allow a master device to act as a proxy for other WSDs and query on their behalf. (Master WSD => Database)

In case of 802.22 systems which are to provide point-to-multipoint broadband access service primarily to rural areas, the BS acts as a proxy for all its associated CPEs and queries the database for each device. If a query is to be grouped or made in a batch mode, all the information related to each device shall be provided to the BS (i.e., the database is not to perform the intersection for all these devices and locations).

….. continued

DATA MODEL REQUIREMENTS (8)

[AMENDED] D.6: The Data Model MUST support specifying channel availability information for single and multiple locations. The database MUST also allow a master device to act as a proxy for other WSDs and query on their behalf. (Master WSD => Database)

…. Continued from previous slide

[Note: This option may be useful to 'batch' the database query process but it is not clear whether this would really increase the data transfer efficiency. In the case of the 802.22 WRAN systems, the base station will need to acquire all the information about the available channels for each of these CPEs (and the related maximum EIRP's) so that the operating channel and the backup channels (to which the WRAN cell will need to move if the current operating channel becomes unavailable to ensure a transparent channel move) can be determined locally from the best 'intersection' of these channels for all the associated CPEs. This will allow database queries for only new CPEs coming on board or being moved, and constraints to be added locally at the base station to execute the 'intersection' process to produce the updated list of operational and backup channels that is to be transmitted to all CPEs for refreshing.

DATA MODEL REQUIREMENTS (9)

[DISAGREE] D.7: The Data Model MUST support specifying channel availability information for an area around a specified location. (Database => Master WSD)

In our opinion, this can be done through the normal query process if a query to the database can be done with dummy device IDs, for example for planning purposes, and hence, we feel that this is not really needed. If a query is done to the database with dummy device ID, the database should not register these new devices and only provide the list of available channels. There should therefore be a need to identify whether the included device ID is a real one or not.

DATA MODEL REQUIREMENTS (10)

[NEW] D.8: The Data Model should support reporting to the database the channels that the master WSD has selected as the operating channel and the backup channels (see requirement O.7).

PROTOCOL REQUIREMENTS

PROTOCOL REQUIREMENTS (1)

[AGREE] P.1: The protocol MUST provide a mechanism for the subject to discover the WS Database it has to use at a given location.

[AGREE] P.2: The protocol MUST support regulatory domain discovery.

[AGREE] P.3: The protocol between the master device and the WS Database MUST support the ability for the database to push~~ing~~ updates ~~in~~ on channel availability changes to subjects.

[AGREE] P.4: The protocol between the master device and the WS Database MUST support mutual authentication and authorization.

[AGREE] P.5: The protocol between the master device and the WS Database MUST support integrity and confidentiality protection.

[AGREE]P.6: The protocol MUST support both username/password and digital certificates based authentication.

PROTOCOL REQUIREMENTS (2)

[NEW] P.7: The protocol MUST require the master WSD to maintain contact with the database as specified by the local regulator as well as to specify and re-register its operating and backup channels with at least the same periodicity.

OPERATIONAL REQUIREMENTS

OPERATIONAL REQUIREMENTS (1)

[AMENDED] O.1: A master device MUST query the WS Database for the available channels as often as required by the regulation (e.g., FCC requires once per day) to verify that the operating channels, and backup channels in the case of providing transparent switch-over, continue to remain available.

[AMENDED] O.2: A master device MUST determine its location ~~with the accuracy~~along with its uncertainty (e.g., FCC requires +/- 50m) and confidence level (e.g., 95%) and send it to the database so that the proper WSD position and buffer distance around the device can be added to make sure that the worst case situation required by the regulation ~~(e.g., FCC requires +/-)~~ is considered in the distance calculations taking place at ~~before placing aquery to~~ the DB.

OPERATIONAL REQUIREMENTS (2)

[AMENDED] O.3: A master device which changes its location during its operation, MUST query the WS Database for available operating channels each time it moves more than the distance specified by the regulation (e.g., FCC specifies 100 m) from the location it occupied when it previously made the query ~~from~~.

[AMENDED] O.4: The WS Database MUST provide the available channel list and the maximum EIRP corresponding to each channel when requested and MAY also provide time constraints for ~~the~~ each channel in the available list ~~and maximum output power~~ to the master device.

OPERATIONAL REQUIREMENTS (3)

[AMENDED] O.5: A master device MUST be able to query the WS Database for itself as well as for its ~~and include the FCC ID of the slave~~ associated devices and compile the channel availability (and maximum EIRP thereof) so that a common channel can be selected for use by all these WSDs to form a network. Furthermore, common channels may also need to be selected in a similar way to become backup channels to allow for network channel switch that would be transparent to the users ~~in the query before allowing the slave device to use the available channel.~~

[AMENDED] O.6: A master device MUST be capable ~~to~~ of validateing the digital certificate of the WS Database and whether it has been revoked or not.

~~O.7: A master device MUST be capable to check the validity of the WS Database certificate and whether it has been revoked or not.~~[Repeat, see O. 6]

OPERATIONAL REQUIREMENTS (4)

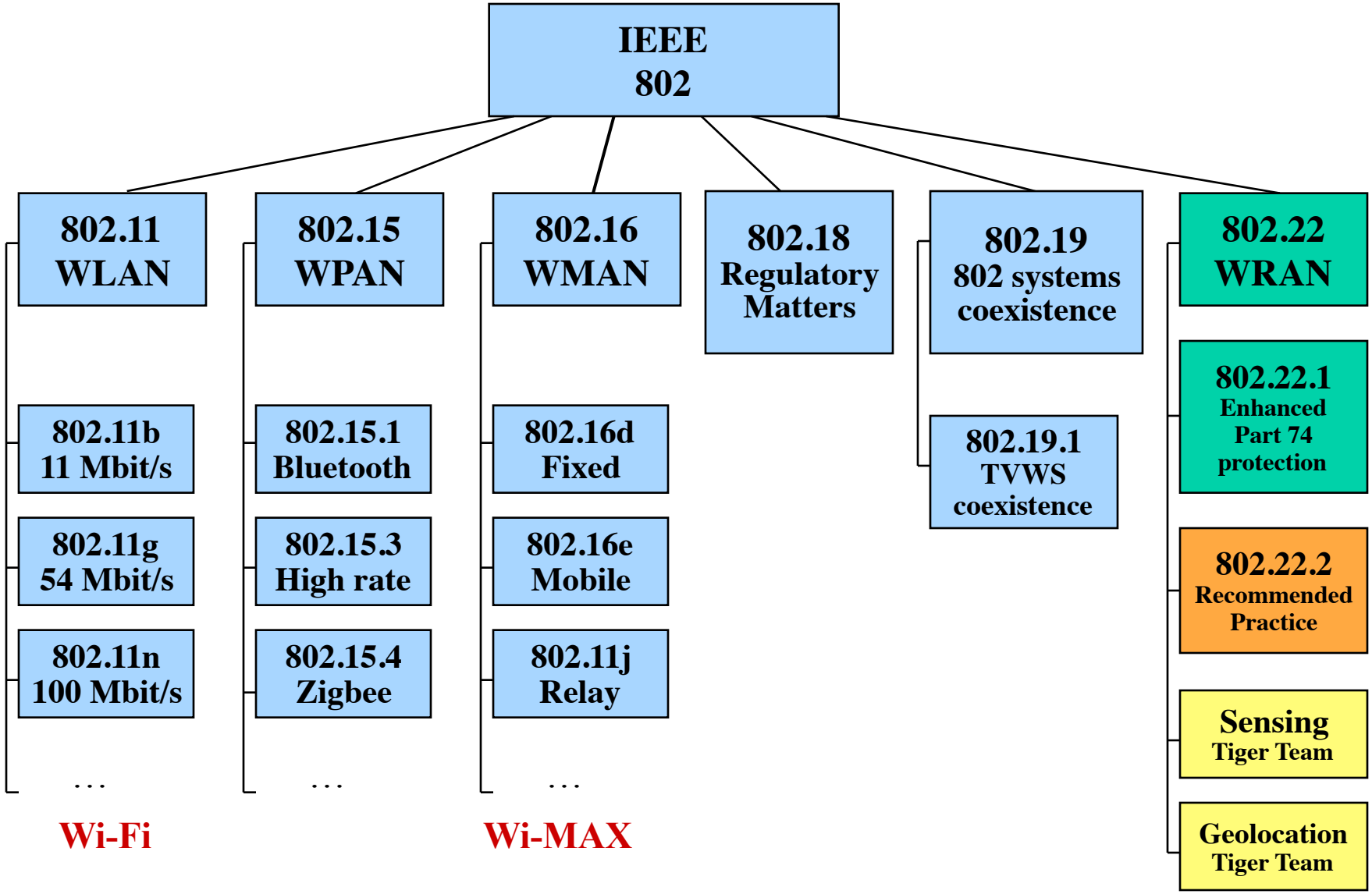
[NEW] O.7: The database must be capable of keeping track of the channels that are currently being utilized by the master devices and the technology that they use (e.g., IEEE 802.22, IEEE 802.11af, etc.).

If a request for the available channel is made by another master WSD from the same area and it is found that the new requesting master device technology cannot co-exist, then that channel should be removed from the available channels list going to this new device. Unless the given master WSD fails to re-query within the specified contact period, the database should make that channel available. Accordingly, the protocol should provide the master WSDs with a means to release their operating channel when not needed.

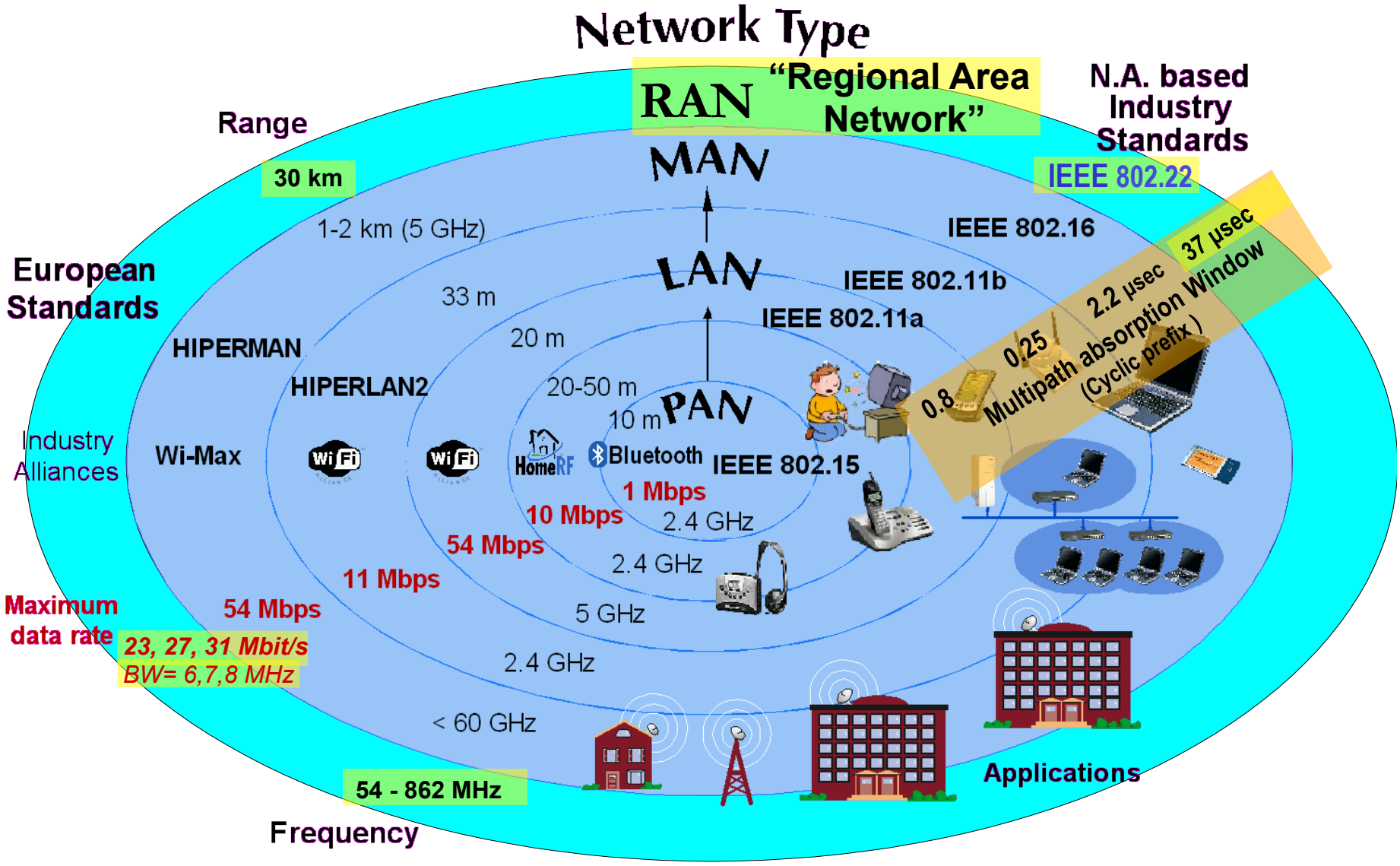
Note that without an active channel management mechanism (e.g., 802.22 spectrum manager), it is unlikely that having the database just specifying which channels are available to protect incumbent services on a 24 hours cycle will be sufficient to allow for proper operation of multiple WSDs in an area without interference being caused among themselves. Without area specific centralized spectrum management that directs and juggles master WSD channel assignments virtually instantaneously, the result will be inefficient use of White Space spectrum.

INTERFACES
Presented Earlier by Gerald Chouinard in Quebec City July 2011

IEEE 802 Standards Process



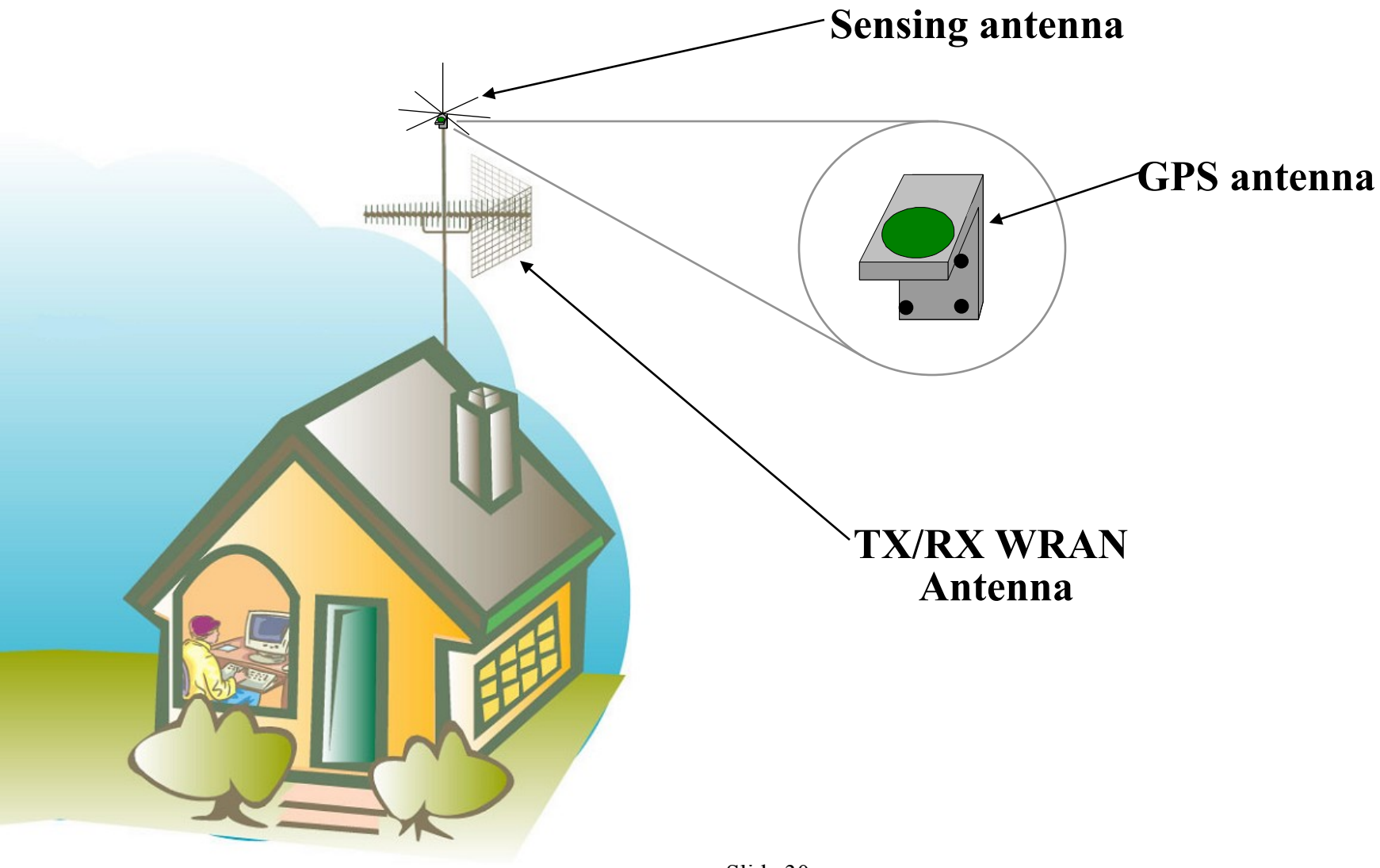
IEEE 802 Standards



IEEE 802.22 WRAN Standard
Key features

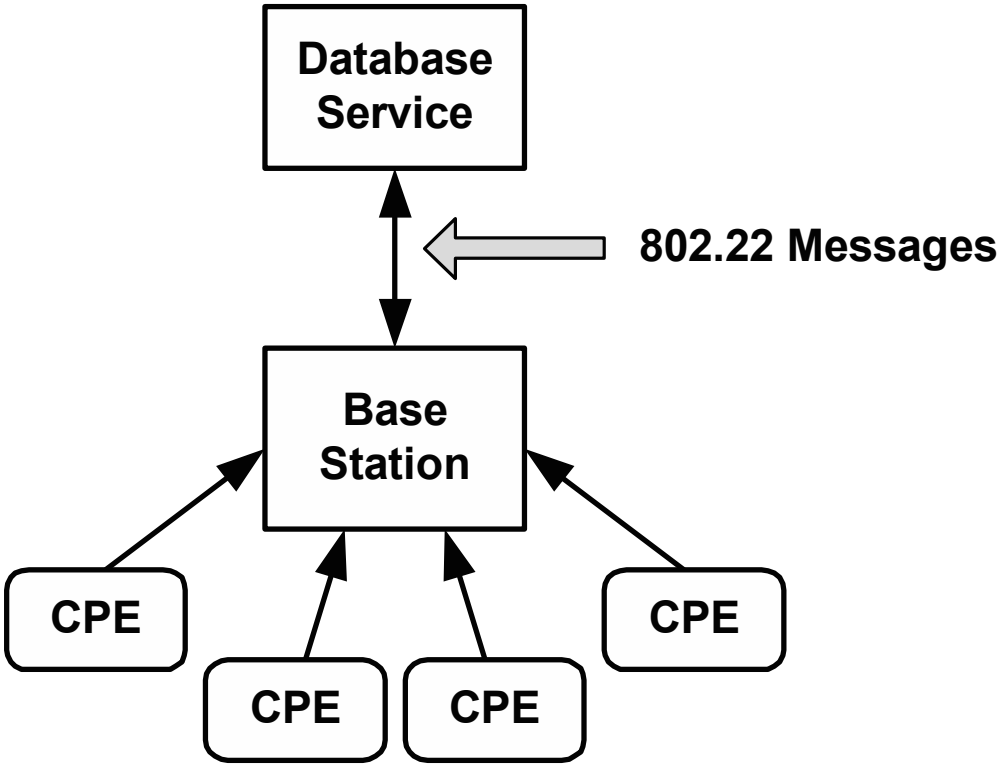
- WRAN: Wireless Regional Area Network
  - Aimed at bringing broadband access to hard-to-reach, low population density areas, typical of rural environments and developing countries
- Operate in vacant channels in TV broadcast bands to take advantage of better signal propagation at lower frequencies
- Operate as license-exempt equipment although the base station (BS) and possibly the customer premise equipment (CPE) have to be professionally installed
- Point-to-multipoint network topology
  - Base station connected to the Internet through a backhaul
  - Base station provides service to up to 512 CPEs (fixed or portable) and controls all their RF characteristics ("master-slave")
- Use cognitive radio capabilities to avoid interference to broadcast incumbents and other WRAN systems
  - Access to databases
  - RF sensing

Typical CPE installation



802.22 database interface model

To comply with the FCC R&O 08-260, the IEEE 802.22 interface to the database will take place entirely between the database service and the BS rather than with its individual CPEs (BS has to find the channel that is common to all its CPEs rather than the CPEs doing it individually (MO&O 10-174: 15.711(e)).



802.22 database interface procedure

- The BS will initially enlist with the database service as a fixed device. It will also enlist all its associated CPEs with their geographic location, device identification, etc., as obtained at association on a real time basis.
- On an ongoing basis, the BS will then query the database (at least once every 24 hours) using the M-DB-AVAILABLE-CHANNEL-REQUEST message so that it can retrieve the channel availability information.
- The database service could also 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 (*this will allow better reaction time than the 24 hours minimum access time while keeping the database traffic to a minimum*).

Security of the database interface

- SSL will be supported on the link between the database service and the BS to provide transport layer security:
  - to allow authentication of the database service provider as well as the WRAN system querying the service
  - to avoid the message exchange being altered on the backhaul connection
- protocols used for device and database service authentication and for interacting with the database:
  EAP-TLS or EAP-TTLS
- database service primitives are exchanged between the CPE/BS and the database service via Attribute Value Pairs of EAP messaging
- formatting of these messages should conform to the authentication service that the database service employs: (e.g., RADIUS/RFC 2865 or DIAMETER/RFC 3588).

Database service primitives

1. **M-DB-AVAILABLE-REQUEST**: Message that allows the BS to verify that it is connected to the database service in order to receive channel availability and maximum allowed EIRP updates.
2. **M-DB-AVAILABLE-CONFIRM:** Message that allows the database service to confirm that the BS is connected to the database service.
3. **M-DEVICE-ENLISTMENT-REQUEST:** Message that allows the BS to enlist with the database service a device that has joined its WRAN network.
4. **M-DEVICE-ENLISTMENT-CONFIRM:** Message that allows the database service to confirm to the BS that the new device has been successfully registered.

Database service primitives

5. **M-DB-AVAILABLE-CHANNEL-REQUEST:** Message by which the BS requests a list of available channels and maximum allowed EIRP per channel from the database service for the specified type of device at the particular location.
6. **M-DB-AVAILABLE-CHANNEL-INDICATION:** Message that is used to return to the BS the list of available channels as provided by the database service in the form of channel number, maximum allowed EIRP, and availability schedule.
7. **M-DB-DELIST-REQUEST:** Message that allows the BS to request the database service to remove the enlistment of a device that was associated with that base station.
8. **M-DB-DELIST-CONFIRM:** Message that is used to inform the BS whether its request to remove the enlistment of a device that was associated with that base station was successfully received and executed by the database service.

M-DB-AVAILABLE-REQUEST

Name	Type	Length	Description
Base station-ID Length	Integer	2 bytes	Length of Base station-ID field (number of characters)
Base station-ID	Character String	Variable	In US, this is FCC-ID
Serial Number Length	Integer	2 bytes	Length of Serial Number field (number of characters)
Serial Number	Character String	Variable	
Database Service URL Length	Integer	2 bytes	Length of database service URL field (number of characters). This is used to set the Locator for the Database service
Database Service URL	Character String	Variable	A fully qualified URL starting with, http:// or https://
Base Station Database Service Access URL Length	Integer	2 bytes	Length of Base Station Database Service URL filed (number of characters)
Base Station Database Service Access URL	Character String	Variable	A fully qualified URL. This is used to set the Locator for the Base Station Access by the Database Service
Base Station Management URL Length	Integer	2 bytes	Length of Base Station Management URL field (number of characters)
Base Station Management URL	Character String	Variable	A fully qualified URL. This is used to set the Locator for the BS Management Service
Timestamp Length	Integer	2 bytes	Length of Timestamp field (number of characters)
Timestamp	Character String	NMEA 0183 $ZDA string	Timestamp of the present request at time of transmission and as encoded in the $ZDA substring of the NMEA 0183 string

M-DB-AVAILABLE-CONFIRM

Name	Type	Length	Description
Base station-ID Length	Integer	2 bytes	Length of Base station-ID field (number of characters)
Base station-ID	Character String	Variable	In US, this is FCC-ID
Serial Number Length	Integer	2 bytes	Length of Serial Number field (number of characters)
Serial Number	Character String	Variable	
Timestamp Length	Integer	2 bytes	Length of Timestamp field (numberof characters)
Timestamp	Character String	NMEA 0183 $ZDA string	Copied from the timestamp in the M-DB-AVAILABLE-REQUEST

M-DEVICE-ENLISTMENT-REQUEST (a)

Name	Type	Length	Description
Device Type	Integer	1 byte	The value identifies the type of device obtained as part of its process to associate 0x00 = Fixed base station 0x01 = Fixed CPE 0x02 = Personal/portable mode 0x03–0xFF = *Reserved*
Device-ID Length	Integer	2 bytes	Length of Device-ID field (number of characters)
Device-ID	Character String	Variable	In US, this is FCC-ID
Serial Number Length	Integer	2 bytes	Length of Serial Number field (number of characters)
Serial Number	Character String	Variable	
Proxy Device-ID Length	Integer	2 bytes	Length of Proxy Device-ID field (number of characters)
Proxy Device-ID	Character String	Variable	This element is the device ID for the device (most likely the controlling BS) that is acting as the proxy to the database service. (In US, this is the FCC-ID.)
Proxy Serial Number Length	Integer	2 bytes	Length of Proxy Serial Number field (number of characters)
Proxy Serial Number	Character String	Variable	This element is the serial number for the device (most likely the controlling BS) that is acting as the proxy to the database service.
Location Data String Length	Integer	2 bytes	Length of Location Data String field (number of characters)
Location Data String	Character String	NMEA 0183	The value identifies the location of the device (latitude, longitude).
Responsible Party Name Length	Integer	2 bytes	Length of Responsible Party Name field (number of characters)
Responsible Party Name	Character String	Variable	
Antenna height	Integer	1 byte	Antenna height above ground level in meters.

M-DEVICE-ENLISTMENT-REQUEST (b)

Name	Type	Length	Description
If (Device Type = 0x00 or 0x01) {			
Contact Name Length	Integer	2 bytes	Length of Contact Name field (number of characters)
Contact Name	Character String	Variable	
Contact Physical Address Length	Integer	2 bytes	Length of Contact Physical Address field (number of characters)
Contact Physical Address	Character String	Variable	
Contact Email Address Length	Integer	2 bytes	Length of Contact Email Address field (number of characters)
Contact Email Address	Character String	Variable	
Contact Telephone Number Length	Integer	2 bytes	Length of Contact Telephone Number field (number of characters)
Contact Telephone Number	Character String	Variable	
}			
Base Station Database Service Access URL Length	Integer	2 bytes	Length of Base Station Database Service URL field (number of characters)
Base Station Database Service Access URL	Character String	Variable	A fully qualified URL. This is used to set the Locator for the Base Station Access by the Database Service.
Database Service URL Length	Integer	2 bytes	Length of Database Service URL field (number of characters)
Database Service URL	Character String	Variable	A fully qualified URL starting with, http:// or https://

M-DEVICE-ENLISTMENT-REQUEST (c)

Name	Type	Length	Description
If (wranIfDatabaseServiceBSAntennaInformationSupportedMib) {			
Antenna information	Character String	72 bytes	Antenna directionality information of the device in dB relative to the main lobe maximum gain for every 5 degree azimuth clockwise starting from the direction of the maximum antenna gain expressed in unit of 0.25 dB over the range –63.75 dB (encoded 0x00) to 0 dB (0xFF). (to allow the database calculation of the channel availability and the maximum allowed EIRP values at the registering location)
Antenna azimuth	Integer	2 bytes	Antenna azimuth in degrees, clockwise from true North
}			
}			
Timestamp Length	Integer	2 bytes	Length of Timestamp field (number of characters)
Timestamp	Character String	NMEA 0183 $ZDA string	Timestamp of the present request at time of transmission and as encoded in the $ZDA substring of the NMEA 0183 string

M-DEVICE-ENLISTMENT-CONFIRM

Name	Type	Length	Description
Device-ID Length	Integer	2 bytes	Length of Device-ID field (number of characters)
Device-ID	Character String	Variable	In US, this is FCC-ID
Serial Number Length	Integer	2 bytes	Length of Serial Number field (number of characters)
Serial Number	Character String	Variable	
Timestamp Length	Integer	2 bytes	Length of Timestamp field (number of characters)
Timestamp	Character String	NMEA 0183 $ZDA string	Copied from the timestamp in the M-DB-AVAILABLE-REQUEST

M-DB-AVAILABLE-CHANNEL-REQUEST

Name	Type	Length	Description
Device Type	Integer	1 byte	The value identifies the type of device at the geolocation registering 0x00 = Fixed base station 0x01 = Fixed CPE 0x02 = Personal/portable mode 0x03–0xFF = *Reserved*
Device-ID Length	Integer	2 bytes	Length of Device-ID field (number of characters)
Device-ID	Character String	Variable	In US, this is FCC-ID
Serial Number Length	Integer	2 bytes	Length of Serial Number field (number of characters)
Serial Number	Character String	Variable	
Location Data String Length	Integer	2 bytes	Length of Location Data String field (number of characters)
Location Data String	Character String	NMEA 0183 Character String	The value identifies the location of the device (latitude, longitude)
Timestamp Length	Integer	2 bytes	Length of Timestamp field (number of characters)
Timestamp	Character String	NMEA 0183 $ZDA string	Timestamp of the present request at time of transmission and as encoded in the $ZDA substring of the NMEA 0183 string

M-DB-AVAILABLE-CHANNEL-INDICATION

Name	Type	Length	Description
Device-ID Length	Integer	2 bytes	Length of Device-ID field (number of characters)
Device- ID	Character String	Variable	In US, this is FCC-ID
Serial Number Length	Integer	2 bytes	Length of Serial Number field (number of characters)
Serial number	Character String	Variable	
Number of Channels Available	Integer	1 byte	
{ If(Number of Channels Available > 0)			If the number of channels is equal to 0, this means that the device cannot operate.

For (i=1; $i \leq$ Number of Channels Available; i++) {
Channel_Number
Max_Allowed_EIRP (dBm)
Availability schedule
}
	Vector of 2×N bytes and a number of pairs of NMEA 0183 $ZDA strings	Variable	List of available channel numbers and corresponding maximum allowed EIRP expressed in dBm over the range –64 dBm (encoded 0x00) to +63.5 dBm (encoded 0xFF) as well as the availability schedule (start and stop date/time) for each channel in Universal date and time system

}			
Status Message	Character String	Variable	Various status messages coming from the database service (e.g., unapproved device flag)
Timestamp Length	Integer	2 bytes	Length of Timestamp field (number of characters)
Timestamp	Character String	NMEA 0183 $ZDA string	Copied from the timestamp in the M-DB-AVAILABLE-CHANNEL-REQUEST

M-DB-DELIST-REQUEST

Name	Type	Length	Description
Device-ID Length	Integer	2 bytes	Length of Device-ID field (number of characters)
Device-ID	Character String	Variable	In US, this is FCC-ID
Serial Number Length	Integer	2 bytes	Length of Serial Number field (number of characters)
Serial Number	Character String	Variable	
Responsible Party Name Length	Integer	2 bytes	Length of Responsible Party Name field (number of characters)
Responsible Party Name	Character String	Variable	
Location Data String Length	Integer	2 bytes	Length of Location Data String
Location Data String	Character String	NMEA 0183 Character string	The value identifies the location of the device (latitude, longitude)

M-DB-DELIST-CONFIRM

Name	Type	Length	Description
Device-ID	Character String	Variable	In US, this is FCC-ID
Serial Number	Character String	Variable	
Responsible Party Name	Character String	Variable	
Location Data String Length	Integer	2 bytes	Length of Location Data String field (number of characters)
Location Data String	Character String	NMEA 0183 Character string	The value identifies the location of the device (latitude, longitude)

References

1. *IEEE Std 802.22-2011™, Standard for Wireless Regional Area Networks—Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the TV Bands, July 2011*
2. *IEEE 802.22 WG inputs to PAWS: https://mentor.ieee.org/802.22/dcn/11/22-11-0127-06-0000-ieee-802-22-inputs-to-ietf-paws.doc*
3. *U.S. FCC, ET Docket 08-260, "Second Report and Order and Memorandum Opinion and Order in the Matter of Unlicensed Operation in the TV Broadcast Bands," November 14, 2008.*
4. *U.S. FCC, ET Docket 10-174, "Second Memorandum Opinion and Order in the Matter of Unlicensed Operation in the TV Broadcast Bands," September 23, 2010.*
5. *NMEA 0183, Interface Standard of the National Marine Electronics Association, Version 4.00 http://www.nmea.org/content/nmea_standards/nmea_083_v_400.asp.*
6. *IETF RFC 2865, "Remote Authentication Dial In User Service (RADIUS)," June 2000.*
7. *[B1] DIAMETER/RFC 3588, "Diameter Base Protocol," September 2003.*
8. *IETF RFC 3748, "Extensible Authentication Protocol (EAP)," June 2004.*