

# White Space use cases & requirements

I-D: [draft-probasco-paws-overview-usecases](#)

**Gabor Bajko, Basavaraj Patil, Scott Probasco**

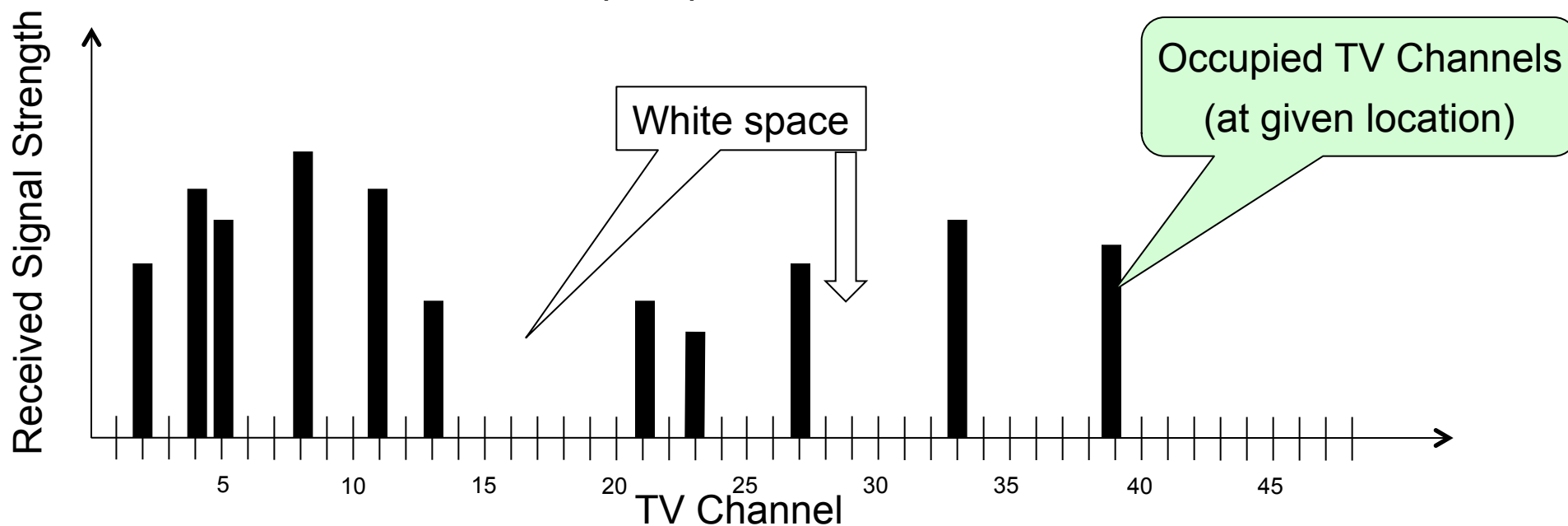
# Overview

- Introduce White Space concept
- Use case: TVWS database discovery
- Use case: Hot-spot, urban internet connectivity service
- Use case: Wide-Area or rural internet broadband access
- Use case: Offloading, moving traffic to a white space network
- Use case: TVWS for backhaul
- Use case: Location based service usage scenario

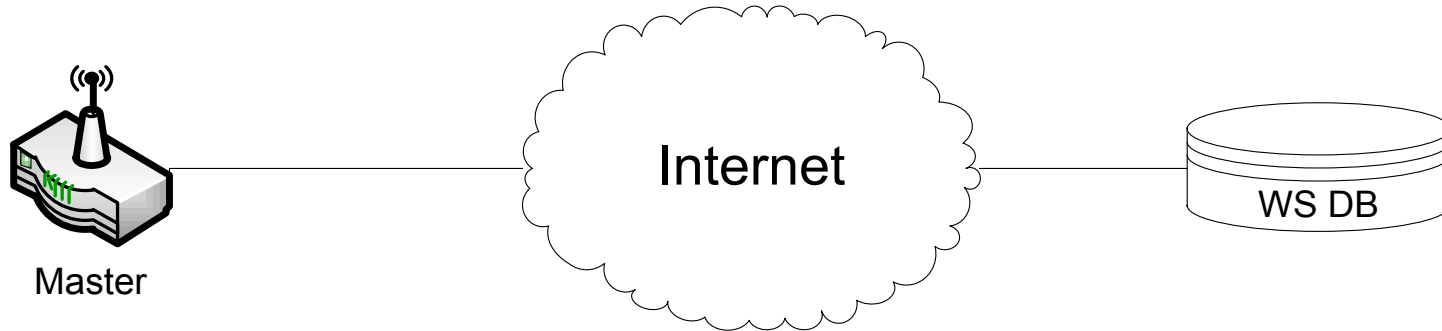


# What is White Space (WS)?

- White space (WS): In a spectrum band that is **licensed** to primary users, the part of spectrum that is unused by the primary user at specific **locations** and sometimes at specific **time**.
  - Example: Television Channels – not every channel is used in every town
- White space allows secondary users to use the portions of spectrum not actually used by the primary user on an **unlicensed** basis.
- The unlicensed user must not cause interference.
- The unlicensed user cannot expect protection from interference



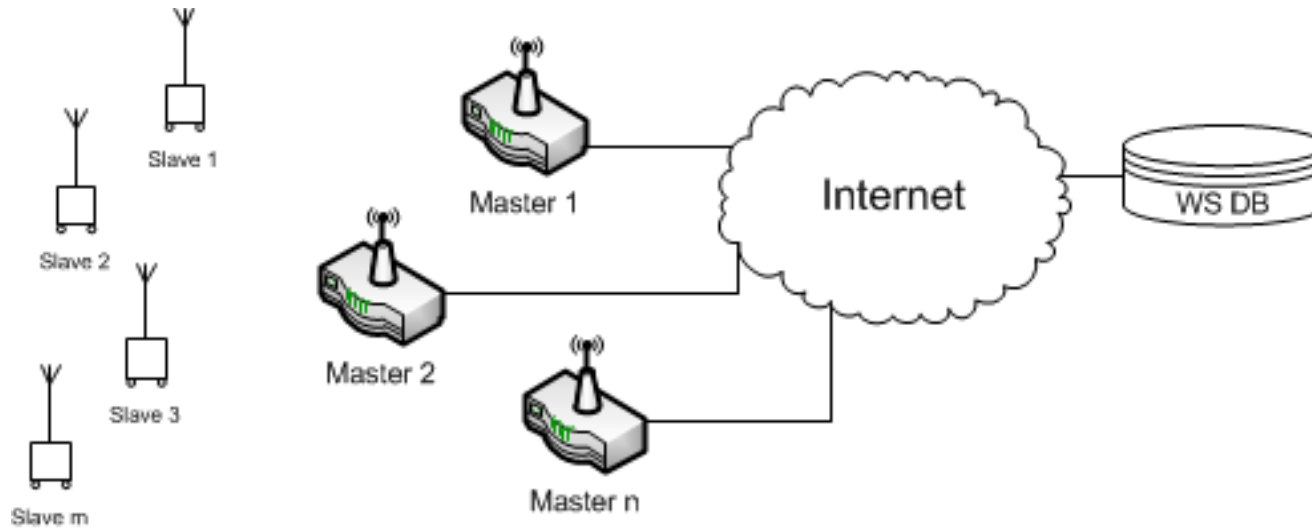
# Use case: TVWS database discovery



## Scenarios

1. Master is 'pre-programmed' with address of (1 or more) database(s)
2. Master does not have an address
3. Master has address but the database is not suitable

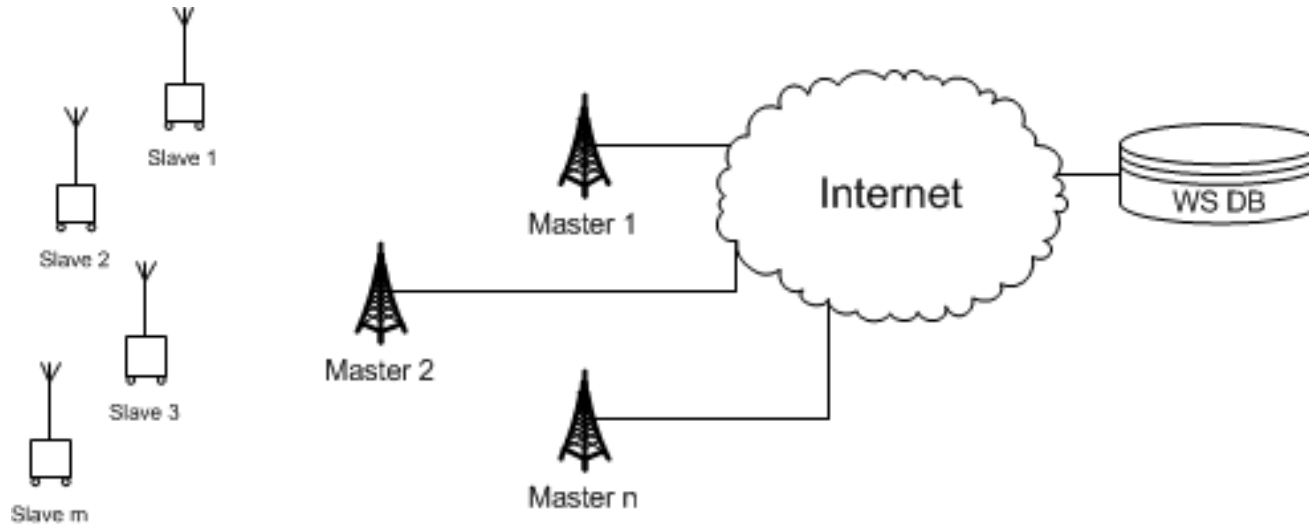
# Use case: Hot-spot, urban internet connectivity service



## Scenarios

1. Multiple Masters
2. Small cells
3. Few available channels
4. Masters are un-coordinated

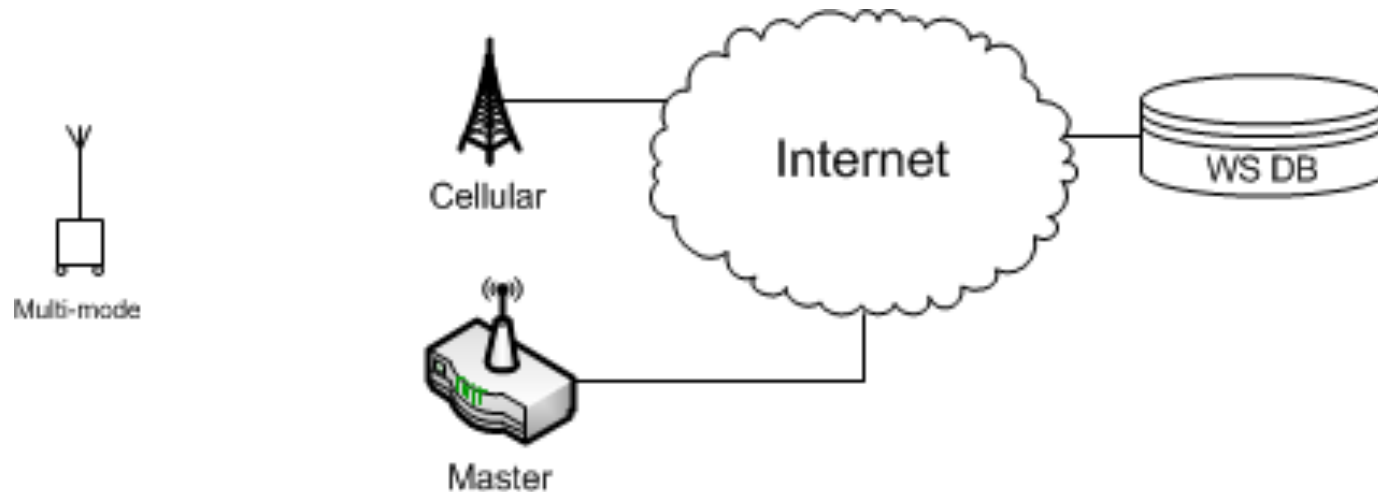
# Use case: Wide-Area or rural internet broadband access



## Scenarios

1. Multiple Masters
2. Large cells
3. Many available channels
4. Masters are coordinated

# Use case: Offloading, moving traffic to a white space network

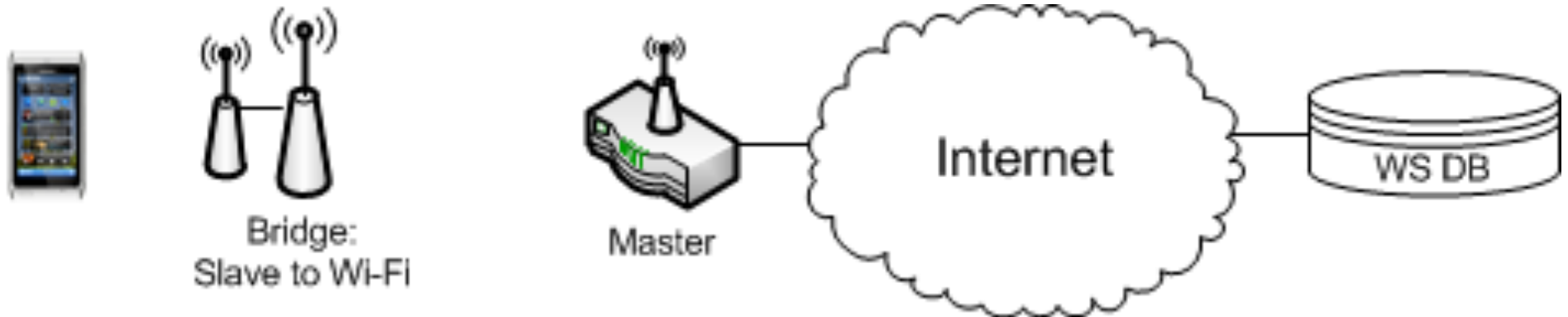


## Scenarios

1. Multimode device (cellular, white space)
2. Cellular is not preferred (cost, RF coverage, data caps, etc...)
3. Move or 'offload' data traffic from cellular to white space



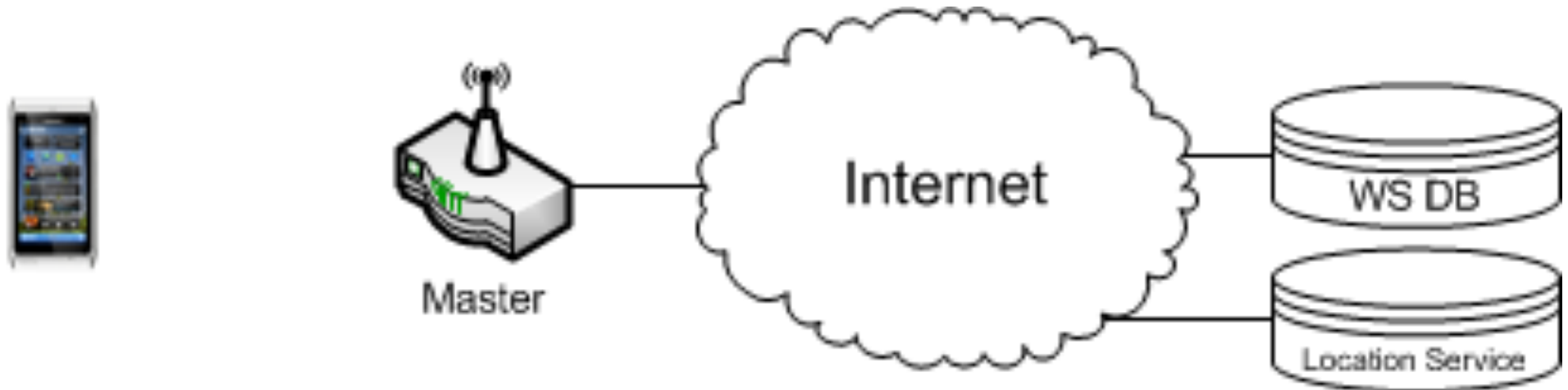
# Use case: TVWS for backhaul



## Scenarios

1. Master establishes white space network
2. Bridge-Slave joins the Master's network
3. Bridge-Wi-Fi provides internet access to Wi-Fi devices

# Use case: Location based service usage scenario



## Scenarios

1. Master registers with WS DB, including location
2. Smart Phone (Slave) connects to Master
3. Smart Phone app provides details of Master to Location Service
4. Location Service contacts WS DB for location

# Requirements - Master

1. A master device MUST include, directly or indirectly, its antenna height in the query to the WS Database.
2. A master device MUST query the WS Database for the available channels at least once a day to verify that the operating channels continue to remain available.
3. A master device MUST determine its location with at least  $\pm 50$  meters accuracy and MUST place that location into the query it makes to the WS Database.
4. A master device MAY indicate the accuracy by which it determined its location in the query to the WS Database.
5. A master device which changes its location during operation MUST query the WS Database for available operating channels each time it moves more than 100 meters from the location it previously made the query.
6. A master device MUST be able to receive channel availability updates from a WS Database.
7. A master device MUST be able to query the WS Database for channel availability information for multiple locations.
8. A master device MUST be able to query the WS Database for channel availability information for a specific area around its current location.
9. A master device MUST query the WS Database and include the FCC ID of the slave device in the query before allowing the slave device to use the available channel.

# Requirements - Database

1. The WS Database **MUST** provide the available channel list when requested and **MAY** also provide time constraints for the channel list and maximum output power to the master device.

# Requirements - Security

1. The protocol between the master device and the WS Database MUST support mutual authentication and authorization.
2. The protocol between the master device and the WS Database MUST support integrity and confidentiality protection.
3. The WS Database MUST support both username/password and digital certificates based authentication of the master device.
4. A master device MUST be capable to validate the digital certificate of the WS Database.
5. A master device MUST be capable to check the validity of the WS Database certificate and whether it has been revoked or not.

