

Dynamic Frequency Selection in 5 GHz mesh networks

Simon Wunderlich

sw@simonwunderlich.de

May 16, 2014



Outline

- 1 Introduction to DFS
 - What is DFS
 - Infrastructure mode
 - IBSS mode

- 2 Current Status
 - Status in Linux
 - Hands on
 - Limitations and Outlook

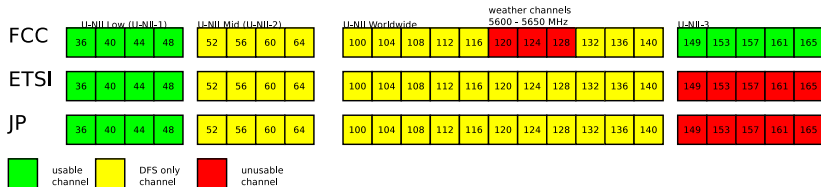
DFS in a nutshell

- DFS = Dynamic Frequency Selection
- most channels in 5 GHz may be used only with DFS enabled
- objective: don't disturb primary users (weather radars, military applications, satellites ...)

No DFS produces strange clouds ...



Why do we want DFS?

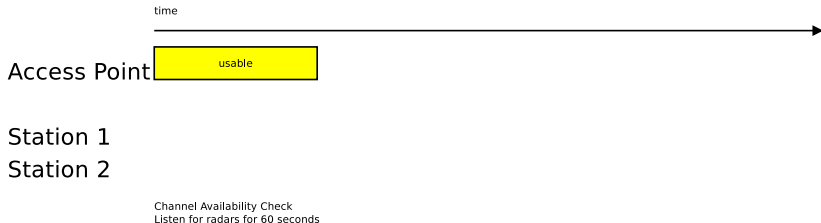


- allows to use much more channels
- many DFS-only channels allow higher transmission power
- IEEE 802.11ac only has one 80 MHz channel, no 160 MHz and only one 80+80MHz channel for US only
- (some) commercial APs (claim to) have it too :)

DFS operations explained

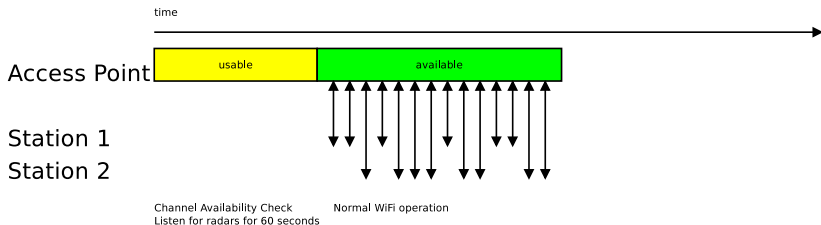
- DFS for WiFi is specified in amendment IEEE 802.11h
- IEEE 802.11h specifies a lot of things, but ...
- the most important part is the Channel Switch Announcement (CSA) frames
- ... and most commercial and open drivers implement only that

DFS operations explained - infrastructure mode (1)



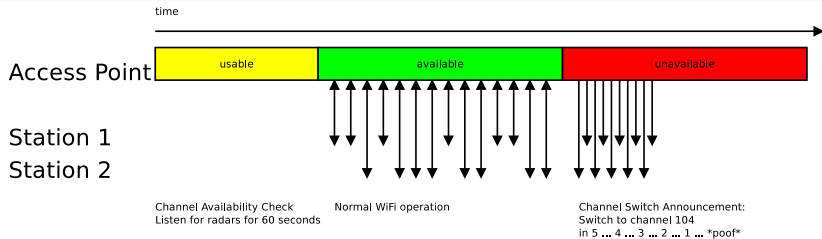
- Before operation: Channel Availability Check (CAC) on the channel to be used
- No transmission, just listen. If no radar is detected => channel becomes available

DFS operations explained - infrastructure mode (2)



- After CAC: AP may start beaconing and accept stations
- Stations do not have to detect radars (although they can, and 802.11h specifies how to report to the AP)

DFS operations explained - infrastructure mode (3)



- When a radar is detected: AP sends Channel Switch Announcement (CSA) in beacons and optionally action frames
- CSA contains: when to switch, and to which channel
- requirement for channel selection: uniform loading, e.g. select channel randomly
- After that, the current channel gets blacklisted ("unavailable") for some time (e.g. 30 minutes)
- Stations follow the AP

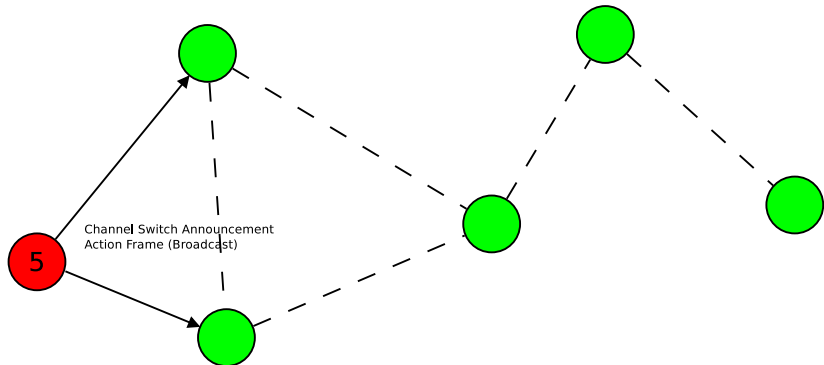
DFS operations explained - IBSS mode (1)

- no single point of coordination
- every station must be able to detect radars (act like a "master")
- information about radars must be flooded over the network

DFS operations explained - IBSS mode (2)

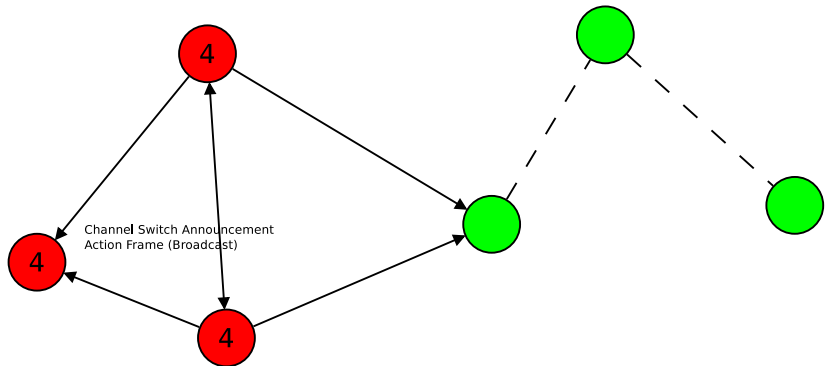
- There is an IBSS DFS element defined in 802.11h and a method to select a "DFS master" who should coordinate using TSF etc, but ...
- more from IEEE 802.11-2012:
 - "The potential for hidden nodes within an IBSS means that the IBSS channel switch protocol is best effort."
 - "It should be noted that this process might be imperfect in that the DFS owner may have incomplete knowledge and there may be no suitable channel."
- if an IBSS station receives a radar, it should send a measurement report to the DFS master - that is most likely to fail in a city wide mesh network.

DFS operations explained - IBSS mode (3)



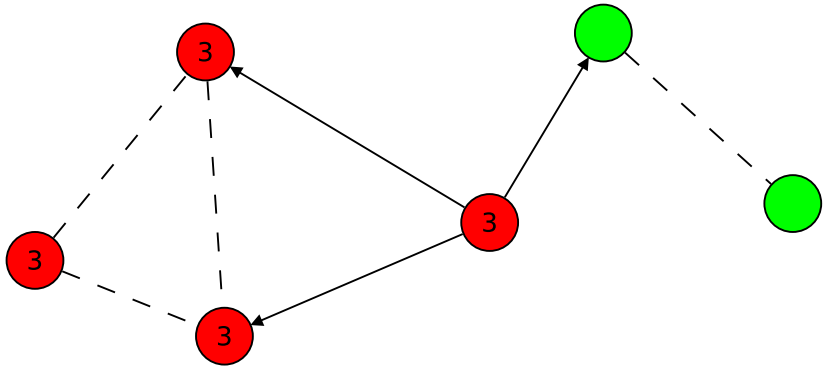
- When a radar is detected, choose a new channel and announce it via CSA
- also send out action frame - makes propagation faster, since the beaconing process is distributed

DFS operations explained - IBSS mode (3)



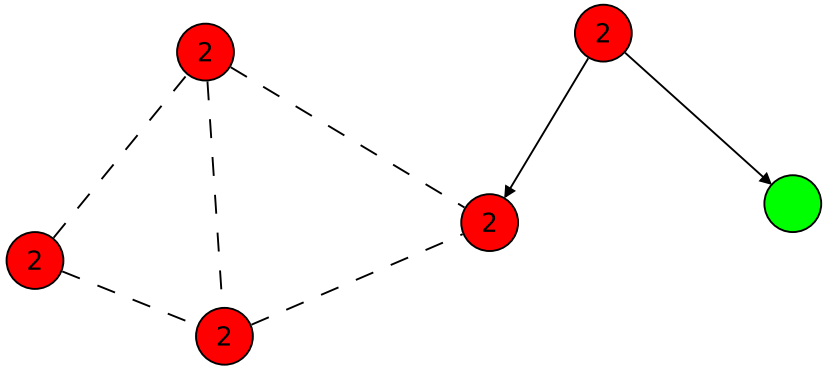
- Other nodes will see the CSA in either beacons or action frames and will do the same

DFS operations explained - IBSS mode (4)

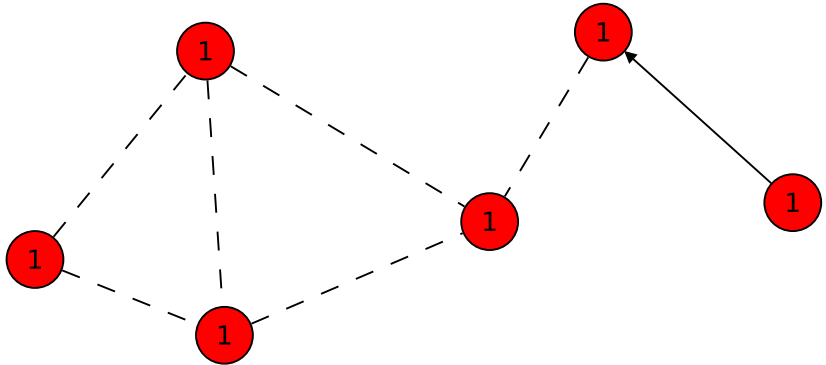


- the channel switch announcement gets distributed in the mesh

DFS operations explained - IBSS mode (5)



DFS operations explained - IBSS mode (6)



DFS operations explained - IBSS mode (7)

poof!

IBSS mode - Things to consider

- Since we have no DFS master, there is a possible race condition: multiple nodes can detect a radar at the same time and choose different channel \Rightarrow decide on a next channel before
- When a channel switch is missed, it would be good to background scan and see if other nodes already changed to the agreed next channel

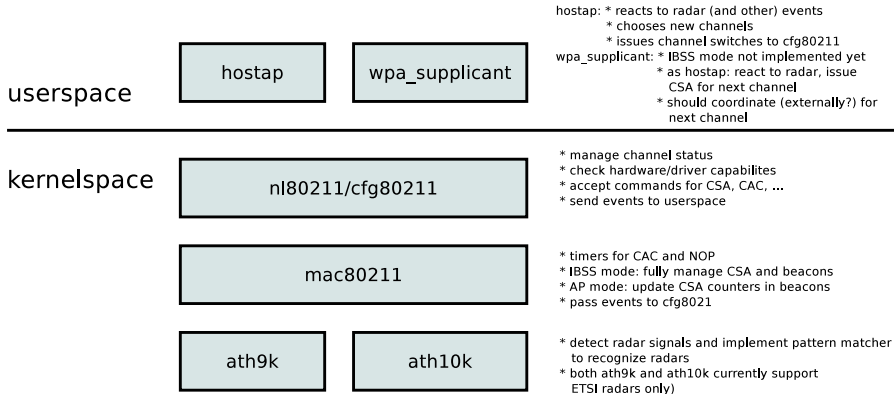
Outline

- 1 Introduction to DFS
 - What is DFS
 - Infrastructure mode
 - IBSS mode
- 2 **Current Status**
 - **Status in Linux**
 - Hands on
 - Limitations and Outlook

Linux implementation

- lots of kernel development done in 2013 (AP mode and IBSS mode, CSA code, ...)
- joint effort sponsored by different parties (Neratec, Texas Instruments, Qualcomm, Tieto, Intel, Fraunhofer FOKUS ...)
- still ongoing development (multi-interface CSA, ...)
- ... and also still a few things to do

Linux implementation



DFS in Linux

- Userspace can check state (available, usable, unavailable)

```
# iw phy0 info
[...]  
* 5500 MHz [100] (20.0 dBm) (passive scanning, no IBSS, radar detection)  
  DFS state: usable (for 218 sec)  
* 5520 MHz [104] (20.0 dBm) (passive scanning, no IBSS, radar detection)  
  DFS state: usable (for 218 sec)  
* 5540 MHz [108] (20.0 dBm) (passive scanning, no IBSS, radar detection)  
  DFS state: usable (for 218 sec)  
* 5560 MHz [112] (20.0 dBm) (passive scanning, no IBSS, radar detection)  
  DFS state: usable (for 218 sec)  
* 5580 MHz [116] (20.0 dBm) (passive scanning, no IBSS, radar detection)  
  DFS state: usable (for 218 sec)  
* 5600 MHz [120] (disabled)  
* 5620 MHz [124] (disabled)  
* 5640 MHz [128] (disabled)  
* 5660 MHz [132] (20.0 dBm) (passive scanning, no IBSS, radar detection)  
  DFS state: usable (for 218 sec)  
* 5680 MHz [136] (20.0 dBm) (passive scanning, no IBSS, radar detection)  
  DFS state: usable (for 218 sec)  
[...]
```

DFS in Linux

- for hostapd, enable ieee80211h=1 (depends on ieee80211d=1)
- hostapd will perform CAC if the channel is not available yet
- all kernel configuration options and country code settings must be right, though ...

```
# cat hostapd.conf
interface=wlan0
driver=nl80211
ssid=testap
hw_mode=a
channel=100
ieee80211d=1
ieee80211h=1
country_code=DE
[...]
```

Current Limitations

- IBSS DFS / CSA is implemented in kernel space, but ...
- wpa_supplicant does not yet support DFS for IBSS mode:
 - IBSS requires a userspace program which chooses the next channel (could be wpa_supplicant or something else)
 - agreement on next channel by an external program would be useful to avoid inconsistencies (e.g. distributed database, alfred, ...)
- no Multi-SSID / multiple devices on one wifi module supported
- real life experience and open source APs with certification still missing
- ath9k/ath10k only support ETSI radar patterns, no FCC or Japan

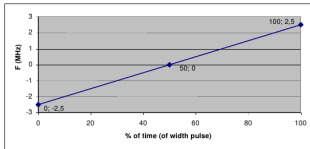
ETSI DFS pattern definitions

Table D.4: Parameters of radar test signals

Radar test signal # (see notes 1 to 3)	Pulse width W [μs]		Pulse repetition frequency PRF (PPS)		Number of different PRFs	Pulses per burst for each PRF (PPB) (see note 5)
	Min	Max	Min	Max		
1	0,5	5	200	1 000	1	10 (see note 6)
2	0,5	15	200	1 600	1	15 (see note 6)
3	0,5	15	2 300	4 000	1	25
4	20	30	2 000	4 000	1	20
5	0,5	2	300	400	2/3	10 (see note 6)
6	0,5	2	400	1 200	2/3	15 (see note 6)

NOTE 1: Radar test signals 1 to 4 are constant PRF based signals. See figure D.1. These radar test signals are intended to simulate also radars using a packet based Staggered PRF. See figure D.2.

NOTE 2: Radar test signal 4 is a modulated radar test signal. The modulation to be used is a chirp modulation with a $\pm 2,5$ MHz frequency deviation which is described below.



NOTE 3: Radar test signals 5 and 6 are single pulse based Staggered PRF radar test signals using 2 or 3 different PRF values. For radar test signal 5, the difference between the PRF values chosen shall be between 20 PPS and 50 PPS. For radar test signal 6, the difference between the PRF values chosen shall be between 80 PPS and 400 PPS. See figure D.3.

NOTE 4: Apart for the Off-Channel CAC testing, the radar test signals above shall only contain a single burst of pulses. See figures D.1, D.3 and D.4. For the Off-Channel CAC testing, repetitive bursts shall be used for the total duration of the test. See figures D.2 and D.5. See also clauses 4.7.2.2, 5.3.8.2.1.3.1 and 5.3.8.2.1.3.2.

NOTE 5: The total number of pulses in a burst is equal to the number of pulses for a single PRF multiplied by the number of different PRFs used.

NOTE 6: For the CAC and Off-Channel CAC requirements, the minimum number of pulses (for each PRF) for any of the radar test signals to be detected in the band 5 600 MHz to 5 650 MHz shall be 18.

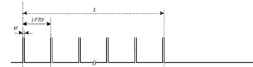


Figure D.1: General structure of a single burst/constant PRF based radar test signal

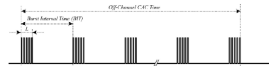


Figure D.2: General structure of a multiple burst/constant PRF based radar test signal

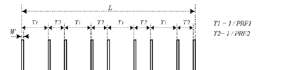


Figure D.3: General structure of a single burst/single pulse based staggered PRF radar test signal

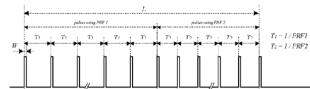


Figure D.4: General structure of a single burst/packet based staggered PRF radar test signal

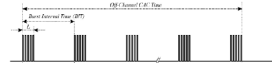


Figure D.5: General structure of a multiple burst/packet based staggered PRF based radar test signal

A world map with countries colored according to regulatory regions. Blue (FCC) includes North America, parts of South America, and some Asian countries. Green (ETSI) includes Europe, Russia, and parts of Africa and Asia. Red (JP) includes Japan, parts of Africa, and some Southeast Asian countries. A legend in the bottom left corner identifies the colors: FCC (blue square), ETSI (green square), and JP (red square).

Outlook

- Multi-Interface support is being worked on by the ath10k developers (Tieto, QCA), still ongoing
- FCC pattern matcher support is included in proprietary Qualcomm/Atheros drivers, maybe they can be ported to ath9k/ath10k?
- IBSS userspace support and channel selection/coordination still open
- use it, test it, certify it! :)

Thank you!

- Thank you very much for your attention!
- Please ask questions or mail me: sw@simonwunderlich.de