

Advanced Networking Lab

Thomas Hendriks

Jakob Struye

March 1, 2017

Lab 2

Frequencies and Channels

In the IEEE 802.11 standards, various channels are defined. Two main frequency bands are used, namely 2.4 GHz and 5GHz. IEEE 802.11a networks use the 5 GHz band, while IEEE 802.11b/g networks operate in the 2.4 GHz band. In both bands, various “channels” have been defined. However, channel separation is not as clean cut as one might expect. In the following setups, you will illustrate this using some simple tests.

2.1 Available channels

Exercise 1: Frequencies

Within the IEEE 802.11 specification, various channels are defined. Depending on the local authorities (Belgisch Instituut voor Postdiensten en Telecommunicatie - Belgian Institute for Postal services and Telecommunications (BIPT) in Belgium [?]), the list of allowed channels can vary. Using `iw` you can get the list of available channels.

! The wireless drivers we use make a difference between the logical interface (`wlan0` as we have used it so far) and the actual physical radio interface. All things related to physical characteristics are actually handled by the physical interface, which is called `phy0` or `phy1`, respectively.

1. To get a correct overview of which frequencies/channels are available in Belgium, use the command `iw phy1 info`.
2. List all frequencies/channels that the `phy1` interface supports.

L2-1-1

Using the command `iw phy1 info`, we got a lot of output, filtering for Frequencies rendered the following result, showing which frequencies the physical interface supports:

The frequencies marked as disabled are frequencies the device does not support, others are supported.

Frequencies:

- 2412 MHz [1] (20.0 dBm)
- 2417 MHz [2] (20.0 dBm)
- 2422 MHz [3] (20.0 dBm)
- 2427 MHz [4] (20.0 dBm)
- 2432 MHz [5] (20.0 dBm)
- 2437 MHz [6] (20.0 dBm)
- 2442 MHz [7] (20.0 dBm)
- 2447 MHz [8] (20.0 dBm)
- 2452 MHz [9] (20.0 dBm)
- 2457 MHz [10] (20.0 dBm)
- 2462 MHz [11] (20.0 dBm)
- 2467 MHz [12] (20.0 dBm)
- 2472 MHz [13] (20.0 dBm)
- 2484 MHz [14] (disabled)

Frequencies:

- 5180 MHz [36] (20.0 dBm)
- 5190 MHz [38] (20.0 dBm)
- 5200 MHz [40] (20.0 dBm)
- 5220 MHz [44] (20.0 dBm)
- 5230 MHz [46] (20.0 dBm)
- 5240 MHz [48] (20.0 dBm)
- 5260 MHz [52] (20.0 dBm) (radar detection)
- 5270 MHz [54] (20.0 dBm) (radar detection)
- 5280 MHz [56] (20.0 dBm) (radar detection)

- 5300 MHz [60] (20.0 dBm) (radar detection)
- 5310 MHz [62] (20.0 dBm) (radar detection)
- 5320 MHz [64] (20.0 dBm) (radar detection)
- 5500 MHz [100] (27.0 dBm) (radar detection)
- 5510 MHz [102] (27.0 dBm) (radar detection)
- 5520 MHz [104] (27.0 dBm) (radar detection)
- 5540 MHz [108] (27.0 dBm) (radar detection)
- 5550 MHz [110] (27.0 dBm) (radar detection)
- 5560 MHz [112] (27.0 dBm) (radar detection)
- 5580 MHz [116] (27.0 dBm) (radar detection)
- 5590 MHz [118] (27.0 dBm) (radar detection)
- 5600 MHz [120] (27.0 dBm) (radar detection)
- 5620 MHz [124] (27.0 dBm) (radar detection)
- 5630 MHz [126] (27.0 dBm) (radar detection)
- 5640 MHz [128] (27.0 dBm) (radar detection)
- 5660 MHz [132] (27.0 dBm) (radar detection)
- 5670 MHz [134] (27.0 dBm) (radar detection)
- 5680 MHz [136] (27.0 dBm) (radar detection)
- 5700 MHz [140] (27.0 dBm) (radar detection)
- 5745 MHz [149] (disabled)
- 5755 MHz [151] (disabled)
- 5765 MHz [153] (disabled)
- 5785 MHz [157] (disabled)
- 5795 MHz [159] (disabled)
- 5805 MHz [161] (disabled)
- 5825 MHz [165] (disabled)
- 5835 MHz [167] (disabled)
- 5845 MHz [169] (disabled)
- 5855 MHz [171] (disabled)
- 5865 MHz [173] (disabled)
- 4920 MHz [-16] (disabled)
- 4940 MHz [-12] (disabled)

- 4960 MHz [-8] (disabled)
- 4980 MHz [-4] (disabled)
- 6040 MHz [208] (disabled)
- 6060 MHz [212] (disabled)
- 6080 MHz [216] (disabled)

You should observe several frequencies that are marked *disabled*. This indicates that the card supports these frequencies, but cannot use them because of Belgian regulations. Also, several frequencies should be marked with *radar detection*. These can be used, but special mechanisms must be put in place in order to avoid interference with radar installations (e.g. airport radar).

Exercise 2: Available UA hotspots

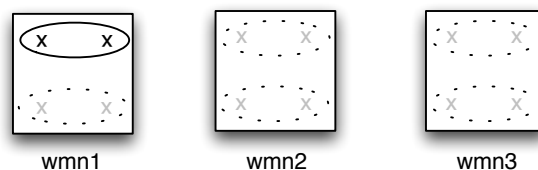


Figure 2.1: Channel separation setup 1

1. Start by building the setup as illustrated in figure 2.1.

⚠ Remark that it is not necessary to configure the SSID or channel, but bring up the interface to activate it.

2. Find out which access points (APs) are active using `iw wlan0 scan`. This command provides an interface to list various settings from the wireless network interface card (wNIC). The manpage or command line help should be self-explanatory.
3. Fill in the following table:

L2-2-1

SSID	frequency(MHz)	BSS
UA-guest	2412	84:d4:7e:27:c0:61
mosaic	2412	08:76:ff:b4:09:c3
eduroam	2412	84:d4:7e:27:b5:80
UA-guest	2412	84:d4:7e:27:b5:81
UAntwerpen	2412	84:d4:7e:27:b5:82
Wireless Antwerpen PATS test	2437	00:1d:7e:1b:11:83
mosaic	2437	08:76:ff:4c:0e:9e
G233	2462	04:1e:64:f2:13:b1
UAntwerpen	2462	00:0b:86:a6:25:75
eduroam	2462	84:d4:7e:27:bc:00
UA-guest	2462	84:d4:7e:27:bc:01
UAntwerpen	2462	84:d4:7e:27:bc:02
eduroam	2462	84:d4:7e:27:a3:e0
UA-guest	2462	84:d4:7e:27:a3:e1
UAntwerpen	2462	84:d4:7e:27:a3:e2
Jan's Wi-Fi Network	2462	f0:99:bf:0c:be:38
TelenetWiFree	2462	06:53:7c:31:a4:85
eduroam	5180	84:d4:7e:27:c2:10
UA-guest	5180	84:d4:7e:27:c2:11
UAntwerpen	5180	84:d4:7e:27:c2:12
community-lab.net	5180	02:ca:ff:ee:ba:be
G233	5220	04:1e:64:f2:13:b2
eduroam	5260	84:d4:7e:27:b5:90
UA-guest	5260	84:d4:7e:27:b5:91
UAntwerpen	5260	84:d4:7e:27:b5:92
eduroam	5300	84:d4:7e:27:c0:70
UA-guest	5300	84:d4:7e:27:c0:71
UAntwerpen	5300	84:d4:7e:27:c0:72
CONFINE-J	5500	dc:9f:db:48:ba:ee
CONFINE-I	5520	dc:9f:db:48:b8:eb
eduroam	5580	84:d4:7e:27:a3:f0
UA-guest	5580	84:d4:7e:27:a3:f1
UAntwerpen	5580	84:d4:7e:27:a3:f2
CONFINE-H	5660	00:0c:42:c3:97:a2
CONFINE-K	5660	dc:9f:db:48:ed:51

2.2 Channel Separation

Exercise 3: Channel overhearing

No. ↓	Time	Source	Destination	Protocol	Info
1	0.000000	ArubaNet_a6:26:80	Broadcast	IEEE 802.11	Beacon frame, SN=2648, FN=0, BI=100, SSID: "UA-vpn"
2	0.001109	ArubaNet_a6:26:81	Broadcast	IEEE 802.11	Beacon frame, SN=2649, FN=0, BI=100, SSID: "UA-visit"
3	0.001684	ArubaNet_a6:26:82	Broadcast	IEEE 802.11	Beacon frame, SN=2650, FN=0, BI=100, SSID: "UA-dwep"
4	0.002089	ArubaNet_a6:26:83	Broadcast	IEEE 802.11	Beacon frame, SN=2651, FN=0, BI=100, SSID: "UA-tkip"
5	0.002511	ArubaNet_a6:26:84	Broadcast	IEEE 802.11	Beacon frame, SN=2652, FN=0, BI=100, SSID: "UA-aes"

▶ Frame 1 (126 bytes on wire (126 bytes captured))
▼ Radiotap Header v0, Length 26
Header revision: 0
Header pad: 0
Header length: 26
▶ Present flags: 0x0000186f
MAC timestamp: 7916884150
▶ Flags: 0x12
Data Rate: 1.0 Mb/s
Channel: 5
Channel frequency: 2432
Channel type: 802.11g (0x0480)
SSI Signal: -73 dBm
SSI Noise: -96 dBm
Antenna: 1
SSI Signal: 23 dB
▶ IEEE 802.11
▼ IEEE 802.11 wireless LAN management frame
▶ Fixed parameters (12 bytes)
▼ Tagged parameters (60 bytes)
▶ SSID parameter set: "UA-vpn"
▶ Supported Rates: 1.0(B) 2.0(B) 5.5 11.0
▶ DS Parameter set: Current Channel: 6
▶ (TIM) Traffic Indication Map: DTIM 0 of 1 bitmap empty
▶ Country Information: Country Code: BE, Any Environment
▶ Power Constraint: Tag 32 Len 1
▶ ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
▶ Extended Supported Rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
▶ Reserved tag number: Tag 171 Len 11

Figure 2.2: Channels in a captured beacon frame.

In the previous exercise, you made an overview of a lot of access points. The next exercise will illustrate the channel overhearing. The information about which channel an AP is working on, is provided in the beacon frames the AP periodically transmits. In figure 2.2, a Wireshark [?] screen shot shows a beacon frame. The Radiotap header indicates the frame was received on channel 5, while the beacon's content shows the AP sending this beacon only operates at channel 6. Channels are thus not cleanly separated. In the next exercise you'll create an overview of the channel overhearing.

1. Start from the setup as shown in figure 2.3.

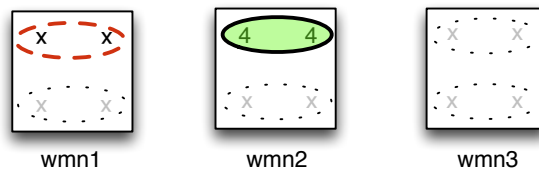


Figure 2.3: Setup for exercise 3.

! Note that the AP should be configured in channel 4 from the b/g range. To be able to do this, you should change the line `hw_mode=a` to `hw_mode=b` in the `hostapd.conf` file.

2. On station (STA)1, on every channel, make a capture `/mnt/L2-3-1.chanID.pcap`
3. Use the following wireshark display filter to only show beacons:
`wlan.fc.type_subtype == 8`
4. Fill out the following table using the obtained information.

L2-3-1

Selected channels	Observed channels in received beacons
1	1,4
2	1,4
3	1,4,6
4	4,6
5	4,6
6	4,6
7	6
8	4,6
9	11,4,6
10	11,4
11	11,4

From this exercise, it should be clear that the channels within the IEEE 802.11b/g range are not strictly separated. Figure 2.4¹ gives you an idea why: the consecutive

¹By Michael Gauthier, Wireless Networking in the Developing World [CC-BY-SA-3.0 (<http://creativecommons.org/licenses/by-sa/3.0>)], via Wikimedia Commons

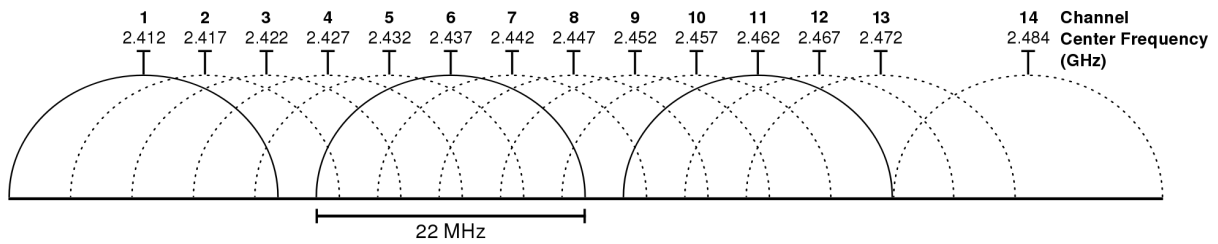


Figure 2.4: 2.4 GHz channels

channels overlap to a certain extent. Therefore, a careful channel planning is crucial in building and deploying wireless networks on these frequencies. In the next exercise, we will take a look at the channel separation in the IEEE 802.11a band.

Exercise 4: Channel separation in IEEE 802.11a

1. Now, change the AP so that it is on channel x.
2. Using `tcpdump` as in the previous exercise, find out in which channels IEEE 802.11a the beacons of this AP can be seen. Save your traces in `/mnt/L2-4-1.chanID.pcap`

L2-4-1

The beacons from our channel could be found in channel 36 and not anymore in channel 40.

2.3 Using the Wireless Channel

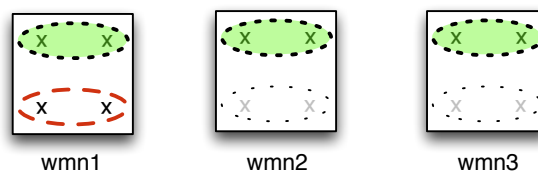


Figure 2.5: Basic ad-hoc network.

Exercise 5: Beacons

In the next few exercises, we will again use an ad-hoc network setup. It is best to reboot the devices before proceeding.

1. Create the network setup as shown in figure 2.5. Perform the following commands on all three stations. Substitute `nodeNumber` with a different number (e.g. 1, 2 and 3) on each node.

```
wmn:~# iw dev wlan0 set type ibss
wmn:~# ip addr add fc00:grID::nodeNumber/64 dev wlan0
wmn:~# ifconfig wlan0 up
wmn:~# iw dev wlan0 ibss join wmn-grID-A <frequency>
```

2. Put interface wlan1 of STA1 in monitor mode on the same frequency.

```
STA1:~# iw dev wlan1 set type monitor
STA1:~# ifconfig wlan1 up
STA1:~# iw dev wlan1 set freq <frequency>
```

3. Check if all stations can reach each other.
4. Perform a `tcpdump` on the monitor interface. Save it to `/mnt/L2-5-1.STA1.pcap`. Let it run for a few seconds and then stop the trace.
5. In your trace file, you should observe beacon frames. Carefully inspect one of the beacon frames in this trace and compare it to a beacon frame captured in the previous exercise (exercise 4). Give the packet IDs of the beacon frames you are comparing and identify the differences in the management frame part.

L2-5-1

For this exercise, we will be comparing packet 2 from traces/L2-4-1.36.pcap and packet 2 from traces/L2-5-1.STA1.pcap. For the purpose of comparing the WLAN management frames, I have included them below:

For the beacon frame captured in exercise 4:

```
1 IEEE 802.11 wireless LAN management frame
   Fixed parameters (12 bytes)
3   Timestamp: 0x00000000082f503b
   Beacon Interval: 0,102400 [Seconds]
5   Capabilities Information: 0x0001
   .... ..1 = ESS capabilities: Transmitter is an
   AP
7   .... ..0. = IBSS status: Transmitter belongs to a
   BSS
   .... ..0. .... 00.. = CFP participation capabilities: No
   point coordinator at AP (0x0000)
```

```

9          .... ...0 .... = Privacy: AP/STA cannot support WEP
          .... ..0. .... = Short Preamble: Not Allowed
11         .... ..0.. .... = PBCC: Not Allowed
          .... 0... .... = Channel Agility: Not in use
13         .... ..0 .... = Spectrum Management: Not Implemented
          .... .0.. .... = Short Slot Time: Not in use
15         .... 0... .... = Automatic Power Save Delivery: Not
          Implemented
          ....0 .... = Radio Measurement: Not Implemented
17         ..0. .... = DSSS-OFDM: Not Allowed
          .0.. .... = Delayed Block Ack: Not Implemented
19         0... .... = Immediate Block Ack: Not Implemented
Tagged parameters (28 bytes)
21     Tag: SSID parameter set: wmn-1-A
        Tag Number: SSID parameter set (0)
23     Tag length: 7
        SSID: wmn-1-A
25     Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [
        Mbit/sec]
        Tag Number: Supported Rates (1)
27     Tag length: 8
        Supported Rates: 6(B) (0x8c)
29     Supported Rates: 9 (0x12)
        Supported Rates: 12(B) (0x98)
31     Supported Rates: 18 (0x24)
        Supported Rates: 24(B) (0xb0)
33     Supported Rates: 36 (0x48)
        Supported Rates: 48 (0x60)
35     Supported Rates: 54 (0x6c)
        Tag: DS Parameter set: Current Channel: 36
37     Tag Number: DS Parameter set (3)
        Tag length: 1
39     Current Channel: 36
        Tag: Traffic Indication Map (TIM): DTIM 1 of 0 bitmap
41     Tag Number: Traffic Indication Map (TIM) (5)
        Tag length: 4
43     DTIM count: 1
        DTIM period: 2
45     Bitmap control: 0x00
          .... ...0 = Multicast: False
47     0000 000. = Bitmap Offset: 0x00
        Partial Virtual Bitmap: 00

```

for the beacon frame captured in exercise 5:

```

IEEE 802.11 wireless LAN management frame
2     Fixed parameters (12 bytes)
        Timestamp: 0x00000000a53c0aa
4     Beacon Interval: 0,102400 [Seconds]
        Capabilities Information: 0x0002

```

```

6      .... 0 = ESS capabilities: Transmitter is a
      STA
      .... 1. = IBSS status: Transmitter belongs to
8      an IBSS
      .... 00.. = CFP participation capabilities:
      Station is not CF-Pollable (0x0000)
10     .... 0 .... = Privacy: AP/STA cannot support WEP
      .... 0. .... = Short Preamble: Not Allowed
12     .... 0... .... = PBCC: Not Allowed
      .... 0... .... = Channel Agility: Not in use
14     .... 0 .... .... = Spectrum Management: Not Implemented
      .... 0... .... = Short Slot Time: Not in use
      .... 0... .... = Automatic Power Save Delivery: Not
      Implemented
16     ...0 .... .... = Radio Measurement: Not Implemented
      ..0. .... .... = DSSS-OFDM: Not Allowed
18     .0.. .... .... = Delayed Block Ack: Not Implemented
      0... .... .... = Immediate Block Ack: Not Implemented
20 Tagged parameters (32 bytes)
      Tag: SSID parameter set: wmn-1-A
22     Tag Number: SSID parameter set (0)
      Tag length: 7
24     SSID: wmn-1-A
      Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [
      Mbit/sec]
26     Tag Number: Supported Rates (1)
      Tag length: 8
28     Supported Rates: 6(B) (0x8c)
      Supported Rates: 9 (0x12)
30     Supported Rates: 12(B) (0x98)
      Supported Rates: 18 (0x24)
32     Supported Rates: 24(B) (0xb0)
      Supported Rates: 36 (0x48)
34     Supported Rates: 48 (0x60)
      Supported Rates: 54 (0x6c)
36     Tag: IBSS Parameter set: ATIM window 0x0
      Tag Number: IBSS Parameter set (6)
38     Tag length: 2
      Atim Windows: 0x0000
40     Tag: Vendor Specific: Microsof: WMM/WME: Information Element
      Tag Number: Vendor Specific (221)
42     Tag length: 7
      OUI: 00-50-f2
44     Vendor Specific OUI Type: 2
      Type: WMM/WME (0x02)
46     WME Subtype: Information Element (0)
      WME Version: 1
48     WME QoS Info: 0x00
      0... .... = U-APSD: Disabled
50     .... 0000 = Parameter Set Count: 0x00
      .000 .... = Reserved: 0x00

```

A first difference we observed is that the capabilities information beacon frame captured in exercise 5 contains different capabilities information than the one captured in exercise 4: the ex5 beacon frame shows that the sender of the beacon frame is a STA and that the network is an ad-hoc network, while in exercise 4 the capabilities reflect that the transmitter is an AP and the network is not ad-hoc. For the tagged parameters section, the ex5 beacon is bigger. It contains some IBSS parameters (ATIM) and vendor specific information about the ad-hoc network. In the ex4 beacon, the tagged parameters contain information about the channel and the Traffic Indication Map.

6. Start a new trace on the monitor interface and save it to `/mnt/L2-5-2.STA1.pcap`
7. While the trace is running, perform two ping tests. You may perform them simultaneously, but it will be easier to answer the next question if you perform them consecutively.
STA2:~# `ping6 -c 5 fc00:grID::3`
STA3:~# `ping6 -s 1400 -c 5 fc00:grID::1`
8. Open your trace file and filter out the beacon frames with the following display filter: `!(wlan.fc.type_subtype == 0x08)`. Apart from the data frames, which kind of frames do you observe?

L2-5-2

The frames other than data (data being QoS Null, Null and Data) (Keeping in mind, not all of these were packets related to what we were doing)

- Action, ie 4380
- Request-To-Send packet 2294
- Clear-To-Send packet 2295
- 802.11 Block Ack 2544
- Acknowledgement, ie 2259
- Probe Response ie 2601
- Probe Request ie 2740
- data = icmp ??
- neighbour discovery stuff?

- VHT NDP Announcement ie 716
-

9. Explain the purpose of those frames.

L2-5-3

The purpose of each of these frames:

- Action, ie 4380 : Action Frames are a type of management frame used to trigger an action in the cell. In this case, a request to group ACK's (add block ack request) into frames before sending them.
 - Request-To-Send packet 2294 : RTS frames are used in the RTS/CTS mechanism and allow stations to request the medium for an amount of time. During that time, the station will be able to send uninterrupted and / or without another station becoming active and causing interference.
 - Clear-To-Send packet 2295 : CTS confirms a RTS request, granting a station the medium for some amount of time.
 - 802.11 Block Ack 2544 : Acknowledgements of multiple frames, grouped together into one block ack packet.
 - Acknowledgement, ie 2259 : used to acknowledge the reception of a frame or packet.
 - Probe Response ie 2601 : Response to a probe request, contains the SSID of the network, information about rates, the kind of network (ad hoc or managed by AP) and the mac address of the AP if there is one, along with various other statistics about the network, in this case about eduroam.
 - Probe Request ie 2740 : Packet broadcast by a station that wants to know what SSID's are available. It is possible for the wanted SSID to be specified in the probe request, in which case we would call it a directed probe request. In this case, the request was simply broadcast.
 - data = icmp ??
 - neighbour discovery stuff?
 - VHT NDP Announcement ie 716 : 802.11ac specific, used in the VHT sounding procedure and beamforming.
-

Exercise 6: Request to Send (RTS)/Clear to Send (CTS)

For this exercise, you will study the RTS/CTS mechanism. This mechanism will clear the channel for each transmission, minimizing the chance of collisions in the channel.

A threshold value is used to determine if RTS/CTS should be used. Larger packets will receive RTS/CTS protections while smaller packets will not. Using RTS/CTS for small packets adds a lot of overhead and hence degrades performance.

1. Start from the setup as for the previous exercise.
2. The RTS/CTS threshold will be set with `iwconfig wlan0 rts 1000`. Perform this command on all nodes.
3. Performing the same `ping6` commands as in the previous exercise. Start a capture session on the monitor interface and save it to `/mnt/L2-6-1.STA1.pcap`
4. You should observe RTS/CTS packets. Which packets are protected by this mechanism? Give an example (packet ID).

L2-6-1

The RTS/CTS exchange in packet slots 1611 and 1612 protects the ping request from STA3 to STA1 in slot 1613. The first ping exchange did not have a RTS/CTS protection because the size of the packets was not high enough at that point. In general, packets that exceed 1000 bytes in size are protected by a RTS/CTS, because that is what we set the threshold to.

5. Compare an RTS and CTS frame. How do they differ? Illustrate using frames from your last trace file.

L2-6-2

Comparing the packets in 1611 (RTS) and 1612 (CTS), we immediately see that the RTS is targeted to the desired receiver while the CTS is broadcast. The RTS message is 6 bytes longer than the CTS message and the important differences are in the final field: for RTS it is 802.11 Request To Send and for CTS it is IEEE 802.11 Clear To Send. The difference in size is because the L2 address of the transmitter of the CTS packet is not included in the CTS, while it is included for the RTS. Aside from that, not much differences can be observed: subtypes and such are different as expected.

As you can see in the RTS/CTS frames, they do not contain any information about the network on which they are transmitted. The RTS/CTS is meant to avoid collisions on the wireless medium, so any node that receives a CTS frame is required to remain silent for the duration included in the CTS frame. The only exception, for obvious reasons, is

the node to which the CTS frame is sent. Capturing RTS/CTS frames (or acknowledgement frames) on a certain channel is always a good indication that some activity is going on in that channel, even if it is impossible to overhear the actual data transmission.

2.4 IEEE 802.11n

Until now, we have only used the wnic's in IEEE 802.11a or b/g mode. "b" is the oldest mode. "g" improves upon "b" by offering significantly higher maximal throughput (54 Mbps versus 11 Mbps). "a" operates at different frequencies and offers the same throughput as "g".

Another mode of operation is called "n". IEEE 802.11n is an amendment to the IEEE 802.11 standard in order to improve throughput over both "a" and "g". It operates at both frequency bands and is defined for bit rates up to 600 Mbps, but very few setups will be able to obtain these speeds.

IEEE 802.11n can use different optimizations, such as the multiple-input, multiple-output (MIMO) principle, 40 MHz wide channels (versus 20 MHz in IEEE 802.11a/b/g), and frame aggregation to improve throughput. The following exercise will demonstrate that IEEE 802.11n channels can indeed be twice as wide as those in IEEE 802.11a, and thus interfere with adjacent IEEE 802.11a channels.

Exercise 7: IEEE 802.11n

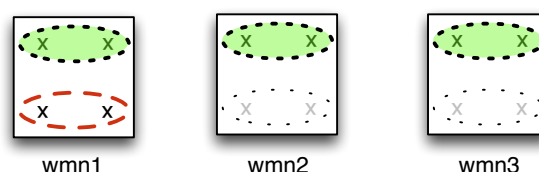


Figure 2.6: IEEE 802.11n ad-hoc network.

As this exercise will use both channels allocated to the mobile and wireless lab, two groups cannot perform this exercise at the same time! Check if no other group is currently working on this course!

1. Reboot all devices. In order to enable IEEE 802.11n mode without any problems, we will start from a blank setup.
2. After they have been rebooted, perform the following on all devices in order to create an ad-hoc network with IEEE 802.11n support in the 5 GHz band:


```
STA:~# iw dev wlan0 set type ibss
STA:~# ip addr add fc00:grID::nodeNumber/64 dev wlan0
STA:~# ifconfig wlan0 up
STA:~# iw dev wlan0 ibss join wmn-grID-A 5180 HT20
```

3. Check that all nodes can reach each other.
4. Set up a monitor interface on channel 36 (5180 MHz) on STA1.
5. Start a trace on the monitor interface and save it to /mnt/L2-7-1.STA1.pcap
6. Start a ping from STA2 to STA3 and from STA3 to STA1. Like before, use different ping sizes:
STA2:~# ping6 -c 5 fc00:grID::3
STA3:~# ping6 -s 1400 -c 5 fc00:grID::1
7. Filter out the beacon frames from your trace. Do you observe packets from both ping sessions? Did you see all packets from these sessions? Why or why not?

L2-7-1

We observed packets of both ping sessions, from the first session only the replies were caught on the monitor interface and for the second session, all ping packets were seen by the monitor.

Not seeing the ping requests of the first ping session could be due to failed demodulations at the monitor, causing it to be not be able to detect the modulated messages sent by STA1 in the first ping session. Because the second ping transmission does originate at STA2, it is less of an issue and that ping traffic is captured without issue. The sniffer machine is not in range of the target wireless devices, or there's too much interference, so the sniffer machine's radio can't successfully demodulate the transmissions. Note that the increasing use of beamforming helps devices steer their RF energy right to where the intended receiver is, which means less of that energy goes to where the sniffer machine is, meaning the sniffer will get a worse signal:noise ratio, and less likelihood of demodulating packets sent at the highest data rates.

8. Set the monitor interface to channel 40 (5200 MHz).
9. Perform the same ping test again, but now save your trace to /mnt/L2-7-2.STA1.pcap
10. Did you capture any packets?

L2-7-2

No packets of the ping exchanges were caught. This is expected since we are now monitoring a different channel.

Exercise 8: 40 MHz channels

In the previous exercise, we enabled IEEE 802.11n, but we did not enable 40 MHz wide channels yet. We will do that now.

1. Deconfigure all wlan0 interfaces.

```
STA:~# iw dev wlan0 ibss leave
```

2. Now, create an ad-hoc network that uses 40 MHz wide channels:

```
STA:~# iw dev wlan0 ibss join wmn-0-A 5180 HT40+
```

3. As in the previous exercise, set the monitor interface of STA1 on channel 36 and perform a capture while sending both pings. Save it to /mnt/L2-8-1.STA1.36.pcap
4. Do the same again, but this time monitor channel 40.
Save your trace in /mnt/L2-8-1.STA1.40.pcap
5. Do you observe any different behaviour in the trace file on channel 36, compared to the previous exercise?

L2-8-1

No, the behaviour is largely the same: we again capture some icmp traffic but it is again not the complete conversation. Because the stations are using the 36 channel (albeit with 40 MHz bands) and we are capturing on channel 36, we capture some icmp packets. The 40 MHz wide bands indicate that the network has a "main" channel, in this case being 36, and extra space to be used if need be. Because our icmp traffic is not enough to fill up the main channel, the extra space remains (largely) unused and we thus observe the same behaviour as in the previous exercise where we only capture part of the icmp exchange.

6. In the trace file on channel 40, which packets have you captured? Why?

L2-8-2

Monitoring on channel 40, we captured no traffic. This is due to the extra space remaining largely unused: only on the 36 channel we would see any of our icmp traffic.

Acronyms

AP access point

BIPT Belgisch Instituut voor Postdiensten en Telecommunicatie - Belgian Institute for Postal services and Telecommunications

CTS Clear to Send

grID group ID

MIMO multiple-input, multiple-output

nic network interface card

RTS Request to Send

STA station

wmn wireless mesh node

wnic wireless network interface card