Advanced Networking Lab

Johan Bergs Bart Braem

February 23, 2017

Lab 1

Basic Configurations

The goal of the first lab is to make you acquainted with the hardware and software needed to perform the tasks in other modules. Furthermore we will have a look at the various sniffing possibilities in wireless networks.

1.1 Device Exploration

Have a closer look a the devices used for this course.

Exercise 1: Getting to know the interfaces

1. Log in on wireless mesh node (wmn)1.
   `ssh root@wmn1`

2. When asked to give a name, enter `AP`

3. Get a list of all available interfaces.
   `AP:~# ifconfig -a`

4. List the interfaces and their Media Access Control (MAC) addresses.
   L1-1-1

eth0	00:0D:B9:25:C5:70
lo	N/A
wlan0	D4:CA:6D:12:1B:A4
wlan1	00:0E:8E:20:83:DF

5. A MAC address is unique per card, but also carries a generic part, identifying the vendor of a card. List the prefixes and find out the vendors (name) of all different interfaces found in the node.

   Google is your friend!

   L1-1-2

eth0	00:0D:B9	PcEngine
lo	N/A	N/A
wlan0	D4:CA:6D	Routerboard.com
wlan1	00:0E:8E	Sparklan

1.2 Access Point Setup

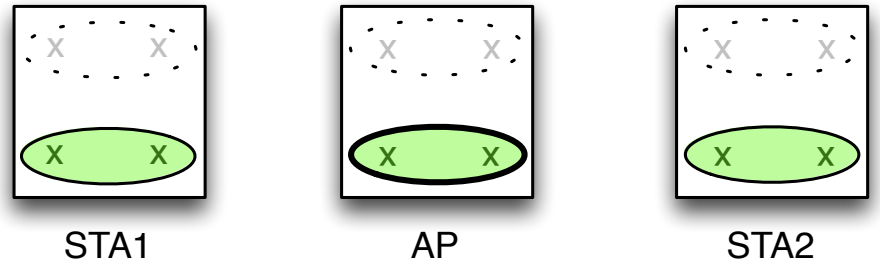

Figure 1.1: The basic infrastructure setup

The goal is to create a basic infrastructure setup as can be found at home. The setup consists of one access point (AP) and two connected stations as shown in figure 1.1. In this case, two laptops are connected to the same AP and can communicate to each other. We will not consider any communication to the outside world.

1.2.1 AP Configuration

To set up this basic infrastructure network, start by configuring the AP.

Exercise 2: Set up an AP

1. Check the wireless parameters of wlan1:
   `AP:~# iwconfig wlan1`

   This should give you some output like

```
wlan1     IEEE 802.11abgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=0 dBm
          RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

   Remark that we did not configure the interface yet!

   Give an explanation for all available parameters which are displayed using `iwconfig` (hint: man pages).
   L1-2-1

Output of the command *iwconfig wlan1*

```
wlan1     IEEE 802.11abgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=0 dBm
          RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

- **IEEE 802.11agbn**: - This first field shows which wireless MAC technologies the device supports on that interface.
- **ESSID:off/any** - The second field specifies the network name (if any) of a network consisting of a group of cells connected via repeaters or infrastructure where users may roam between the cells. When this field is set to off or any, ESSID checking is disabled.

- **Mode:managed**: Specifies the operating mode of the device and tells us what kind of network it operates in as well as what the function of the node is in the network.
  I this case the mode is set to Managed which means that the node connects to a network composed of many access points where roaming is enabled.

- **Access Point**: Specifies which access point the card is connected to. When configuring, it is possible to specify which access point the card should try to register to. An access point can be chosen, it can be set to ”any”, ”auto” or ”off”.
- **Tx-power=0dBm**: For network cards supporting multiple transmit powers, this setting allows you to set the transmit power in dBm. It also allows you to specify power control and radio using ”auto”, ”fixed” and ”on” or ”off” respectively.

- **RTS thr:off**: This parameter specifies when the RTS/CTS mechanism will be used and can be set to ”auto”, ”fixed” and ”off”. RTS/CTS adds overhead but increases throughput in situaties with hidden nodes or a large number of active nodes.

- **Fragment thr:off**: Similar to the RTS threshold this parameter can be ”auto”, ”fixed” or ”off” and allows you to specify the maximum fragment size. Fragmentation can reduce error penalties in a noisy environment. On some cards, this threshold can be higher than the maximum packet size which will enable Frame Bursting.

- **Encryption key:off**: This parameter allows manipulation of encryption, scrambling keys and security mode. It can be used to change security keys, disable or enable encryption and change the security mode (implications of this are dependent on the type of card).

- **Power Management:off**: Used to manipulate power management scheme parameters and mode. It allows you to disable or enable power management as well as specify which types of packets should be received and choose the period between wake ups.

---

2. Configure the wlan1 interface using your assigned channel and the extended Service Set ID (ESSID):

```
interface=wlan
driver=nl80211
logger_syslog=-1
logger_syslog_level=2
logger_stdout=-1
logger_stdout_level=2
debug=4
hw_mode=a
channel=x
macaddr_acl=0
auth_algs=3
eapol_key_index_workaround=0
eap_server=0
wpa=0
ssid=wmn-gid-A
```

This file can be found on the devices as `hostapd.conf`. Edit it to change the channel number, interface name and ESSID, and then perform the following:
`AP:~# hostapd -B hostapd.conf`

`AP:~# iwconfig` should now return something like:

```
wlan1     IEEE 802.11abgn  Mode:Master  Tx-Power=20 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off
```

1.2.2 Station Configuration

Exercise 3: Configuring the wireless stations

We will now configure *both* stations and verify they get associated with the AP you just created. Make sure to repeat the commands to configure the second station.

1. Bring up the interface:
   `STA1:~# ifconfig wlan1 up`

2. Configure the interface to connect to our AP:
   `STA1:~# iw dev wlan1 connect wmn-grID-A`

3. Do the same on station (STA)2.

When you run `iwconfig`, the `Access Point` parameter should show the MAC address of the AP and show identical frequencies and ESSIDs on both stations.

```
wlan1     IEEE 802.11abgn  ESSID:"wmn-0-A"
          Mode:Managed  Frequency:5.24 GHz  Access Point: 00:00:11:22:33:44
          Bit Rate=1 Mb/s   Tx-Power=5 dBm
          RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=12/70  Signal level=-164 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:4   Missed beacon:0
```

4. What parameters are different in your output compared to the output above?
L1-3-1

- ESSID is set to wmn-1-A and not wmn-0-A
- Frequency: 5.18GHz and not 5.24GHz because we used channel 36.
- Access Point shows the MAC Address of our AP.
- Bitrate: 6Mb/s and not 1Mbs.
- Tx-Power: set to 20 dBm and not 5 dBm.
- Link quality: set to 48/70 and not 12/70.
- Sign level: set to -62 dBm and not -164 dBm.
- Invalid misc: We had 6 packets lost that were not caused by hardware failure and not 4.

If the output for both stations confirms the association between the two wireless stations and the AP, the actual L2 connection between these three devices is up and running. To verify the connection, we will configure IP addresses on the stations and have them communicate.

Exercise 4: Verifying the basic setup

1. Configure the IP address of STA1 and STA2:
```
STA1:~# ip addr add fc00::grID::1/64 dev wlan1
STA2:~# ip addr add fc00:grID::2/64 dev wlan1
```

2. Start a ping session from STA1 to STA2. Give the minimum, maximum and average round trip time (RTT):
   `STA1:~# ping6 -c 30 fc00:grID::2`
   L1-4-1

Minimum RTT: 1.091ms
Maximum: 2.712ms
Avg: 1.361ms

---

3. Perform a ping between the same devices as before, but this time, use the wired IP addresses. Again write down the same values.
   L1-4-2

Minimum: 0.254ms
Maximum: 0.636ms (outlier)
Average: 0.274ms

Remark that we did not (yet) enable L3 capabilities at the AP.

1.3 Wireless Sniffing

Using the basic network we constructed in the previous section, we will go through the various sniffing modes available in wireless networks. The main difference between wired and wireless networks is obviously the fact that the transmission medium (radio waves vs. cable) is shared amongst all wireless users. Therefore, sniffing the network offers a lot more opportunities in wireless systems.

The first setup is shown in figure 1.2 and corresponds to the basic setup we created in the previous section.

Exercise 5: First scan

1. Make sure the Neighbor Discovery (ND) cache of both STAs is cleared.
   `STA2:~# ip neigh flush dev wlan1`

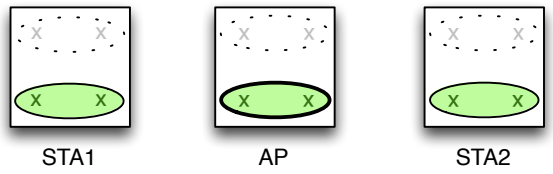

Figure 1.2: Wireless packet capture setup

```
STA1:~# ip neigh flush dev wlan1
```

You can always check the state of the cache using `ip neigh show`

2. On the AP and on both STAs, start a packet capture using `tcpdump` and save it to `/mnt/L1-5-1.snif-location.pcap`

   This is the time to make sure that you have a remote location mounted with `sshfs` in /mnt!

   ```
   AP:~# tcpdump -i wlan1 -w /mnt/L1-5-1.AP.pcap
   STA1:~# tcpdump -i wlan1 -w /mnt/L1-5-1.STA1.pcap
   STA2:~# tcpdump -i wlan1 -w /mnt/L1-5-1.STA2.pcap
   ```

3. Start a ping session from STA1 to STA2. Limit the ping to only two requests.
   `STA1:~# ping6 -c 2 fc00:grID::2`

4. Which type of packets can be seen in the AP trace file? You can open the trace file with wireshark on the remote computer.
   L1-5-1

5. Now, take a closer look at the MAC headers. Which type of link layer headers show up on the packets?
   L1-5-2

From the tracefile made on the AP, it is impossible to see if we made a wired or wireless trace. Let's more closely examine the tracefiles made on the stations, where a difference will become apparent.

Exercise 6: Scanning other interfaces

Open the trace files made on both the sending and receiving station.

1. You should observe duplicate entries. Describe which duplicates are observed in each file (use packet numbers!):
   L1-6-1

2. Take a closer look at the MAC addresses of the duplicate packets using Wireshark. What addresses are used on the frames? Are they identical?
   L1-6-2

`tcpdump` will automatically put the interface in *promiscuous mode*. This means all packets which can be read by the wireless interface will be delivered up the networking stack even though the destination MAC address does not correspond to the address of the specific card. Each interface receives all packets sent by the AP. If the destination MAC address is not that of the receiving interface, the packet is normally dropped. In promiscuous mode, however, these packets are nevertheless stored in the trace file. Now repeat the previous exercise but disable the promiscuous mode.

Exercise 7: Disabling promiscuous mode

1. Make sure the ND cache is cleared on STA1 and STA2.
   ```
   STA1:~# ip neigh flush dev wlan1
   STA2:~# ip neigh flush dev wlan1
   ```

2. On STA1, start a packet capture not using promiscuous mode using `tcpdump` and save it to `/mnt/L1-7-1.STA1.pcap`
   ```
   STA1:~# tcpdump -i wlan1 -p -w /mnt/L1-7-1.STA1.pcap
   ```

3. Start a ping session from STA2 to STA1.
   `STA2:~# ping6 -c 2 fc00:grID::1`

4. Do you still observe the duplicate entries?
   L1-7-1

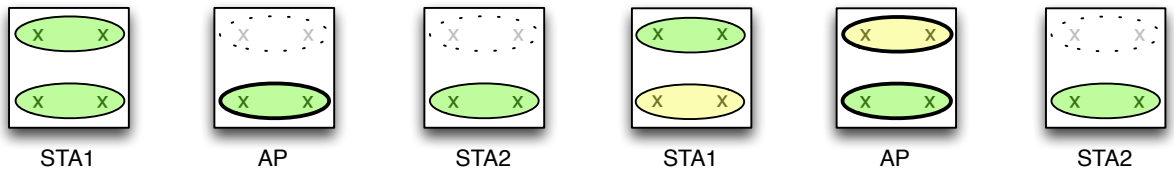

Figure 1.3: Third party scanning

Exercise 8: Third party scanning

So far, we only sniffed the network on nodes which took part of the network activity. Let's introduce another party, which just wants to listen to what is happening on the channel. Imagine a notebook eavesdropping on the traffic of a wireless cell. First we will add it to the same ESSID and later on change it to a different ESSID. The intended setups are shown in figure 1.3a and 1.3b. The first situation then compares to a situation where a laptop is connected to your home network and is sniffing the traffic of other active stations in this network, while the latter situation can be seen as you being connected to your network, trying to sniff the network of a neighbour on the same channel, but using a different network name.

We'll start from the previous setup.

It is essential that you bring `wlan1` down on STA1 first.

1. Bring `wlan1` down on STA1.
   `STA1:~# ifconfig wlan1 down`

2. Add `wlan0` of STA1 to get the setup of 1.3a:
   `STA1:~# ifconfig wlan0 up`

```
STA1:~# iw dev wlan0 connect essid wmn-grID-A
STA1:~# ip addr add fc00:grID::1/64 dev wlan0
```

3. Now, reintroduce `wlan1` of STA1 to the network.
   ```
   STA1:~# ifconfig wlan1 up
   STA1:~# iw dev wlan1 connect wmn-grID-A
   ```

4. Configure `wlan1` with the following IP address:
   ```
   STA1:~# ip addr add fc00:grID:1::1/64 dev wlan1
   ```
   Remark that this IP address belongs to a different subnet! This is in preparation of the next part of the exercise.

5. Repeat steps 1 to 3 from exercise 5 , but in step 2, start the capture only on `wlan1` of STA1 and save it to `/mnt/L1-8-1.STA1.A.pcap`

6. To change the `wlan1` interface to another ESSID, we first need another AP managing this ESSID (figure 1.3b). Configure a second AP interface on the AP node, this time using "wmn-group ID (grID)-B" as essid
   Copy the previous hostapd.conf file and change the ssid and interface.

7. Make sure `wlan1` of STA1 is connected to the wmn-grID-B network.

8. Repeat the same exercise again, saving the trace to `/mnt/L1-8-1.STA1.B.pcap`

9. Compare the results from both tests. How do these two setups compare to a wired setup?
   L1-8-1

Exercise 9: Pinging the AP

In the previous exercises, we have used the AP only as a L2 device. The AP can of course also be configured as a L3 device. We will now configure the AP as a L3 device and perform the same ping test again, but this time from STA1 to AP.

1. Add an IP address on `wlan0` of the AP:
   ```
   AP:~# ip addr add fc00:grID:1::3/64 dev wlan0
   ```

2. On STA1, start a packet capture on `wlan1` and save it to `/mnt/L1-9-1.STA1.pcap`
   `STA1:~# tcpdump -i wlan1 -w /mnt/L1-9-1.STA1.pcap`

3. Start a ping session from STA1 to AP. Limit the ping to only two requests.
   `STA1:~# ping6 -c 2 fc00:grID:1::3`

4. In the trace files, do you observe duplicate entries? Why or why not?
   L1-9-1

Exercise 10: Sniffing in monitor mode

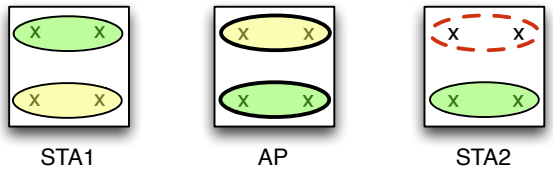

Figure 1.4: Introducing a monitoring interface.

Until now, not much difference has been observed compared to network sniffing on a wired network - apart from observing duplicate packets. In the next exercises we will broaden the setups to show the actual differences. Firstly, the monitor interface will be introduced. Configuring a wireless network interface card in monitor mode will enable you to see all traffic that is present in a certain channel. In figure 1.4 the next setup is shown. We continue from the previous setup and add an extra interface.

1. Configure the monitoring device:
   `STA2:~# iw dev wlan0 set type monitor`

2. Bring the monitor interface up:
   `STA2:~# ifconfig wlan0 up`

3. Configure the channel:
   `STA2:~# iw dev wlan0 set channel x`

Remark that it is not necessary to configure an ESSID. Why?
L1-10-1

4. Clear the ND caches:
   ```
   STA2:~# ip neigh flush dev wlan1
   STA1:~# ip neigh flush dev wlan0
   ```

5. Start a capture session on the monitor interface and save it to `/mnt/L1-10-2.STA2.pcap`
   ```
   STA2:~# tcpdump -i wlan0 -w /mnt/L1-10-2.STA2.pcap
   ```

6. Start a ping session from STA1 to STA2.
   ```
   STA1:~# ping6 -c 2 fc00:grID::2
   ```

7. Open the capture file in Wireshark.

   - What type of frames are visible within the trace? Give an example (packet number) of each.
     L1-10-2

   - What type of link layer headers are visible now?
     L1-10-3

   - A radiotap header should also be visible before the link layer header. This header is not actually transmitted, but is used to communicate transmission statistics between the driver and kernel. As such, it reports on various transmission statistics as the signal strength and the used antenna. Select a packet (give the packetID within the trace), and list which items are present. Although the format is standardized, the actual content depends on the driver and hardware used.
     L1-10-4

- Describe the path a packet takes to be delivered from one station to another. Give a detailed overview of the various addresses in the headers. Identify the frames (packet ID) from the trace you use to illustrate this.
  L1-10-5

Remember the traces you made containing duplicate packets? The duplicates can now be clearly observed in the traces from a monitor interface. Each transmission from one station to another, both connected to the same AP is always relayed over the AP. The sender thus first recorded its transmission and then detected the relayed frame on the air. Frames which are sent to an AP, are discarded by other stations. This explains why a third station did not show duplicate packets. Finally, an access point will only report one occurrence in `tcpdump` traces, as the relaying of a frame is done transparently to the kernel in the hardware/driver.

Exercise 11:

Finally, we will repeat exercise 8. We will be sending traffic on both wireless networks and monitor the channel. The setup remains unchanged (see figure 1.4).

1. Clear the ND caches as before. Be sure to delete all ND entries on all wireless network interface cards (wnics)!
2. Start a scan on the monitor interface of STA2 and save it to `/mnt/L1-11-1.STA2.pcap`
   ```
   STA2:~# tcpdump -i wlan0 -w /mnt/L1-11-1.STA2.pcap
   ```
3. Perform a ping from STA1 to AP and start a ping from STA2 to STA1, both on `wlan1`. This means we will inject traffic on both wireless networks.

   These pings can be performed consecutively. Make sure they are in the same capture session.
   ```
   STA1:~# ping6 -c 2 fc00:grID:1::3
   STA2:~# ping6 -c 2 fc00:grID::1
   ```
4. Which ping session(s) is/are visible in the trace?
   L1-11-1

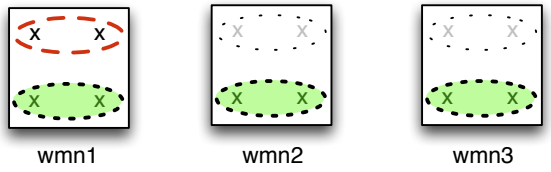

Figure 1.5: Basic ad-hoc network.

1.4 Ad-Hoc Networks

In the next section, we will set up a basic ad-hoc network. Contrary to the infrastructure network we used in the previous section, ad-hoc networks are built from identically configured hosts, without a central entity in charge. Let's start right away to build our first ad-hoc network.

Exercise 12: Basic ad-hoc network

1. To ensure all interfaces are in the default state, reboot all devices:
   ```
   AP:~# reboot
   STA1:~# reboot
   STA2:~# reboot
   ```

2. The basic setup is shown in figure 1.5. All nodes will have the same configuration: mode, ESSID and channel.
   ```
   STA1:~# iw dev wlan1 set type ibss
   STA2:~# iw dev wlan1 set type ibss
   STA3:~# iw dev wlan1 set type ibss
   ```

3. Assign IP addresses to all interfaces and activate them:
   ```
   STA1:~# ip addr add fc00:grID::1/64 dev wlan1
   STA2:~# ip addr add fc00:grID::2/64 dev wlan1
   STA3:~# ip addr add fc00:grID::3/64 dev wlan1
   STA1:~# ifconfig wlan1 up
   STA2:~# ifconfig wlan1 up
   STA3:~# iwconfig wlan1 up
   ```

4. Configure all interfaces with a ESSID and a channel:
   ```
   STA1:~# iw dev wlan1 ibss join wmn-grID-A <frequency>
   ```

```
STA2:~# iw dev wlan1 ibss join wmn-grID-A <frequency>
STA3:~# iw dev wlan1 ibss join wmn-grID-A <frequency>
```

The frequency you should use here can be found in the introduction section.

5. To monitor the traffic in the channel, set up a monitor interface on STA1:
```
STA1:~# iw dev wlan0 set type monitor
STA1:~# ifconfig wlan0 up
STA1:~# iw dev wlan0 set freq <frequency>
```

6. Scan using the monitor interface and save it to `/mnt/L1-12-1.STA1.pcap`
```
STA1:~# tcpdump -i wlan0 -w /mnt/L1-12-1.STA1.pcap
```

7. Verify that the nodes now all can reach each other:
```
STA1:~# ping6 -c 2 fc00:grID::2
STA2:~# ping6 -c 2 fc00:grID::3
STA3:~# ping6 -c 2 fc00:grID::1
```

8. Describe how data is exchanged between the various hops. How does this compare to infrastructure mode? Motivate your findings by selecting frames (give the packet ID) from the trace file and describe their MAC header and addressing scheme.
L1-12-1

9. Repeat the ping tests from exercise 4 (from STA1 to STA2 and write down the requested values. Do you observe a significant change in timings?
L1-12-2

Minimum: 0.853ms Maximum: 1.536ms Average: 1.194

Faster: not via AP but direct

Acronyms

AP access point

ESSID extended Service Set ID

grID group ID

MAC Media Access Control

ND Neighbor Discovery

nic network interface card

RTT round trip time

SSID Service Set ID

STA station

wmn wireless mesh node

wnic wireless network interface card