Lab 1

Robert Moller

June 1, 2022

ProtIoT

Part 1

1.1 Select a node, and by zooming on the "Network window", you may see three different zones (green, gray and white). What is the meaning of each zone?

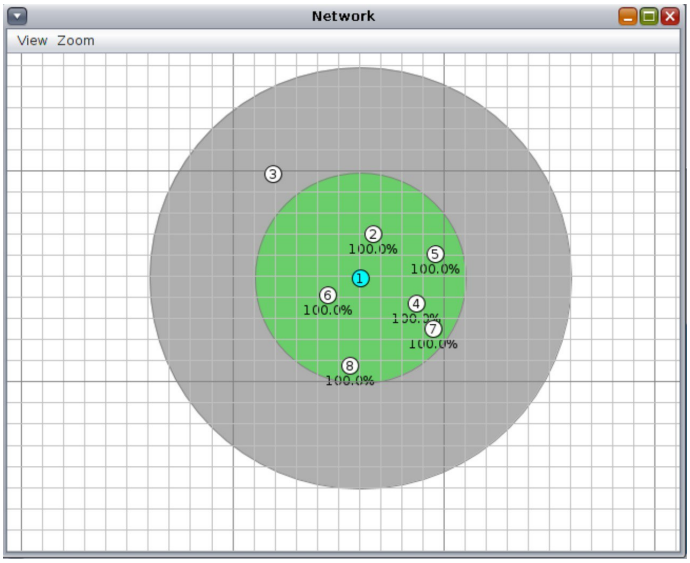

Figure 1

After clicking on a node we can see the three zones appear with the node in the centre. The green circle indicates the communication range the node is capable of transmitting to. All other node within this area can communicate with the node. Any nodes in the gray circle is not able to directly communicate with the selected node, as it is in the interference range. The nodes in the interference range might still be affected by the signal from the selected node in the form of interference on other signals or partially correct packets. The white area indicates that no signal from the selected node will reach this far, putting any node in this area it will not receive interference or partial packets.

1.2 What is the MAC layer protocol and the access method used by the motes? What is the channel check rate?

The Medium Access Control (MAC) layer protocol is in charge of collision avoidance when transmitting radio packets and is one layer above the Radio Duty Cycling (RDC) layer. It will retry the transmission if it detects a collision. Contiki doesn't do process anything on the MAC level but it uses two alternatives: Carrier Sense Multiple Access (CSMA) and NullMAC, that achieves similar results. For it's RDC layer, Contiki uses ContikiMAC which wakes up the radio in intervals checking for any activity and keeps it turned on for the duration of activity plus one interval more. The rate of which we wake the radio to check for activity is the channel check rate, and by default this is 8Hz.

1.3 At what time interval, the motes wake up? Refer to the Timeline window.

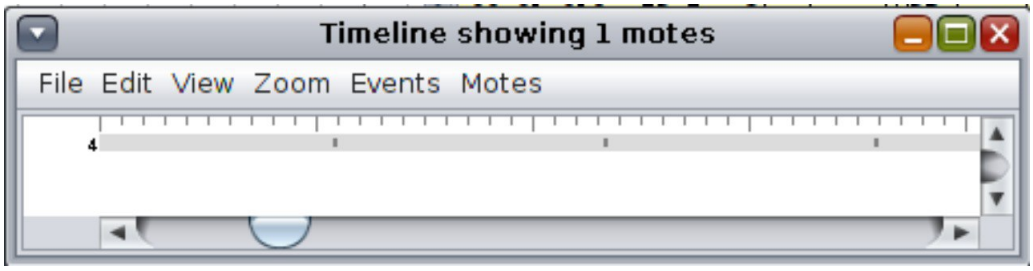

Figure 2: The radio on/off events for a single mote

From taking note of the times when the radio wakes up we can estimate that each mote wakes up approximately twice every 126ms for a duration of 1ms.

1.4 What is the rate in kbits/s of the IEEE 802.15.4?

Frequency	Data Rate
2.4 GHz	250 kb/s
915 MHz	40 kp/s
868 MHz	20 kp/s

Table 1: IEEE 802.15.4 data rate for different frequencies

As defined by IEEE 802.15.4, the data rate in kb/s is stated in Table 1 and demonstrates that a higher frequency yields a higher data rate.

Part II

Now we will create a network composed by five motes and one border router (node 1).

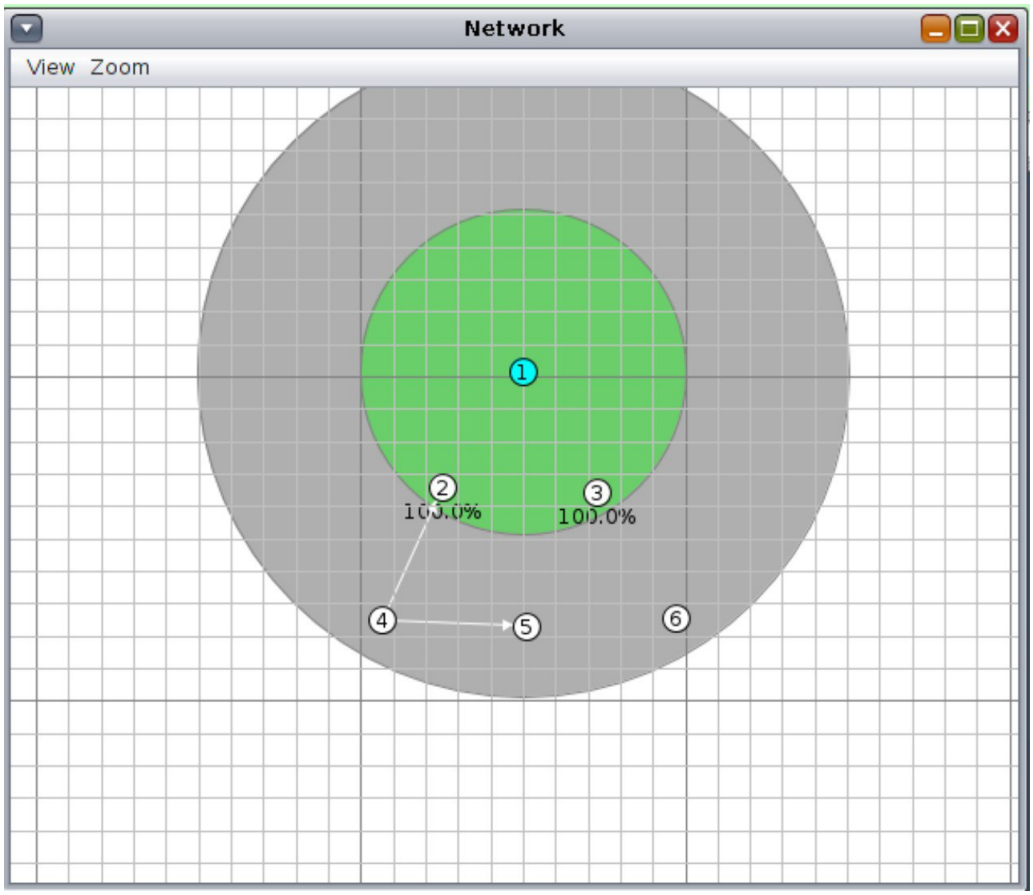

Figure 3: Network topology

2.1 What kind of pattern do you recognize?

I recognize a that each node can reach any of the other node either in their transmission range or outside through nodes within transmission range. This indicates that a peer to peer topology is applicable.

Now, we open the serial socket (server) on the RPL border router in Cooja on the node 1:

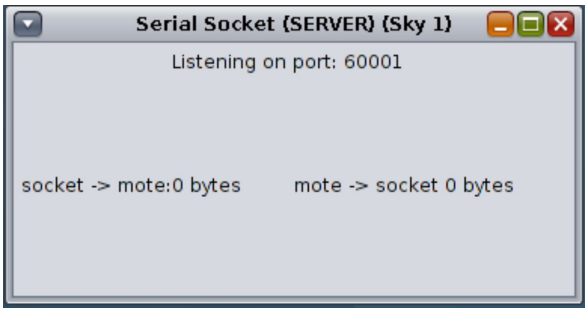

Figure 4: Serial socket for node 1

We create a channel between Cooja and the OS, and assigns the address prefix to the border router:

```
usertp@usertp-VirtualBox: ~/contiki-2.7/examples/ipv6/rpl-border-router
usertp@usertp-VirtualBox:~/contiki-2.7/examples/ipv6/rpl-border-router$ make connect-router-cooja
TARGET not defined, using target 'native'
sudo ../../../tools/tunslip6 -a 127.0.0.1 aaaa::1/64
[sudo] password for usertp:
slip connected to ``127.0.0.1:60001''
opened tun device ``/dev/tun0''
ifconfig tun0 inet `hostname` up
ifconfig tun0 add aaaa::1/64
ifconfig tun0 add fe80::0:0:0:1/64
ifconfig tun0

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:127.0.1.1  P-t-P:127.0.1.1  Mask:255.255.255.255
          inet6 addr: fe80::1/64 Scope:Link
          inet6 addr: aaaa::1/64 Scope:Global
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Figure 5: $ make connect-router-cooja

2.2 Look at the pattern of messages in Cooja now: what changed? Why?

```
01:19.418  ID:2  DATA send to 1 'Hello 1'
01:27.088  ID:1  DATA send to 1 'Hello 1'
01:44.558  ID:3  DATA send to 1 'Hello 1'
01:50.761  ID:6  DATA send to 1 'Hello 1'
02:05.835  ID:5  DATA send to 1 'Hello 2'
02:09.522  ID:4  DATA send to 1 'Hello 2'
02:14.129  ID:3  DATA send to 1 'Hello 2'
02:24.229  ID:6  DATA send to 1 'Hello 2'
02:49.520  ID:2  DATA send to 1 'Hello 2'
02:53.720  ID:1  DATA send to 1 'Hello 2'
03:04.697  ID:1  DATA send to 1 'Hello 3'
03:05.292  ID:3  DATA send to 1 'Hello 3'
03:18.590  ID:2  DATA send to 1 'Hello 3'
03:19.503  ID:6  DATA send to 1 'Hello 3'
03:26.507  ID:5  DATA send to 1 'Hello 3'
03:50.780  ID:4  DATA send to 1 'Hello 3'
04:17.681  ID:1  DATA send to 1 'Hello 4'
04:31.883  ID:4  DATA send to 1 'Hello 4'
04:38.175  ID:3  DATA send to 1 'Hello 4'
04:41.053  ID:5  DATA send to 1 'Hello 4'
```

(a) Part 1 mote output

```
25:53.820  ID:4  DATA send to 1 'Hello 25'
26:07.140  ID:4  DATA send to 1 'Hello 26'
26:13.286  ID:3  DATA send to 1 'Hello 26'
26:17.125  ID:5  DATA send to 1 'Hello 26'
26:31.387  ID:6  DATA send to 1 'Hello 26'
26:46.692  ID:2  DATA send to 1 'Hello 26'
27:06.324  ID:2  DATA send to 1 'Hello 27'
27:11.054  ID:4  DATA send to 1 'Hello 27'
27:24.425  ID:6  DATA send to 1 'Hello 27'
27:53.324  ID:3  DATA send to 1 'Hello 27'
27:59.695  ID:5  DATA send to 1 'Hello 27'
28:25.687  ID:4  DATA send to 1 'Hello 28'
28:29.683  ID:6  DATA send to 1 'Hello 28'
28:29.858  ID:1  # [1024 bytes, no line enc
28:33.581  ID:3  DATA send to 1 'Hello 28'
28:42.301  ID:2  DATA send to 1 'Hello 28'
```

(b) Part 2 mote output

Figure 6: Comparing mote output

In Fig. 6a and Fig. 6b we can see the mote output for part 1 and 2. When comparing these two we can see that the mote output in Fig. 6a appears to be seemingly random in order and all of the motes send packets towards mote 1, even itself. in Fig. 6b we can see the mote output follow a more defined pattern and every mote except the router (mote 1) is sending packets to mote 1. This is because we now have a clearly defined router at mote 1 while previously mote 1 was acting like a client.

Now we will record the simulation output in a pcap file, to be opened in Wireshark. To do so, you need to have the "Radio message" window opens, and ensuring analyze of 6LoWPAN trace pcap. If needed reload the simulation, and repeat the precedent steps. Ping the address of the node 6. Let the simulation run for some times at least 200 seconds.

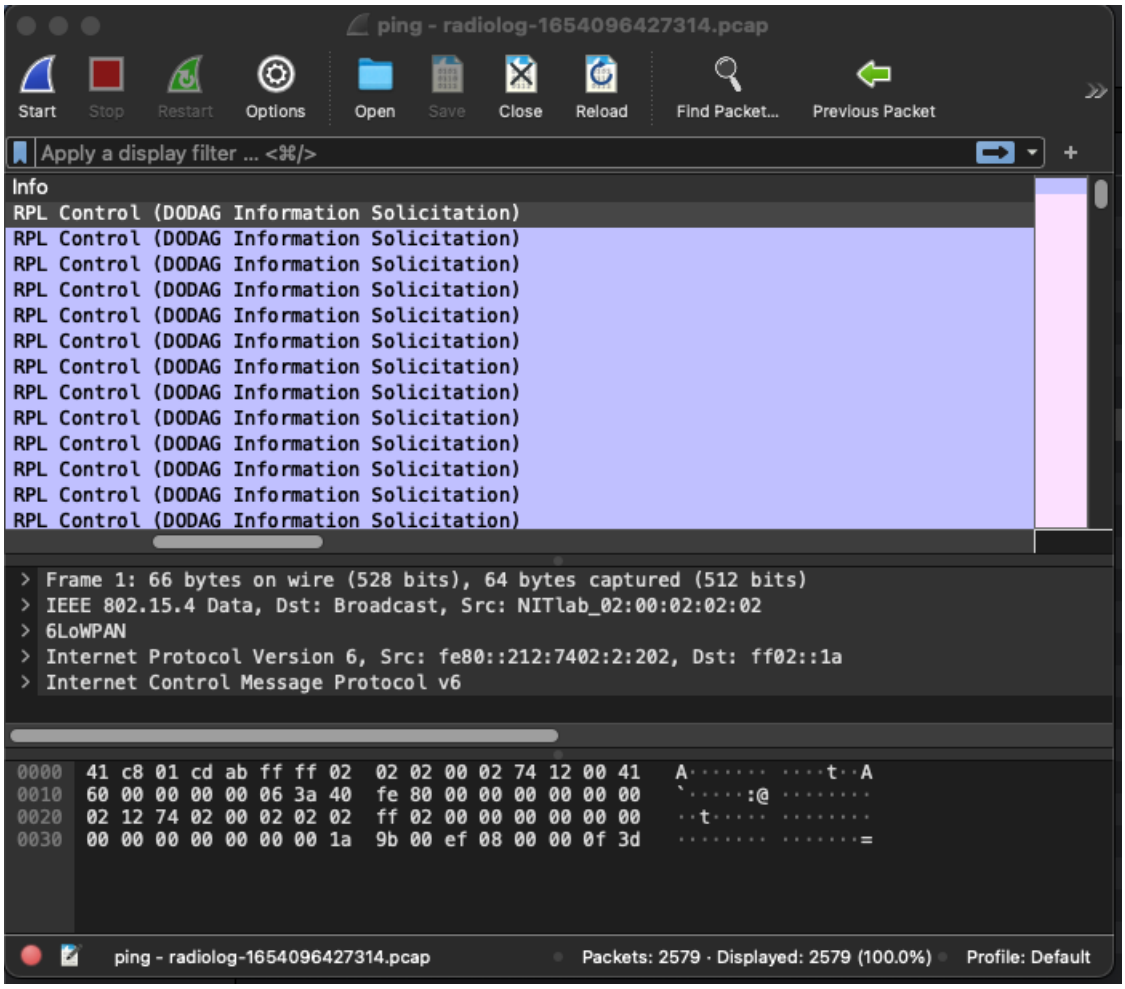

Figure 7: Wireshark on radiolog

2.a. IEEE 802.14.5

Locate the first UDP packet and extend the FCF (Frame Control Field) field.

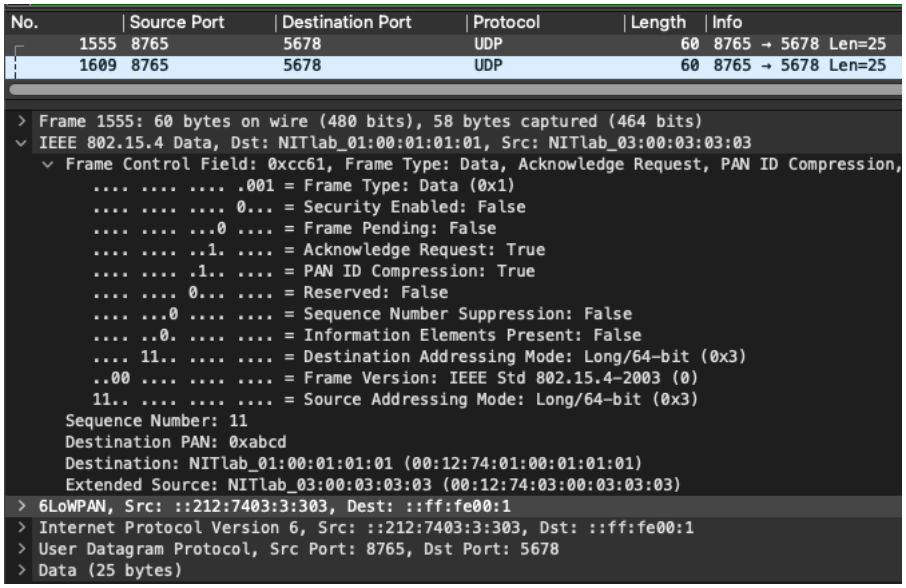

Figure 8: The first UDP message (IEEE 802.15.4 layer)

2.a.1 What is the meaning of PAN ID compression field? What is the ID of the PAN?

The Personal Area Network (PAN) ID compression field as seen in 8 is there to reduce the message overhead. When set to true, only the first packed will contain the PAN ID and from then and forwards the parties will have to keep this in their state because the PAN ID will not appear again in these packets. For my example, the initial UPD packet in Wireshark is the 6th ping and it has PAN ID compression enabled which means the PAN ID is not apparent in this packet trace. The PAN ID is a 16 bit identifier for the PAN the devices are communicating between. In cases where it is unnecessary to include the PAN ID, it will be omitted. E.g. when both parties are communicating from the same PAN.

2.a.2 What is the destination address mode?

The destination address mode indicates in what way we address the destination. It is a 2 bit field in this packet trace and each number classifies a mode: 0x0 tells us that we have to look in a device binding table for the destination address because it is not provided in the packet, 0x1 tells us that there is a address included but it is a multicast address, 0x2 includes a unicast or broadcast address, while 0x4 tells us the provided address identifies a specific device. For each of these the size of the address varies.

2.a.3 How long are the destination and source addresses? What is the difference with WiFi and Ethernet?

The destination and source address length depends on the destination address mode used: 0x0 it is 0 bits long, 0x1 and 0x2 it is 16 bits long, and when it's 0x3 the addresses are 64 bits long. When it comes to WiFi and Ethernet, the addesses are 4 bits.

In our example the UDP packet is 64 bits long.

2.a.4 Does the source PAN field exist? Why?

No the source PAN field exist because when the destination wishes to reply they need to know in which PAN they should target for their destination.

Now locate the first RPL mesage. It should be a DIS message.

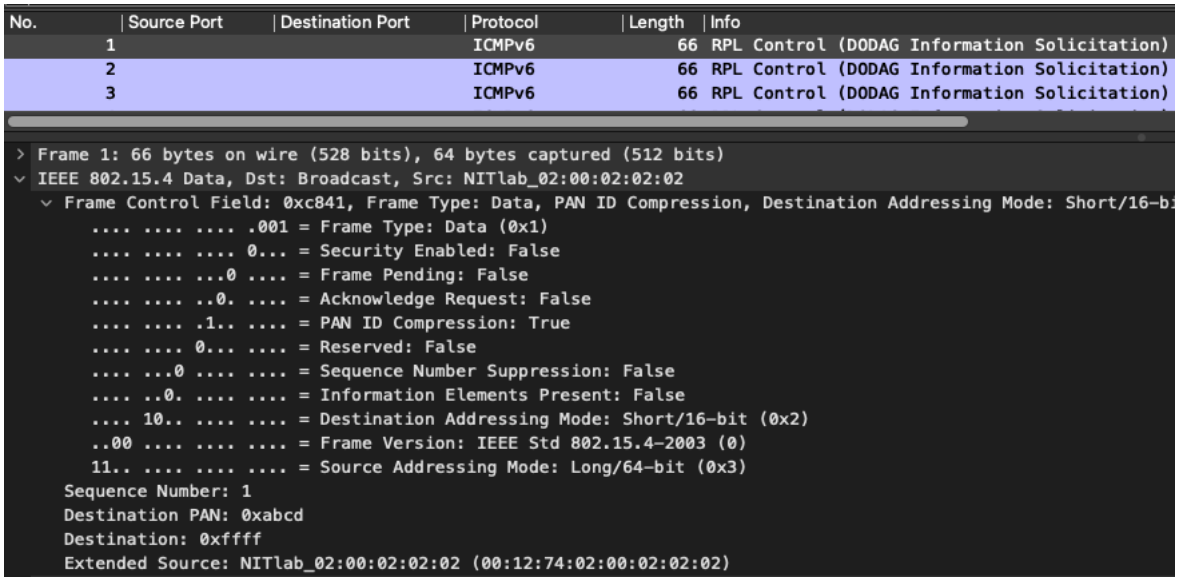

Figure 9: The first RPL message (IEEE 802.15.4 layer)

2.a.5 What is the destination address mode? Why is it different from the one used in the UDP packet?

As seen in Fig. 9, the destination addressing mode is **0x2 (16-bit)**. This is because the node sending this message is trying to solicit information from nearby nodes through a broadcast, while in 2.a.2 we were looking at a ping directed at a specific node.

2.b. 6LoWPAN

Locate the first UDP packet, and extend the FCF field.

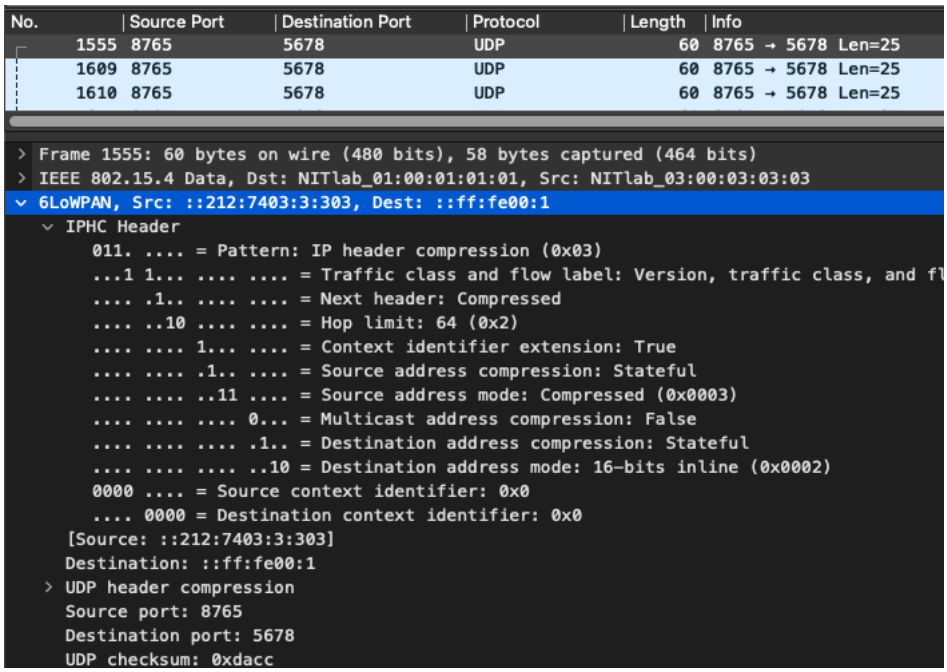

Figure 10: The first UDP message (LoWPAN layer)

2.b.1 What type of discriminator is used?

0x3 Compressed Header is the type descriminator used.

2.b.2 Does the packet uses header compression?

The packet uses IPHC compression.

2.b.3 What is the relation between the IEEE 802.15.4 and IPv6 adrdresses?

In order to keep minimal/none state on a device we are required to use the specific address of the destination device. The reason why it uses IPv6 and not IPv4 is because IPv4 does not provide a sufficient number of addresses for the desired use cases which is mainly a suite of internet connected devices, or Internet of Tings (IoT).

2.b.4 Reconstitute the non compressed header (please detail the process)?

2.c. RPL

2.c.1 Why all the nodes start by sending a DIS message? What is the purpose?

The nodes start by sending a Destination Oriented Directed Acyclic Graph (DODAG) Information Solicitation in order to buil the the graph of available nodes.

Locate the first DAO from node 1 (root). I could not find any DAO in my packet trace from node 1.

2.c.2 Why after receiving this message the other nodes stop sending DIS and start sending a DIO message? What is the purpose of this message (DIO)? What is the IPv6 destination address? Why?

The nodes stop sending DODAG Information Solicitation (DIS) messages after receiving a DAO and they start sending Destination Information Object (DIO) because they now know a router is present and they will broadcast their presence.

2.c.3 For each node indicates its rank in the DAG? How much is incremented the rank? What is the maximum value?

For rank N1 it increments with k, rank N2 and N3 with k+1, rank N4 to N6 with k+2. And it's max value is k + n where n is the count of hop it would take to root.

Locate a DIA message.

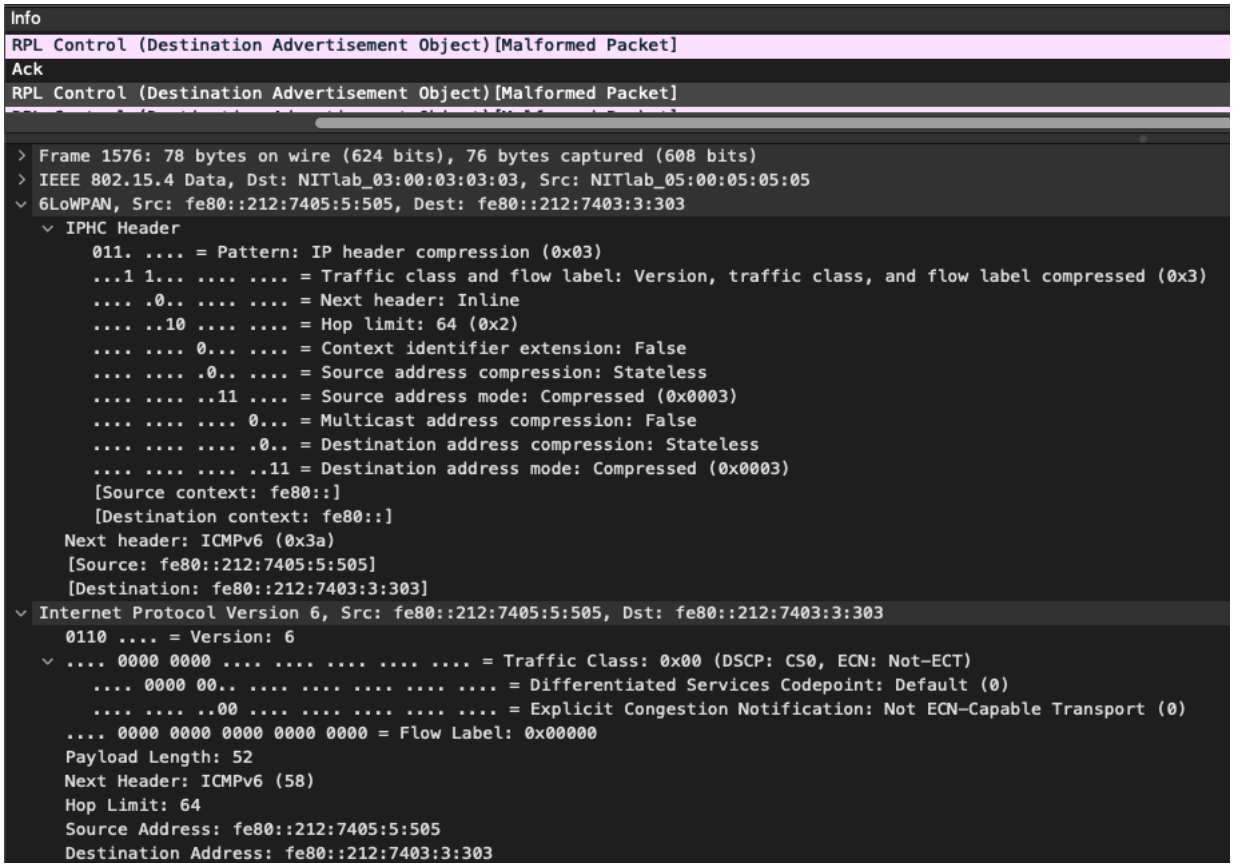

Figure 11: The first DIA message (LoWPAN layer)

2.c.4 What is its purpose? What is the IPv6 destination address? Why?

It's purpose is to let other nodes know that it is a possible destination, and the destination address is fe80::212:7403:3:303 as seen in Fig. 11.

2.c.5 Summarize the messages exchanged between the nodes to create the DAG with node 1 as root? Please elaborate your answer.