Tcpdump

Contents

1 Sniffing the private network

- We see that the GEDEX once powered will send data to the default IP address `192.168.1.207`.

```
# tcpdump tcpdump -i eth0 -nn
14:27:43.126030 IP 192.168.1.18.1234 > 192.168.1.207.1234: UDP, length 1104
...

# tcpdump tcpdump -i eth0 -nn -x -c1
```

- However it also use the default destination MAC address `00:19:66:32:2e:2a`.

```
# tcpdump tcpdump -i eth0 -nn -e
14:29:12.115233 00:07:ed:a1:b2:c4 > 00:19:66:32:2e:2a, ethertype IPv4 (0x0800), length 1146: ...
```

So, the GEDEX doesn't make ARP query to make the corespondance between MAC and IP.

- Sniffing bytes on a special port:

```
# tcpdump tcpdump -i eth0 -nn -X port 1235
16:27:52.233635 IP 192.168.1.207.41889 > 192.168.1.18.1235: UDP, length 4
        0x0000:  4500 0020 f29c 4000 4011 c3fe c0a8 01cf  E.....@.@.......
        0x0010:  c0a8 0112 a3a1 04d3 000c 844f 0004 ff00  ...........O....
```

tcpdump -i eth0 -nn -X port 1235

note: TCPDUMP set network interfaces into promiscuous mode.

```
# tail /var/log/syslog
Jun  4 01:42:30 narval kernel: eth2: Promiscuous mode enabled.
Jun  4 01:42:30 narval kernel: device eth2 entered promiscuous mode
```