State of the Network

BornHack 2017
NOC Team
noc@bornhack.org

Important stuff

So, we think you should know!

- We do NOT collect data for “fun” (or profit)
- We respect your privacy
- NO packet captures, except for solving problems
  We dont even have central mirror port for sniffing pre-configured
- NO IDS or traffic analysis, not even netflow
- DHCPD has the MAC addresses, but only HLK has access, and will delete before leaving BH
- UniFi controller has MAC addresses, but will ALSO be deleted before leaving BH
- Note: Upstream ISP required by law to do some logging in DK

Preparations

Before getting here, we did:

- Asked RIPE NCC for IPv4, IPv6 and AS number
- Asked Bornfiber Peter Krupl for assistance in configuring uplink, thank you Peter
- Gathered some devices, cables, found the ones from last year
- Created a NOC team on the BornHack page but forgot to plan when those people would arrive :-)

Hardware used

- Core switching Juniper EX3300
- Core routing Juniper SRX240
  (next year OpenBSD if I am doing it)
- PoPs made with boxes from the BRK
- Wired Brocade switches in PoPs
  Three series and OLD, SSH needs insecure config to connect
- Wifi Ubiquity UniFi AP Pro, AC Lite, and old AP
- Service VMs on VMware ESXi, shout out to Tobias for providing server and help

Major problems

Beginning:

- DHCP floods, ARP floods, duplicates AP=> switchport misconfiguration and wirelessly uplinked APs
- Power outages, rain and water
- Fiber converter, fried by thunder
- Didn't got around to making the 802.1x – very sorry

Minor problems

- UniFi Controller, some wireless uplinks by default
- Relearning my Brocade skills, will forget them in a week
- Rogue DHCP server, will need to have better switches/switchport security
- Some other funky DHCP problems reported by a few users, but “works for me” was checked on tent by Morten
- GeoIP puts us in Germany, always a problem for temp networks

Flooding

[NMS-VM] fuck-dhcp.cap [Wireshark 1.12.1 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	JuniperN_8c:b5:04	Broadcast	ARP	60	Who has 151.217.1.135? Tell 151.217.0.1
2	0.012454	151.217.0.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xabcd0587
3	0.013207	151.217.0.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xabcd0587
4	0.014021	151.217.0.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xabcd0587
5	0.019182	151.217.0.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xabcd0587
6	0.020023	151.217.0.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xabcd058f
7	0.020803	151.217.0.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xabcd058f
8	0.021986	151.217.0.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xabcd058f
9	0.023060	151.217.0.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xabcd0587
10	0.024128	151.217.0.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xabcd0587
11	0.024829	JuniperN_8c:b5:04	Broadcast	ARP	60	Who has 151.217.3.223? Tell 151.217.0.1
12	0.025610	JuniperN_8c:b5:04	Broadcast	ARP	60	Who has 151.217.1.25? Tell 151.217.0.1
13	0.026352	JuniperN_8c:b5:04	Broadcast	ARP	60	Who has 151.217.3.103? Tell 151.217.0.1
14	0.027575	151.217.0.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xabcd0587
15	0.028654	151.217.0.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xabcd058f
16	0.029714	151.217.0.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xabcd058f
17	0.030768	151.217.0.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xabcd0587
18	0.031840	151.217.0.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xabcd058f

```
0000  ff ff ff ff ff ff 40 b4  f0 8c b5 04 08 00 45 00   ......@. ......E.
0010  01 48 73 56 00 00 01 11  ad 75 97 d9 00 01 ff ff   .HsV.... .u......
0020  ff ff 00 43 00 44 01 34  20 1b 02 01 06 00 ab cd   ...C.D.4  .......
0030  05 8f 00 00 00 00 00 00  00 00 97 d9 00 7f 00 00   ........ ........
```

File: "caps/fuck-dhcp.cap" 30 M... Packets: 100000 · Displayed: 100000 (100.0%) · Loa... Profile: Default

Succes and achivements

- With NOC supporter help we have solved lots of problems, made new friends, learned $stuff
- Built a network spanning 350m from North1 PoP to South3 PoP
- 8 PoPs including the core room with server hosting
- Put out MORE than 1km of network cable to connect main sites, achievement unlocked :-) around 900m fiber, rest copper
- Provided a reasonable stable network with some people reporting 480Mbps/620Mbps at times
- Some phones reported 8ms latency and 220/220Mbps on wireless, monday before the event really started
- My phone has reported 150/150Mbps during event at times, mostly latency has been in range of 8-20ms – to Copenhagen servers
- Lot more usage than last year, use moar bandwidth

PoPs / datenklos

LibreNMS switches

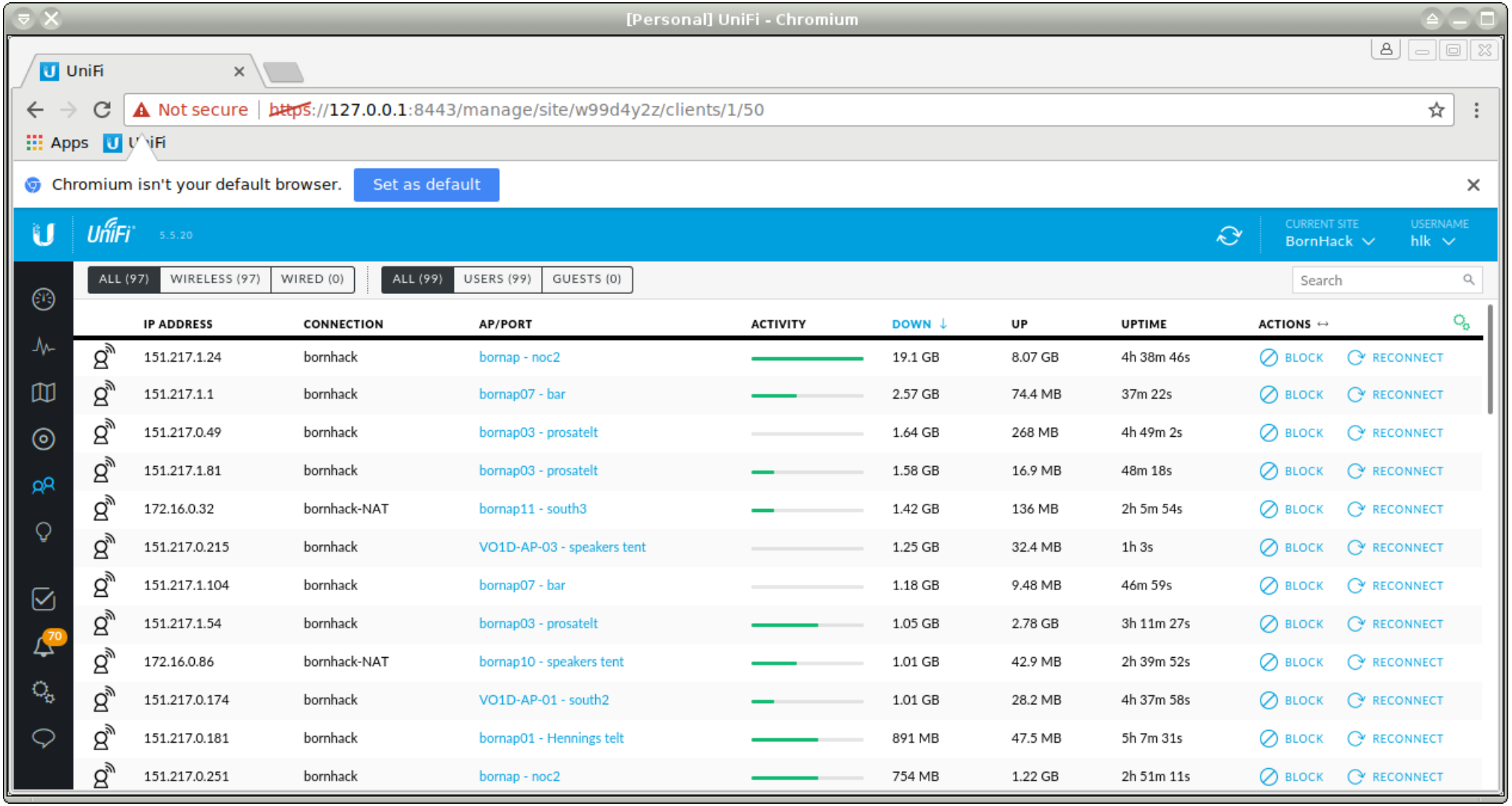
LibreNMS | Overview | Devices | Services | Ports | Health | Alerts

Lists: Basic | **Detail** | **Graphs:** Bits | CPU | Load | Memory | Uptime | Storage | Disk I/O | Poller | Ping | Temperature

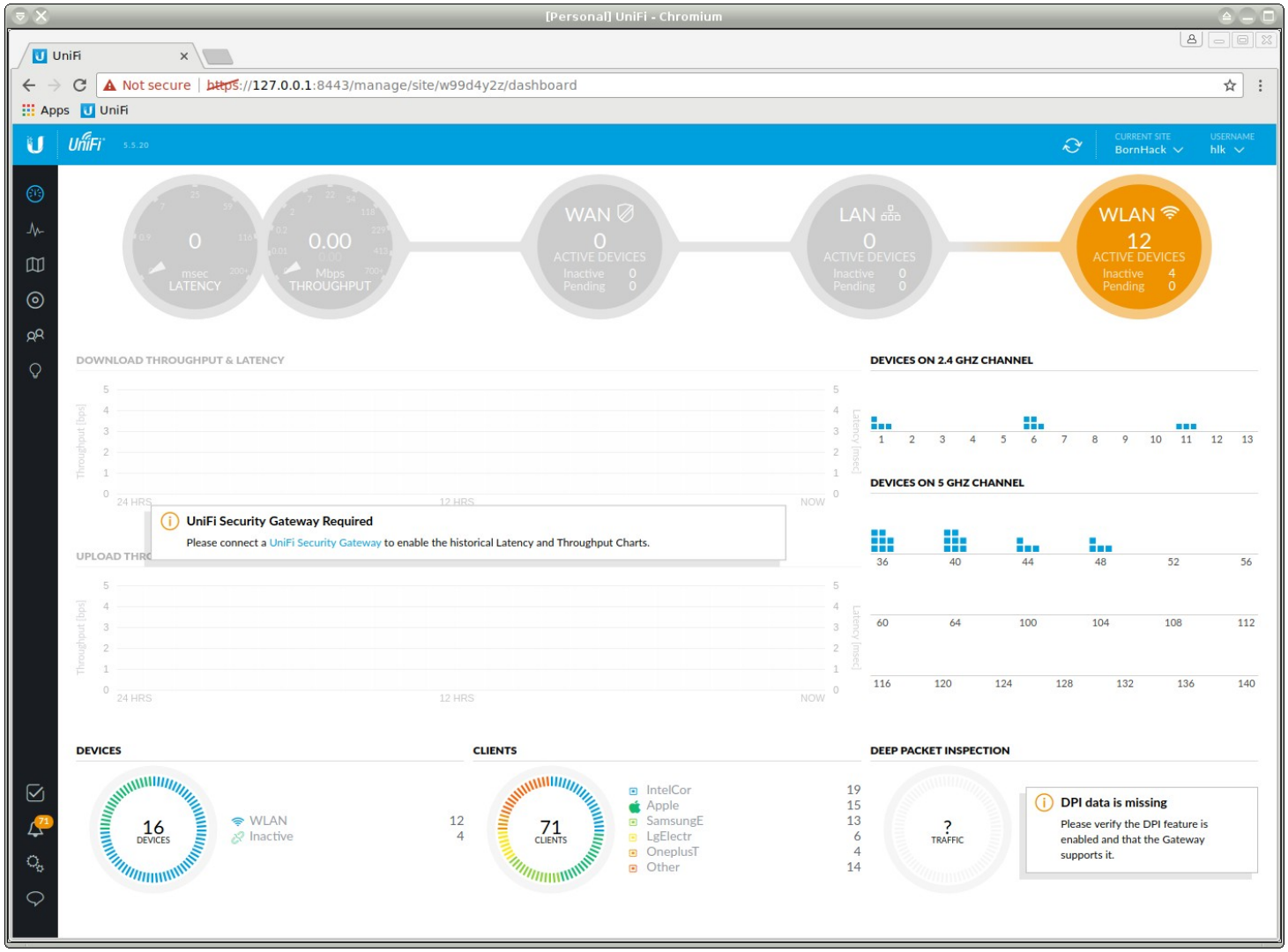
Hostname | All OSes | All Versions | All Platforms | All Featuresets | All Locations

Status	Vendor	Device	Metrics	Platform	Operating System
up		**born-core-01**	100 13	Juniper EX3300	Juniper JunOS 15.1R2.9
up		**north1** north1	25		Foundry Networking
up		**south1** south1	25 4	snFWS624GSwitch	Brocade IronWare FWS07400c
up		**south2** south2	29 3	snICX643024Switch	Brocade IronWare ICX64S08030h
up		**south3** south3			Foundry Networking
up		**southwest1** southwest1	49		Foundry Networking
up		**west1** west1	25 4	snFWS624GSwitch	Brocade IronWare FWS07400c
up		**west2** west2	25		Foundry Networking

Wireless 12 APs working



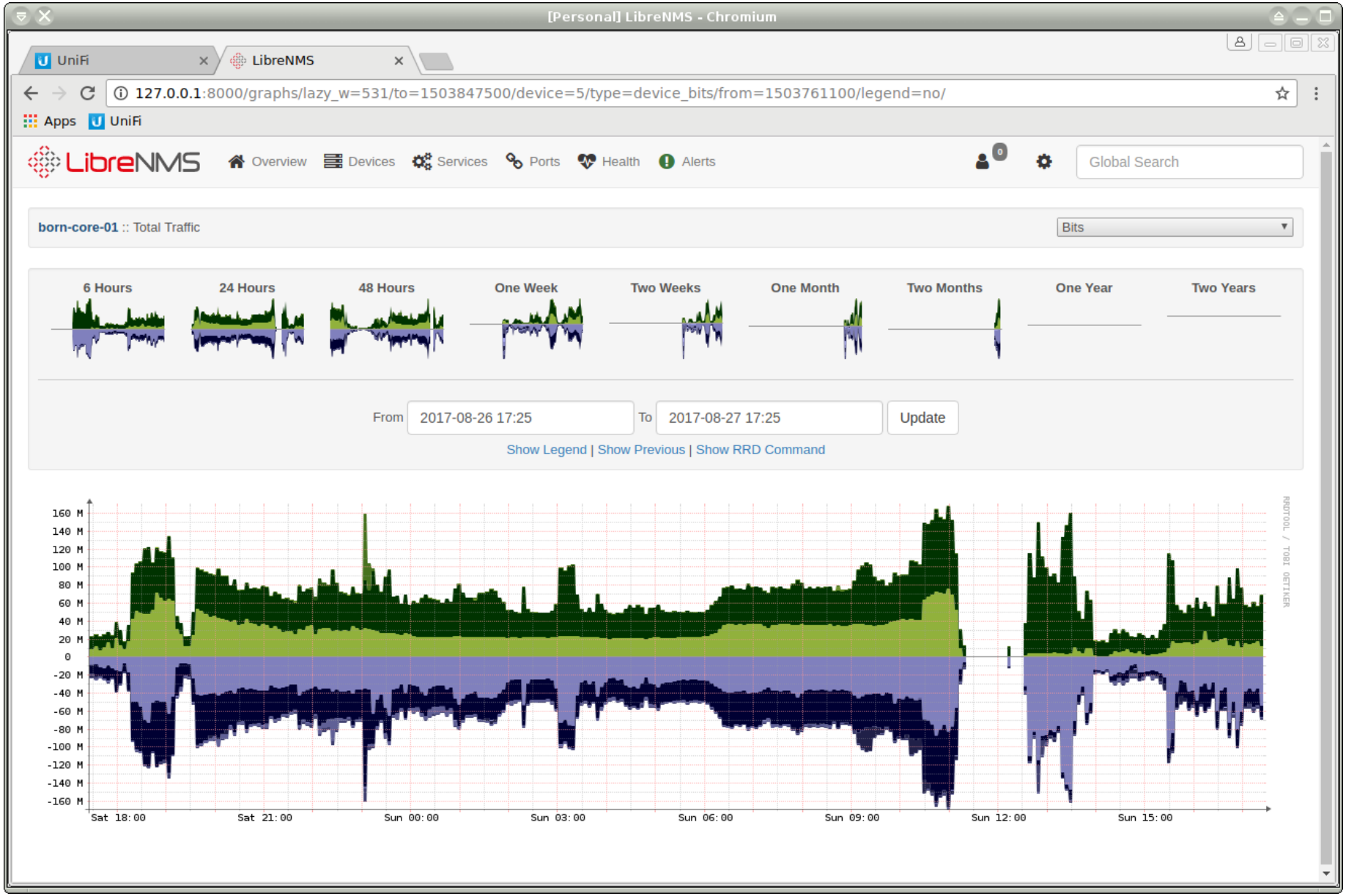
UniFi is pretty easy, and “OK”



Some stats

- UniFi controller reports 469 clients seen!
- One client has downloaded 128Gb :-)
- Another client uploaded 40Gb
-

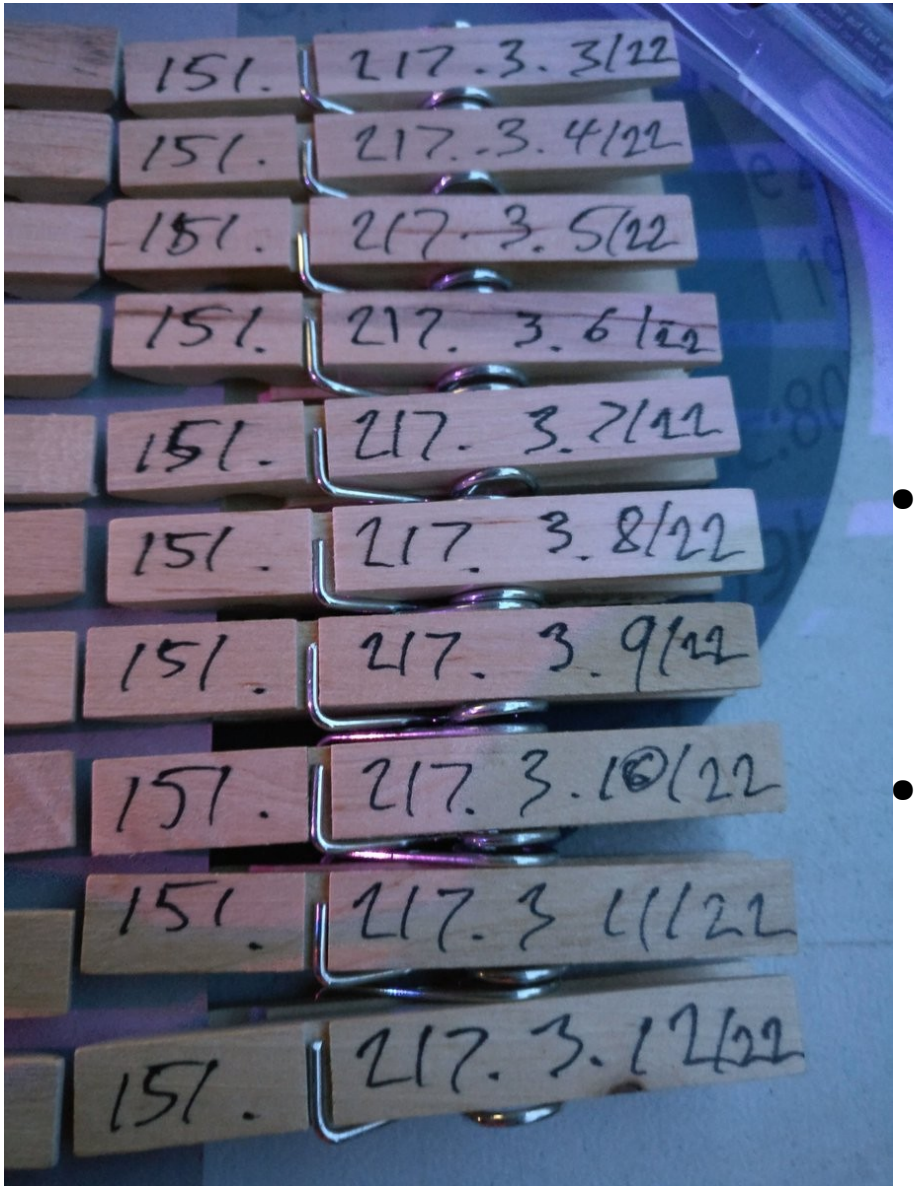
Bandwidth and power outage



Lessons learned

- Second year, was not prepared enough
- Project requires NOC architects, Server people, NOC Helpdeskers – initially we had me on-site on Sunday and Monday…
- BUT then 8 people showed up and helped, sorry for not remembering all names, but Mortenx2, Eightdot etc. you saved me/us!
- Goal next year, have 2x JN-CIS SP, 2x server people, +5 NOC support
- Bring more fiber converters, one fried and cheap

PEG DHCP



PEG DHCP RFC2322 was implemented https://en.wikipedia.org/wiki/Peg_DHCP

- PEG DHCP worked REALLY well, “DHCP giving you problems, take a peg, done”
- Make PEGs for wifi and wired, two colors
  We are splitting this up next year

Conclusion

- We did it, there was a network
- We need more preparation, pre-camp NOC setup meeting

Some software tools used

- UniFi Controller running on Ubuntu, easy
- OpenBSD conserver, DHCPD and other stuff
  http://conserver.com/ - serial connections
- LibreNMS for stats – autodiscover yay!
  https://www.librenms.org/
- Oxidized for getting config from devices
  https://github.com/ytti/oxidized
- Plus usual suspects, tcpdump, wireshark, ping, nmap, traceroute