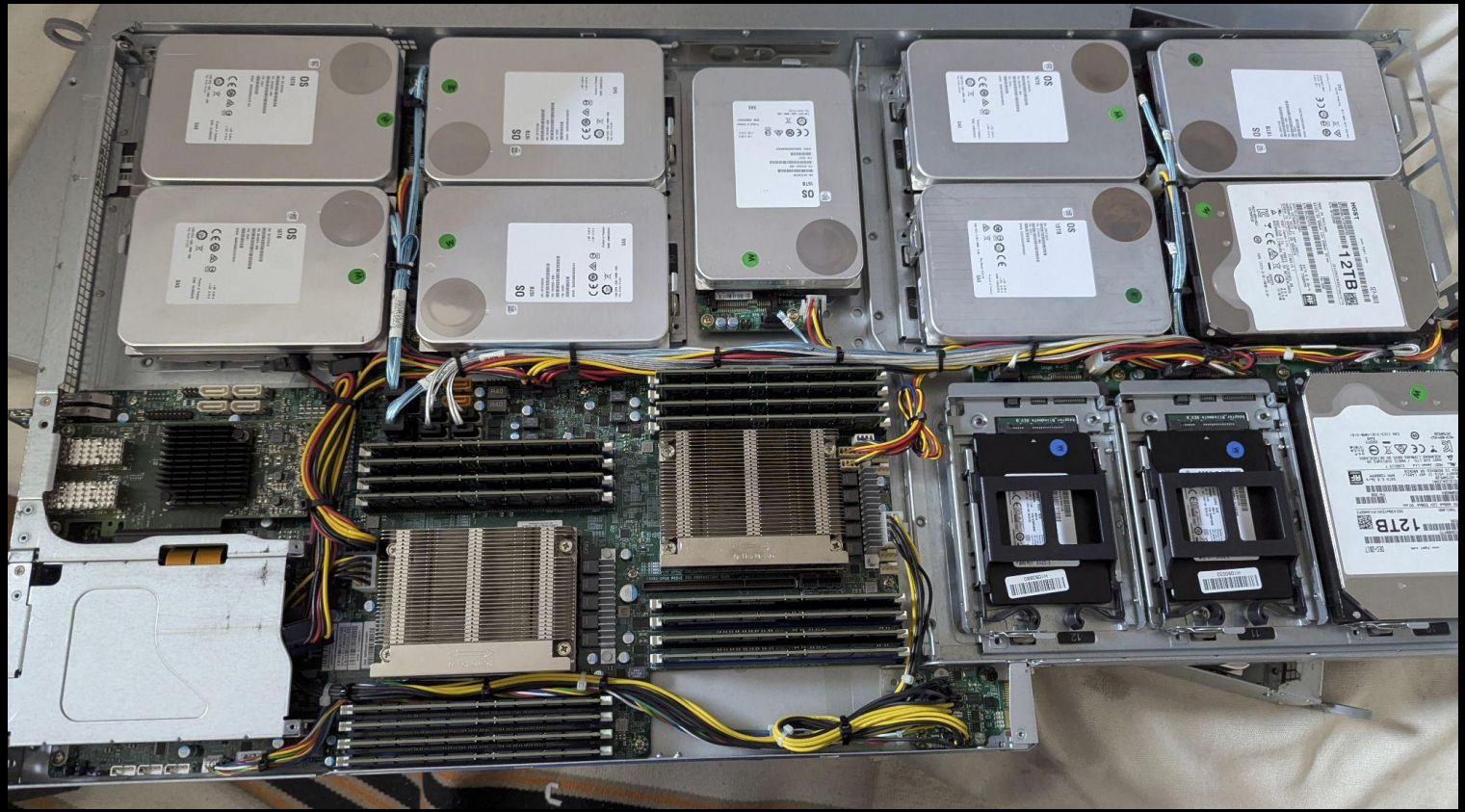
Picking uncontested private IP subnets with usage data

Last min lightning talk for NetLDN #63

I recently installed new servers

- Like, 130kg of them, what a pain in the ass

I recently installed new servers



I recently installed new servers

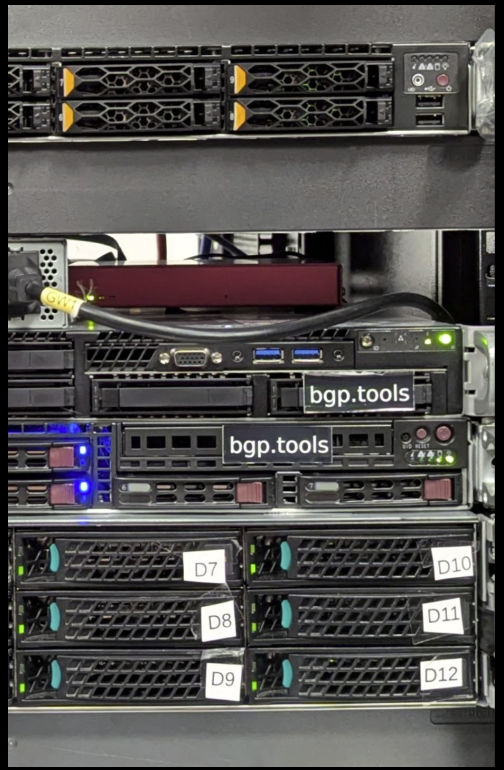
- Like, 130kg of them, what a pain in the ass
- I got these racked and installed, and immediately left the country for a break

I recently installed new servers

- Like, 130kg of them, what a pain in the ass
- I got these racked and installed, and immediately left the country for a break
- My thinking was that this would be fine because I can always VPN into the OOB/IPMI switch to set up the new machines

I recently installed new servers

- Like, 130kg of them, what a pain in the ass
- I got these racked and installed, and immediately left the country for a break
- My thinking was that this would be fine because I can always VPN into the OOB/IPMI switch to set up the new machines
- This involves a long time favorite device, the ALIX alix2d13, (the red device), running OpenWRT and Wireguard



Side notes, check how deep your racks are

Day 0

Day 14

Anyway

Arrived in $Country and started the VPN, only to discover that my OOB range (*aka, the OpenWRT default of 192.168.1.0/24*) also collided with the LAN of the WiFi at the house I was using (some NETGEAR LTE WiFi device)

This is not a disaster as I can just "ip route add {1234} dev vpn0" to work around it, but it's annoying to do that ***if there is currently a disaster***

So clearly I should renumber this OOB LAN to be safer in the future, But what to?

RFC1918

RFC 1918 Address Allocation for Private Internets February 1996

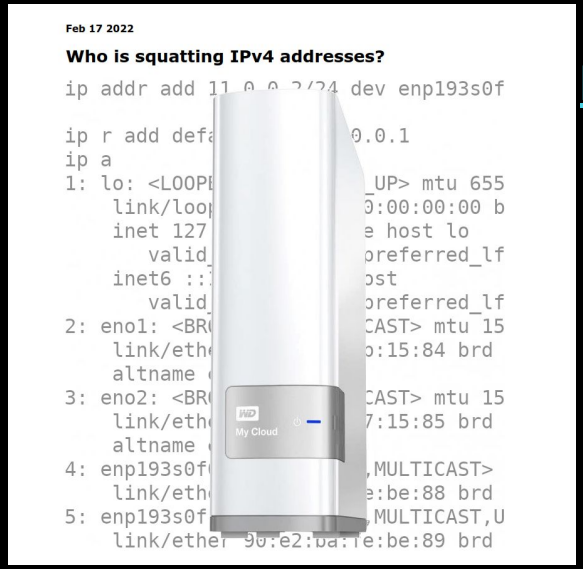
3. Private Address Space

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

10.0.0.0	-	10.255.255.255	(10/8 prefix)
172.16.0.0	-	172.31.255.255	(172.16/12 prefix)
192.168.0.0	-	192.168.255.255	(192.168/16 prefix)

No vibes today, I want data

- It would be nice to have a data source that would tell us what people (home networks mostly) use as their RFC1918 LAN ranges
- It turns out in a previous blog posts i'd already found the answer to this:



https://blog.benjojo.co.uk/post/ip-address-squatting

"Who is squatting IPv4 addresses?"

"WD Cloud" devices leak their users LAN

- These devices have a TLS certificate so that you can securely talk to them from outside, these certificates are stored on the device, and have a WAN (aka your public ip that would be accessed port forwarding), and a LAN (so that the app can automatically force connections to use the LAN rather than the WAN)
- Because they have a TLS certificate, the certificate is logged in Certificate Transparency (CT) logs
- This means we can figure out all WD Cloud users

Example DNS name

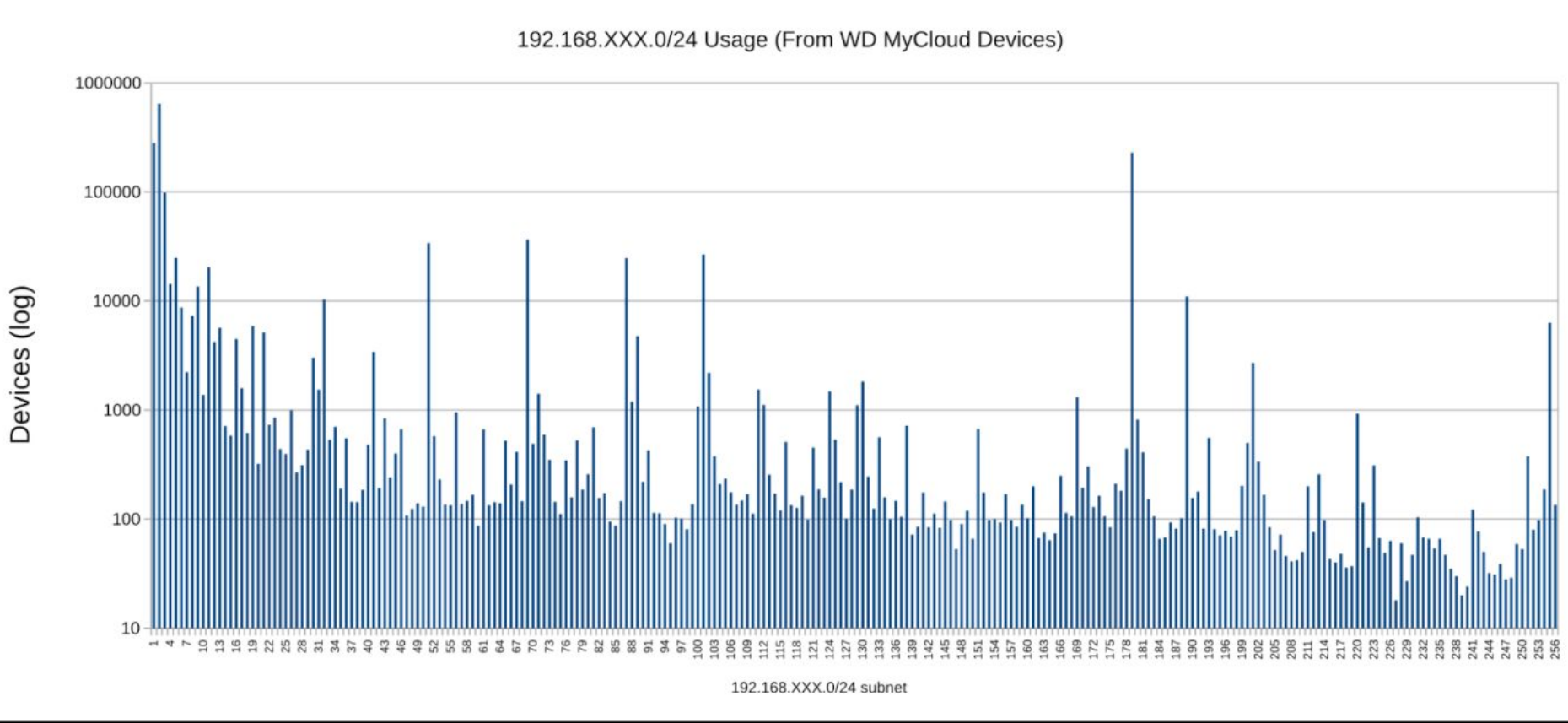
```
$ cat remote-wd | grep 0675828b-2e8c-4be5-96e7-0a595fbae6dc

192.168.1.103,device-local-0675828b-2e8c-4be5-96e7-0a595fbae6dc.remotewd.com

223.255.150.74,device-0675828b-2e8c-4be5-96e7-0a595fbae6dc.remotewd.com
```

Surprising no one, homes rarely use 172.16.0.0/12

Private Address Range	Count of Devices
192.168.0.0/16	1,602,092
172.16.0.0/12	22,132
10.0.0.0/8	149,901

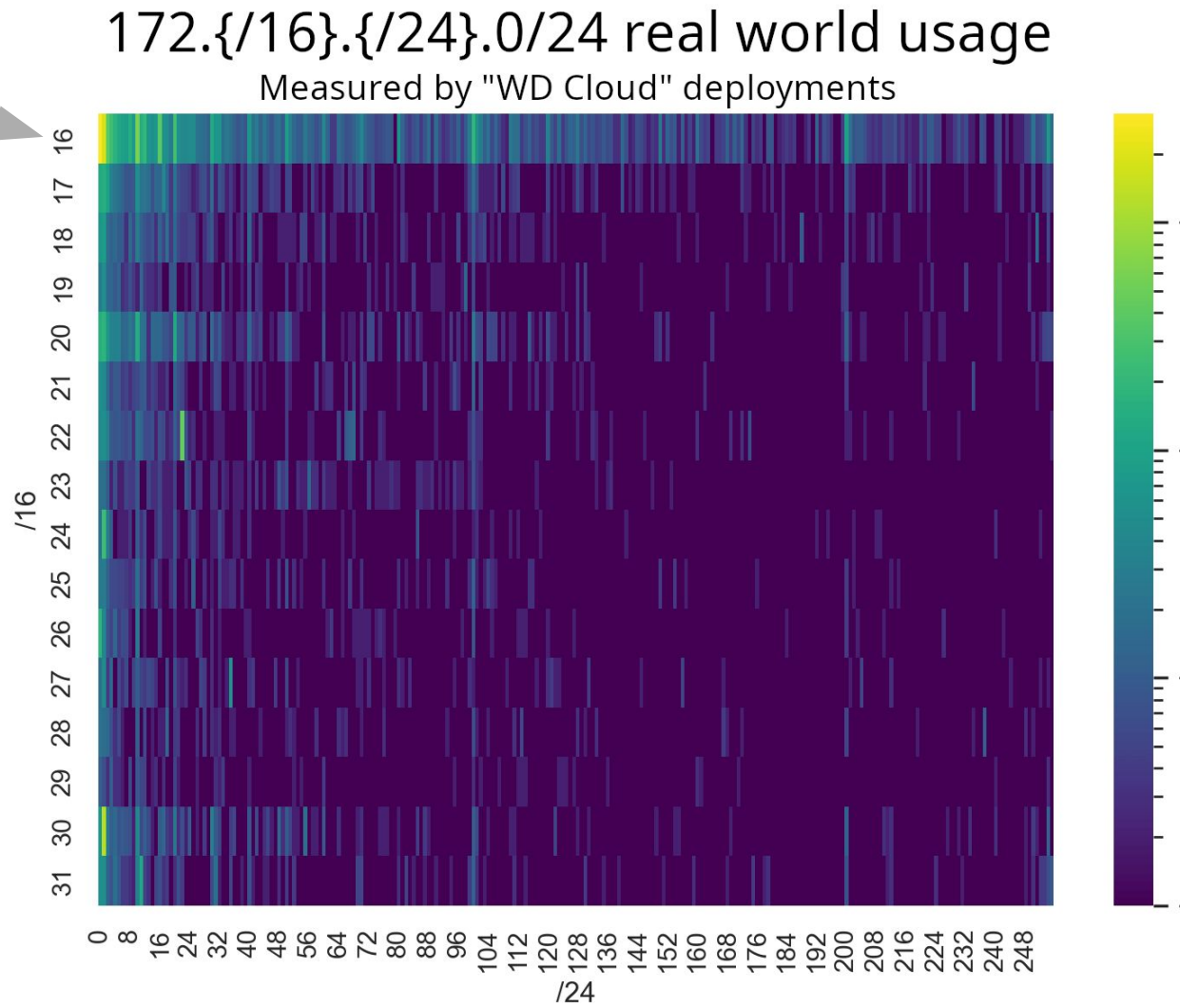
192.168.0.0/16 usage is huge (also unsurprising)

IP Block	Count	Known Default User
192.168.1.0/24	647,220	Common Default
192.168.0.0/24	280,952	Common Default
192.168.178.0/24	229,398	FritzBox
192.168.2.0/24	98,341	Common Default
192.168.68.0/24	36,555	TP-Link
192.168.50.0/24	33,942	TP-Link
192.168.100.0/24	26,695	Huawei
192.168.4.0/24	24,834	Zyxel
192.168.86.0/24	24,736	Google WiFi?
192.168.10.0/24	20,381	Zyxel/Motorola
192.168.3.0/24	14,311	Huawei
192.168.8.0/24	13,554	Huawei
192.168.188.0/24	11,000	FritzBox


192.168.XXX.0/24 Usage (From WD MyCloud Devices)
Devices (log)
1000000
100000
10000
1000
100
10
192.168.XXX.0/24 subnet

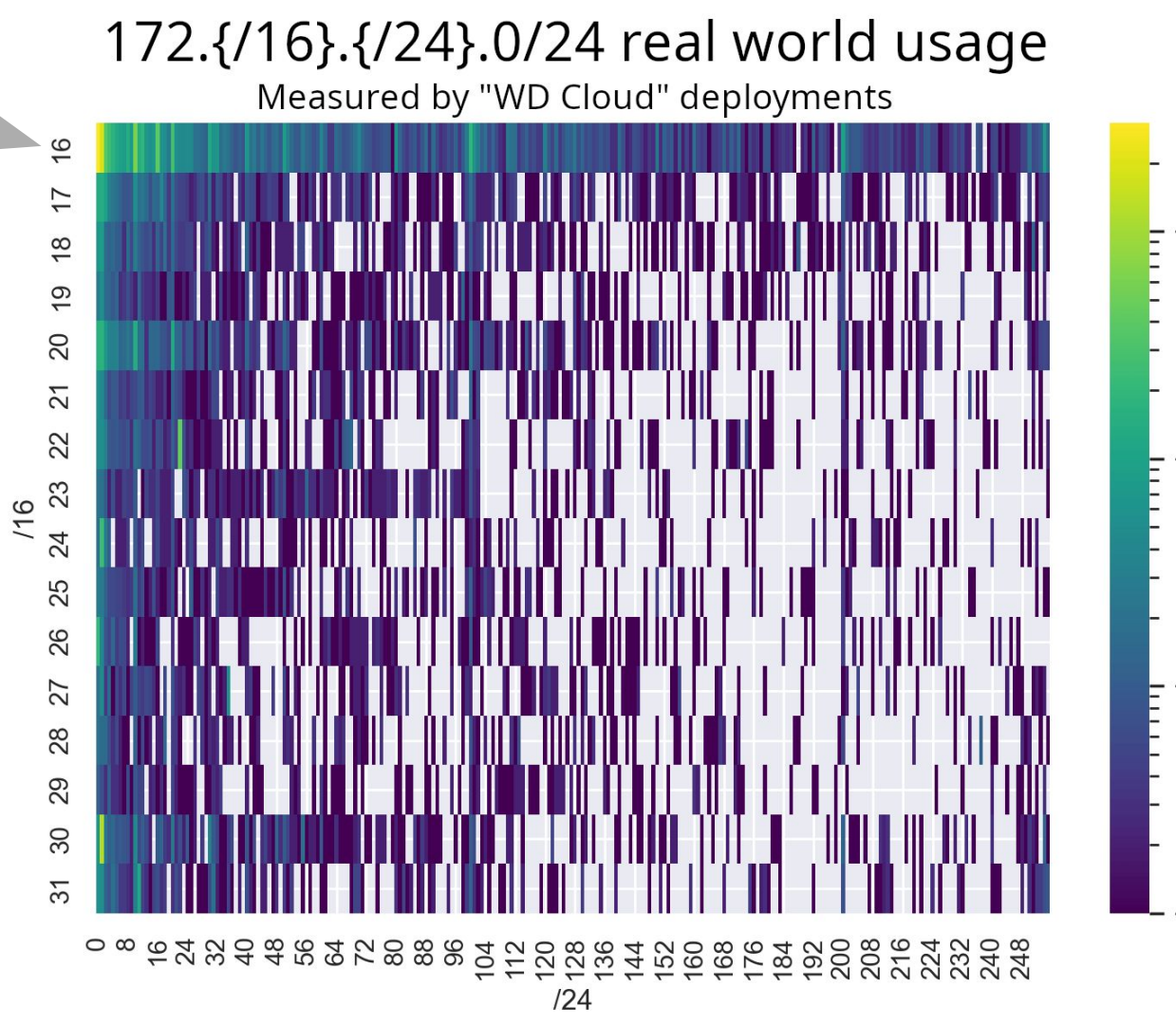
172.16.0.0/12

People clearly mostly use it as a /16

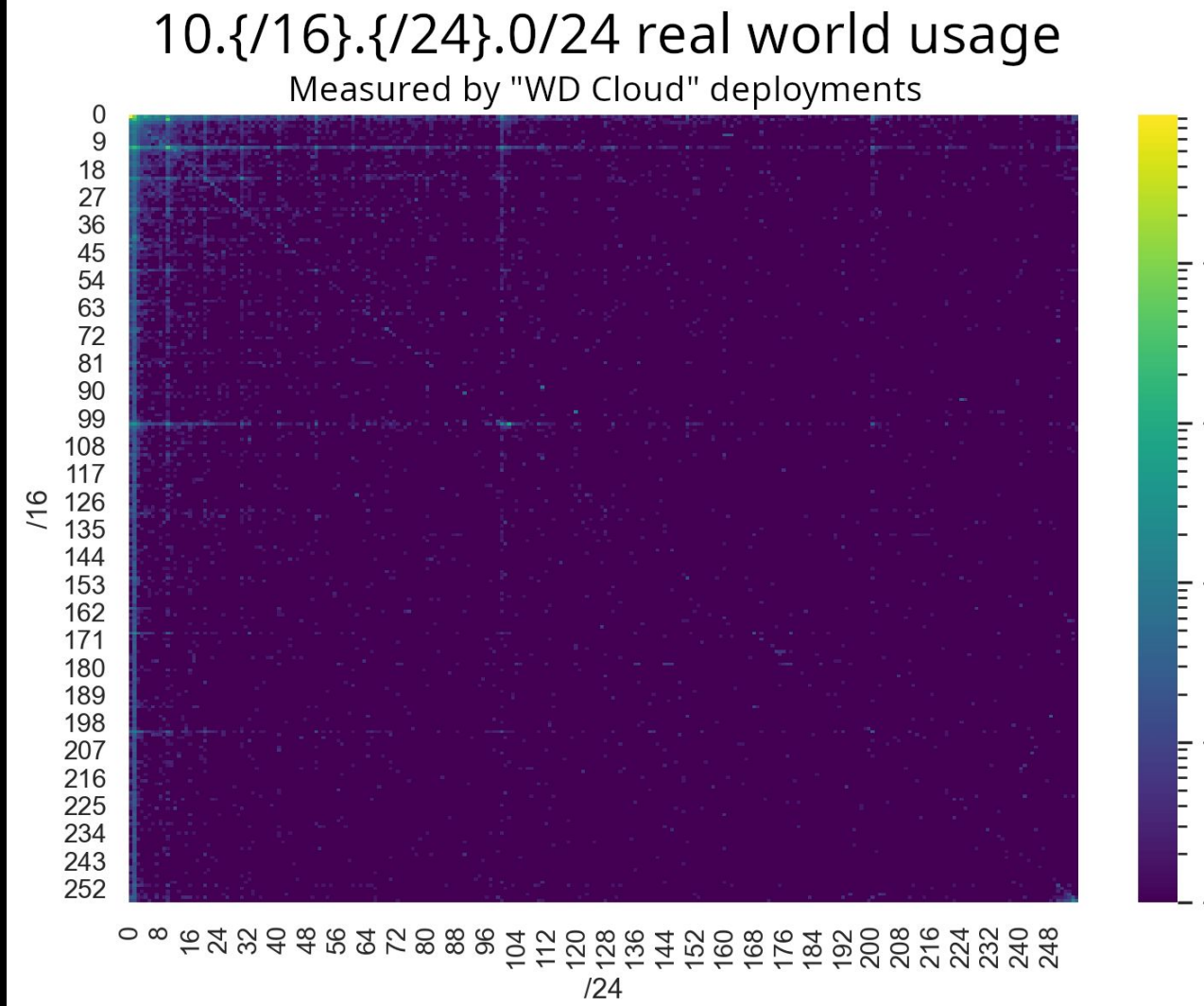


172.16.0.0/12

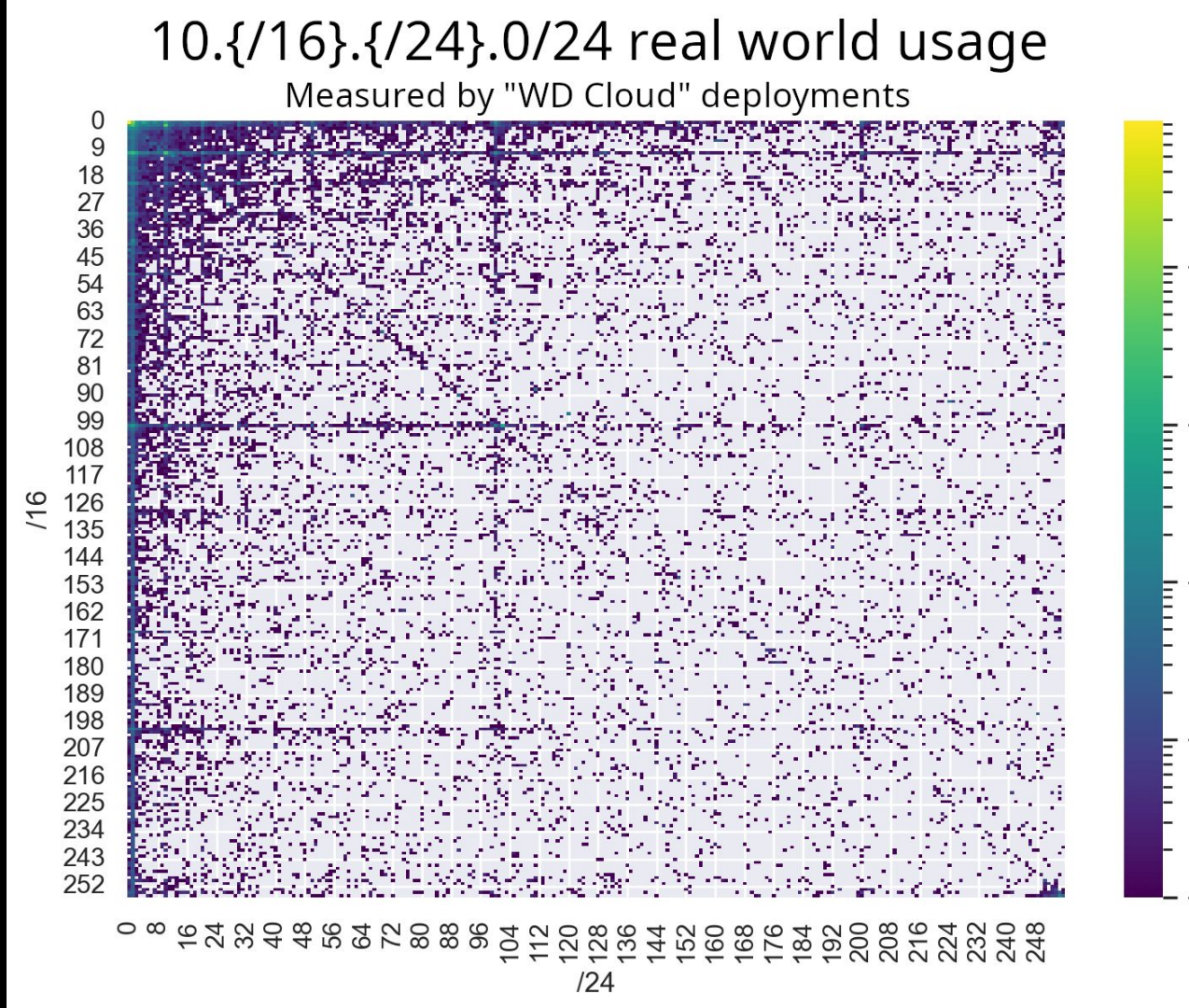
People clearly mostly use it as a /16



10.0.0.0/8


10.{/16}.{/24}.0/24 real world usage
Measured by "WD Cloud" deployments
/16
0
9
18
27
36
45
54
63
72
81
90
99
108
117
126
135
144
153
162
171
180
189
198
207
216
225
234
243
252
/24
0
8
16
24
32
40
48
56
64
72
80
88
96
104
112
120
128
136
144
152
160
168
176
184
192
200
208
216
224
232
240
248

10.0.0.0/8


10.{/16}.{/24}.0/24 real world usage
Measured by "WD Cloud" deployments
/16
0
9
18
27
36
45
54
63
72
81
90
99
108
117
126
135
144
153
162
171
180
189
198
207
216
225
234
243
252
/24
0
8
16
24
32
40
48
56
64
72
80
88
96
104
112
120
128
136
144
152
160
168
176
184
192
200
208
216
224
232
240
248

So what subnets do I use then?

There are 55,388 /24 subnets without known users, one of them should be listed below for you to use that has been randomly picked from that list:

```
10.234.236.0/24
```

In case you want to play with this data yourself, you can find all of the subnet numbers here (Zip file)

https://blog.benjojo.co.uk/post/picking-unused-rfc1918-ip-space

tl;dr

- You should probably prefer 10.0.0.0/8, as 172.16.0.0/12 may interfere with existing vpn solutions
- You can't just solve this problem with IPv6
  - Not everything (especially annoying shit like IPMI/Automatic Transfer switch) supports v6 in a nice way
  - Browsers have issues where if you do not have a IPv6 default route installed, it wont even query for AAAA, even if you have a split horizon VPN with v6 routes pushed
  - Even if it does work, I don't trust it to work during a emergency where access to this vpn ***really matters***
- There is a cool amount of data available for the taking in TLS certs
  - Plex has to do similar things to the WD Clouds, however fixed this problem in a interesting way

Questions?