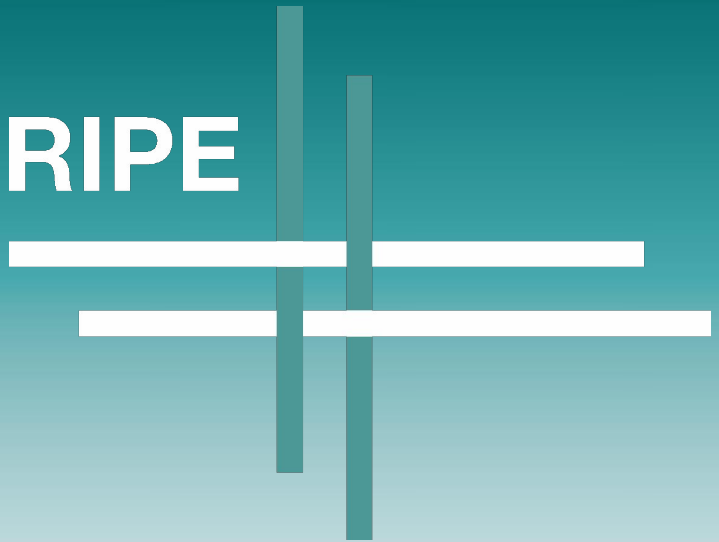
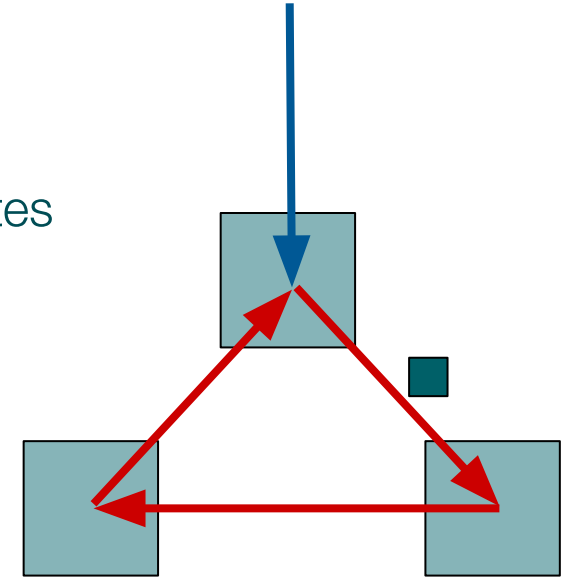



# Routing Loops: The Phantom Menace

Alexander Zubkov
Qrator Labs CZ s.r.o.
green@qrator.net

# Routing loop

- the packet is “infinitely” routed in a loop
  - finitely (TTL)
- dynamic routing
  - transient
  - Internet (BGP) convergence ~minutes
  - stuck routes
- configuration errors
  - persistent
  - unused IP space
  - NAT pools



# Unused IP space

- bad configuration
  - router A (provider)
    - 192.0.2.0/24 → router B
  - router B (client)
    - 192.0.2.128/25 → router C
    - default → router A
- use null-route
  - router B (client): 192.0.2.0/24 → null
- forbid spoof when possible (BCP38)
  - Sender Address Verification

# Problems

- link utilization
  - TTL >200, 2 hops => 100x amplification
  - DoS target
  - $$$
- other
  - DoS means
  - inferring the ability of spoof

# References


The Risks and Dangers of Amplified Routing Loops (Andree Toonk)

Flooding Attacks by Exploiting Persistent Forwarding Loops (Jianhong Xia, Lixin Gao, Teng Fei)

Weaponizing Middleboxes for TCP Reflected Amplification (Kevin Bock, Abdulrahman Alaraj, Yair Fax, Yair Fax, Eric Wustrow, Dave Levin)

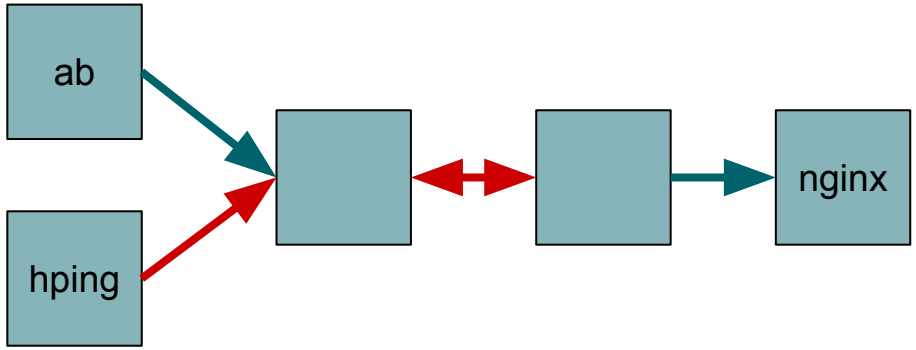
> "We were unable to terminate the barrage of packets sent to us … the traffic stopped after approximately six days … We believe the reason they finally stopped was because the routing loop eventually dropped a packet."

Using Loops Observed in Traceroute to Infer the Ability to Spoof (Qasim Lone, Matthew Luckie, Maciej Korczyński, Michel van Eeten)

Hunting down the stuck BGP routes (Ben Cox)

# Simulation

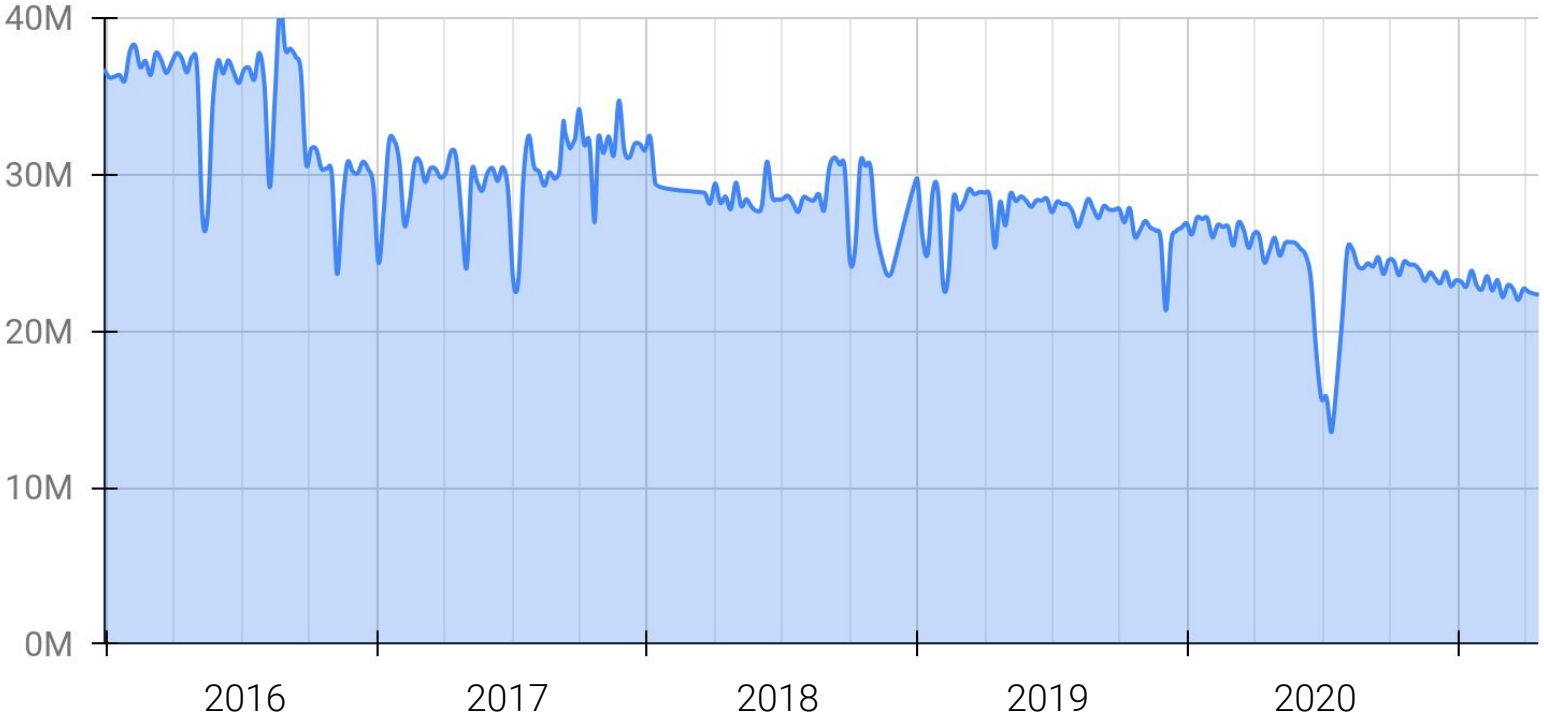
- 3 servers
- 2 switches
- links
  - server — switch 10G
  - switch — switch 40G
- hping -2 -p 80 -t 220 [-d 1400] [-i u20|--flood] ...
- ab -r -t 300 -n 10000000 -c 100 ...



# Simulation

| type | flood rate | link util. | req/s | ms/req | slowdown |
|---|---|---|---|---|---|
| normal | 0 | 0 | 27.8k | 3.6 | |
| direct | 450M | 450M | 27.6k | 3.6 | |
| direct | 5.8G | 5.8G | 28.1k | 3.6 | |
| direct | 9.9G | 9.9G | 257 | 389 | 108x |
| loop | 440M | 39G | 5.3k | 18.8 | 5.2x |
| loop | 5.6G | 39G | 3.8k | 28.8 | 8x |
| loop (small) | 280M | 30G | 28.1k | 3.6 | |
| loop (small) | 570M | 30G | 27.5k | 3.6 | |

# Historical data by Qrator.Radar (https://radar.qrator.net/)



# Counting loops

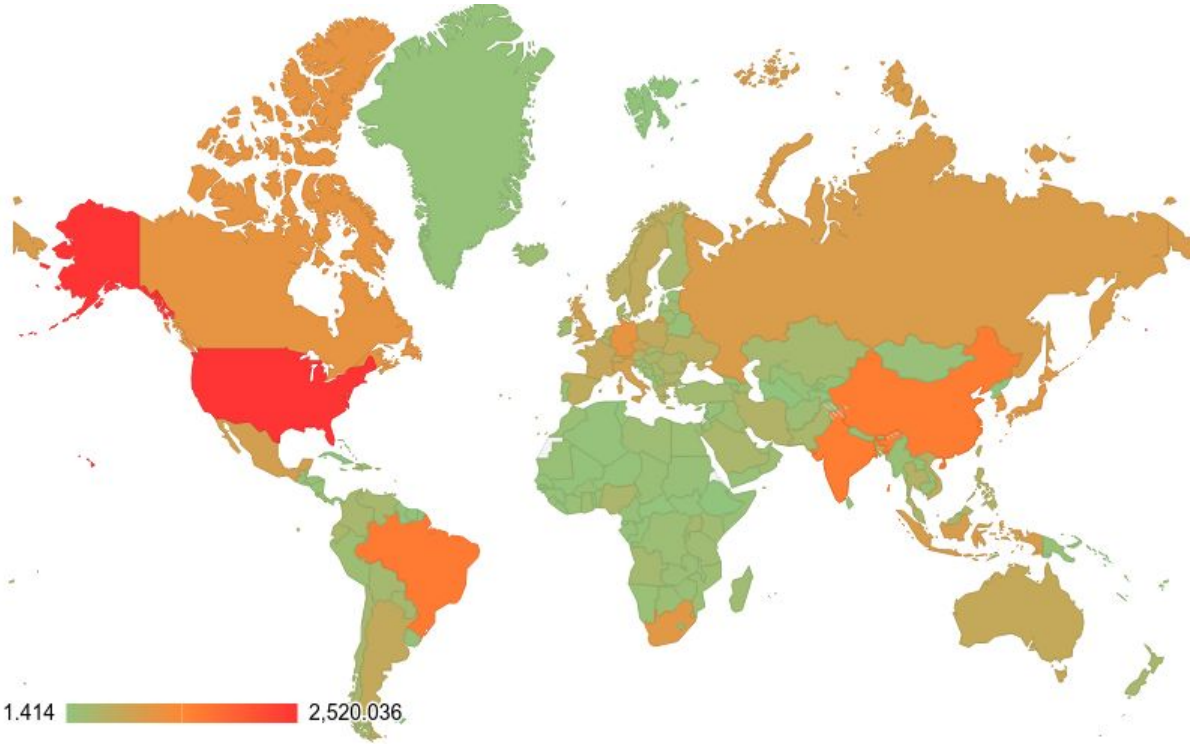
- scan internet
  - icmp, 4 probes, ttl 125-128
  - catch ttl exceeded
- 28.3M loops (1.1% of active space)
  - and there are more
- 25.5k destination ASs (35% of active ASs)
  - CDN, DDoS mitigation too, big names
- amplification
  - 4.23 replies per unique IP
  - sometimes >100k replies

# Counting loops

- >100k unique loops (hard to count)
  - hard to count: rare replies, repeating hops, multiple hops
- 585k unique router IPs in loops
  - from 20.0k ASs
  - 18.9k ASs have both loop destinations and routers
- length from 1 to 34 hops
  - 2 hops is the most popular
- span up to 7 ASs, up to 8 countries (according to geodb)
- rtt up to 18s

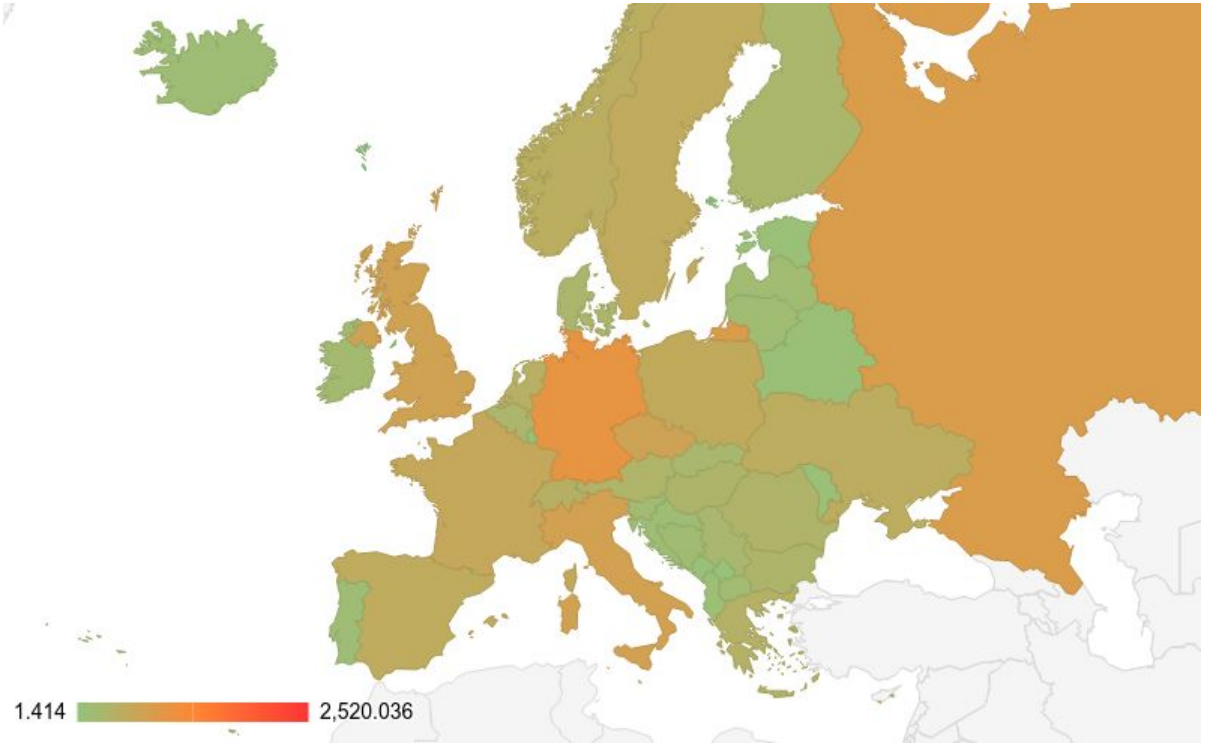
# Loop destinations by country (World)

| | |
|---|---|
| 22.4% | United States |
| 7.6% | Brazil |
| 7.2% | China |
| 7.0% | India |
| 3.6% | South Korea |
| 3.5% | Germany |
| 3.4% | Canada |
| 3.0% | Japan |
| 2.9% | South Africa |
| 2.4% | Russia |

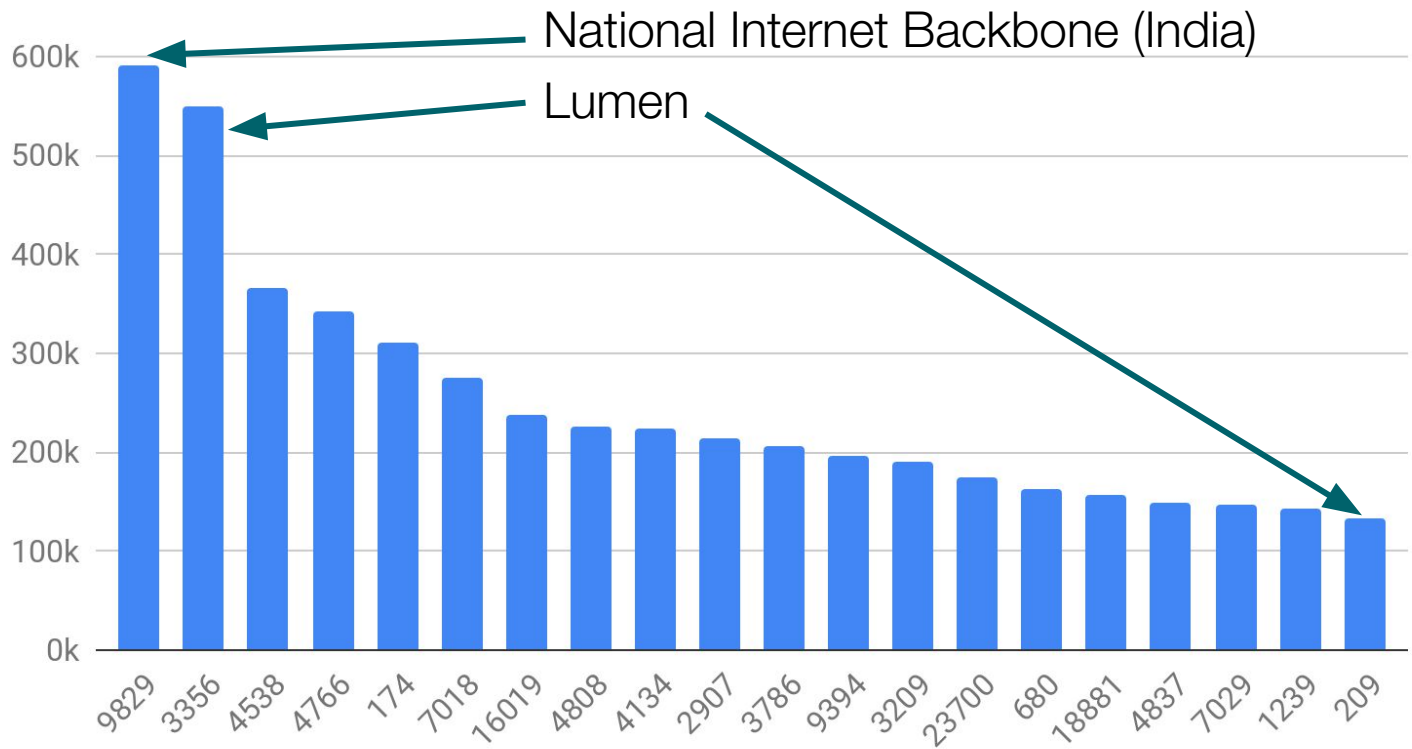


# Loop destinations by country (Europe)

| | |
|---|---|
| 3.5% | Germany |
| 2.4% | Russia |
| 1.9% | Italy |
| 1.8% | UK |
| 1.7% | Czechia |
| 1.2% | France |
| 1.1% | Poland |
| 1.0% | Sweden |
| 0.9% | Spain |
| 0.8% | Ukraine |



# Loop destinations by ASN (top 20, 17.6% of all loops)



# The net is dark and full of terrors

## 2 hops, but …

```
28. 1.208.160.1
29. 1.208.161.1, 210.206.207.194
30. 1.208.161.1
31. 1.208.161.1, 210.206.207.194
```

## 1 IP, but 2 hops RTT pattern

```
15. 195.43.166.44    65.2
16. 195.43.166.44   558.6
17. 195.43.166.44    75.4
18. 195.43.166.44   573.1
```

## 15 of 17 are missing

```
42. dis4-torontoxn_ae1.net.bell.ca
43. 67.69.163.242
44. ???
45. ???
46. ???
47. ???
48. ???
49. ???
50. ???
51. ???
52. ???
53. ???
54. ???
55. ???
56. ???
57. ???
58. ???
```

# The net is dark and full of terrors

## 34 hops in a single network

```
12. sto-ste-dr1-ar1.sto-vas29-dr1.bahnhof.net (176.10.180.142)
13. sto-vas29-dr1-ar1.sto-kn4-ar1.bahnhof.net (176.10.180.145)
14. sto-kn4-dr1.sto-kn5-dr1.bahnhof.net (176.10.181.40)
15. sto-kn5-dr1.sto-kn5-dr2.bahnhof.net (176.10.179.243)
16. sto-kn5-dr2.sto-sh-dr1.bahnhof.net (176.10.179.245)
17. sto-sh-dr1.sto-ss-dr1.bahnhof.net (176.10.179.247)
18. sto-ss-dr1.sto-ens-dr1.bahnhof.net (176.10.179.249)
19. sto-ens-dr1.sto-ars-dr1.bahnhof.net (176.10.178.115)
20. sto-ars-dr1.sto-orby-dr1.bahnhof.net (176.10.178.117)
21. sto-orby-dr1.hde-hud-dr1.bahnhof.net (176.10.178.69)
22. hde-hud-dr1.bot-tul-dr1.bahnhof.net (46.59.112.185)
23. bot-tul-dr1.bot-tb-dr1.bahnhof.net (85.24.151.19)
24. bot-tb-dr1.sod-sdt-dr2.bahnhof.net (176.10.181.148)
25. sod-sdt-dr2.sod-sdt-dr1.bahnhof.net (176.10.181.146)
26. sod-sdt-dr1.sod-hfv-ar1.bahnhof.net (46.59.113.229)
27. bka-tgv1-ar1.sod-hfv-ar1.bahnhof.net (176.10.179.67)
28. sod-hfv-ar1.bka-tgv1-ar1.bahnhof.net (176.10.179.66)
29. sod-hfv-ar1.sod-sdt-dr1.bahnhof.net (46.59.113.228)
30. sod-sdt-dr1.sod-sdt-dr2.bahnhof.net (176.10.181.147)
31. sod-sdt-dr2.bot-tb-dr1.bahnhof.net (176.10.181.149)
32. bot-tb-dr1.bot-tul-dr1.bahnhof.net (85.24.151.18)
33. bot-tul-dr1.hde-hud-dr1.bahnhof.net (46.59.112.184)
34. hde-hud-dr1.sto-orby-dr1.bahnhof.net (176.10.178.68)
35. sto-orby-dr1.sto-ars-dr1.bahnhof.net (176.10.178.116)
36. sto-ars-dr1.sto-ens-dr1.bahnhof.net (176.10.178.114)
37. sto-ens-dr1.sto-ss-dr1.bahnhof.net (176.10.179.248)
38. sto-ss-dr1.sto-sh-dr1.bahnhof.net (176.10.179.246)
39. sto-sh-dr1.sto-kn5-dr2.bahnhof.net (176.10.179.244)
40. sto-kn5-ar1.sto-soder-dr1.bahnhof.net (176.10.180.78)
41. sto-soder-dr1.sto-soder-dr2.bahnhof.net (176.10.181.59)
42. sto-soder-dr1.sto-pio-dr1.bahnhof.net (176.10.178.126)
43. sto-pio-dr1.sto-ste-dr3.bahnhof.net (176.10.181.223)
44. sto-ste-dr2.sto-ste-dr3.bahnhof.net (176.10.178.177)
45. sto-ste-dr2.sto-ste-dr1.bahnhof.net (176.10.178.174)
```

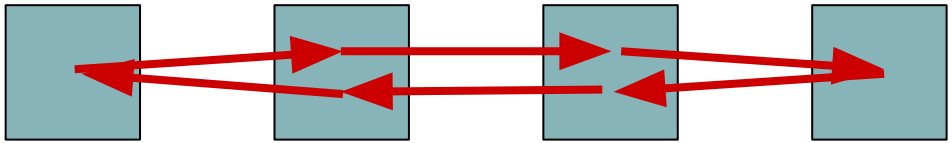
## 33 hops, 16 are missing

```
48. be-1412-cr12.pittsburgh.pa.ibone.comcast.net (96.110.38.158)
49. be-301-cr14.350ecermak.il.ibone.comcast.net (96.110.39.157)
50. be-1214-cs02.350ecermak.il.ibone.comcast.net (96.110.35.53)
51. be-1211-cr11.350ecermak.il.ibone.comcast.net (96.110.35.6)
52. be-302-cr11.1601milehigh.co.ibone.comcast.net (96.110.37.150)
53. be-1311-cs03.1601milehigh.co.ibone.comcast.net (96.110.39.73)
54. be-1314-cr14.1601milehigh.co.ibone.comcast.net (96.110.39.122)
55. be-304-cr14.champa.co.ibone.comcast.net (96.110.39.13)
56. be-1214-cs02.champa.co.ibone.comcast.net (96.110.37.245)
57. be-1211-cr11.champa.co.ibone.comcast.net (96.110.37.198)
58. be-302-cr01.seattle.wa.ibone.comcast.net (96.110.36.214)
59. be-10846-pe01.seattle.wa.ibone.comcast.net (68.86.86.90)
60. 96-87-8-90-static.hfc.comcastbusiness.net (96.87.8.90)
61. border1.ae2-bbnet2.sef.pnap.net (63.251.160.68)
62. usd-30.edge1.sef.pnap.net (64.94.137.194)
63. core.sea.dedicated.com (167.160.89.2)
64. 167.160.89.18
65. ???
66. ???
67. ???
68. ???
69. ???
70. ???
71. ???
72. ???
73. ???
74. ???
75. ???
76. ???
77. ???
78. ???
79. ???
80. ???
```

# The net is dark and full of terrors

“Flat” loop?

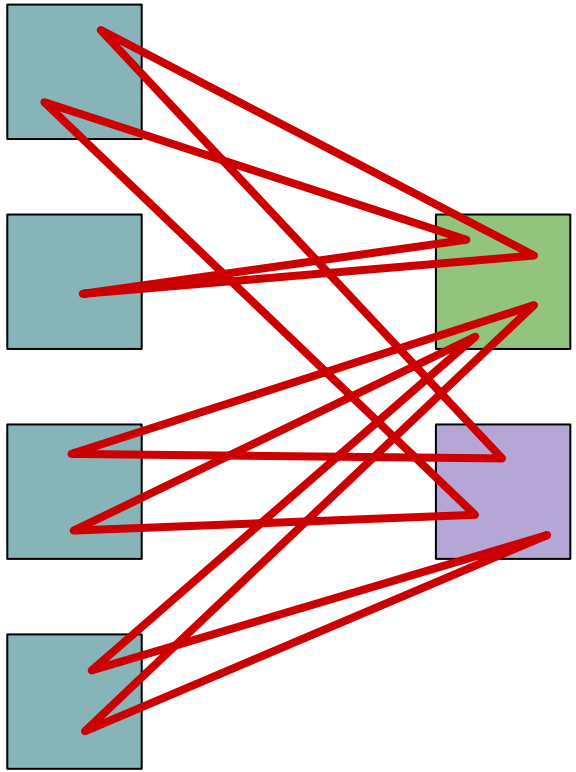
```
15. 140.156.broadband18.iol.cz (109.81.156.140)
16. 194.228.159.255
17. 194.228.190.142
18. 194.228.190.141
19. 194.228.190.142
20. 194.228.159.255
```



# The net is dark and full of terrors

## WTF?

```
37. AS23498   delivery.optix.ca (69.77.169.22)
38. AS174     38.131.181.74
39. AS23498   158.106.103.38
40. AS174     38.131.181.74
41. AS23498   delivery.optix.ca (69.77.169.22)
42. AS395965  69.194.36.66
43. AS23498   158.106.103.62
44. AS174     38.131.181.74
45. AS23498   69.77.169.42
46. AS395965  69.194.36.66
47. AS23498   69.77.169.42
48. AS174     38.131.181.74
49. AS23498   158.106.103.62
50. AS395965  69.194.36.66
```



# Easter eggs

- fun traceroutes
  - bad.horse
  - Star Wars
  - xmas.futile.net
- all dead now :(
- with one “exception”
  - routing loop!

```
11. ae0-1203.edge00.sov.uk.hso-group.net (46.17.60.117)
12. ???
13. ae0-1203.edge00.sov.uk.hso-group.net (46.17.60.117)
14. ???
```

```
15:  xoxoxoxoxoxo.Ho.Ho.Ho.xoxoxoxoxoxo
16:  ooooxooooooxooo.V.ooooooxooooxoooo
17:  ooxooooooxooooo.MMM.ooooooooxxooooxo
18:  oooxooooooxooo.EEEEE.oooxooooooxoooo
19:  ooooxooxooox.RRRRRRR.ooooooxooooox
20:  oxooooooxoo.RRRRRRRRR.oooxooooooxo
21:  xoooxooooo.YYYYYYYYYY.oooxooooxoo
22:  ooxooooooxooooo.CCC.ooooooooxooooxoo
23:  oooooxooo.HHHHHHHHHHHHH.oxooooxoooo
24:  ooxooxoo.RRRRRRRRRRRRRR.ooxooooxoo
25:  oxoooxo.IIIIIIIIIIIIIIII.oooxooxo
26:  oooxoo.SSSSSSSSSSSSSSSSS.ooxooooo
27:  oooxooooxoooooo.TTT.ooooooooooooxoo
28:  ooxoo.MMMMMMMMMMMMMMMMMMMM.oooxo
29:  xxoo.AAAAAAAAAAAAAAAAAAAAAA.oxoo
30:  oxo.SSSSSSSSSSSSSSSSSSSSSSS.ooo
31:  ooxooooooooooo.XXX.ooooooooooooxo
32:  oxooooooooooo.XXX.ooooooooooooxxo
33:  Oh.the.weather.outside.is.frightful
34:  But.the.fire.is.so.delightful
35:  And.since.weve.no.place.to.go
36:  Let.It.Snow.Let.It.Snow.Let.It.Snow
37:  xXx
38:  It.doesnt.show.signs.of.stopping
39:  And.Ive.bought.some.corn.for.popping
40:  The.lights.are.turned.way.down.low
41:  Let.It.Snow.Let.It.Snow.Let.It.Snow
42:  xXx
...
```