



DEBUGGING THE IMPOSSIBLE

THE BIT-FLIPPING STORY



CSA-14LY SPACE STATION

> LEVEL #1: LIVING QUARTERS <

| UPLINK READY |



Warning warning:
The air filtration
system of the living
quarters of CSA-14LY
is offline.

We need your help to reset
the air filtration system.
Hurry! Without air it's really
starting to suck in here ...

OPEN AIR FILTRATION
CONTROLS



The Sad Trombone Orchestra

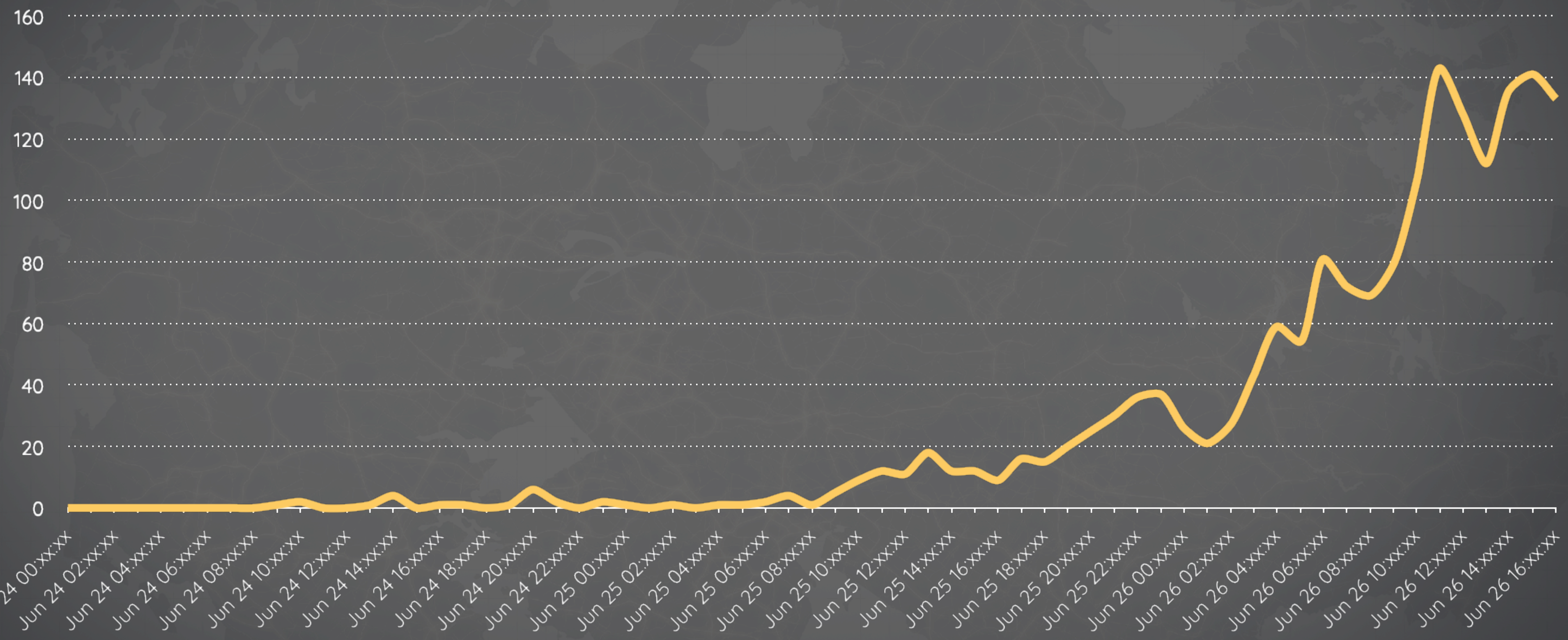


DEBUGGING THE IMPOSSIBLE



THE BIT-FLIPPING STORY

Health Check Failures





Create a test that triggers the problem

```
while curl -k -s https://direct.ip.of.a.backend  
do  
    sleep 1  
done
```




Spot the problem (pcap taken at A)

```
10:08:08.346990 IP A.60752 > B.443: Flags [S], seq 3109040127, win 64240, length 0
10:08:08.355178 IP B.443 > A.60752: Flags [S.], seq 2484654689, ack 3109040128, win 65160, length 0
10:08:08.355198 IP A.60752 > B.443: Flags [.] , ack 1, win 502, length 0
10:08:08.362804 IP A.60752 > B.443: Flags [P.], seq 1:518, ack 1, win 502, length 517
10:08:08.401071 IP B.443 > A.60752: Flags [.] , seq 1:1449, ack 518, win 506, length 1448
10:08:08.401087 IP A.60752 > B.443: Flags [.] , ack 1449, win 501, length 0
10:08:08.435439 IP B.443 > A.60752: Flags [P.], seq 4097:4208, ack 518, win 506, length 111
10:08:08.435450 IP A.60752 > B.443: Flags [.] , ack 1449, win 501, length 0
10:08:09.107535 IP B.443 > A.60752: Flags [.] , seq 1449:2897, ack 518, win 506, length 1448
10:08:15.183708 IP B.443 > A.60752: Flags [.] , seq 1449:2897, ack 518, win 506, length 1448
10:08:15.183755 IP A.60752 > B.443: Flags [.] , ack 2897, win 494, length 0
```




Spot the problem (pcap taken at A)

```
10:08:08.346990 IP A.60752 > B.443: Flags [S], seq 3109040127, win 64240, length 0
10:08:08.355178 IP B.443 > A.60752: Flags [S.], seq 2484654689, ack 3109040128, win 65160, length 0
10:08:08.355198 IP A.60752 > B.443: Flags [.], ack 1, win 502, length 0
10:08:08.362804 IP A.60752 > B.443: Flags [P.], seq 1:518, ack 1, win 502, length 517
10:08:08.401071 IP B.443 > A.60752: Flags [.], seq 1:1449, ack 518, win 506, length 1448
10:08:08.401087 IP A.60752 > B.443: Flags [.], ack 1449, win 501, length 0
10:08:08.435439 IP B.443 > A.60752: Flags [P.], seq 4097:4208, ack 518, win 506, length 111
10:08:08.435450 IP A.60752 > B.443: Flags [.], ack 1449, win 501, length 0
10:08:09.107535 IP B.443 > A.60752: Flags [.], seq 1449:2897, ack 518, win 506, length 1448
10:08:15.183708 IP B.443 > A.60752: Flags [.], seq 1449:2897, ack 518, win 506, length 1448
10:08:15.183755 IP A.60752 > B.443: Flags [.], ack 2897, win 494, length 0
```




```
# iptables-save | grep state
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

# sysctl net.netfilter.nf_conntrack_log_invalid=6 # 6 = TCP

# dmesg
...
nf_ct_proto_6: bad checksum IN= OUT= SRC=B DST=A LEN=899 TOS=0x00 PREC=0x00 TTL=51 ID=56562 DF
PROTO=TCP SPT=443 DPT=43948 SEQ=2289994758 ACK=1425635188 WINDOW=504 RES=0x00 ACK PSH URGP=0
```




Is it Me or Not Me?





It is Not Me

```

00000410: ed79 d7c6 12f7 f96b e70e 440d 55e3 f94e .y....k..D.U..N
00000420: a217 d587 1c42 0a55 d4fc c2a4 2346 fad2 .....B.U....#F..
00000430: d424 4adb f6a2 8df9 8f32 56f5 c343 a94d .$J.....2V..C.M
00000440: 8356 85b6 8c60 022e aa21 d5b7 c8ea 9423 .V...`...!.....#
00000450: 3a64 c8e7 dd3a c323 7f52 501b e393 76c6 :d...:.#.RP...v.
00000460: f231 6a70 a7c9 7f4b fe40 a3e3 27d9 8d09 .1jp...K.@..'...
00000470: d345 c041 7dae 98e0 405f cc40 a2eb b9f3 .E.A}...@_@....
00000480: de87 94aa c8ae 38ab 969d b719 fdab e9a9 .....8.....
00000490: 2a19 e9dd 983d 0cb9 462d 0374 9e21 c1b6 *....=..F-.t.!..
000004a0: 4bab 0db0 c469 df85 92a6 a9ac c232 e46e K....i.....2.n
000004b0: 15b1 619a 2fa2 02fe 8a26 cae6 a2dc 6b0e ..a./....&....k.
000004c0: 83c0 e19a 7cfd b56a 0a98 cbff d1ea 6ace ....l..j.....j.
000004d0: 8009 ca99 3e17 77ec f200 de20 9e6f e691 ....>.w.... .o..

```

Sent at B

```

00000410: ed79 d7c6 12f7 f96b e70e 440d 55e3 f94e .y....k..D.U..N
00000420: a217 d587 1c42 0a55 d4fc c2a4 2346 fad2 .....B.U....#F..
00000430: d424 4adb f6a2 8df9 8f32 56f5 c343 a94d .$J.....2V..C.M
00000440: 8356 85b6 8c60 022e aa21 d5b7 c8ea 9423 .V...`...!.....#
00000450: 3a64 c8e7 dd3a c323 7f52 501b e393 76c6 :d...:.#.RP...v.
00000460: f231 6a70 a7c9 7f4b fe40 a3e3 27d9 8d09 .1jp...K.@..'...
00000470: d345 c040 7dae 98e0 405f cc40 a2eb b9f3 .E.@}...@_@....
00000480: de87 94aa c8ae 38ab 969d b719 fdab e9a9 .....8.....
00000490: 2a19 e9dd 983d 0cb9 462d 0374 9e21 c1b6 *....=..F-.t.!..
000004a0: 4bab 0db0 c469 df85 92a6 a9ac c232 e46e K....i.....2.n
000004b0: 15b1 619a 2fa2 02fe 8a26 cae6 a2dc 6b0e ..a./....&....k.
000004c0: 83c0 e19a 7cfd b56a 0a98 cbff d1ea 6ace ....l..j.....j.
000004d0: 8009 ca99 3e17 77ec f200 de20 9e6f e691 ....>.w.... .o..

```

Received at A



Not the best ticket

To: Helpdesk of DC2
Subject: Packet Corruption

Dear DC2,

Someone is flipping bits in some of the packets.

Please fix,

Frank



#NLNOG to the rescue!

The screenshot shows a Twitter thread on the #nlnog hashtag. The thread includes several tweets, with the most visible ones from a user named Haakjes. The tweets discuss a network issue related to a checksum error.

N #nlnog

H Haakjes
ik heb random packetless omdat de checksum 1 bit verkeerd is, tcpdump -vv zegt dan: cksum 0xcce (incorrect → 0xccf) (edited)

H Haakjes
iemand enig idee wat dit kan veroorzaken?



Make it easy to see the problem

```
$ curl http://B/AAAAAAAAAAAAAAAAAAAAA.....AAAAAA
```

```
HTTP/1.1 302 Found  
content-length: 0  
location: https://B/AAAAAAAAAAAAAAAAAAAAA.....AAAAAA  
cache-control: no-cache
```




Make it easy to see the problem

```
0x00d0: 4141 4141 4141 4141 4141 4141 4141 4141 4141 4141
0x00e0: 4141 4141 4141 4141 4141 4141 4141 4141 4141 4141
0x00f0: 4141 4140 4141 4141 4141 4141 4141 4141 4141 4141
0x0100: 4141 4141 4141 4141 4141 4141 4141 4141 4141 4141
0x0110: 4141 4141 4141 4141 4141 4141 4141 4141 4141 4141
```




Make it easy to see the problem

```
0x00d0: 4141 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAAAA
0x00e0: 4141 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAAAA
0x00f0: 4141 4140 4141 4141 4141 4141 4141 4141 4141  AAA@AAAAAAAAAAAAAA
0x0100: 4141 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAAAA
0x0110: 4141 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAAAA
```




Findings so far (with help of #NLNOG)

- ▶ Bit flips from DC2 to OVH
- ▶ Bit flips from DC2 to TransIP
- ▶ No bit flips from DC2 to A2B Internet



DEBUGGING THE IMPOSSIBLE

THE BIT-FLIPPING STORY

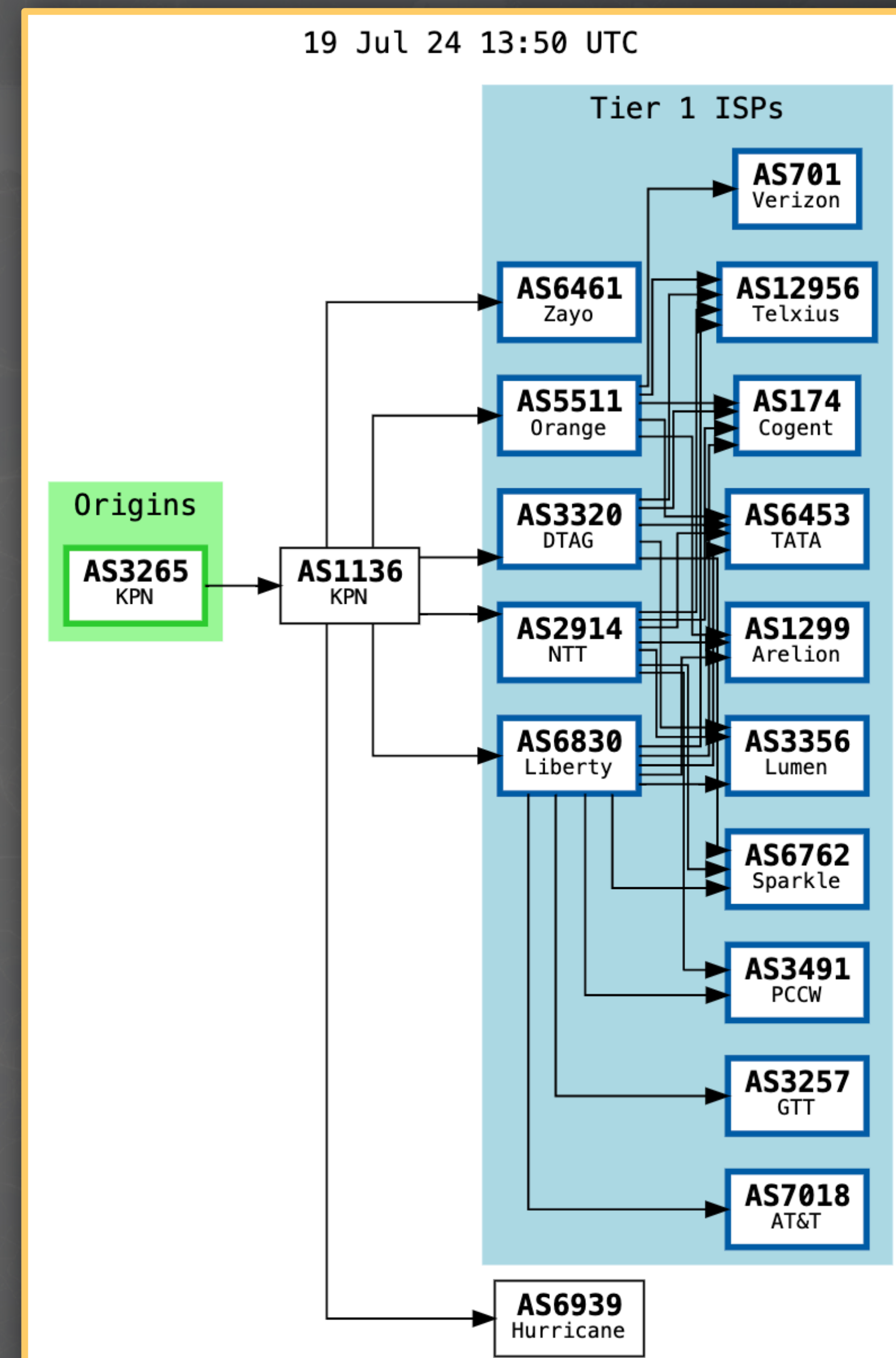
Is it just me?

✓ Our Servers

✓ AS3265 - DC2 (was XS4ALL, now KPN)

□ AS1136 - KPN

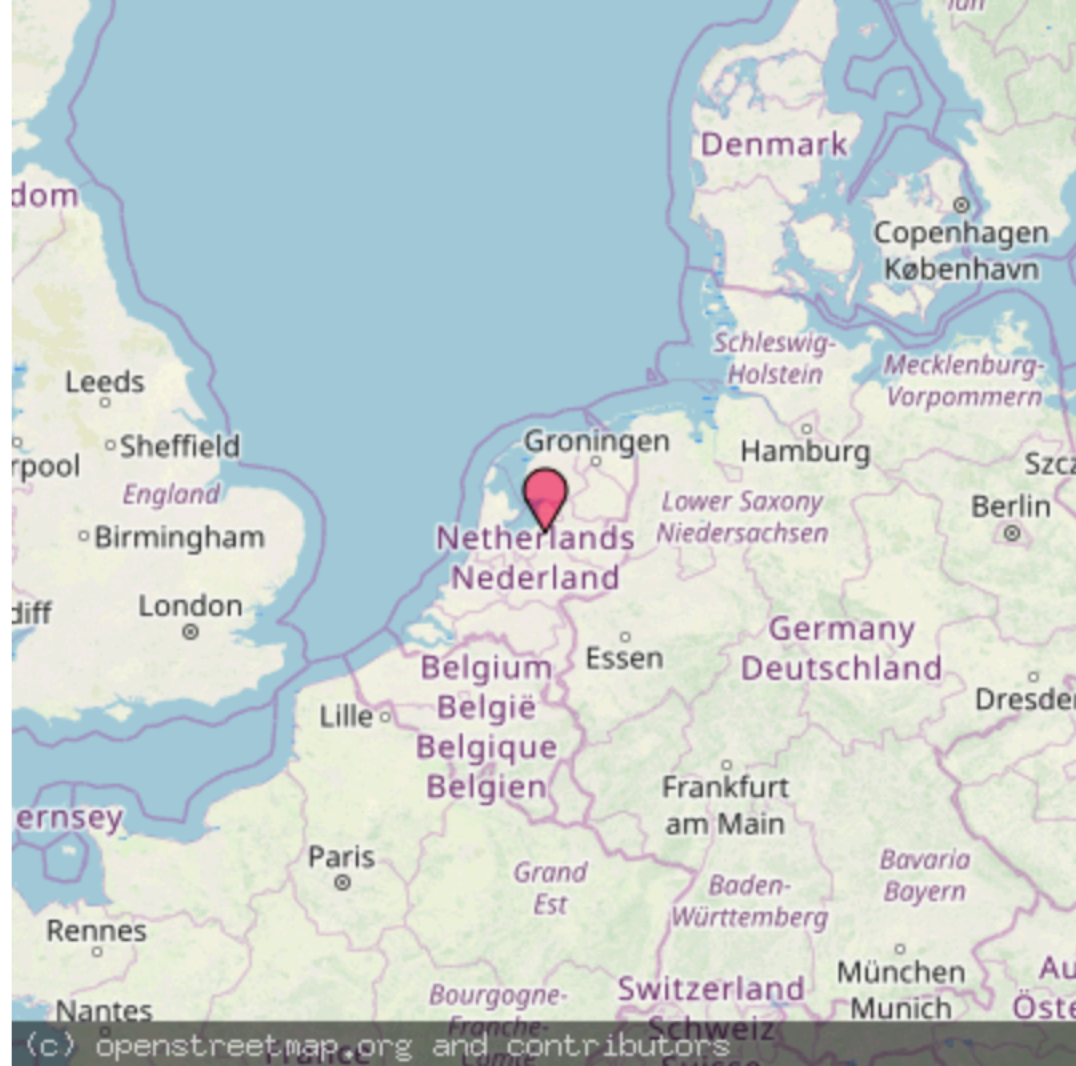
□ Something bigger



AS1136 - KPN B.V.

Summary AS1136

<table style="width: 100%; border-collapse: collapse;"> <tr><td style="padding: 2px 5px;">AS Number</td><td style="padding: 2px 5px;">1136 (AS1136/ASN1136)</td></tr> <tr><td style="padding: 2px 5px;">Organization</td><td style="padding: 2px 5px;">KPN B.V.</td></tr> <tr><td style="padding: 2px 5px;">Allocation date</td><td style="padding: 2px 5px;">1993-09-01 by RIPE</td></tr> <tr><td style="padding: 2px 5px;">Number IPv4 address</td><td style="padding: 2px 5px;">6,747,648</td></tr> <tr><td style="padding: 2px 5px;">ASRank ?</td><td style="padding: 2px 5px;">78</td></tr> <tr><td style="padding: 2px 5px;">Number of prefixes</td><td style="padding: 2px 5px;">414 (IPv4) / 17 (IPv6)</td></tr> <tr><td style="padding: 2px 5px;">Has Bogon prefixes</td><td style="padding: 2px 5px;">No</td></tr> <tr><td style="padding: 2px 5px;">Number of peers</td><td style="padding: 2px 5px;">55 (IPv4) / 47 (IPv6)</td></tr> <tr><td style="padding: 2px 5px;">Number of domains hosted</td><td style="padding: 2px 5px;">28,794</td></tr> <tr><td style="padding: 2px 5px;">Number of adult domains hosted</td><td style="padding: 2px 5px;">4</td></tr> <tr><td style="padding: 2px 5px;">Number of NS records hosted</td><td style="padding: 2px 5px;">641</td></tr> <tr><td style="padding: 2px 5px;">Number of MX records hosted</td><td style="padding: 2px 5px;">14,249</td></tr> <tr><td style="padding: 2px 5px;">Number of SPAM hosts</td><td style="padding: 2px 5px;">7</td></tr> <tr><td style="padding: 2px 5px;">Number of open proxies</td><td style="padding: 2px 5px;">0</td></tr> </table>	AS Number	1136 (AS1136/ASN1136)	Organization	KPN B.V.	Allocation date	1993-09-01 by RIPE	Number IPv4 address	6,747,648	ASRank ?	78	Number of prefixes	414 (IPv4) / 17 (IPv6)	Has Bogon prefixes	No	Number of peers	55 (IPv4) / 47 (IPv6)	Number of domains hosted	28,794	Number of adult domains hosted	4	Number of NS records hosted	641	Number of MX records hosted	14,249	Number of SPAM hosts	7	Number of open proxies	0	<table style="width: 100%; border-collapse: collapse;"> <tr><td style="padding: 2px 5px;">Country</td><td style="padding: 2px 5px;">Netherlands (NL </td></tr> <tr><td style="padding: 2px 5px;">Continent</td><td style="padding: 2px 5px;">Europe</td></tr> <tr><td style="padding: 2px 5px;">Capital</td><td style="padding: 2px 5px;">Amsterdam</td></tr> </table>	Country	Netherlands (NL	Continent	Europe	Capital	Amsterdam
AS Number	1136 (AS1136/ASN1136)																																		
Organization	KPN B.V.																																		
Allocation date	1993-09-01 by RIPE																																		
Number IPv4 address	6,747,648																																		
ASRank ?	78																																		
Number of prefixes	414 (IPv4) / 17 (IPv6)																																		
Has Bogon prefixes	No																																		
Number of peers	55 (IPv4) / 47 (IPv6)																																		
Number of domains hosted	28,794																																		
Number of adult domains hosted	4																																		
Number of NS records hosted	641																																		
Number of MX records hosted	14,249																																		
Number of SPAM hosts	7																																		
Number of open proxies	0																																		
Country	Netherlands (NL																																		
Continent	Europe																																		
Capital	Amsterdam																																		



DNS Records

Domain Records

IPv4 with Domains

NS Records

MX Records

PTR Records

Number of open proxies

0


DNS Records

Domain Records

IPv4 with Domains

NS Records

MX Records

PTR Records 

10 entries per page

Search...

Domain	DomainRank	IPv4
amsterdam.nl	68	
efteling.com	55	
nielsvm.org	53	
vb.net	53	
cz.nl	53	
bitstorm.org	51	
berthub.eu	48	
nicon.nl	48	
abp.nl	47	
doenietzomoeilijk.nl	46	

Showing 1 to 10 of 50 entries

< 1 2 3 4 5 >

Prefixes and Peers

Prefixes V4

Prefixes V6

Peers V4

Peers V6



berthub.eu

```
0x0090: 6f6e 7465 6e74 2d54 7970 653a 2074 6578 ontent-Type:.tex
0x00a0: 742f 6874 6d6c 0d0a 436f 6e74 656e 742d t/html..Content-
0x00b0: 4c65 6e67 7468 3a20 3136 390d 0a43 6f6e Length:.169..Con
0x00c0: 6e65 6374 696f 6e3a 206b 6565 702d 616c nection:.keep-al
0x00d0: 6976 650d 0a4c 6f63 6174 696f 6e3a 2068 ive..Location:.h
0x00e0: 7474 7073 3a2f 2f62 6572 7468 7562 2e65 ttps://berthub.e
0x00f0: 752f 4141 4141 4141 4141 4141 4141 4141 u/AAAAAAAAAAAAAAAA
0x0100: 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAA
0x0110: 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAA
0x0120: 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAA
0x0130: 4141 4140 4141 4141 4141 4141 4141 4141 AAA@AAAAAAAAAAAAAAAA
0x0140: 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAA
```




DEBUGGING THE IMPOSSIBLE

THE BIT-FLIPPING STORY

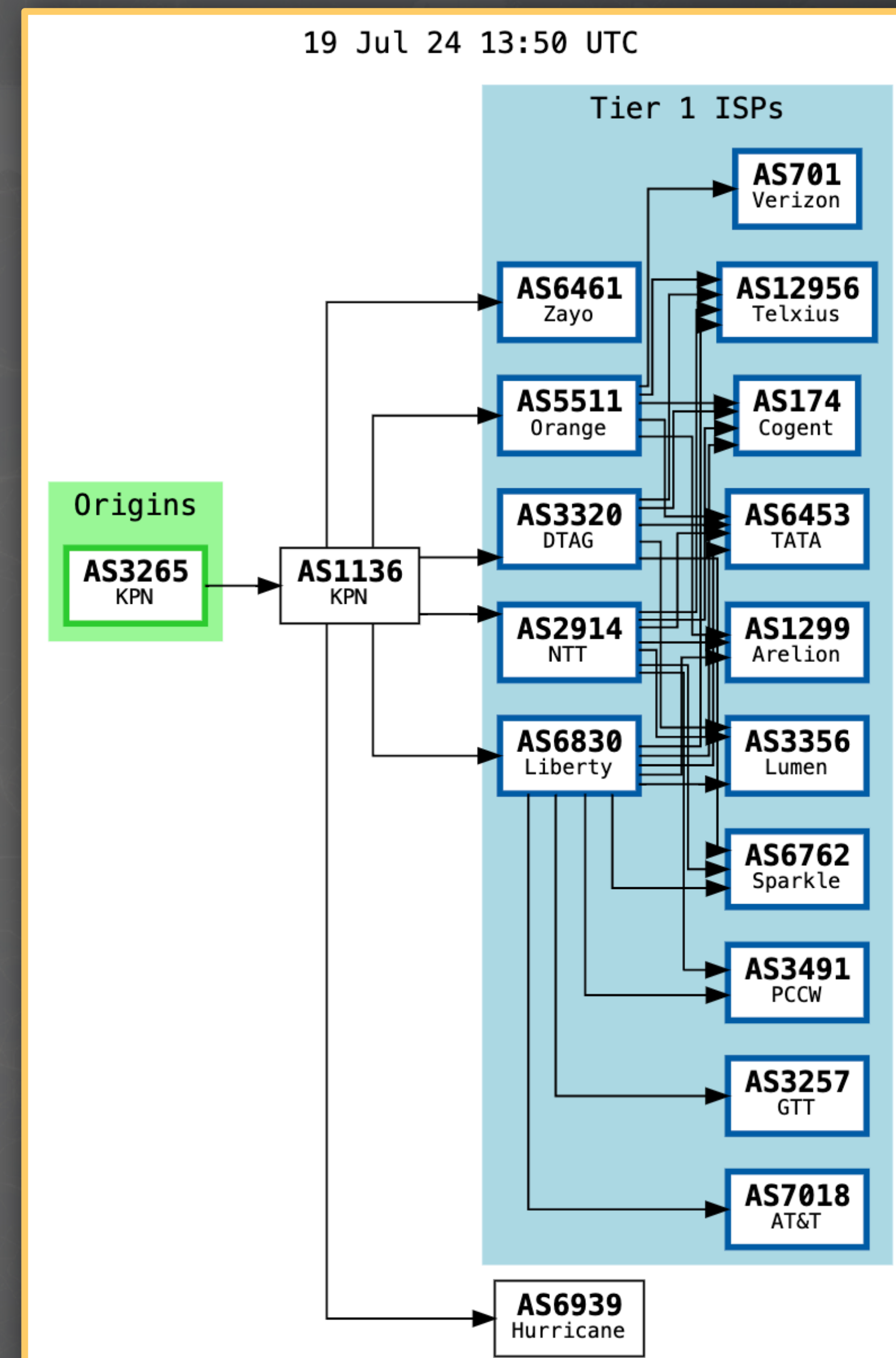
Is it just me?

✓ Our Servers

✓ AS3265 - DC2 (was XS4ALL, now KPN)

✓ AS1136 - KPN

☐ Something bigger



Files

main + 🔍

Go to file t

bitflipper.py

bitflipper.sh

bitflipper / bitflipper.sh

bitflipperdev Update bitflipper.sh

f882215 · 4 months ago History

Code Blame Executable File · 121 lines (105 loc) · 3.5 KB Code 55% faster with GitHub Copilot

Raw 📄 ⬇️ 📄 ⌵ 📄

```
1  #!/bin/bash
2
3  # set target and outgoing interface
4  TARGET=$1
5  OUTGOING_INTERFACE=$2
6  HOST=$3
7  WHEN=$(date +%Y-%m-%d-%H:%M:%S)
8  TARGET_PCAP="bitflipper_${TARGET}_${HOST}_${WHEN}.pcap"
9  REPORT="bitflipper_${TARGET}_${HOST}_${WHEN}.txt"
10
11  REQS=(date shasum tee python3 curl grep mtr tcpdump tail cat)
12  REQSMISSING=0
13  for cmd in ${REQS[@]}; do
14      if [ ! -x "$(which ${cmd})" ]; then
15          echo "Prerequisite ${cmd} not found and/or not executable"
16          REQSMISSING=1
17      fi
18  done;
19  [ ${REQSMISSING} == 1 ] && exit 1;
20
21  echo "Running $0 $*" | tee -a $REPORT
22  echo "Script $(shasum $0)" | tee -a $REPORT
23
24  if [ -z "$HOST" ]
25  then
26      echo "Usage: $0 <target ip> <outgoing interface> <hostname (for the host header)>"
27      exit 1
28  fi
29
30  echo "Testing if we can make the system return our data in the path"
31  CURL_PATH=$(python3 -c 'print("A"*2048)')
32  CURL_HOST=$(python3 -c 'print("C"*2048)')
33
34  if ! curl -v http://$TARGET/$CURL_PATH -H Host:\ $CURL_HOST -k -m 30 2>&1 | grep -v '^>' | grep -i '\(AAAAAAAA\)\|(CCCCCCCC\)' >/dev/null
35  then
36      echo "Not working with CCCC in host and AAAA in path, trying with the correct host"
37      CURL_HOST=$HOST
38      if ! curl -v http://$TARGET/$CURL_PATH -H Host:\ $CURL_HOST -k -m 30 2>&1 | grep -v '^>' | grep -i AAAAAAAA >/dev/null
39      then
40          echo "Could not find any way to make curl return our AAAAA data"
```




- ▶ Specify a target IP/hostname
- ▶ Record a traceroute (TCP and ICMP)
- ▶ Start tcpdump
- ▶ Send 1000 HTTP requests that return AAAAAAAAAA
- ▶ Stop tcpdump
- ▶ Look for AAA@AAA
- ▶ Upload all results to 6paster
- ▶ Print 6paster URL to share

Running ./bitflipper.sh REDACTED ens3 certifiedsecure.org
Script f8b4fdcbefca9aeca1554e42963b6c769deffb10 ./bitflipper.sh

Using the following request: curl http://REDACTED/AAA...AAA -H Host:\ CCC...CCC -k -m 30

Start: 2024-07-01T19:34:23+0000

HOST: ubuntu		Loss%	Snt	Last	Avg	Best	Wrst	StDev
1.	AS??? ???	100.0	10	0.0	0.0	0.0	0.0	0.0
2.	AS??? ???	100.0	10	0.0	0.0	0.0	0.0	0.0
3.	AS20857 f2.r2.ams0.transip.net (77.72.151.126)	0.0%	10	2.9	1.3	0.4	6.4	1.9
	AS20857 f1.r2.ams0.transip.net (77.72.151.124)							
	AS20857 f2.r1.ams0.transip.net (77.72.151.122)							
4.	AS20857 r1-a0.e1.ams0.transip.net (157.97.168.9)	0.0%	10	0.5	0.7	0.5	1.0	0.2
	AS20857 r2-a0.e1.ams0.transip.net (157.97.168.10)							
5.	AS57866 cr0.nikhef.nl.fusixnetworks.net (37.139.140.234)	0.0%	10	0.8	1.1	0.7	2.6	0.6
6.	AS57866 br0.eqxam6.nl.fusixnetworks.net (37.139.139.23)	0.0%	10	17.7	2.7	0.8	17.7	5.3
7.	AS??? ???	100.0	10	0.0	0.0	0.0	0.0	0.0
8.	AS6830 cz-prg02b-rr5-em1-55.aorta.net (84.116.136.178)	0.0%	10	1.7	1.6	1.3	2.2	0.3
	AS6830 cz-prg02b-rr5-em0-50.aorta.net (84.116.136.174)							
9.	AS6830 cz-prg01a-ra4-ae-98-55.aorta.net (84.116.136.177)	20.0%	10	7208.	2674.	1.6	7208.	3032.1
	AS6830 cz-prg02a-ra2-ae-98-50.aorta.net (84.116.136.173)							
10.	AS??? ???	100.0	10	0.0	0.0	0.0	0.0	0.0
11.	AS??? ???	100.0	10	0.0	0.0	0.0	0.0	0.0
12.	AS3265 0.ae10.xrc2.3d12.xs4all.net (194.109.5.118)	0.0%	10	2.7	4.9	2.7	12.7	2.9
	AS3265 0.ae11.xrc1.1d12.xs4all.net (194.109.5.102)							
13.	AS3265 REDACTED	0.0%	10	3.8	4.1	3.8	4.4	0.2

Start: 2024-07-01T19:34:42+0000

HOST: ubuntu		Loss%	Snt	Last	Avg	Best	Wrst	StDev
1.	AS20857 v1035.l11.ams4.transip.net (37.97.137.220)	0.0%	10	23.0	19.4	2.6	80.5	22.6
2.	AS20857 l11.f1.ams4.transip.net (77.72.151.20)	0.0%	10	12.0	14.2	5.0	21.6	5.4
3.	AS20857 f1.r1.ams0.transip.net (77.72.151.120)	0.0%	10	0.9	0.6	0.4	1.5	0.3
4.	AS20857 r1-a0.e1.ams0.transip.net (157.97.168.9)	0.0%	10	0.6	8.6	0.6	37.8	13.8
5.	AS57866 cr0.nikhef.nl.fusixnetworks.net (37.139.140.234)	0.0%	10	0.7	0.8	0.6	1.0	0.1
6.	AS57866 br0.eqxam6.nl.fusixnetworks.net (37.139.139.23)	0.0%	10	1.9	3.0	0.8	14.5	4.3

4.	AS20857	r1-a0.e1.ams0.transip.net (157.97.168.9)	0.0%	10	0.5	0.7	0.5	1.0	0.2
	AS20857	r2-a0.e1.ams0.transip.net (157.97.168.10)							
5.	AS57866	cr0.nikhef.nl.fusixnetworks.net (37.139.140.234)	0.0%	10	0.8	1.1	0.7	2.6	0.6
6.	AS57866	br0.eqxam6.nl.fusixnetworks.net (37.139.139.23)	0.0%	10	17.7	2.7	0.8	17.7	5.3
7.	AS???	???	100.0	10	0.0	0.0	0.0	0.0	0.0
8.	AS6830	cz-prg02b-rr5-em1-55.aorta.net (84.116.136.178)	0.0%	10	1.7	1.6	1.3	2.2	0.3
	AS6830	cz-prg02b-rr5-em0-50.aorta.net (84.116.136.174)							
9.	AS6830	cz-prg01a-ra4-ae-98-55.aorta.net (84.116.136.177)	20.0%	10	7208.	2674.	1.6	7208.	3032.1
	AS6830	cz-prg02a-ra2-ae-98-50.aorta.net (84.116.136.173)							
10.	AS???	???	100.0	10	0.0	0.0	0.0	0.0	0.0
11.	AS???	???	100.0	10	0.0	0.0	0.0	0.0	0.0
12.	AS3265	0.ae10.xrc2.3d12.xs4all.net (194.109.5.118)	0.0%	10	2.7	4.9	2.7	12.7	2.9
	AS3265	0.ae11.xrc1.1d12.xs4all.net (194.109.5.102)							
13.	AS3265	REDACTED	0.0%	10	3.8	4.1	3.8	4.4	0.2

Start: 2024-07-01T19:34:42+0000

HOST: ubuntu

			Loss%	Snt	Last	Avg	Best	Wrst	StDev
1.	AS20857	v1035.l11.ams4.transip.net (37.97.137.220)	0.0%	10	23.0	19.4	2.6	80.5	22.6
2.	AS20857	l11.f1.ams4.transip.net (77.72.151.20)	0.0%	10	12.0	14.2	5.0	21.6	5.4
3.	AS20857	f1.r1.ams0.transip.net (77.72.151.120)	0.0%	10	0.9	0.6	0.4	1.5	0.3
4.	AS20857	r1-a0.e1.ams0.transip.net (157.97.168.9)	0.0%	10	0.6	8.6	0.6	37.8	13.8
5.	AS57866	cr0.nikhef.nl.fusixnetworks.net (37.139.140.234)	0.0%	10	0.7	0.8	0.6	1.0	0.1
6.	AS57866	br0.eqxam6.nl.fusixnetworks.net (37.139.139.23)	0.0%	10	1.9	3.0	0.8	14.5	4.3
7.	AS33915	nl-ams09c-ri1-ae-10-0.aorta.net (213.46.183.25)	0.0%	10	1.2	1.2	1.1	1.3	0.0
8.	AS6830	de-fra04d-rc1-ae-1-35.aorta.net (84.116.138.5)	60.0%	10	1.2	1.4	1.2	1.4	0.1
9.	AS6830	cz-prg02a-ra2-ae-98-50.aorta.net (84.116.136.173)	80.0%	10	1.8	1.8	1.8	1.8	0.0
10.	AS33915	213.46.182.206	70.0%	10	95.2	90.1	86.7	95.2	4.5
11.	AS???	???	100.0	10	0.0	0.0	0.0	0.0	0.0
12.	AS3265	0.ae10.xrc2.3d12.xs4all.net (194.109.5.118)	0.0%	10	4.1	7.7	4.1	26.4	7.1
13.	AS3265	REDACTED	0.0%	10	4.2	4.2	4.0	4.3	0.1

Finding packets with bitflips

Bitflips found!

```

0x0450:  4141 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAAAA
0x0460:  4141 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAAAA
0x0470:  4141 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAAAA
0x0480:  4141 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAAAA
0x0490:  4141 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAAAA
0x04a0:  4141 4141 4141 4141 4141 4141 4141 4141 4141  AAAAAAAAAAAAAAAAAA

```


Finding packets with bitflips
Bitflips found!

```
0x0450: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0460: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0470: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0480: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0490: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x04a0: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x04b0: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x04c0: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x04d0: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x04e0: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x04f0: 4141 4140 4141 4141 4141 4141 4141 4141 4141 AAA@AAAAAAAAAAAAAA
0x0500: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0510: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0520: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0530: 4141 4141 4141 410d 0a53 7472 6963 742d AAAAAA..Strict-
0x0540: 5472 616e 7370 6f72 742d 5365 6375 7269 Transport-Securi
0x0550: 7479 3a20 6d61 782d 6167 653d 3331 3533 ty:.max-age=3153
0x0560: 3630 3030 0d0a 0d0a 6000....
```

--

```
0x0310: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0320: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0330: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0340: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0350: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0360: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0370: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0380: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0390: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x03a0: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x03b0: 4141 4140 4141 4141 4141 4141 4141 4141 4141 AAA@AAAAAAAAAAAAAA
0x03c0: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x03d0: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x03e0: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x03f0: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0400: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
0x0410: 4141 4141 4141 4141 4141 4141 4141 4141 4141 AAAAAAAAAAAAAAAAAA
```




Findings so far (with help of #nlnoG)

- ▶ Bit flips from DC2 to OVH
- ▶ Bit flips from DC2 to TransIP
- ▶ Bit flips from KPN FTTH to TransIP
- ▶ Bit flips from KPN FTTH to Freedom
- ▶ No bit flips from DC2 to A2B Internet



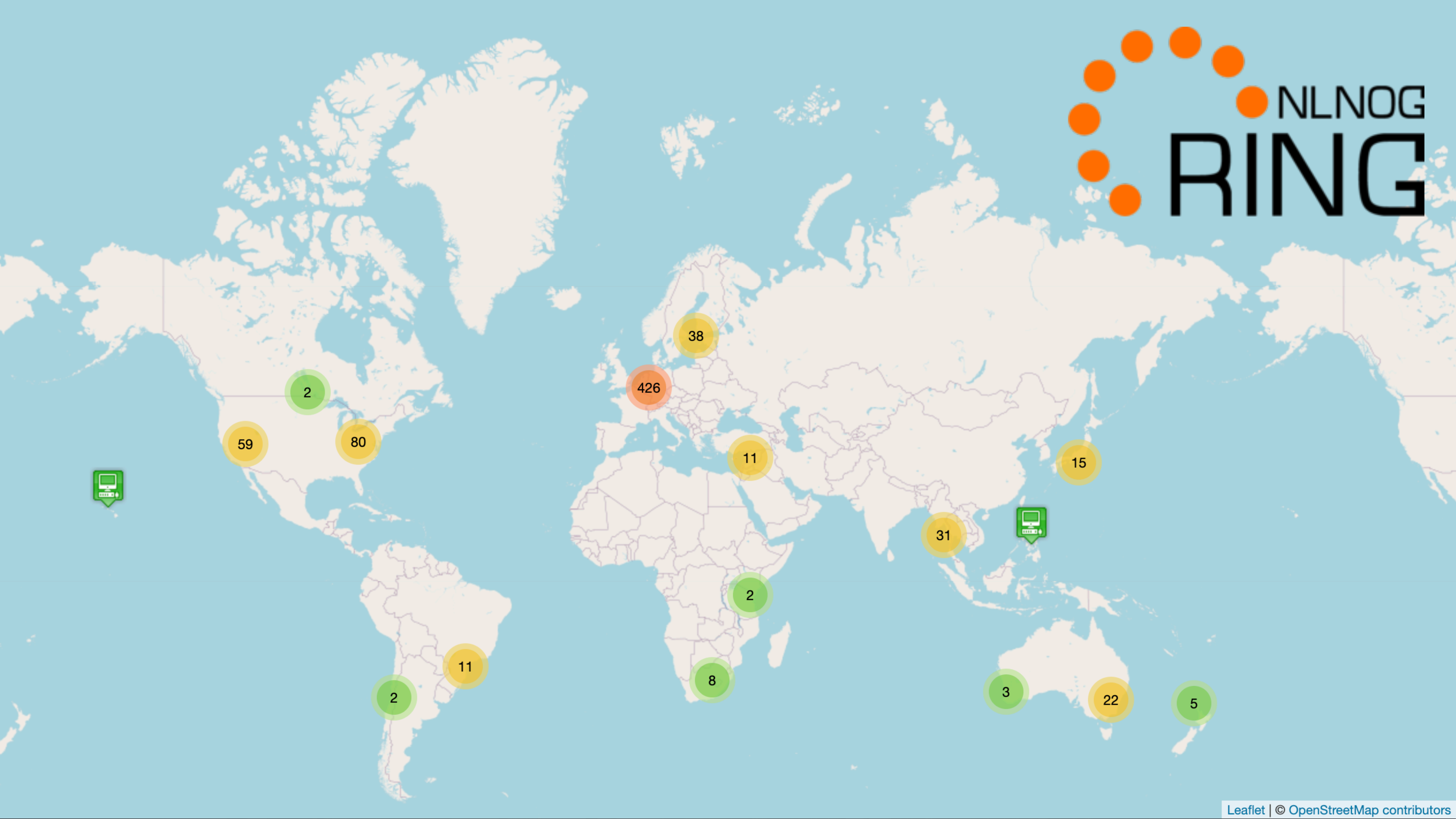
Where in the route is the problem?

HOST: ovh06.ring.nlnog.net

- 1. AS16276 51.89.116.1
- 2. AS??? 192.168.143.254
- 3. AS??? 10.13.120.254
- 4. AS??? 10.13.118.38
- 5. AS??? 10.13.118.54
- 6. AS??? 10.73.41.16
- 7. AS??? 10.73.249.66
- 8. AS16276 be105.ams-gsa1-sbb1-nc5.nl.eu
- 9. AS??? 10.200.4.133
- 10. AS??? kpn-as1136.kpn-asd-dc2.nl-ix.net
- 11. AS??? ???
- 12. AS3265 0.ae11.xrc2.3d12.xs4all.net
- 13. AS3265 REDACTED

HOST: VM in TransIP

- 1. AS20857 v1035.l11.ams4.transip.net
- 2. AS20857 l11.f1.ams4.transip.net
- 3. AS20857 f1.r1.ams0.transip.net
- 4. AS20857 r1-a0.e1.ams0.transip.net
- 5. AS57866 cr0.nikhef.nl.fusixnetworks.net
- 6. AS57866 br0.eqxam6.nl.fusixnetworks.net
- 7. AS33915 nl-ams09c-ri1-ae-10-0.aorta.
- 8. AS6830 de-fra04d-rc1-ae-1-35.aorta.net
- 9. AS6830 cz-prg02a-ra2-ae-98-50.aorta.net
- 10. AS33915 213.46.182.206
- 11. AS??? ???
- 12. AS3265 0.ae10.xrc2.3d12.xs4all.net
- 13. AS3265 REDACTED





77 of 685 ring nodes detected bit flipping

```
6connect01
accenture01
  ahdde01
  amazon02
  amazon18
  atom01
boxed-it01
businessconnect01
  c3noc01
  cesnet01
clearnetworx01
connectria01
  copaco01
  dcsone01
  denic01
  ebox02
  edgoo02
  epsilon01
equinixnl01
  ficolo01
  fiebig01
  franceix01
  hextet01
  hostin01
hosting4real01
  in2ip01
  inberlin01
  infowest01

interconnect01
  inxza02
  ionos01
  ipbde01
jointtransit01
kantonsschulezug01
  lagis01
  linode11
  linode20
  linode21
  luna01
  marbis01
  massar01
  mauve01
  mciu01
  mfiles01
  moji01
  msu01
natesales01
neutrinet01
  newvm01
  nimag01
nordunet01
  ovh01
  ovh05
  ovh08
  poznan01
  riepert01

ripe01
rootnl01
signet01
skyway01
speakup01
strato01
suomi01
surfnet01
techfutures01
  teleag01
  tigron01
  transip01
  v4less01
  v4less03
  vancis01
  vangulik01
  viatel03
  vimexx01
  vultr05
  vultr12
worldstream01
```




PLACE YOUR BETS

Findings so far (with help of #NLNOG and NLNOG Ring)

- ▶ Bit flips outgoing from AS1136 to 77 ring nodes
- ▶ Bit flips incoming from some websites to AS1136
- ▶ If a path has bit flips
 - ▶ then 1.5% of the TCP/UDP connections have bit flips
 - ▶ ICMP never has bit flips
- ▶ If a connection has bit flips
 - ▶ then 5% of the packets have bit flips
- ▶ Bits flip from 1 to 0 at bytes 0x00b3, 0x133, 0x1b3, 0x2b3, etc
 - ▶ But not always at all of the bytes



Working theory

- ▶ Link Aggregation chooses port based on L2 and L3 headers
 - ▶ src ip, dst ip, src port, dst port, protocol
- ▶ One of the ports has broken memory
- ▶ Packet is written to memory and then read from memory
 - ▶ A bit is written as 1, but read from memory as 0



bitflipper.py:

- ▶ Setup 400 connections (UDP, source port starting at 40000)
 - ▶ Send 150 packets with 1000 times "A" as one long string
 - ▶ Server will echo all packets
- ▶ Very quick to test
 - ▶ 60.000 packets over UDP
- ▶ Low chance of false negative



Probability we see no bit flips on a bad path

- ▶ Probability of a connection not having bit flips: 98.5%
- ▶ Probability of a connection having bit flips: 1.5%
 - ▶ Probability of a packet having no bit flips: 95%
- ▶ Probability of 400 connections with 150 packets and no bit flips
 - ▶ $(0.985 + (0.015 * 0.95^{150}))^{400} = 0.0023 = 0.23\%$



Locating the path with bit flips

- ▶ Reroute part of the network and test
- ▶ Binary search



INC#11173026 - Afgehandeld

Geachte,

U ontvangt deze melding omdat u voor dit incident op de distributielijst staat. Het incident INC#11173026 betreffende Packet corruption on DC2 Network, is afgehandeld.

Oplossing:

For the bitflip issue. For +/- 2 weeks there were reports of packetloss which resulted from flipping bits in payload of IP packets. The NLNOG community was very active with this issue and somebody wrote testscripts and the NLnog Ringnode network was used for reproducing this issue which was reproducible on +/- 50-60 networks from in total 700 networks tested.

In this maintenance window we were able by switching a lot of traffic to redundant paths to isolate it to 1 single 100Gig port between KPN and NL-IX.

When NL-IX reloaded their linecard on which this port was connected to, problems were solved and we have extensively tested it and were not able to reproduce the issue anymore.

NL-IX will investigate if they want to pro-active hardware-replace this card. For now, all seems stable and the port in question is taking traffic and doing fine.

This issue was highly visible and spoken about in the (dutch) network community.



Debugging the impossible:

- ▶ Continuously test your production environment as a user
- ▶ Make problems repeatable, visible and impossible to ignore
- ▶ Enable others to easily replicate and research the problem
- ▶ NLNOG Community and NLNOG Ring are critical infrastructure



DEBUGGING THE IMPOSSIBLE

THE BIT-FLIPPING STORY