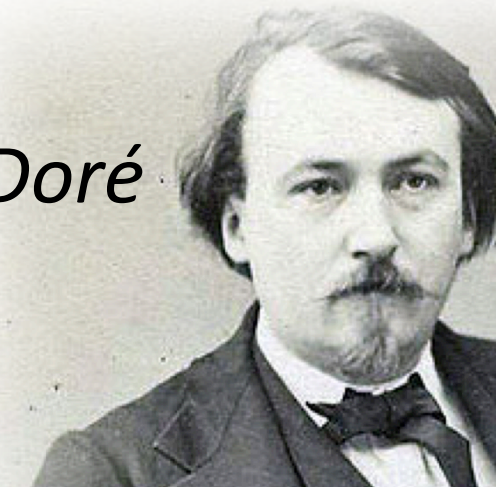
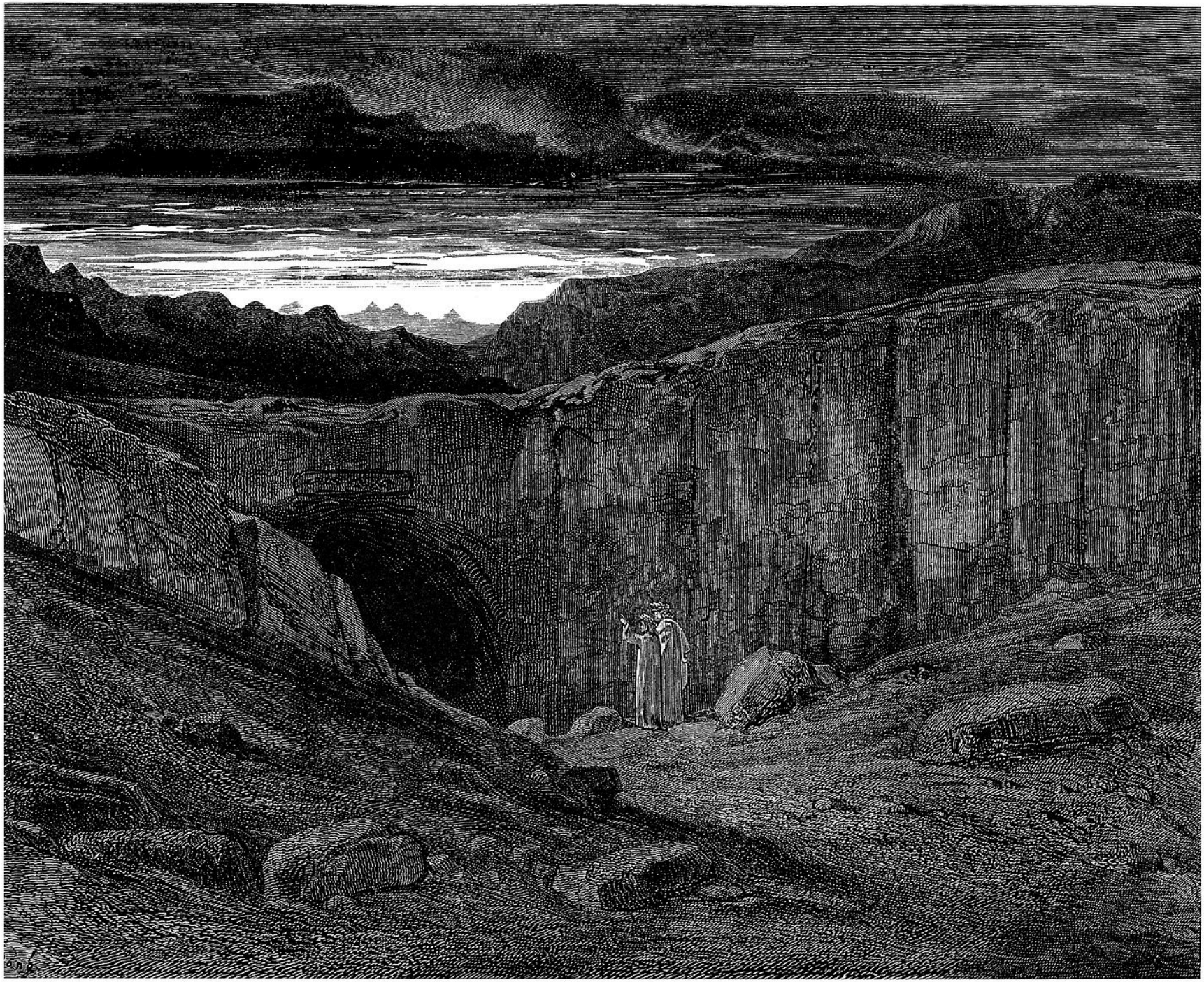
The Decline and Fall of Teredo

George Michaelson

ggm@apnic.net

With assistance from Gustave Doré






It says
“welcome to Hell: We have cookies”

Auto Tunnels From Hell…

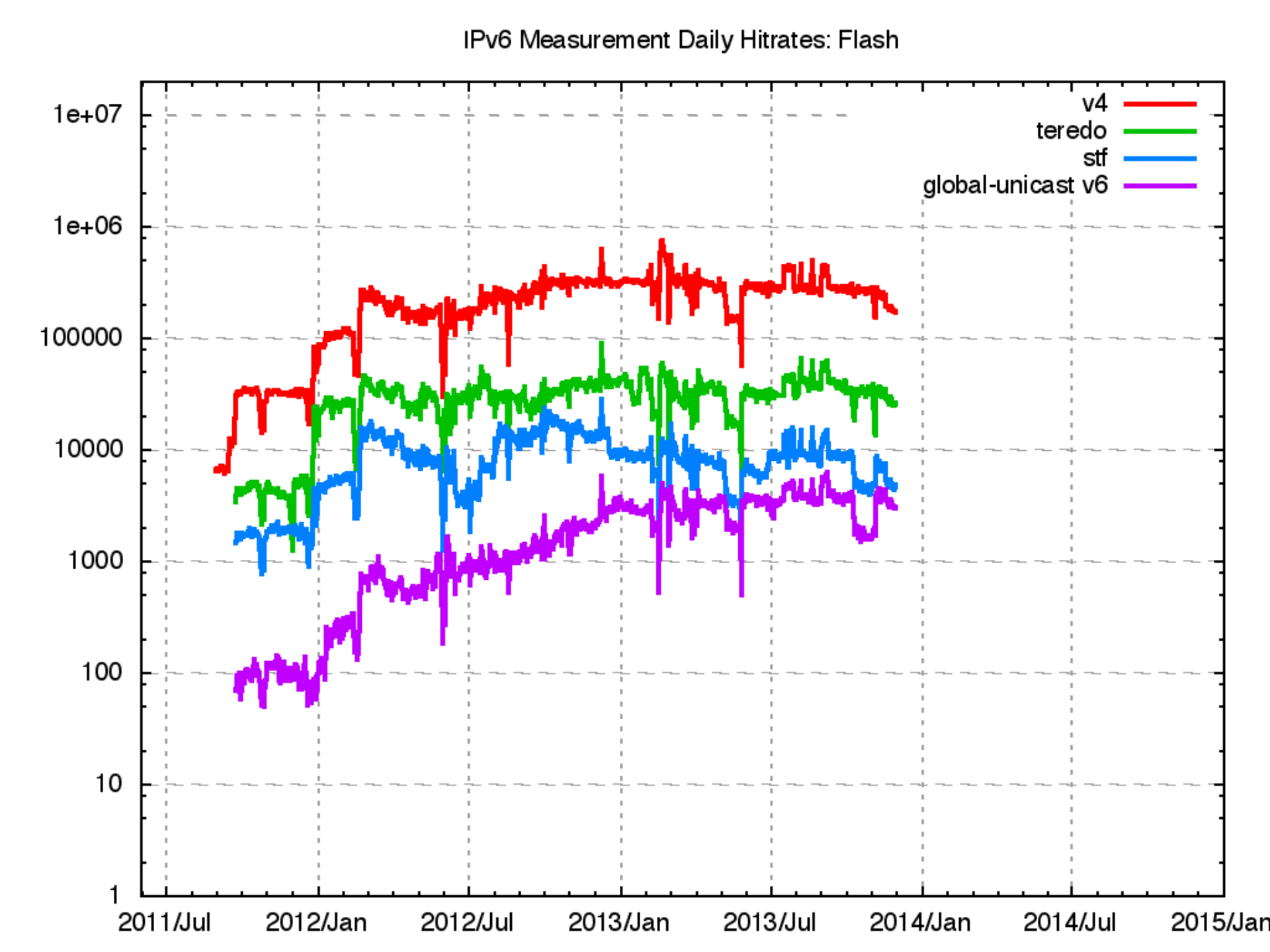
Auto Tunnels From Hell…

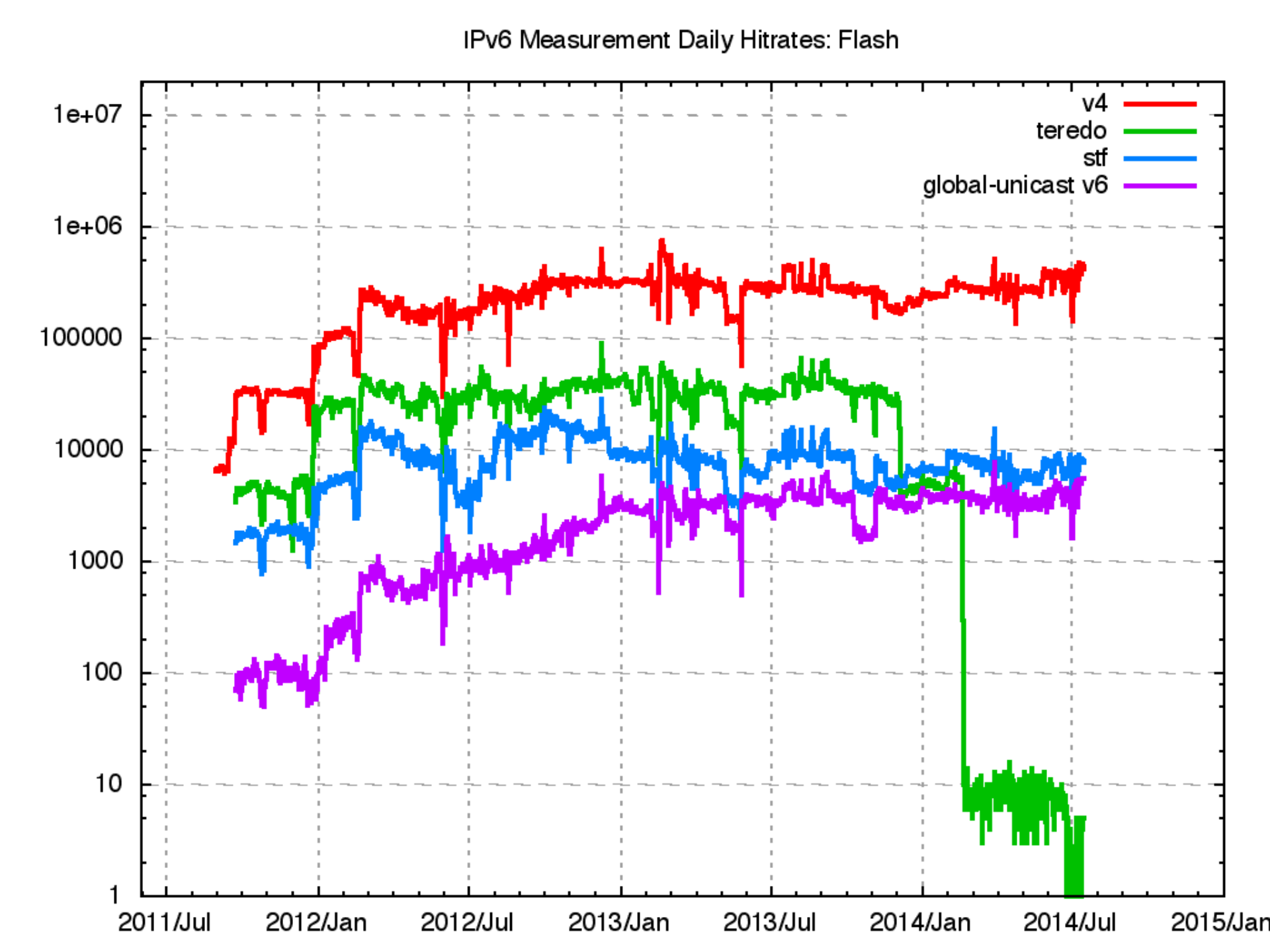
Auto Tunnels From Hell…

Auto Tunnels From Hell…

Seeing many?

- Yep.


IPv6 Measurement Daily Hitrates: Flash
v4
teredo
stf
global-unicast v6
1e+07
1e+06
100000
10000
1000
100
10
1
2011/Jul
2012/Jan
2012/Jul
2013/Jan
2013/Jul
2014/Jan
2014/Jul
2015/Jan


IPv6 Measurement Daily Hitrates: Flash
v4
teredo
stf
global-unicast v6
1e+07
1e+06
100000
10000
1000
100
10
1
2011/Jul
2012/Jan
2012/Jul
2013/Jan
2013/Jul
2014/Jan
2014/Jul
2015/Jan

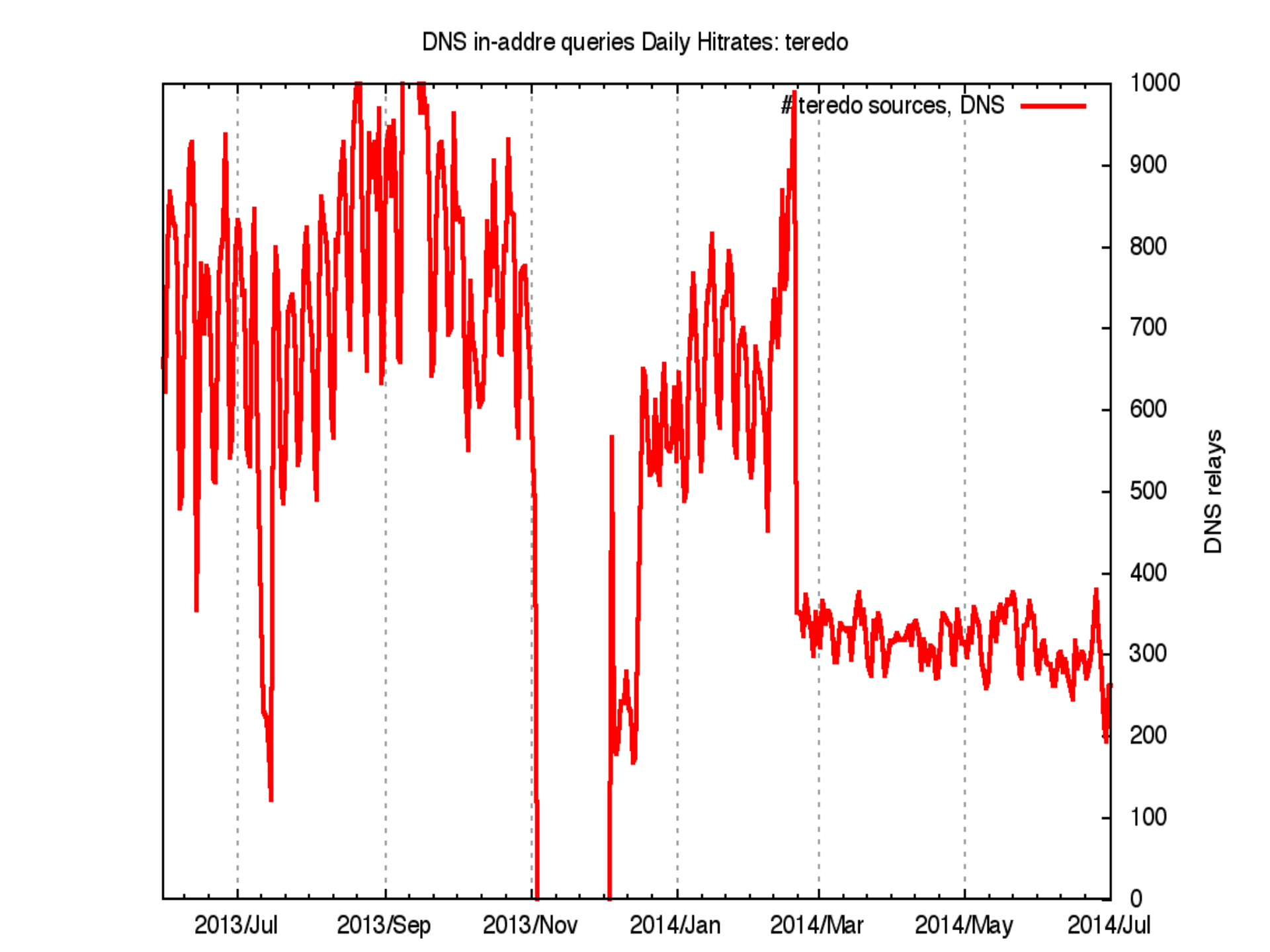
Wahappen?

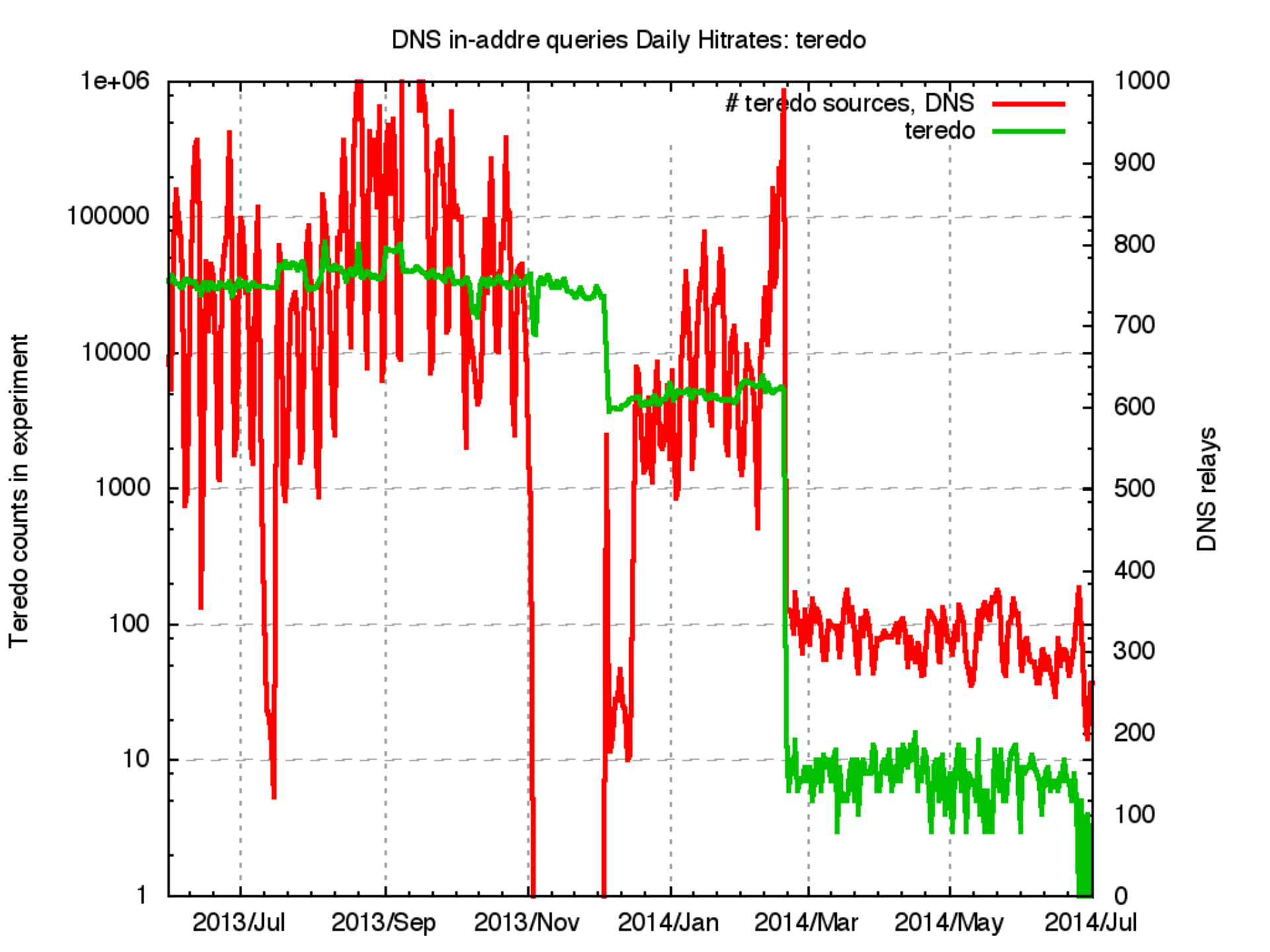
- Looks like end of 2013, something changed.
- Then Early 2014, something really changed.
- It changed so much, we stopped tickling teredo out: it seemed to have died.

- Whodidit?

Can we see it anywhere else?

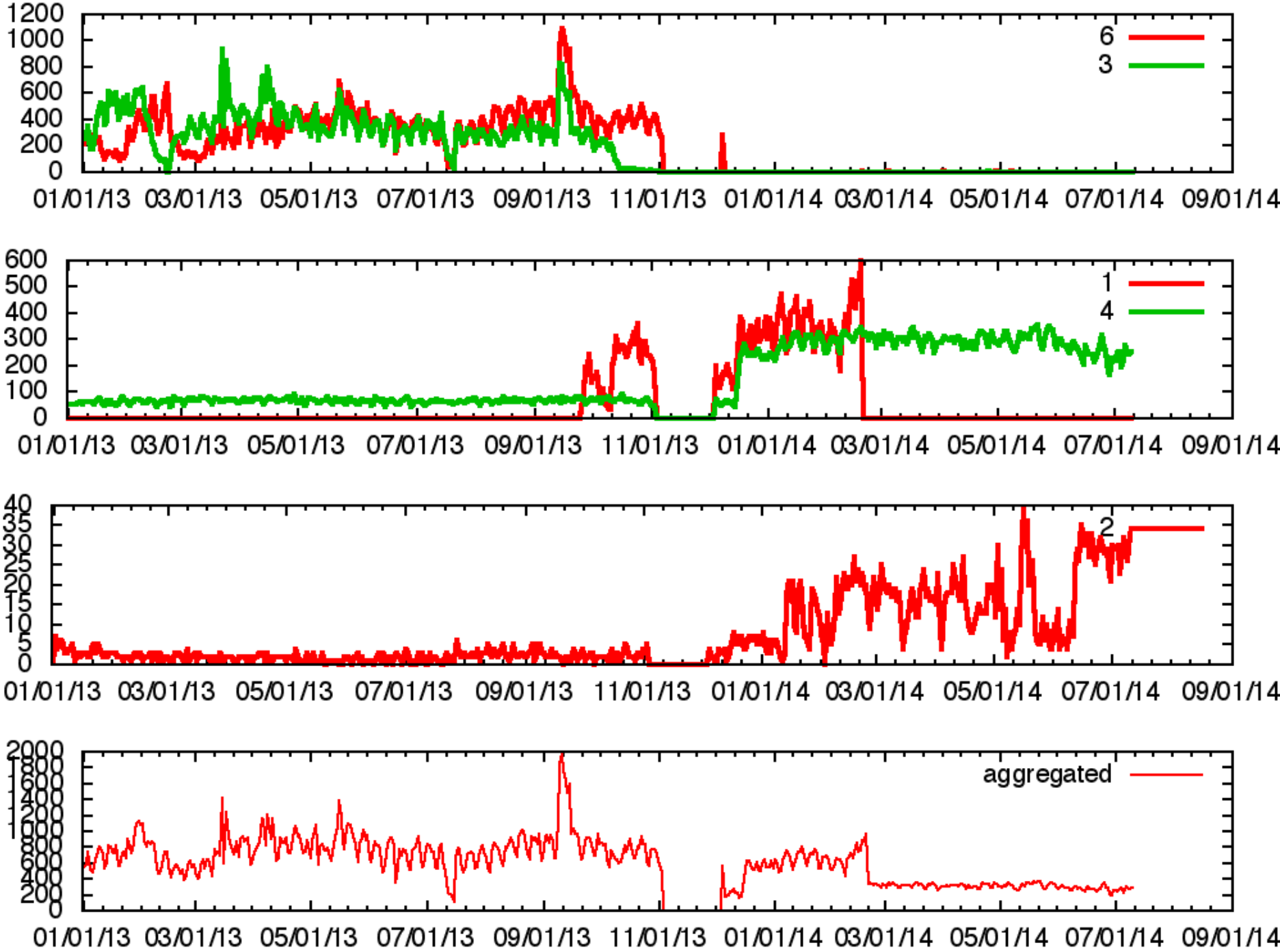
- Yep. Seen it in the DNS.


DNS in-addre queries Daily Hitrates: teredo
teredo sources, DNS
1000
900
800
700
600
500
400
300
200
100
0
DNS relays
2013/Jul
2013/Sep
2013/Nov
2014/Jan
2014/Mar
2014/May
2014/Jul


DNS in-addre queries Daily Hitrates: teredo
teredo sources, DNS
teredo
Teredo counts in experiment
DNS relays
1e+06
100000
10000
1000
100
10
1
1000
900
800
700
600
500
400
300
200
100
0
2013/Jul
2013/Sep
2013/Nov
2014/Jan
2014/Mar
2014/May
2014/Jul

It Ain't us.

- Pretty much the same time we saw a huge decline in Teredo into the 1x1 experiment, DNS sees a huge decline in sources using Teredo to ask DNS questions.
- Hmm. I wonder if the Teredo "ecology" has changed….
- Count instances of the teredo 'server' address embedded in the seen sources..
- 5 stand out:


1200
1000
800
600
400
200
0
6
3
01/01/13 03/01/13 05/01/13 07/01/13 09/01/13 11/01/13 01/01/14 03/01/14 05/01/14 07/01/14 09/01/14
600
500
400
300
200
100
0
1
4
01/01/13 03/01/13 05/01/13 07/01/13 09/01/13 11/01/13 01/01/14 03/01/14 05/01/14 07/01/14 09/01/14
40
35
30
25
20
15
10
5
0
2
01/01/13 03/01/13 05/01/13 07/01/13 09/01/13 11/01/13 01/01/14 03/01/14 05/01/14 07/01/14 09/01/14
2000
1800
1600
1400
1200
1000
800
600
400
200
0
aggregated
01/01/13 03/01/13 05/01/13 07/01/13 09/01/13 11/01/13 01/01/14 03/01/14 05/01/14 07/01/14 09/01/14

Withdrawn Teredo Relays

- 2013, Nov 4th inside subnets
  - 94.245.121.0/24
  - 65.55.158.0/24
    - Both cease to be seen in DNS reverse lookups.
- Who routes those netblocks?

Withdrawn Teredo Relays

- 2013, Nov 4th inside subnets
  - 94.245.121.0/24
  - 65.55.158.0/24
    - Both cease to be seen in DNS reverse lookups.
- Who routes those netblocks?

  - AS8075

Withdrawn Teredo Relays

- 2013, Nov 4th inside subnets
  - 94.245.121.0/24
  - 65.55.158.0/24
    - Both cease to be seen in DNS reverse lookups.
- Who routes those netblocks?
  - AS8075 MICROSOFT-CORP-MSN-AS-BLOCK
    - Microsoft Corporation,US

Microsoft.

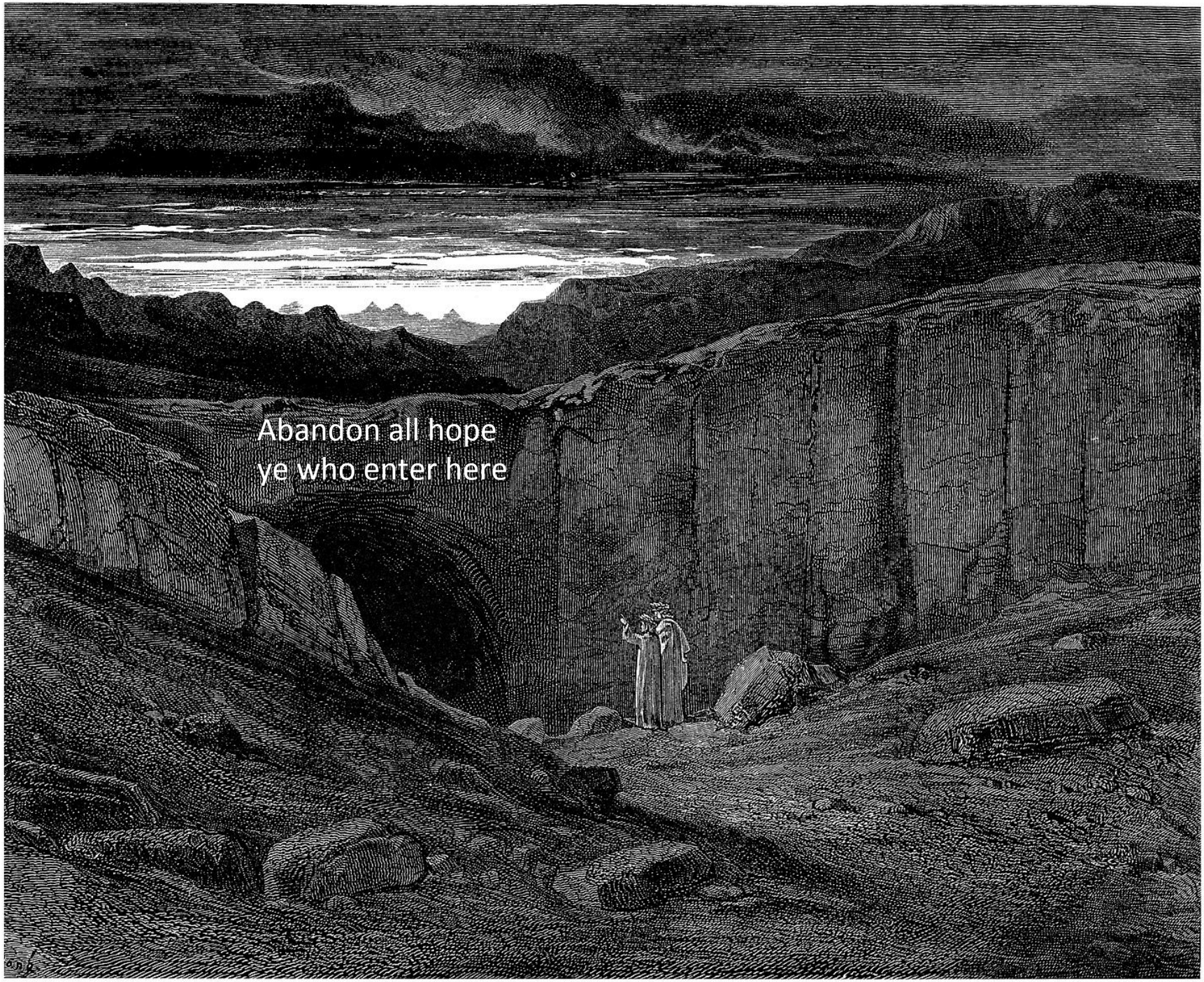
- It looks like Microsoft decided to get out of the Teredo business.
- But it also looks like there are enough other people running teredo, that its not impossible to find a service“out there”
- But.. The Microsoft service hasn’t actually gone away…
- It appears to provide ‘who am I’ endpoint signalling but not carrying IPv6 data
  - You can find out who you are, but you can’t go anywhere.

Tunnels are bad

- Zombie tunnels are possibly worse?

Tunnels are bad: please stop.

174	COGENT-174 - Cogent Communications,US
680	DFN Verein zur Foerderung eines Deutschen Forschungsnetzes e.V.,DE
1680	NV-ASN 013 NetVision Ltd.,IL
1955	HBONE-AS HUNGARNET,HU
2847	LITNET Kaunas University of Technology,LT
8075	MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation,US
12414	NL-SOLCON SOLCON,NL
15725	IKS IKS Service GmbH,DE
22652	FIBRENOIRE-INTERNET - Fibrenoire Internet Inc.,CA
25192	CZNIC-AS CZ.NIC, z.s.p.o.,CZ
29259	DE-IABG-TELEPORT IABG mbH,DE
29432	TREX-AS TREX Regional Exchanges Oy,FI
31242	TKPSA-AS 3S S.A.,PL
37105	NEOLOGY-AS,ZA
62121	BITGUARDIANS carbon14.dk v/Lars Brun Nielsen,DK


Abandon all hope
ye who enter here