



Pollution in 1.0.0.0/8

Or why having 1.2.3.4 might not be that cool after all....

Mark Dranse <markd@ripe.net>

and

Franz Schwarzingler <franz@ripe.net>

RIPE NCC



Background

- Many networks filter unallocated address space (bogons)
 - Some time passes
- Unallocated addresses become allocated
 - Filters are not always well maintained
 - Freshly allocated space is not fully reachable
- ISPs and users complain
 - RIRs get some of the blame



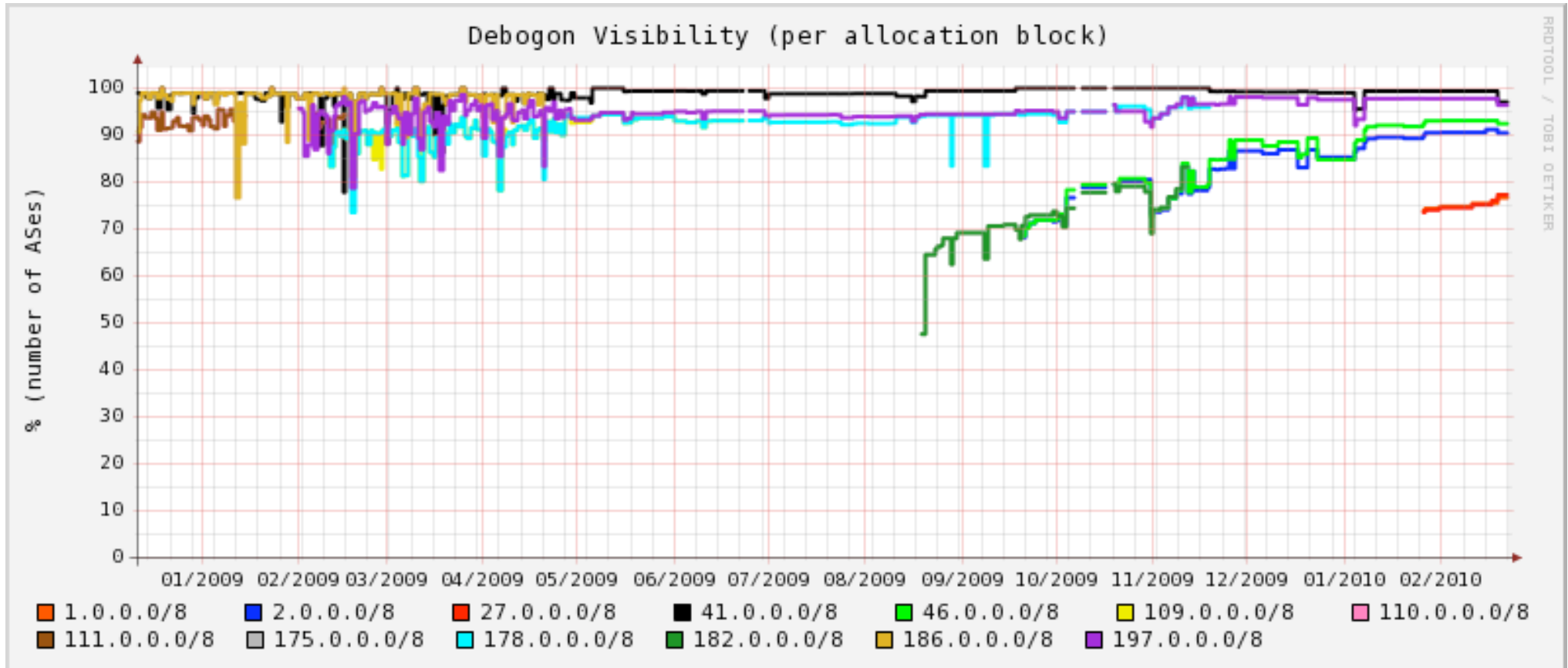
Debogon Project

- Mitigate issues surrounding new address space
 - Increase communications
 - Provide tools to measure and monitor reachability
- Using existing RIS infrastructure since 2005
 - Announce a few prefixes from new /8s
 - Provide target IPs for ping/traceroute
 - Measure reachability and produce graphs

<http://www.ris.ripe.net/debogon/>



Debogon Reports



- Combined yearly report for all /8s



Debogon Tools

[RIPE NCC](#)
[LIR Portal](#)
[RIPE](#)
[About RIPE NCC](#) | [Contact](#) | [Search](#)


Routing Information Service

you are here: [home](#) -> [RIPE NCC Projects](#) -> [RIS](#)

RIS:

- [RIS Home Page](#)
- [RIS Raw Data](#)
- [Documentation](#)
- [Analysis using RIS](#)
- [Contact Us](#)
- [Send Feedback](#)

✉ All comments and suggestions to improve our tools are welcome, please [let us know](#).

Debogon prefix reachability

This tool checks reachability of arbitrary addresses using **ping** or **traceroute** sourced from addresses within the RIRs (RIPE NCC, AFRINIC, APNIC, LACNIC) *debogon* prefixes originated on rrc03.ripe.net (or from the RIPE NCC's own 193.0.0.0/21 prefix).

Source Address Range:

Destination Address:

Traceroute Ping

<http://www.ripe.net/cgi-bin/debogon.cgi>



The 1.0.0.0/8 story

- “Reserved” since 1981
- Changed to “unallocated” by IANA in 2008
- Allocated to APNIC in January 2010 ‘randomly’
 - Added to the debogon report as usual
 - 1.255.0.0/16
 - 1.50.0.0/22
 - As a special experiment, we also announced:
 - 1.1.1.0/24
 - 1.2.3.0/24



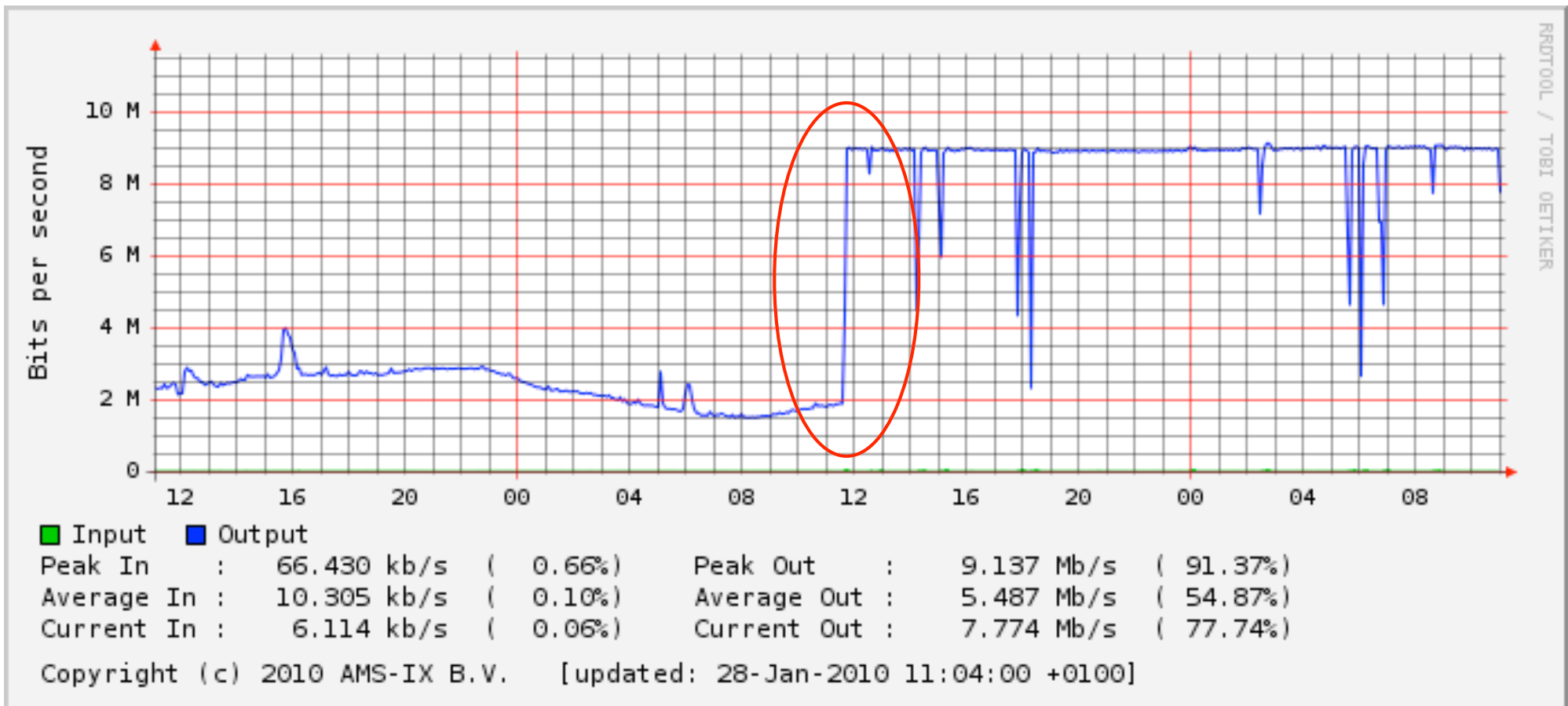
Measurement Setup

- RIS Remote Route Collector (rrc03.ripe.net)
 - Connected to 3 Dutch IXPs
 - AMS-IX
 - NL-IX
 - GN-IX
 - AMS-IX port is 40 100 MBit/s
 - Outbound traffic via RIPE NCC network
 - About 100 active peers



27th January 2010

- Announcements began just before midday
 - Instantly maxed out our AMS-IX port





RIS View

This prefix had multiple originating ASes:

<u>Origin AS</u>	<u>AS Name</u>	<u>First Seen</u>	<u>Last Seen</u>
AS12654	RIPE-NCC-RIS-AS RIPE NCC RIS project	2010-01-27 10:38:23 UTC	2010-02-02 05:36:29 UTC
AS8218	NEO-ASN AS Confederation of Neotelecoms, euNetworks AG and Upstreamnet gmbh	2009-05-18 16:40:27 UTC	2010-01-15 12:56:13 UTC
AS45899	VNPT-AS-VN VNPT Corp	2009-12-25 14:24:44 UTC	2009-12-25 15:37:43 UTC

This prefix comes from the **1.0.0.0/8** block allocated to **APNIC** by the [IANA](#).

Related (overlapping) prefixes seen by RIS in the last 30 days

<u>Prefix</u>	<u>Origin AS</u>	<u>AS name</u>	<u>First seen</u>	<u>Last seen</u>
1.0.0.0/8	21345	MESSAGELABS-EU MessageLabs Symantec Hosted Services	2010-01-11 21:01:06 UTC	2010-01-12 20:06:35 UTC
1.0.0.0/8	1733	CENTAF-SWA - 754th Electronic Systems Group	2010-02-01 10:20:44 UTC	2010-02-01 11:46:57 UTC
1.0.0.0/8	65333	-Private Use AS-	2010-01-11 21:01:06 UTC	2010-01-11 21:01:49 UTC
1.1.1.0/24	12654	RIPE-NCC-RIS-AS RIPE NCC RIS project	2010-01-27 10:38:23 UTC	2010-02-02 05:36:29 UTC
1.1.1.0/30	38091	HELLONET-AS-KR CJ-CABLENET	2010-01-07 07:49:40 UTC	2010-01-07 08:08:41 UTC

Note: Prefixes **marked orange** are currently not announced. The entries refer to announcements in the past.



RIS View

- 14 distinct ASes
- 26 prefixes
- /30 to /13

<u>Prefix</u>	<u>Origin AS</u>	<u>First seen</u>	<u>Last seen</u>
1.1.1.0/30	262710	2010-02-12 17:28:04 UTC	2010-02-12 17:46:30 UTC
1.1.1.0/24	8218	2009-05-18 16:40:27 UTC	2010-01-15 12:56:13 UTC
1.2.3.0/24	12637	2010-02-06 23:45:04 UTC	2010-02-07 02:47:35 UTC
1.1.1.0/24	12637	2010-02-06 23:45:04 UTC	2010-02-07 02:47:35 UTC
1.1.0.0/24	3549	2010-01-08 23:56:18 UTC	2010-01-12 12:16:16 UTC
1.120.0.0/13	23148	2009-12-21 21:39:58 UTC	2010-01-04 16:32:48 UTC
1.2.3.0/24	36561	2010-03-02 00:53:16 UTC	2010-03-02 07:59:00 UTC
1.1.1.0/24	36561	2010-03-02 00:50:26 UTC	2010-03-02 07:59:00 UTC
1.10.25.0/24	28006	2010-02-27 15:53:12 UTC	2010-02-27 18:07:04 UTC
1.1.88.0/24	39386	2009-12-15 09:53:02 UTC	2009-12-15 09:54:50 UTC
1.1.1.0/24	45899	2009-12-25 14:24:44 UTC	2009-12-25 15:37:43 UTC
1.1.1.0/30	3313	2009-12-30 09:04:24 UTC	2009-12-30 09:04:36 UTC
1.80.0.0/13	23148	2009-12-21 21:39:58 UTC	2010-01-04 16:32:48 UTC
1.1.1.0/24	3549	2010-02-24 11:55:42 UTC	2010-02-24 12:09:46 UTC
1.50.0.0/22	0	2010-02-16 15:59:56 UTC	2010-02-18 07:59:00 UTC
1.1.88.0/24	4645	2009-12-01 11:00:09 UTC	2009-12-20 23:59:00 UTC
1.1.2.0/30	3313	2009-12-30 09:05:06 UTC	2009-12-30 09:05:15 UTC
1.255.0.0/16	12654	2010-01-27 10:38:23 UTC	2010-03-02 07:59:00 UTC
1.2.3.0/24	12654	2010-01-27 10:38:23 UTC	2010-02-24 07:59:00 UTC
1.2.3.0/24	7575	2010-03-01 06:36:19 UTC	2010-03-01 11:23:28 UTC
1.1.1.0/30	38091	2010-01-07 07:49:40 UTC	2010-01-07 08:08:41 UTC
1.40.0.0/13	23148	2009-12-21 21:39:58 UTC	2010-01-04 16:32:48 UTC
1.1.1.0/24	7575	2010-03-01 06:36:19 UTC	2010-03-01 11:23:28 UTC
1.255.0.0/16	0	2010-02-16 15:59:56 UTC	2010-02-18 07:59:00 UTC
1.50.0.0/22	12654	2010-01-27 10:38:23 UTC	2010-03-02 07:59:00 UTC
1.1.1.0/24	12654	2010-01-27 10:38:23 UTC	2010-02-24 07:59:00 UTC

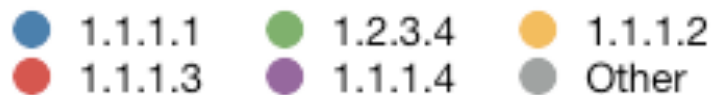
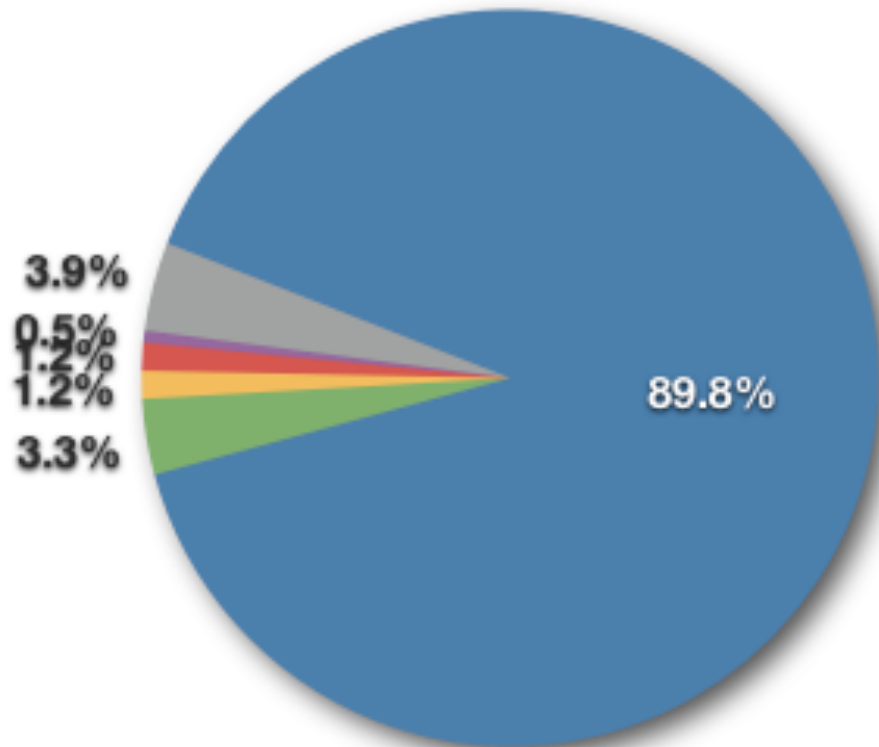


Some analysis

- 900k packet sample taken on 28th January
- Looked at:
 - Sources
 - Destinations
 - Protocols

Packet destinations

Destination Addresses in 1/8 (Percent of Packets)



- Two busiest destinations:
 - 90% of packets to 1.1.1.1
 - 3.3% of packets to 1.2.3.4

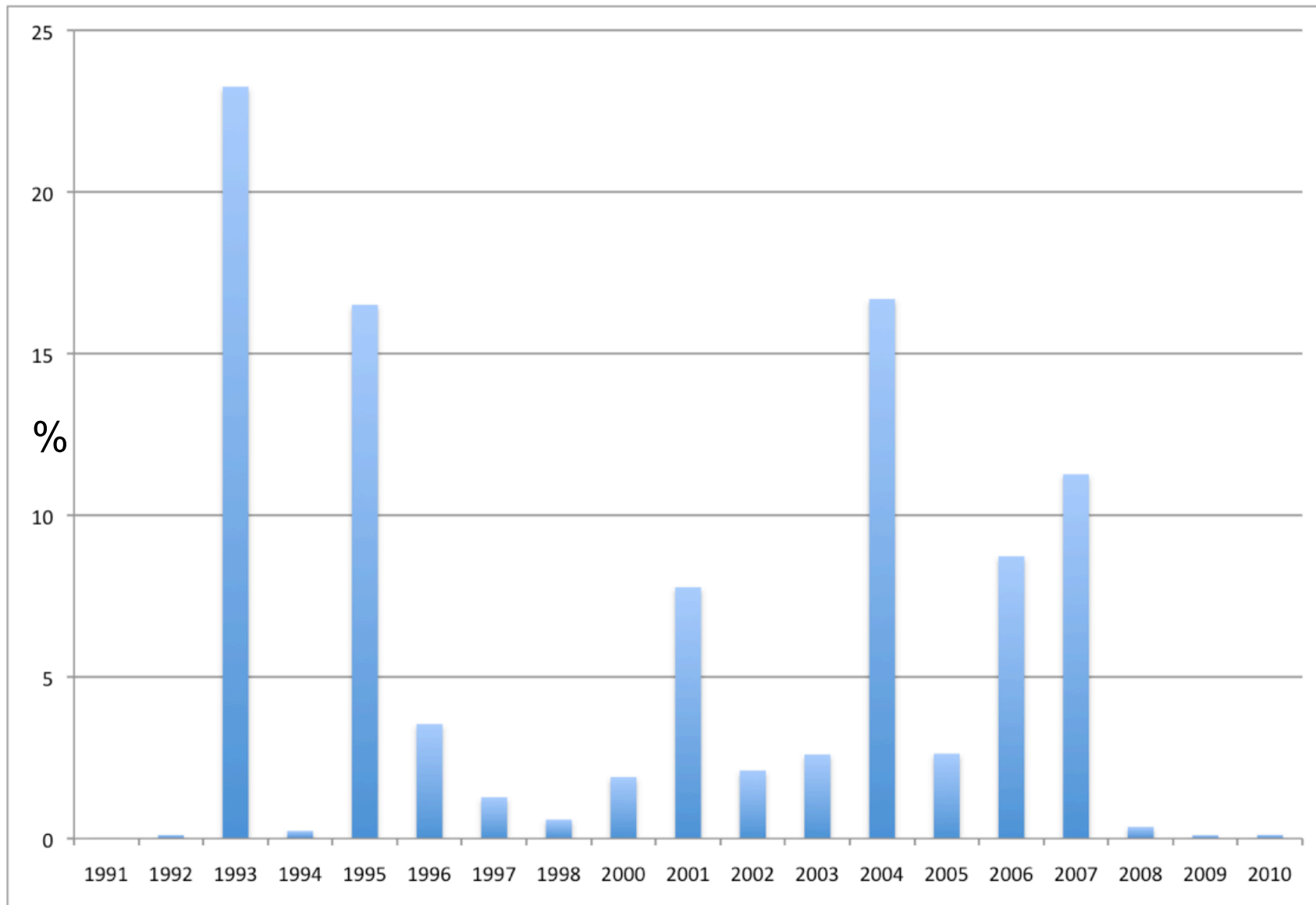


Packet Sources

- 96,160 unique IP addresses
 - 95% sent \leq 10 packets
 - 33% sent 1 packet
- 30% of packets from 23 IP addresses
 - 4.4% from 1 IP address
- 90% from 43 /8s
 - 15% claims to originate from 10/8



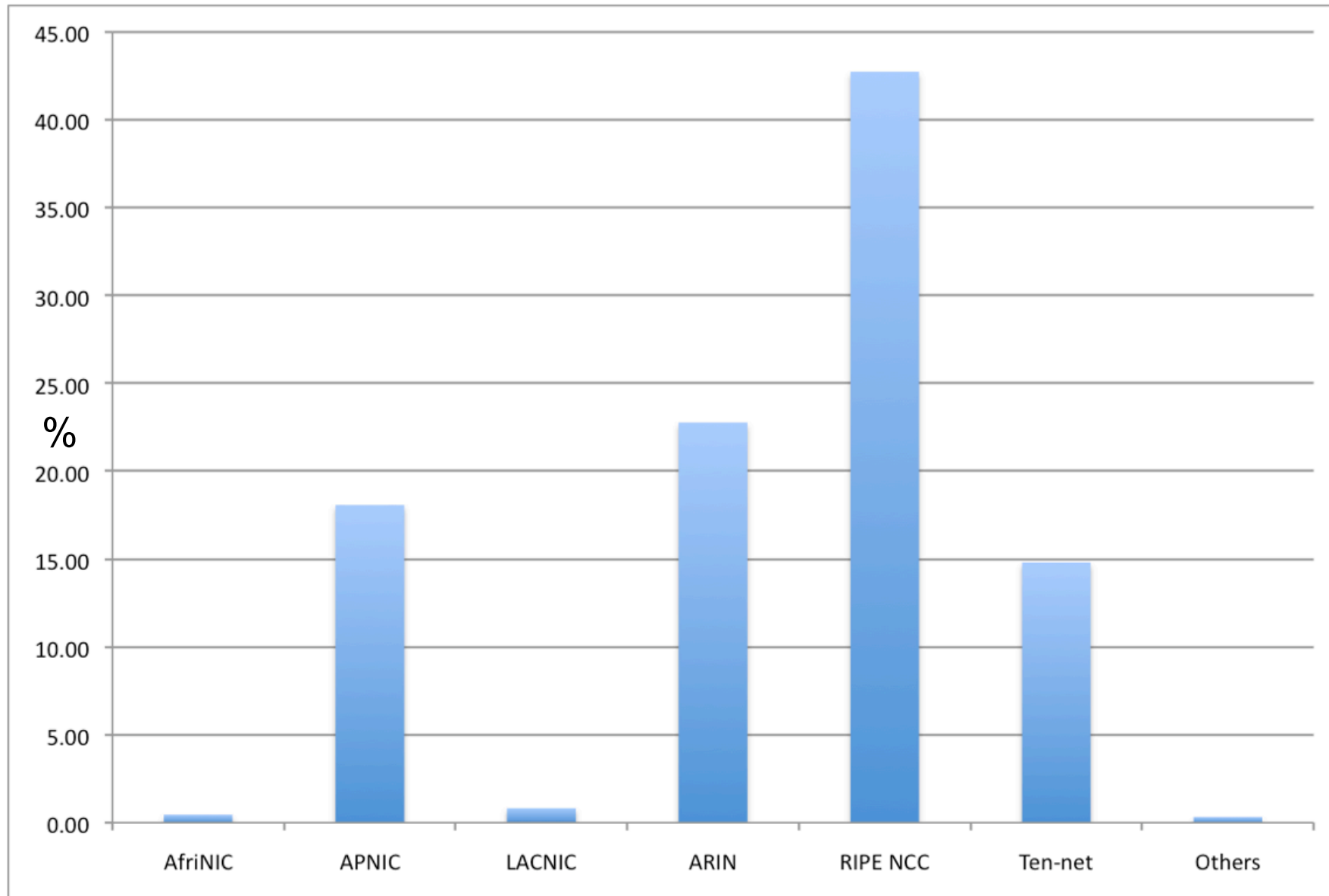
Packet Sources



Year in which parent /8 was allocated



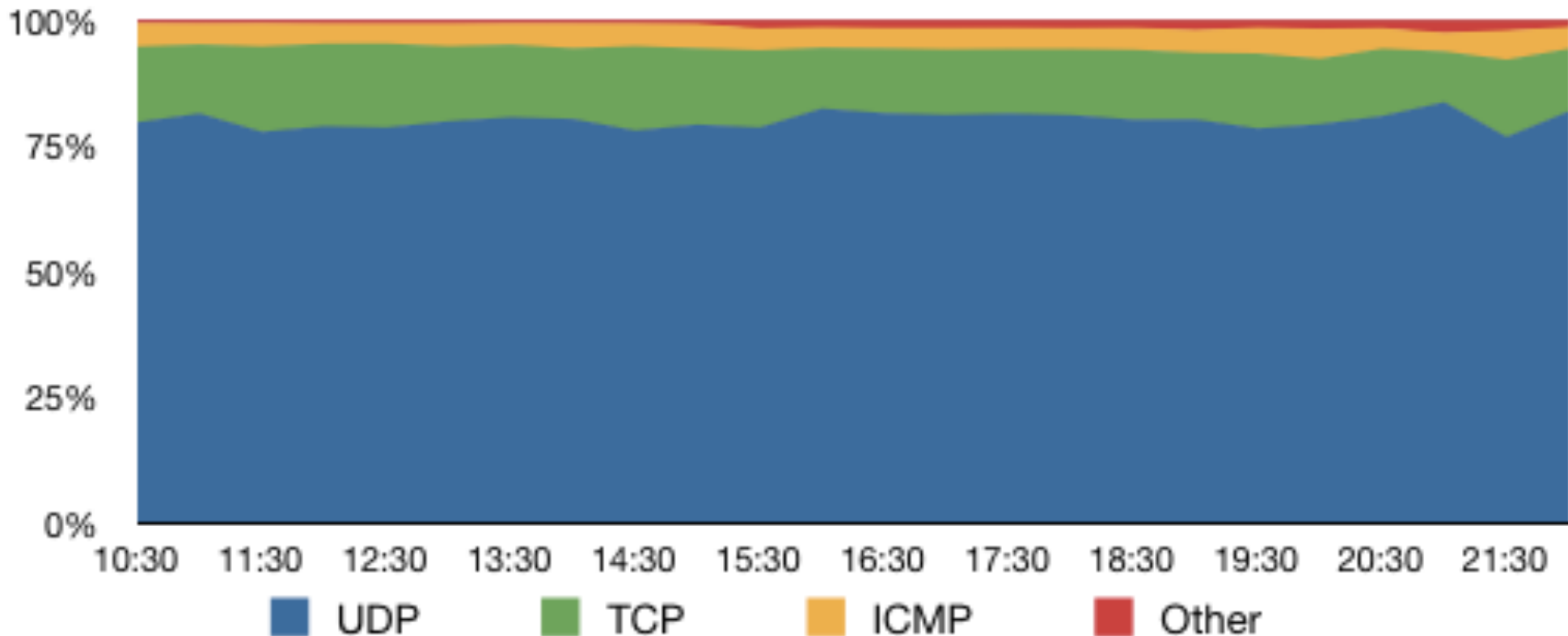
Packet Sources



Responsible RIR for parent /8

What was the traffic?

Percent of Packets Over Time

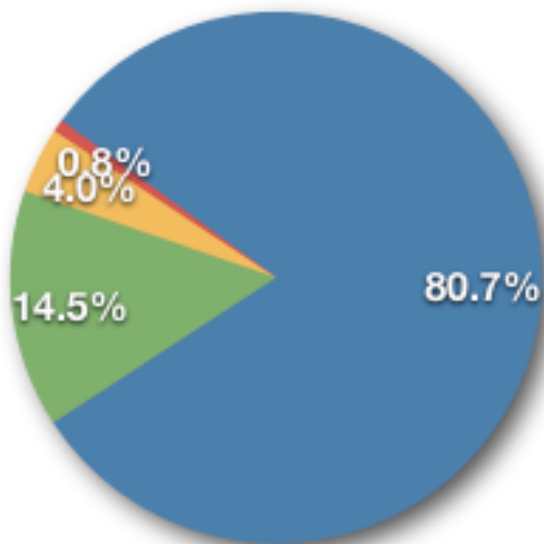




What was the traffic?

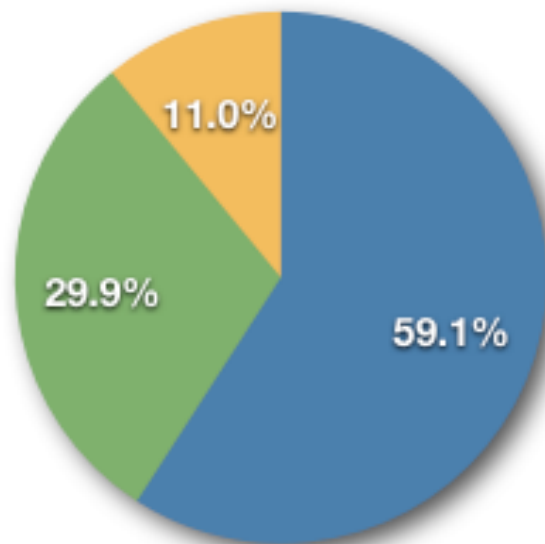
- 80% UDP traffic
 - 60% SIP INVITE (VoIP) scans *
 - 30% Media Gateway Protocol
- 20 %TCP traffic
 - 50% HTTP
 - 5.4% SMTP

Traffic in 1/8



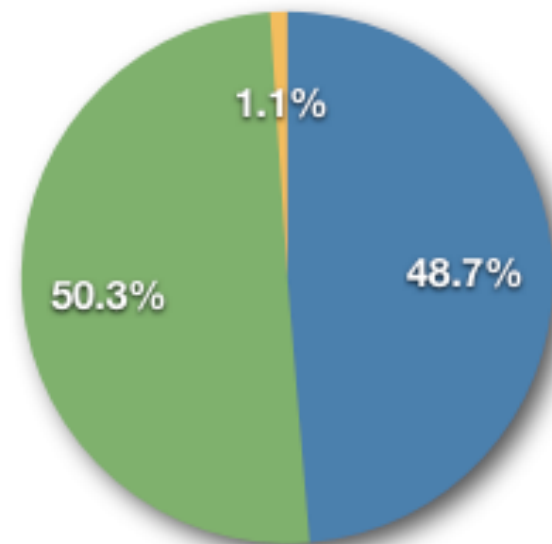
● UDP
● ICMP Traffic
● TCP
● Other

UDP Traffic in 1/8



● Port 15206
● Media Gateway Control Protocol
● Other

TCP Traffic in 1/8



● Attempted HTTP connections
● Other
● "Established" HTTP connections

* Thanks to Sandro Gauci and others for pointing this out!



Feedback

- Give it to me!
- Don't give it to me!
- Don't give it to anyone!
- How representative is this?
 - Is it just 'normal' background noise?
 - Isolated data point?



Further Research

- Comparison with other prefixes
- Announce for longer
 - From a “real” network with high capacity
- Collect more data
 - Don’t just analyse small samples



References

- RIPE Labs
 - <http://labs.ripe.net/content/pollution-18>
 - <http://labs.ripe.net/node/195>
- Debogon Report
 - <http://www.ris.ripe.net/debogon>
- APOPS list
 - <http://archive.apnic.net/mailling-lists/apops/archive/2010/02/>
- Reddit.com
 - http://www.reddit.com/r/programming/comments/axltd/pollution_in_10008/

Questions?

