Background Radiation in IP

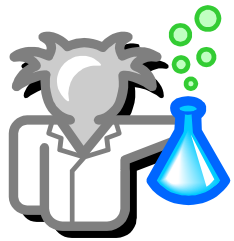
Geoff Huston

George Michaelson

APNIC R&D

Manish Karir

Merit



Network "Background Radiation"

- Most network traffic is the result of some form of initial two-party rendezvous function
- But there is a subset of network traffic that is completely unsolicited (and generally unanswered)
  - "leakage" and "backscatter" from private networks
  - badly configured hosts and equipment
  - probes and scans
- This unsolicited traffic forms a constant background of network activity, or "background radiation"

APNIC's Situation

As we get down to the last few /8s in IPv4 there is a concern that some parts of these networks have a history of prior use that add to the background traffic level

In 2010 APNIC has been allocated (among others):

- **1.0.0.0/8** – often used in ad-hoc private contexts
- **14.0.0.0/8** – originally designated for use in interfacing to public X.25 networks
- **223.0.0.0/8** – used in ad hoc private contexts

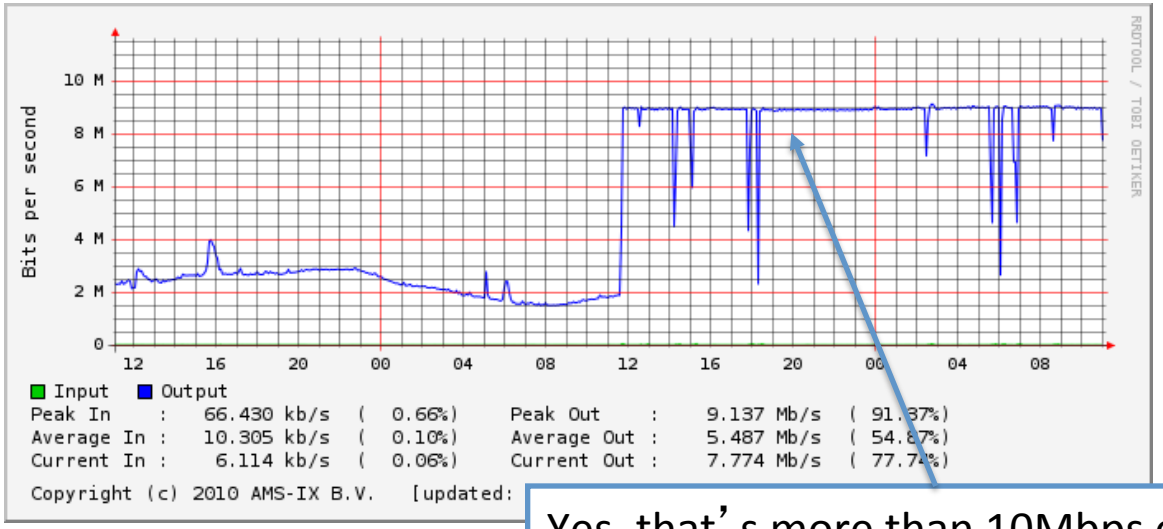
“Background Radiation” Questions

- How intense is this background radiation?
- Do some parts of the IPv4 address space attract consistently higher levels of background traffic than other parts?
- Are there “toxic hot spots” in the IPv4 address space?
- Can this be rectified, or are we stuck with it?
- How bad is IPv6? And will it get worse over time?

First Warnings

- 27 January 2010 RIPE NCC announces 1.1.1.0/24, 1.2.3.0/24, 1.50.0.0/22 and 1.255.0.0/16

http://labs.ripe.net/content/pollution-18

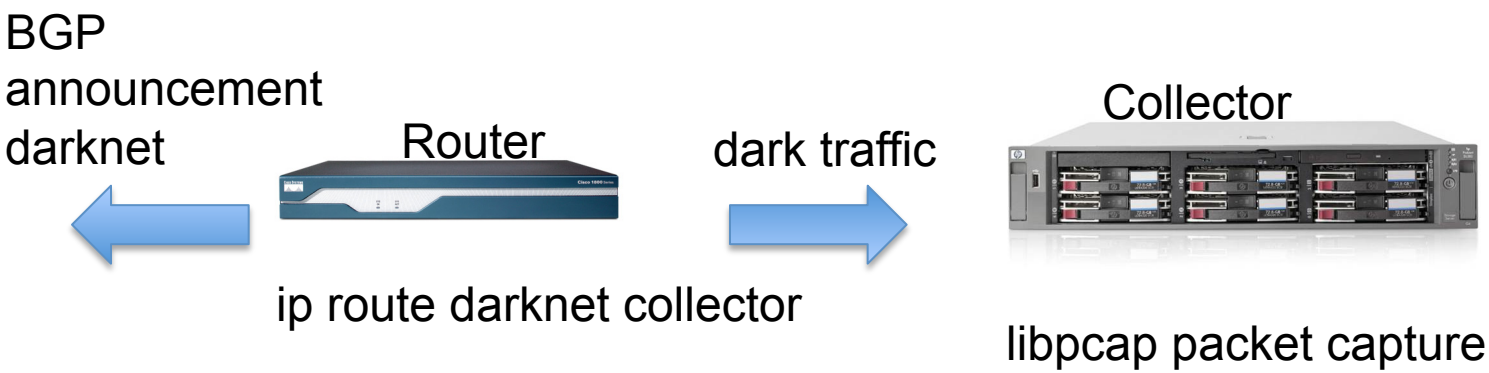


Yes, that's more than 10Mbps of traffic!

Studying 1/8

- There are some questions here:
  - Just how “bad” is 1.0.0.0/8?
  - Is this uniform, or are there “hot spots”?
  - Is this malign traffic or just private use leakage?
  - Is this “normal” when compared to other /8s?
- APNIC has commenced a program of analysis of the spectrum of “background” traffic in the /8s passed to APNIC by the IANA, prior to allocation to try and answer these questions

IP Radiation Detector



Passive Detector: all incoming traffic is recorded
collector emits no traffic in response

Active Detector (Internet sink*): all incoming traffic recorded
ICMP, TCP and UDP responses generated
Application responses for HTTP, FTP, SMB,…

* "On the Design and Use of Internet Sinks for Network Abuse Monitoring",
Vinod Yegneswaran1 and Paul Barford1 and Dave Plonka, University of Wisconsin, Madison
In *Proceedings of Symposium on Recent Advances in Intrusion Detection, 2004*
http://pages.cs.wisc.edu/~pb/isink_final.pdf

Bigger, Badder, Faster

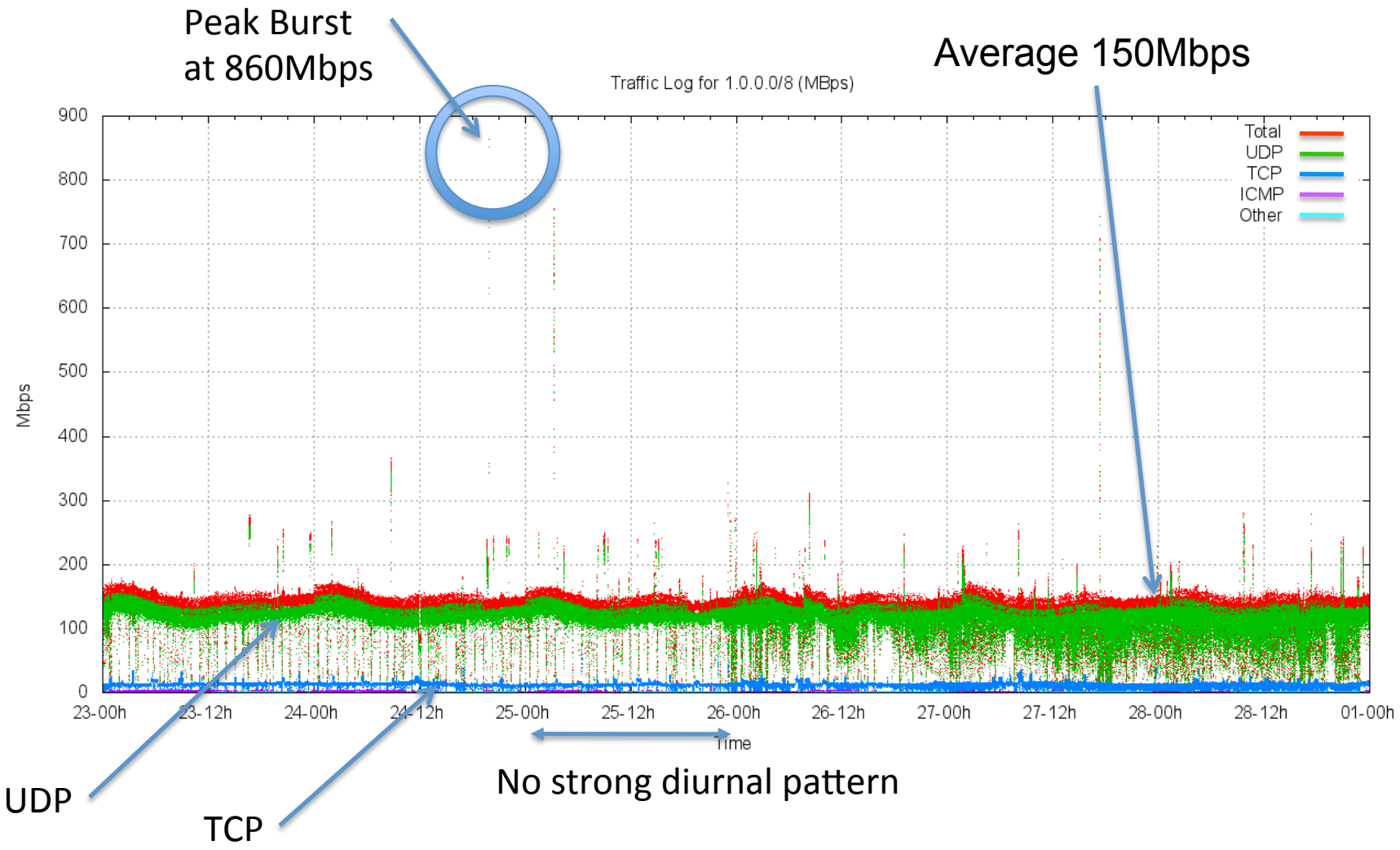
- To do this we needed multi-gig access and traffic collectors and multi-Tb disk space
  - this exceed's APNIC's lab systems and transit capacity
- We sought collaborators in the R&D Ops community for assistance in this work
  - we had many responses, for which we are grateful
  - We have been working with Merit, NTT, AARNet, Google and YouTube

    all of whom have been fantastic collaborators – thanks!
- One week announcements of /8 address blocks
  - Then working through the resultant packet data

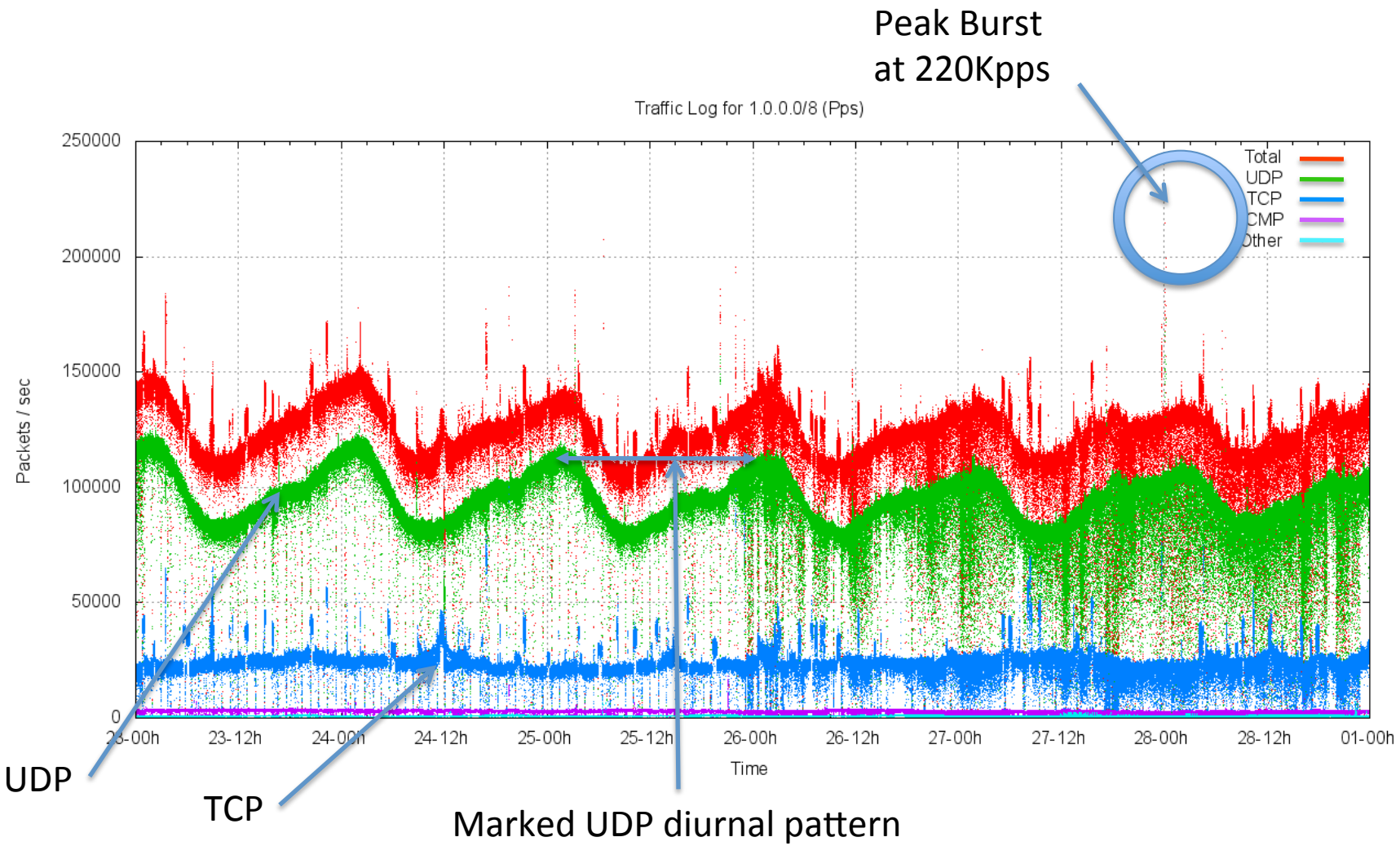
Testing 1/8

- Merit (AS237) announced 1.0.0.0/8 from 23 Feb until 1 March 2010
  - Collected 7.9Tb of packet capture data

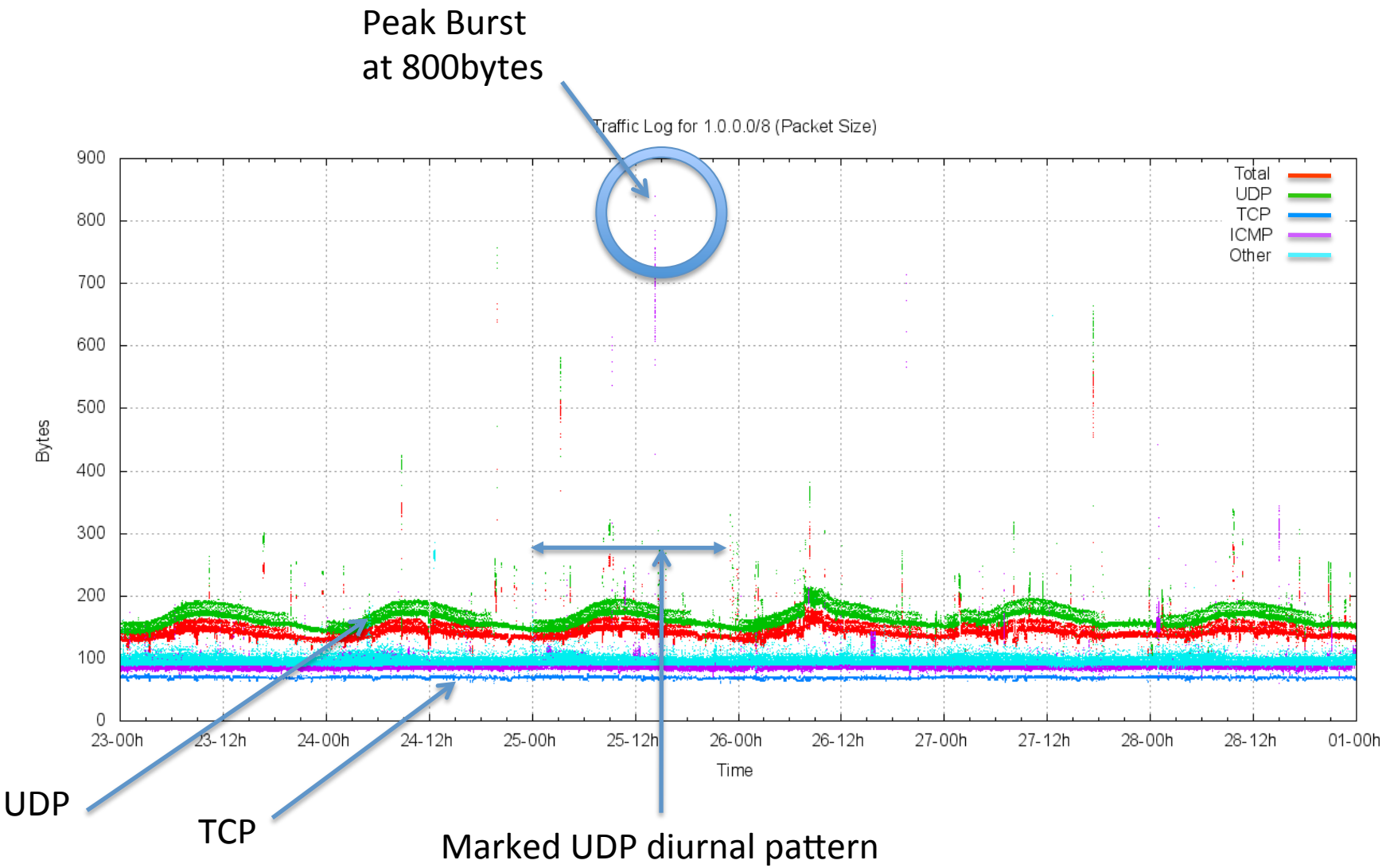
Traffic to 1.0.0.0/8



Packet Rate to 1.0.0.0/8



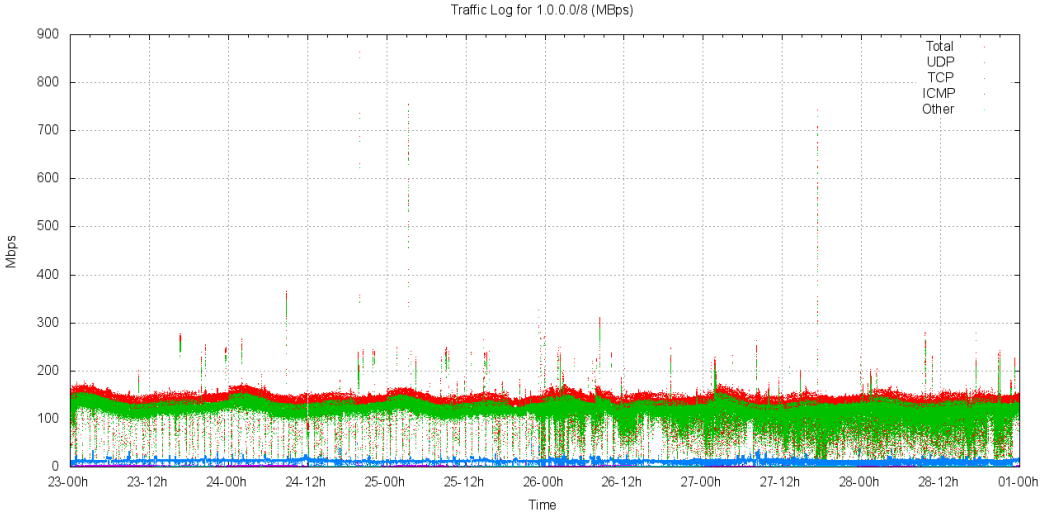
Packet Size to 1.0.0/8

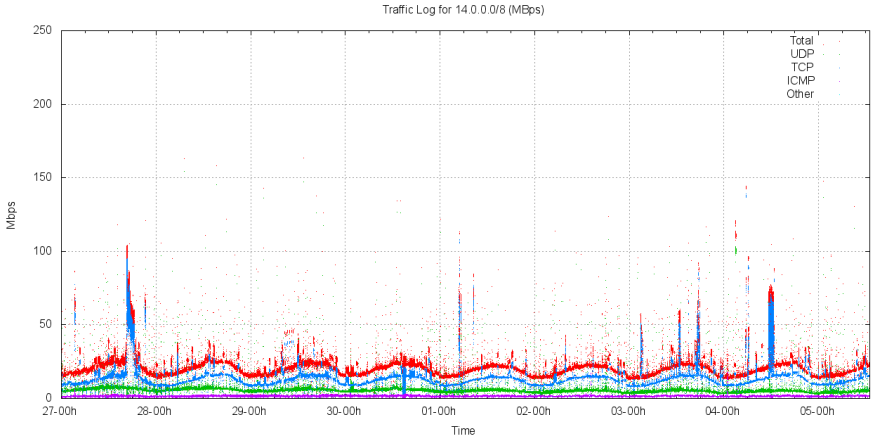


Is this traffic “normal”?

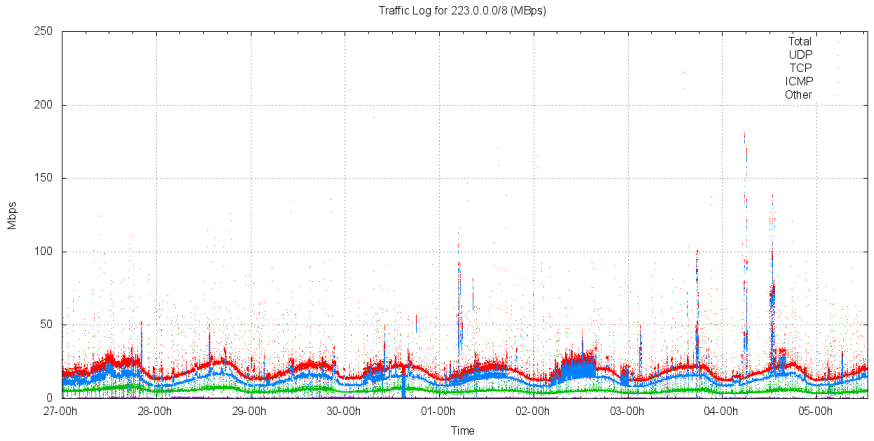
- We have also examined the traffic profile of two more address blocks: 14.0.0.0/8 and 223.0.0.0/8
  - similar experimental setup of a 7 day advertisement of the /8 address block using a passive collector

Traffic profile of 1/8





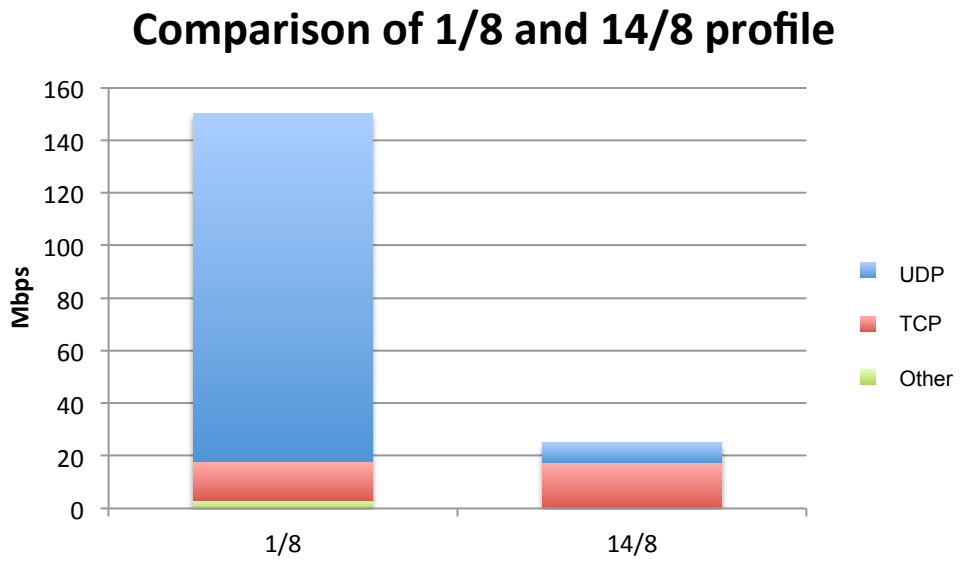
Traffic profile of 14/8



Traffic profile of 223/8

1.0.0.0/8 is *very* different

	1.0.0.0/8	14.0.0.0/8 & 223.0.0.0/8
Average Traffic	150Mbps	25Mbps
UDP	88%	30%
TCP	10%	70%
Diurnal Variation	4%	45%



Comparison of Traffic Types

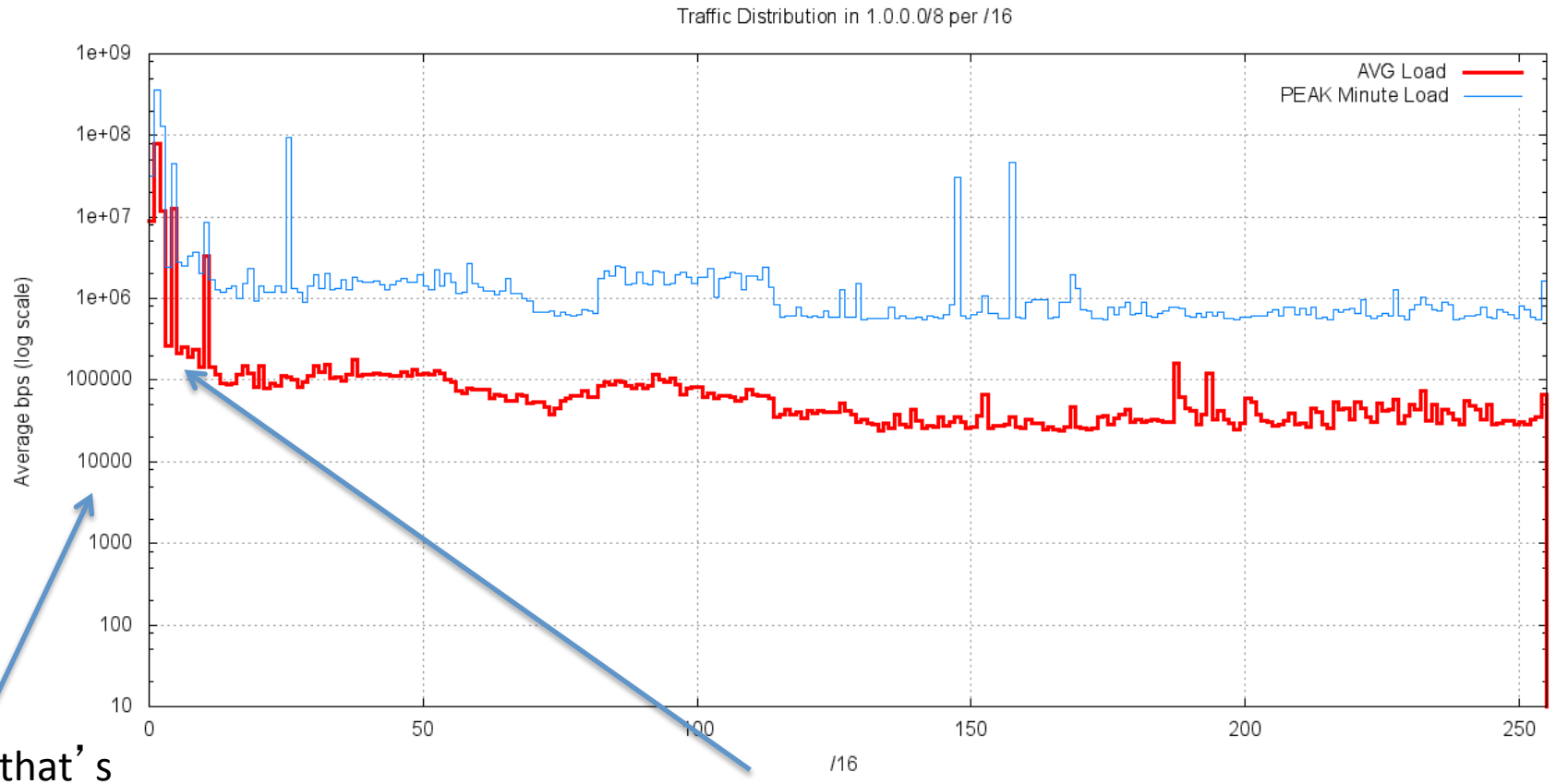
1/8:

- Scanning and Probes: 18% (27Mbps)
- Backscatter: 2% (3Mbps)
- Misconfiguration: 80% (120Mbps)

14/8

- Scanning and Probes: 70% (17Mbps)
- Backscatter: 6% (1.5Mbps)
- Misconfiguration: 24% (6.5Mbps)

What's going on in 1/8?



Yes, that's a Log Scale!

The "hot spots" appear to lie in the low /16s

10 /24's receive 75% of packets

Subnet /24	Packets	%
1.1.1.0	4797420185	44.5
1.4.0.0	1884458639	17.5
1.0.0.0	1069156477	9.9
1.2.3.0	199452209	1.8
1.1.168.0	62347104	0.5
1.10.10.0	26362000	0.2
1.0.168.0	18988771	0.1
1.1.0.0	18822018	0.1
1.0.1.0	14818941	0.1
1.2.168.0	12484394	0.1

1.1.1.1 – UDP port 15206

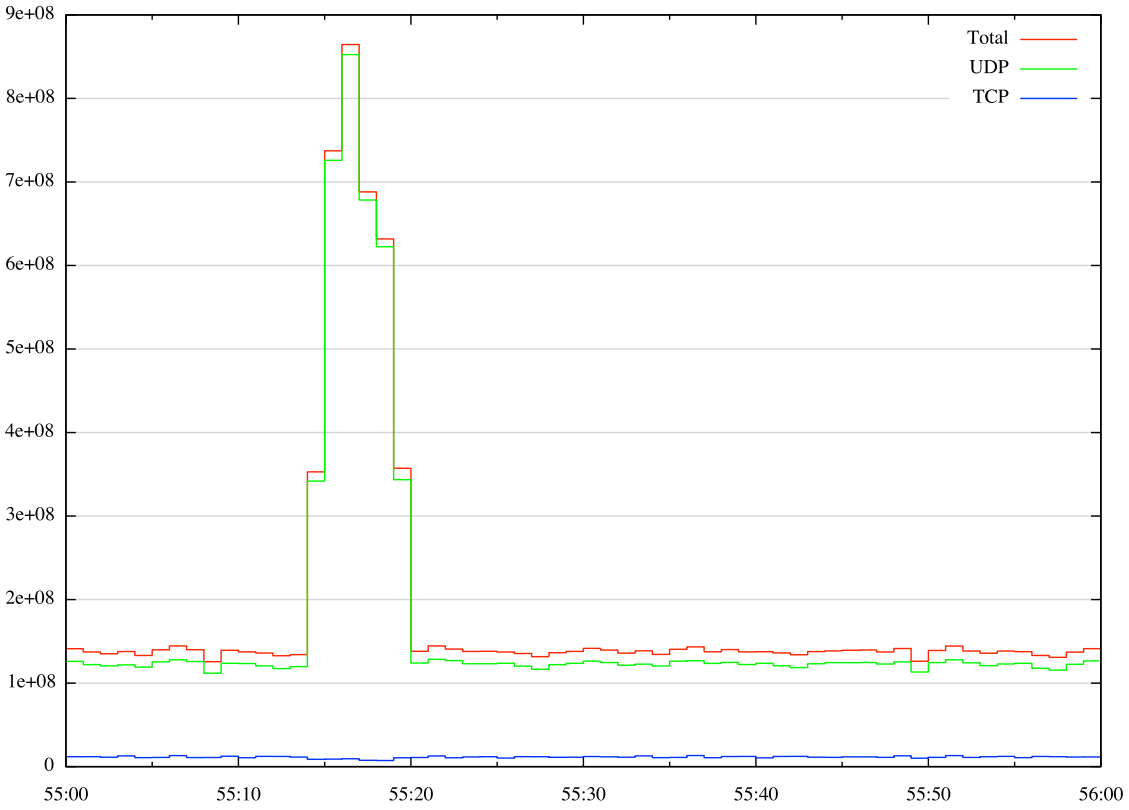
34.5% of all packets (and 50.1% of all bytes) received are UDP packets to 1.1.1.1, destination port 15206.

UDP Port 15206 to 1.1.1.1

- Most of the payloads looks like version 2 RTP packets
  - 75% of all bytes to this port have 0x8000 first 16 bits (first two bits is the version number and the next 14 all 0)
  - the majority of packets are 214 bytes in size (89.4%)
- Is this a small set of leaking devices?
  - All this coming from only 1036 /24s
  - And from only 1601 source ports seemingly unrelated to the ephemeral port ranges
  - Payload is PCMU – a compressed audio format
  - Is this a VOIP device with a configured default VOIP server setting of 1.1.1.1?

An 860Mbps Peak…

Is 6 seconds of UDP directed at 1.1.1.1



That 6 second traffic burst …

- All these UDP packets are:
  - sourced from 206.225.8.22
  - sent to 1.1.1.1
  - total of 8192 bytes in length (pre fragmentation)
  - agile in source and destination ports
  - no "obvious" content in payload
- Some form of transient "leak" from inside a data centre?
- Or…

```
05:55:14.606498 IP 206.225.8.22.38031 > 1.1.1.1.2803: UDP, length 8192
05:55:14.606568 IP 206.225.8.22.38031 > 1.1.1.1.2803: UDP, length 8192
05:55:14.606642 IP 206.225.8.22.38031 > 1.1.1.1.2803: UDP, length 8192
05:55:14.606856 IP 206.225.8.22.45951 > 1.1.1.1.3942: UDP, length 8192
05:55:14.607031 IP 206.225.8.22.45951 > 1.1.1.1.3942: UDP, length 8192
05:55:14.607268 IP 206.225.8.22.45951 > 1.1.1.1.3942: UDP, length 8192
05:55:14.607500 IP 206.225.8.22.54295 > 1.1.1.1.767: UDP, length 8192
05:55:14.607905 IP 206.225.8.22.35964 > 1.1.1.1.5859: UDP, length 8192
05:55:14.608174 IP 206.225.8.22.35964 > 1.1.1.1.5859: UDP, length 8192
05:55:14.608466 IP 206.225.8.22.33462 > 1.1.1.1.5125: UDP, length 8192
05:55:14.608853 IP 206.225.8.22.43554 > 1.1.1.1.3999: UDP, length 8192
05:55:14.608926 IP 206.225.8.22.43554 > 1.1.1.1.3999: UDP, length 8192
05:55:14.609208 IP 206.225.8.22.53075 > 1.1.1.1.5175: UDP, length 8192
05:55:14.606498 IP 206.225.8.22.38031 > 1.1.1.1.2803: UDP, length 8192
05:55:14.606568 IP 206.225.8.22.38031 > 1.1.1.1.2803: UDP, length 8192
05:55:14.606642 IP 206.225.8.22.38031 > 1.1.1.1.2803: UDP, length 8192
05:55:14.606856 IP 206.225.8.22.45951 > 1.1.1.1.3942: UDP, length 8192
05:55:14.607031 IP 206.225.8.22.45951 > 1.1.1.1.3942: UDP, length 8192
05:55:14.607268 IP 206.225.8.22.45951 > 1.1.1.1.3942: UDP, length 8192
05:55:14.607500 IP 206.225.8.22.54295 > 1.1.1.1.767: UDP, length 8192
05:55:14.607905 IP 206.225.8.22.35964 > 1.1.1.1.5859: UDP, length 8192
05:55:14.608174 IP 206.225.8.22.35964 > 1.1.1.1.5859: UDP, length 8192
05:55:14.608466 IP 206.225.8.22.33462 > 1.1.1.1.5125: UDP, length 8192
05:55:14.608853 IP 206.225.8.22.43554 > 1.1.1.1.3999: UDP, length 8192
05:55:14.608926 IP 206.225.8.22.43554 > 1.1.1.1.3999: UDP, length 8192
05:55:14.609208 IP 206.225.8.22.53075 > 1.1.1.1.5175: UDP, length 8192
 …
```

Endian Confusion

- What is it with 1.1.168.0, 1.0.168.0, 1.2.168.0?
  - Most of the packets are going to: 1.1.168.192, 1.0.168.192, 1.2.168.192.

    Does anyone see anything familiar here?
- These IPs are really just 192.168.x.1, in host-byte order (little-endian)
  - someone is running some private network code and not doing a call to `htonl(ip_addr)`, and we are catching the data in network 1
  - Do other /8s see a similar leak? yes!

1.4.0.0

- For 1/8, 17.5% of all packets (and 10% of all bytes) received are UDP packets to 1.4.0.0, destination ports 33368, 514, 33527, 3072, 33493
  - Surprisingly most of these could be interpreted as DNS traffic
  - Most appear to be valid queries
  - leakage from a “private” DNS resolver configured on 1.4.0.0?

What can we do about it?

- The following /24s are being withheld from general allocation by APNIC:
  - 1.0.0.0/24
  - 1.1.1.0/24
  - 1.2.3.0/24
  - 1.4.0.0/24
  - 1.10.10.0/24
- If further investigation reveals that the traffic to any of these /24s abates to a normal background level in the future, then these addresses would be returned to the APNIC unallocated address pool at that time.

What can we do about it (cont)?

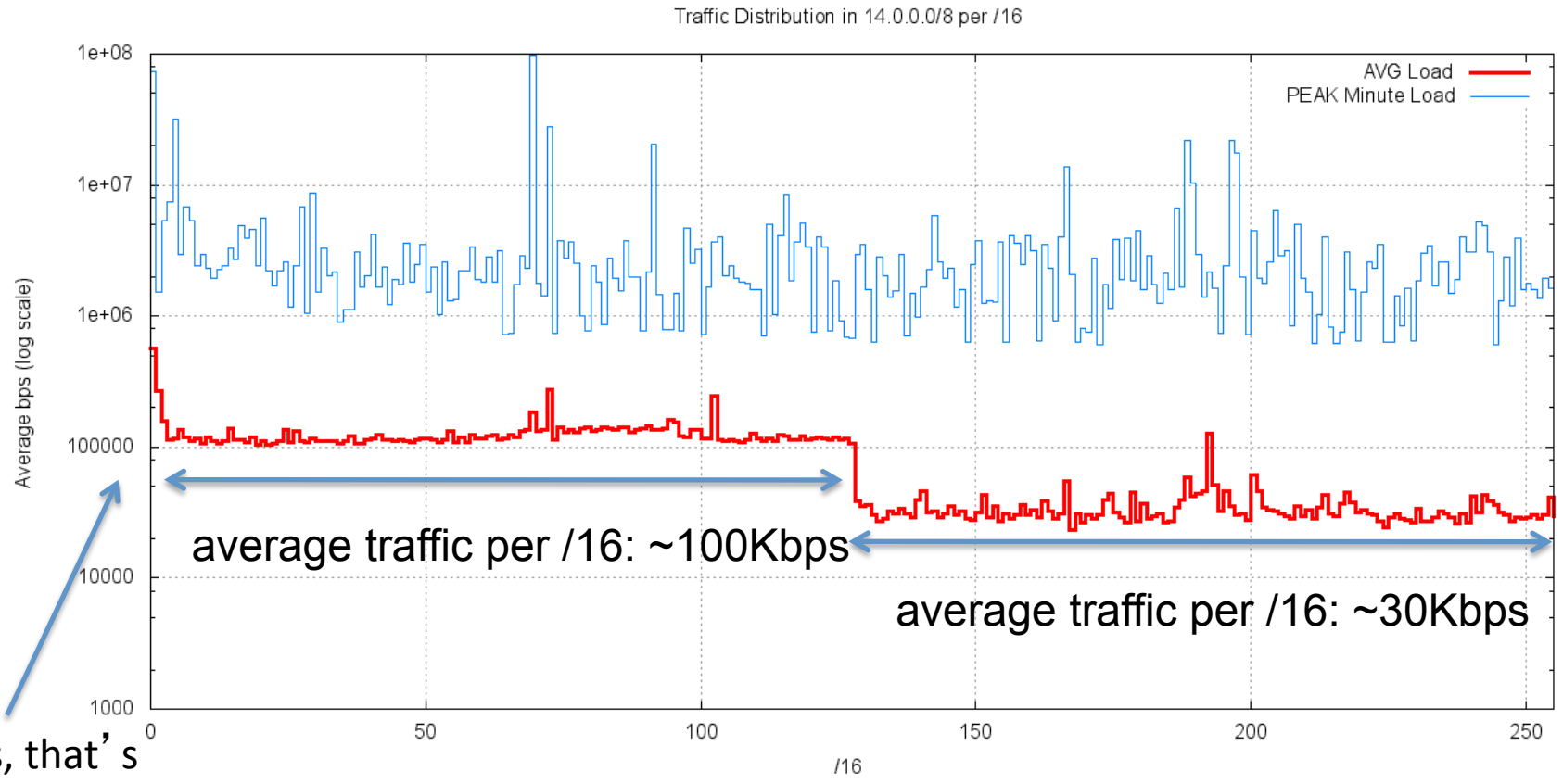
- The following /16s are temporarily marked as reserved and withheld from general allocation by APNIC:

1.0.0.0/16	1.5.0.0/16	1.20.0.0/16
1.1.0.0/16	1.6.0.0/16	1.32.0.0/16
1.2.0.0/16	1.7.0.0/16	1.37.0.0/16
1.3.0.0/16	1.8.0.0/16	1.187.0.0/16
1.4.0.0/16	1.10.0.0/16	

What about the other /8s?

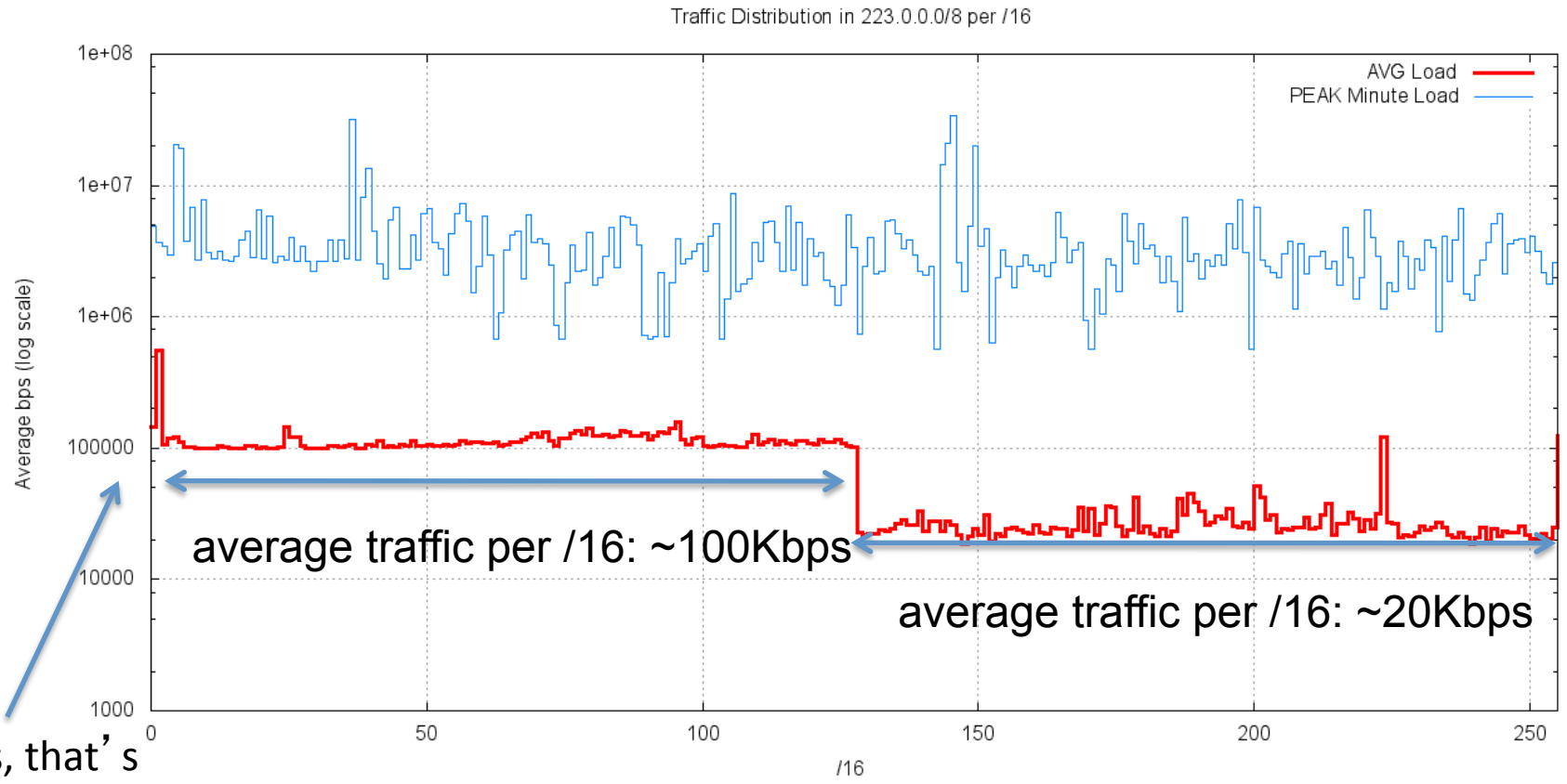
- APNIC has also tested 14/8 and 223/8 prior to commencing allocation

14.0.0.0/8 Profile



Yes, that's a Log Scale!

223.0.0.0/8 Profile



Yes, that's a Log Scale!

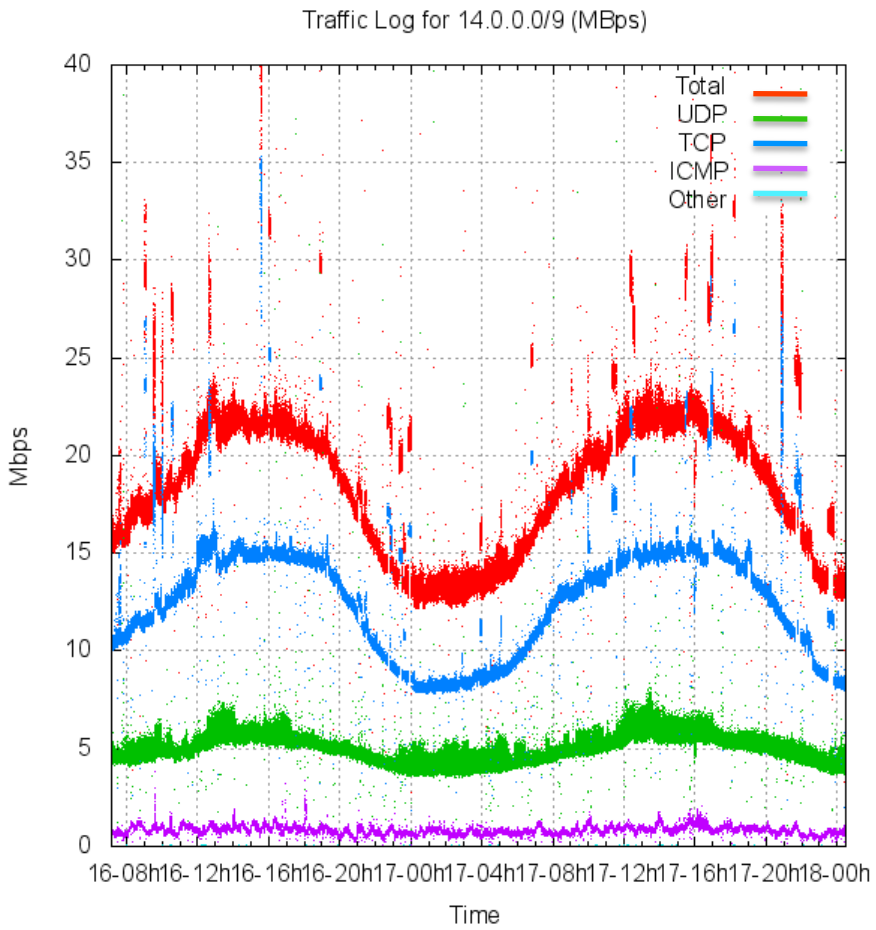
What's in the low half of these /8s?

Conficker!

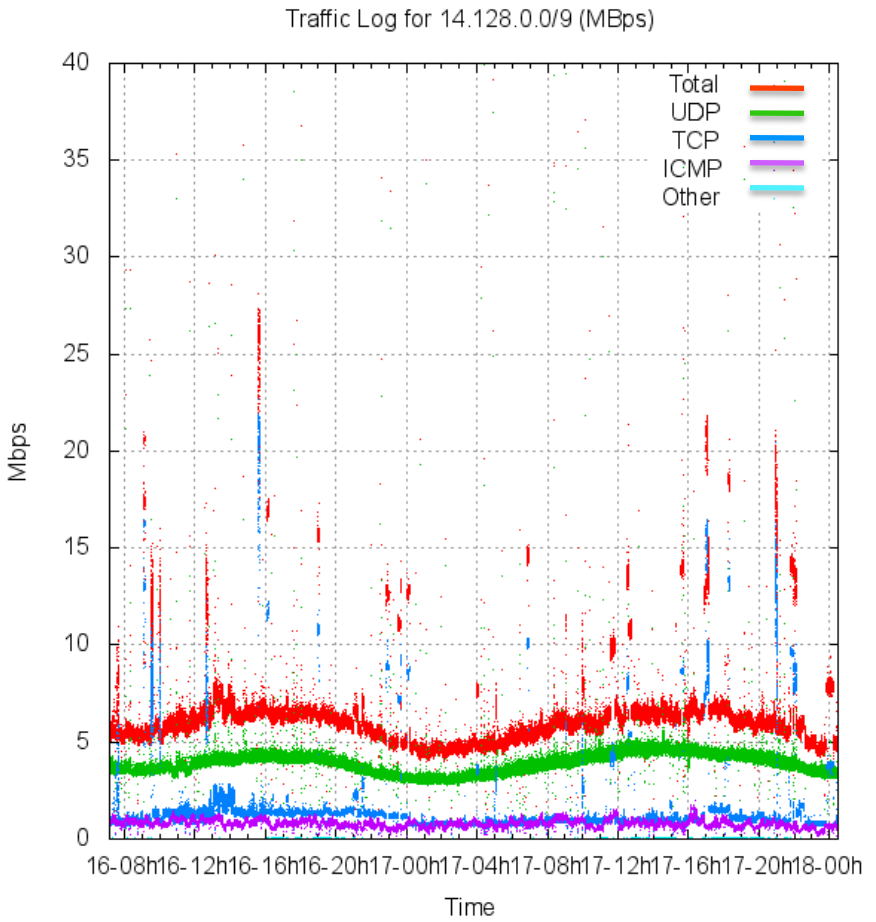
- conficker will not scan addresses with bit 9 set
- the "low" half of each /8 is scanned by various conficker-infected hosts at a rate of ~24,000 packets per second

comparing /9s in 14/8

Low Half



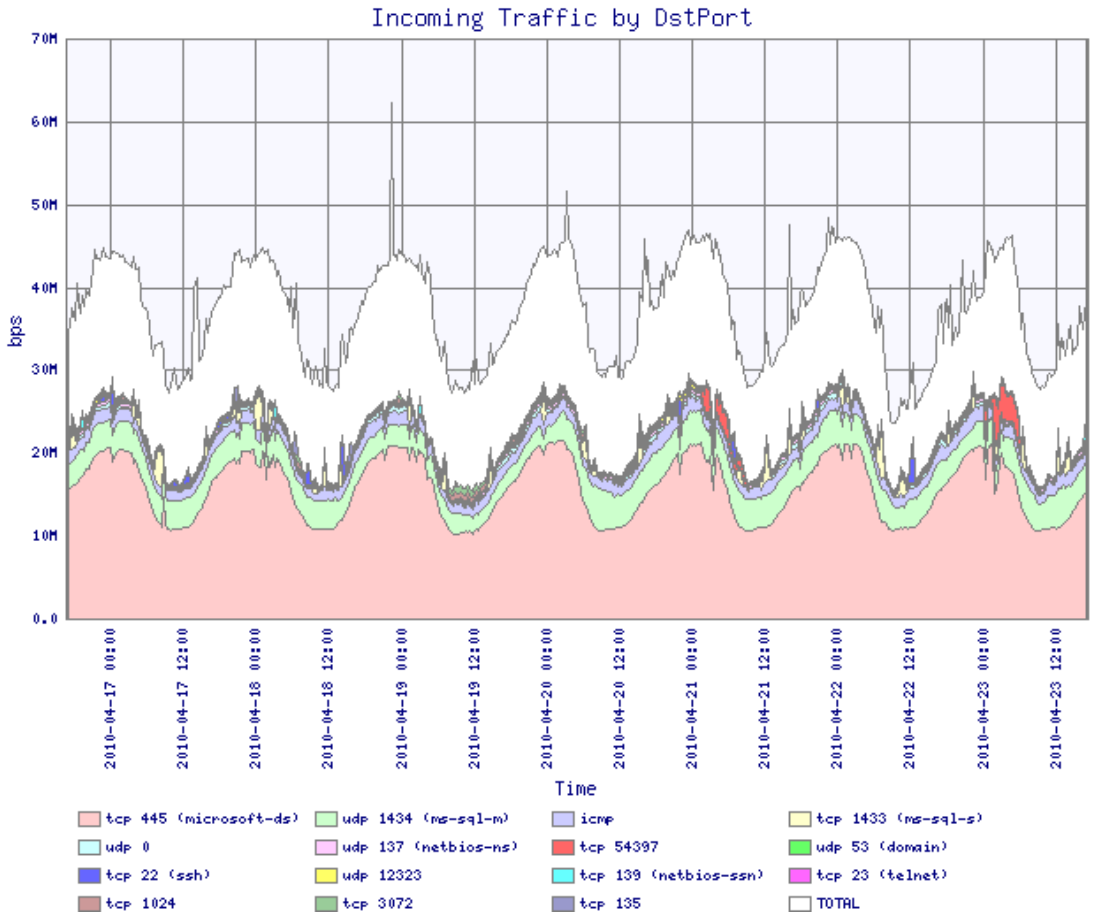
High Half



Extract from Tomoya Yoshida's JANOG Report

Per Protocol and Port

A half is tcp/445(Conficker , Downadup), second udp/1434(sql-slammer)



TCP destination ports in 14/8

Low Half

TCP Port	%	Packet Count
445	82.9%	3132836308
1433	1.7%	63876218
22	0.6%	22555596
139	0.5%	19185536
23	0.4%	15325619
135	0.4%	14307267
25	0.3%	9723041
9415	0.2%	8536035
1755	0.2%	8416185
4899	0.2%	8392818

High Half

TCP Port	%	Packet Count
1433	13.0%	61352758
22	4.0%	18769025
445	3.9%	18341810
135	3.8%	18092100
23	3.2%	15304995
139	2.8%	13192532
25	2.0%	9619182
4899	1.8%	8500798
9415	1.8%	8408492
1755	1.8%	8408303

Toxic Radiation in 14.0.0.0/8

TCP Port	%	Port / Attack
445	73.65%	MS Server / conficker
1433	1.5%	SQL Server / various
22	0.5%	ssh / probes
139	0.5%	netbios / various
23	0.4%	telnet / probes
135	0.4%	MS RPC / Blaster
25	0.3%	SMTP
9415	0.2%	koobface proxies
1755	0.2%	MS media streaming
4899	0.2%	radmin

Conficker appears to be the most virulent current Internet virus by far, with a total traffic profile of 12Mbps per /8, or 2.5 Gbps in total across the entire IPv4 address space.

What can we do about it?

- Temporary reservations of the “hot spots” in 14.0.0.0/8 and 223.0.0.0/8

Prefix
14.0.0.0/24
14.0.15.0/24
14.1.0.0/24
14.192.72.0/24
14.102.128.0/24
14.102.129.0/24

Prefix
223.0.0.0/24
223.1.0/24
223.223.223.0/24
223.255.255.0/24

IPv4 Background Radiation

- We understand that the IPv4 address space is now heavily polluted with background traffic
  - Background levels of traffic associated with scanning, backscatter, mis-configuration and leakage from private use contexts contributing to the traffic volume
  - Average background traffic level in IPv4 is around 300 – 600 bps per /24
  - There is a "heavy tail" to this distribution, with some /24s attracting well in excess of 1Mbps of continuous traffic
  - The "hottest" point in the "dark" IPv4 network appears to be 1.1.1.0/24. This prefix attracts some 100Mbps as a constant incoming traffic load

IPv4 Background Radiation

- Most of this traffic is port scanning for well known vulnerabilities:
  - predominately scanning for and by Windows systems
  - exploiting vulnerabilities where patches already exist
  - where the scanning sources are well distributed – these are bot-scanners
  - TCP Port 445 / Conficker is the most virulent scanner in today's IPv4 Internet
- Many users don't appear perform Windows software upgrades - why?*

* The answer is left as an exercise for the reader!

IPv4 Background Radiation

- Total background traffic level across the entire IPv4 address range is estimated to be some 5.5Gbps
- On average, every IPv4 address will receive one packet every 69 seconds
  - addresses in the "high" /9 of each /8 will receive a packet every 120 seconds
  - address in the "low" /9 will receive a packet every 20 seconds

IPv4 vs IPv6

- Darknets in IPv4 have been the subject of numerous studies for many years
- What about IPv6?
- Does IPv6 glow in the dark with toxic radiation yet?

IPv6 - 2400::/12

Allocated to APNIC on 3 October 2006

Currently 2400::/12 has:

709 address allocations, spanning a total of:

16,629 /32's

71,463,960,838,144 /64's

1.59% of the total block

323 route advertisements, spanning a total of:

9,584 /32's

41,164,971,903,233 /64's

0.91% of the /12 block

0.91% of the block is covered by existing more specific advertisements

0.68% of the block is unadvertised allocated address space

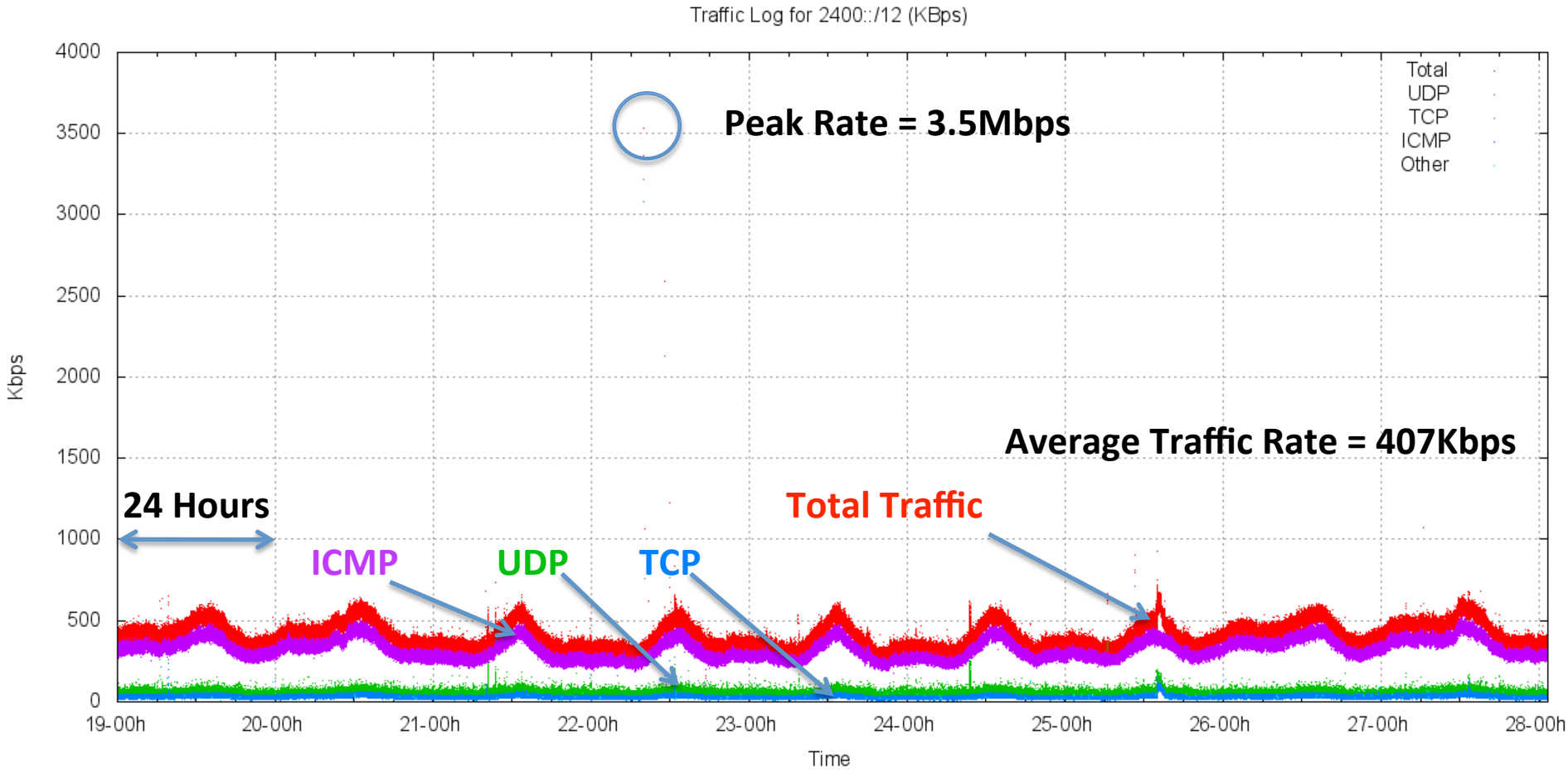
98.41% of the block is unadvertised and unallocated

Advertising 2400::/12

Darknet experiment performed between 19th June 2010 – 27th June 2010

- Advertised by AS7575 (AARNet)
- Passive data collection (no responses generated by the measurement equipment)

Total Traffic Profile for 2400::/12



Traffic Profile

Average Traffic Rate: 407 Kbps (726 packets per second)

- ICMP: 323 Kbps (611 pps)
- UDP: 54 Kbps (68 pps)
- TCP: 30 Kbps (45 pps)

This is predominately ICMP echo request ping traffic:

23:25:10.715973 IP6 2001:0:4137:9e76:2c7c:b94e:44b5:fb49 > 2408:a6:7b:0:45ca:2a3:d194:5990: ICMP6, echo request, seq 30134, length 12
23:25:10.716473 IP6 2001:0:4137:9e76:2c7c:b94e:44b5:fb49 > 2408:e2:e193:0:45be:4c21:2d64:a724: ICMP6, echo request, seq 54944, length 12
23:25:10.717722 IP6 2002:b01:107::b01:107.42176 > 2408:f3:1fff:2de:6432:1d4:c99a:61b7.58816: UDP, length 30
23:25:10.717972 IP6 2002:bb4d:1706::bb4d:1706.57530 > 2408:e2:c062:0:e0cc:a0e4:ef3:bb2e.59987: S 4266862600:4266862600(0) win 8192 <mss 1220,nop,wscale 8,nop,nop,sackOK>
23:25:10.718097 IP6 2001:0:4137:9e76:2c7c:b94e:44b5:fb49 > 2408:f1:c39f:0:7962:4cee:8a0e:caf4: ICMP6, echo request, seq 12104, length 12
23:25:10.719346 IP6 2001:0:4137:9e74:24da:19b5:9d17:e5a2 > 2408:43:ffff:28b:b0b0:f37:a03d:68f2: ICMP6, echo request, seq 19357, length 12
23:25:10.720595 IP6 2001:0:5ef5:73bc:34d0:39eb:a972:b2b3 > 2408:45:e0b5:0:b53b:5538:29ba:7db: ICMP6, echo request, seq 48700, length 12
23:25:10.722094 IP6 2002:bb0b:930a::bb0b:930a.36160 > 2408:e1:e221:0:907:e8fd:5d9d:a13d.42034: UDP, length 30
23:25:10.723094 IP6 2001:0:4137:9e74:382e:2042:4494:dcbb > 2408:a6:60d0:0:1158:3cac:d354:6270: ICMP6, echo request, seq 20067, length 12
23:25:10.724468 IP6 2002:ae60:d1aa::ae60:d1aa.56494 > 2408:52:823d:0:79f7:60bc:354b:48c1.42757: S 288897054:288897054(0) win 8192 <mss 1220,nop,nop,sackOK>
23:25:10.724593 IP6 2002:ae60:d1aa::ae60:d1aa.51448 > 2408:52:823d:0:79f7:60bc:354b:48c1.42757: UDP, length 30
23:25:10.728965 IP6 2001:0:4137:9e76:58:b42f:42e5:8677 > 2408:144:a043:0:80a6:ae82:9f2:94dc: ICMP6, echo request, seq 41229, length 12
23:25:10.729715 IP6 2001:0:cf2e:3096:183a:2cf8:2301:fffb > 2408:164:e14c:0:2c22:696c:ccf:cfd4: ICMP6, echo request, seq 22249, length 12
23:25:10.730089 IP6 2001:0:4137:9e76:58:b42f:42e5:8677 > 2408:f1:600b:0:a89d:33b5:d596:ed54: ICMP6, echo request, seq 22045, length 12
23:25:10.732838 IP6 2001:0:4137:9e74:1091:efc:42b8:1dd6 > 2408:143:9fff:7d4:dcd1:c401:e0a7:2513: ICMP6, echo request, seq 54208, length 12
23:25:10.733962 IP6 2001:0:4137:9e74:2875:87b4:42c4:3ea1 > 2408:f1:c205:0:4c03:51f2:a875:f7af: ICMP6, echo request, seq 60039, length 12
23:25:10.733966 IP6 2001:7b8:3:1f:0:2:53:2.53 > 2401:d400:20:0:20b:cdff:fe9a:d89b.19626: 47081*- 1/0/0 A 127.0.0.4 (69)
23:25:10.734837 IP6 2002:bd29:9806::bd29:9806.1410 > 2408:f1:632c:0:782c:167d:c9aa:333f.10229: S 3391249916:3391249916(0) win 16384 <mss 1220>
23:25:10.736086 IP6 2002:bb4a:204c::bb4a:204c.37641 > 2408:a5:237e:0:a5da:ec55:3ab3:c536.51276: UDP, length 30
23:25:10.744457 IP6 2001:0:5ef5:73bc:b2:345e:7fd8:ee9e > 2408:162:ffff:5a3:21b:8bff:feed:1c68: ICMP6, echo request, seq 6766, length 12
23:25:10.745456 IP6 2001:0:4137:9e76:cd3:100d:36cd:ea2a > 2408:f1:628d:0:5c8c:f981:b720:f145: ICMP6, echo request, seq 6763, length 12
23:25:10.753451 IP6 2002:bd0f:7871::bd0f:7871.57032 > 2408:e2:e14f:0:88ec:687a:79fe:6dea.15763: S 544576302:544576302(0) win 8192 <mss 1220,nop,nop,sackOK>
23:25:10.754075 IP6 2001:0:4137:9e76:57:2d2f:415e:43c8 > 2408:43:dfff:cc0:940f:b92b:8864:1b4d: ICMP6, echo request, seq 5992, length 12
23:25:10.755075 IP6 2001:0:4137:9e76:24f4:353f:36d5:5780 > 2408:a7:6258:0:ddc4:1b3a:a86f:9b5: ICMP6, echo request, seq 40996, length 12
23:25:10.755699 IP6 2001:0:4137:9e74:854:2f9f:42d1:3235 > 2408:e2:e1be:0:e9de:98aa:37d6:3bfe: ICMP6, echo request, seq 8655, length 12
23:25:10.756824 IP6 2a01:e35:2e42:db40:a45f:e5b1:dce1:831c.42176 > 2408:41:4349:0:89c0:46cc:f238:56d7.52213: UDP, length 30
23:25:10.757074 IP6 2001:0:4137:9e76:3ce8:647:44f2:f9a7 > 2408:143:a11c:0:21b:63ff:fea0:543: ICMP6, echo request, seq 8185, length 12
23:25:10.758073 IP6 2001:0:4137:9e76:1890:1a7b:24bd:cf68 > 2408:f1:632c:0:782c:167d:c9aa:333f: ICMP6, echo request, seq 61665, length 12
23:25:10.758077 IP6 2001:0:cf2e:3096:ce7:4674:8239:5876 > 2408:e2:c129:0:551e:74f2:3cc1:dfcb: ICMP6, echo request, seq 9465, length 12
23:25:10.758697 IP6 2001:0:4137:9e74:30c2:2e8f:36f0:2d5f > 2408:e2:dfff:78:658e:f68:f572:46d6: ICMP6, echo request, seq 46187, length 12
23:25:10.760821 IP6 2001:0:4137:9e76:18fc:d66d:448d:8ec0 > 2408:140:e2af:0:c8e4:3305:4b85:9ce4: ICMP6, echo request, seq 45787, length 12
23:25:10.760946 IP6 2001:0:4137:9e76:db:cfb:347a:3315 > 2408:c7:dfff:ef3:211:2fff:fef7:1202: ICMP6, echo request, seq 50222, length 12
23:25:10.763320 IP6 2001:0:4137:9e74:2c62:d306:448e:43a5 > 2408:f3:1fff:2de:6432:1d4:c99a:61b7: ICMP6, echo request, seq 62359, length 12
23:25:10.765069 IP6 2002:bd0f:de91::bd0f:de91.53404 > 2408:151:84ce:0:b16d:78bf:8a2a:ecbf.20734: UDP, length 30
23:25:10.765073 IP6 2001:0:4137:9e76:105b:18af:2545:d977 > 2408:50:840d:0:4121:6280:80ad:9f16: ICMP6, echo request, seq 53376, length 12
23:25:10.767567 IP6 2001:0:4137:9e74:0:fbe2:448f:4e63 > 2408:143:8b63:0:f4f3:56c5:628:a982: ICMP6, echo request, seq 31170, length 12
23:25:10.772815 IP6 2001:0:4137:9e74:3ce9:32a4:bdc7:5561 > 2408:66:2108:0:d821:e8df:b9dc:e744: ICMP6, echo request, seq 27160, length 12
23:25:10.773939 IP6 2001:0:4137:9e76:cfb:d06:3774:57be > 2408:152:c058:0:fc10:bf39:97c8:47d7: ICMP6, echo request, seq 11647, length 12
23:25:10.774563 IP6 2002:bb65:201::bb65:201.47237 > 2408:80:3fff:817:9dc:e8a8:1c76:a85a.26344: UDP, length 33

This is predominately ICMP echo request traffic

- There's a lot of 2002::/16 6to4 source addresses
  - Some of these 2002:: sources are 6to4 cpe
  - Most are windows end systems
- There are also a lot of Teredo 2001:0::/32 sources
- And remarkably little unicast IPv6 source addresses
- And the destinations are predominately in 2408::/16

23:25:10.715973 IP6 2001:0:4137:9e76:2c7c:b94e:44b5:fb49 > 2408:a6:7b:0:45ca:2a3:d194:5990: ICMP6, echo request, seq 30134, length 12
23:25:10.716473 IP6 2001:0:4137:9e76:2c7c:b94e:44b5:fb49 > 2408:e2:e193:0:45be:4c21:2d64:a724: ICMP6, echo request, seq 54944, length 12
23:25:10.717722 IP6 2002:b01:107::b01:107.42176 > 2408:f3:1fff:2de:6432:1d4:c99a:61b7.58816: UDP, length 30
23:25:10.718097 IP6 2001:0:4137:9e76:2c7c:b94e:44b5:fb49 > 2408:f1:c39f:0:7962:4cee:8a0e:caf4: ICMP6, echo request, seq 12104, length 12
23:25:10.722094 IP6 2002:bb0b:930a::bb0b:930a.36160 > 2408:e1:e221:0:907:e8fd:5d9d:a13d.42034: UDP, length 30
23:25:10.724593 IP6 2002:ae60:d1aa::ae60:d1aa.51448 > 2408:52:823d:0:79f7:60bc:354b:8c1.42757: UDP, length 30
23:25:10.728965 IP6 2001:0:4137:9e76:58:b42f:42e5:8677 > 2408:144:a043:0:80a6:ae82:9f2:94dc: ICMP6, echo request, seq 41229, length 12
23:25:10.729715 IP6 2001:0:cf2e:3096:183a:2cf8:2301:fffb > 2408:164:e14c:0:2c22:696c:ccf:cfd4: ICMP6, echo request, seq 22249, length 12
23:25:10.730089 IP6 2001:0:4137:9e76:58:b42f:42e5:8677 > 2408:f1:600b:0:a89d:33b5:d596:ed54: ICMP6, echo request, seq 22045, length 12
23:25:10.734837 IP6 2002:bd29:9806::bd29:9806.1410 > 2408:f1:632c:0:782c:167d:c9aa:333f.10229: S 3391249916:3391249916(0) win 16384 <mss 1220>
23:25:10.736086 IP6 2002:bb4a:204c::bb4a:204c.37641 > 2408:a5:237e:0:a5da:ec55:3ab3:c536.51276: UDP, length 30
23:25:10.744457 IP6 2001:0:5ef5:73bc:b2:345e:7fd8:ee9e > 2408:162:ffff:5a3:21b:8bff:feed:1c68: ICMP6, echo request, seq 6766, length 12
23:25:10.745456 IP6 2001:0:4137:9e76:cd3:100d:36cd:ea2a > 2408:f1:628d:0:5c8c:f981:b720:f145: ICMP6, echo request, seq 6763, length 12
23:25:10.755075 IP6 2001:0:4137:9e76:24f4:353f:36d5:5780 > 2408:a7:6258:0:ddc4:1b3a:a86f:9b5: ICMP6, echo request, seq 40996, length 12
23:25:10.757074 IP6 2001:0:4137:9e76:3ce8:647:44f2:f9a7 > 2408:143:a11c:0:21b:63ff:fea0:543: ICMP6, echo request, seq 8185, length 12
23:25:10.758073 IP6 2001:0:4137:9e76:1890:1a7b:24bd:cf68 > 2408:f1:632c:0:782c:167d:c9aa:333f: ICMP6, echo request, seq 61665, length 12
23:25:10.758077 IP6 2001:0:cf2e:3096:ce7:4674:8239:5876 > 2408:e2:c129:0:551e:74f2:3cc1:dfcb: ICMP6, echo request, seq 9465, length 12
23:25:10.758697 IP6 2001:0:4137:9e74:30c2:2e8f:36f0:2d5f > 2408:e2:dfff:78:658e:f68:f572:46d6: ICMP6, echo request, seq 46187, length 12
23:25:10.763320 IP6 2001:0:4137:9e74:2c62:d306:448e:43a5 > 2408:f3:1fff:2de:6432:1d4:c99a:61b7: ICMP6, echo request, seq 62359, length 12
23:25:10.767567 IP6 2001:0:4137:9e74:0:fbe2:448f:4e63 > 2408:143:8b63:0:f4f3:56c5:628:a982: ICMP6, echo request, seq 31170, length 12
23:25:10.772815 IP6 2001:0:4137:9e74:3ce9:32a4:bdc7:5561 > 2408:66:2108:0:d821:e8df:b9dc:e744: ICMP6, echo request, seq 27160, length 12
23:25:10.773939 IP6 2001:0:4137:9e76:cfb:d06:3774:57be > 2408:152:c058:0:fc10:bf39:97c8:47d7: ICMP6, echo request, seq 11647, length 12
23:25:10.774563 IP6 2002:bb65:201::bb65:201.47237 > 2408:80:3fff:817:9dc:e8a8:1c76:a85a.26344: UDP, length 33

what the …?

IP6 xxxx:3000:0:1::174 > 2406:ac7b:4a65:174e:c07a:8804:655:87: ICMP6, destination unreachable, unreachable route 20cd:6124::b002:d200:30fe:0, length 59

IP6 xxxx:3000:0:1::153 > 2406:d2c0:47f9:f424:c07a:875a:5ad:87: ICMP6, destination unreachable, unreachable route e348:3352::b002:d200:c33b:0, length 53

IP6 xxxx:3000:0:1::153 > 2406:eef2:ad3d:7299:c07a:8761:e01:87: ICMP6, destination unreachable, unreachable route be7f:336c::b002:d200:fbd6:0, length 67

<etc>

what the … ?

ICMP destination unreachable messages…

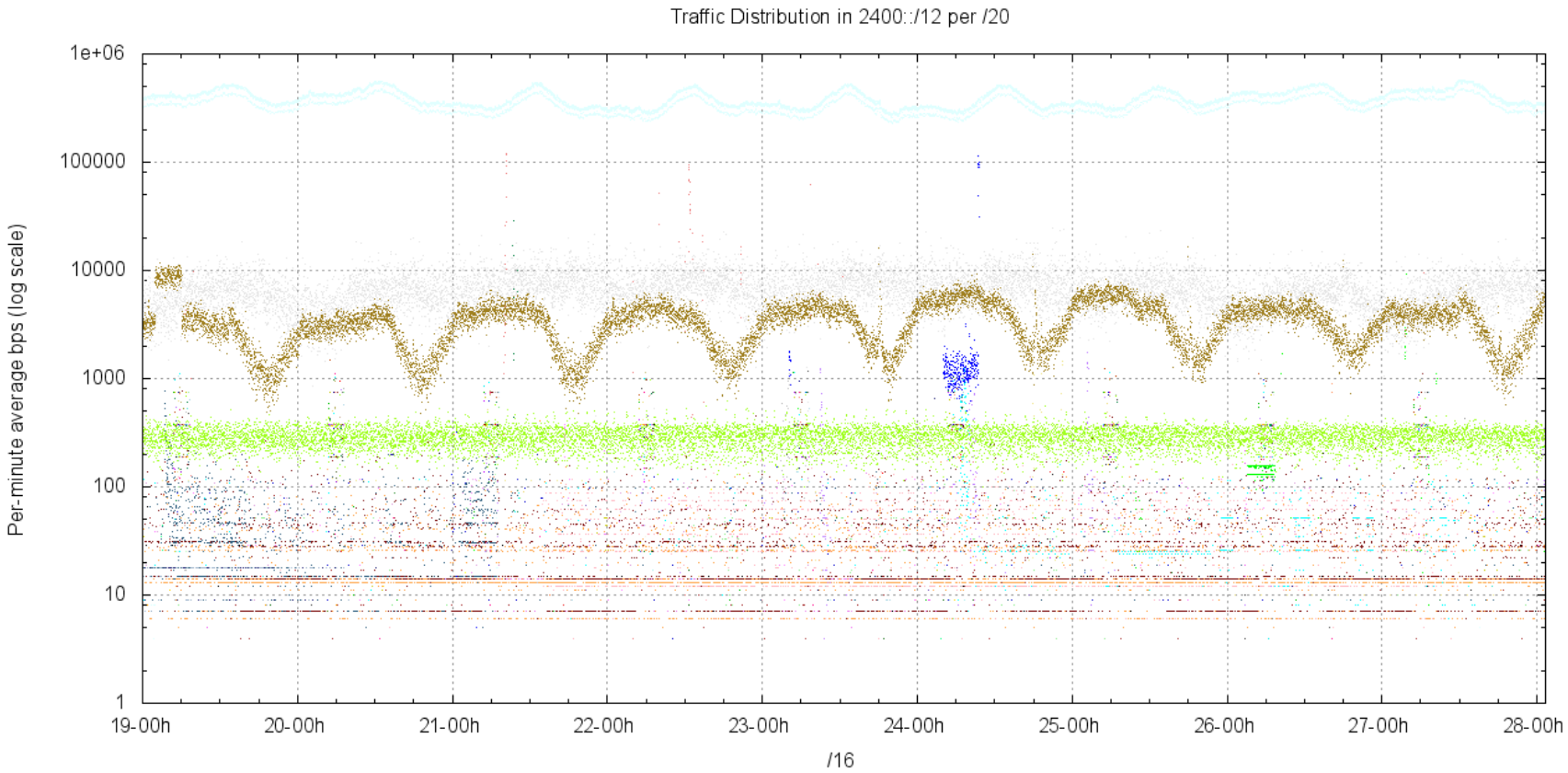
That's someone saying "you can't get there from here!"

But the packet is being sent to an unreachable source address!

Thats a double misconfig of both source AND destination addresses!

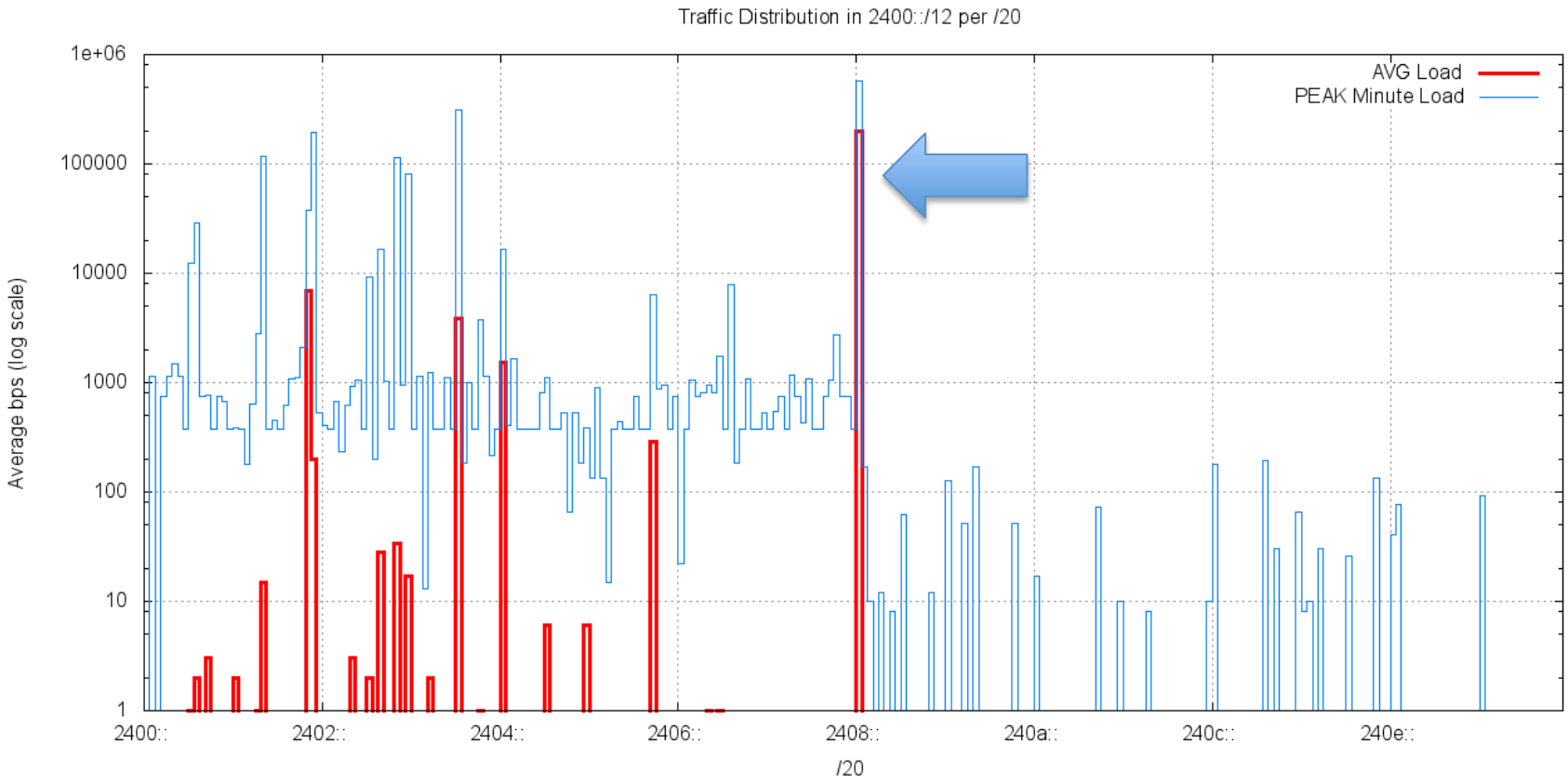
well done!

Destination Address Distribution



This is not a uniform distribution – one /20 is the target of most of the dark IPv6 traffic

Destination Address Distribution



Top 5 /20s in 2400::/12

2408:0000:/20	197Kbps	Allocated: 2408::/22 – NTT East, JP
2401:d000::/20	7Kbps	8 x /32 allocations in this block
2403:8000::/20	4Kbps	4 x /32 allocations in this block
2404:0000::/20	1Kbps	29 allocations in this block
2405:b000::/20	0.3Kbps	4 x /32 allocations in this block

Is This Leakage or Probing?

- There is no direct equivalent of RFC1918 private use addresses in IPv6

  (well, there are ULAs, but they are slightly different!)

- In IPv6 it's conventional to use public IPv6 addresses in private contexts

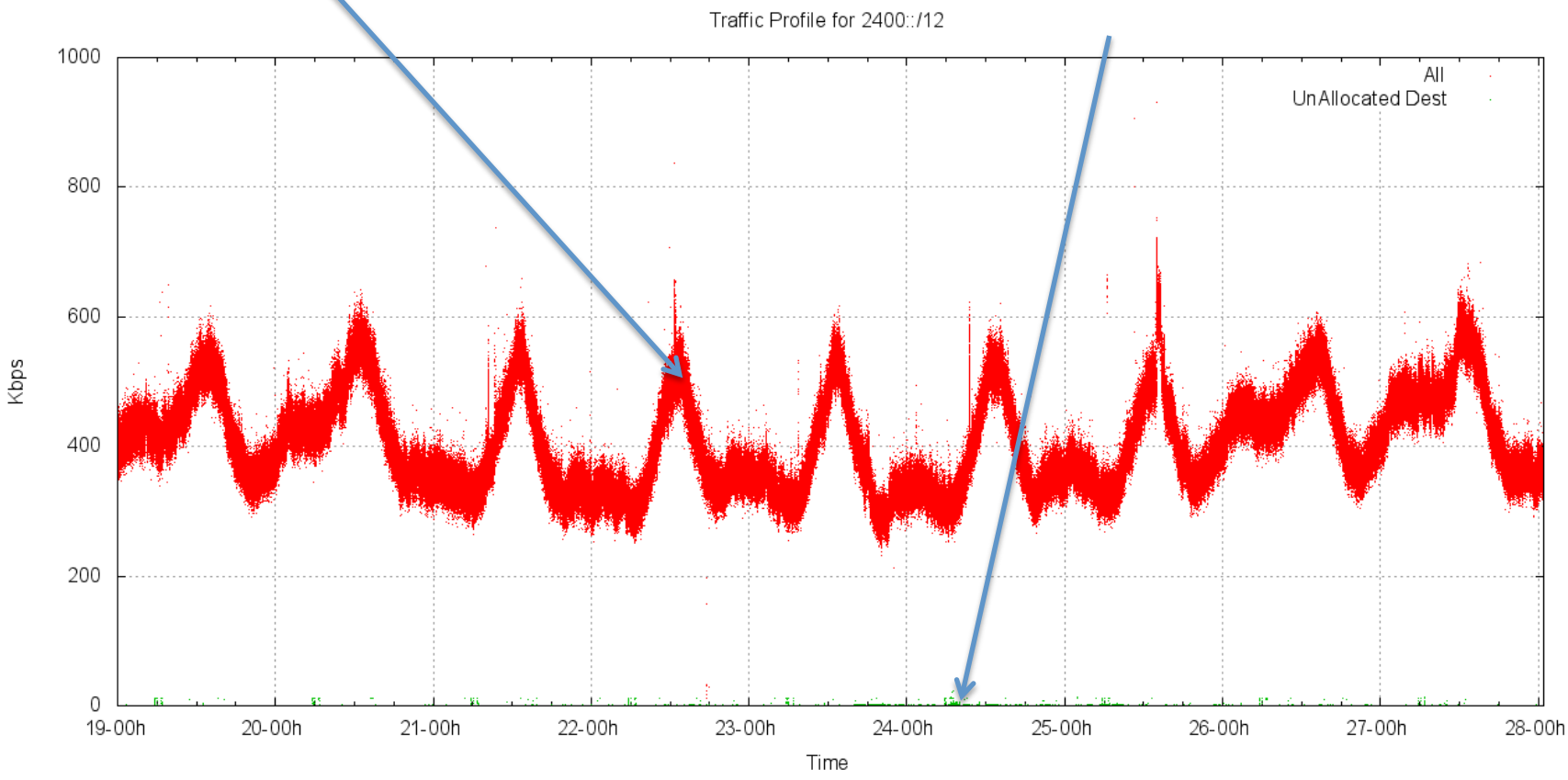
- **How much of this "dark" IPv6 traffic is a result of "leakage" from private contexts into the public network?**

- Filter the captured packets using the address allocation data

Allocated vs Unallocated Dark Traffic

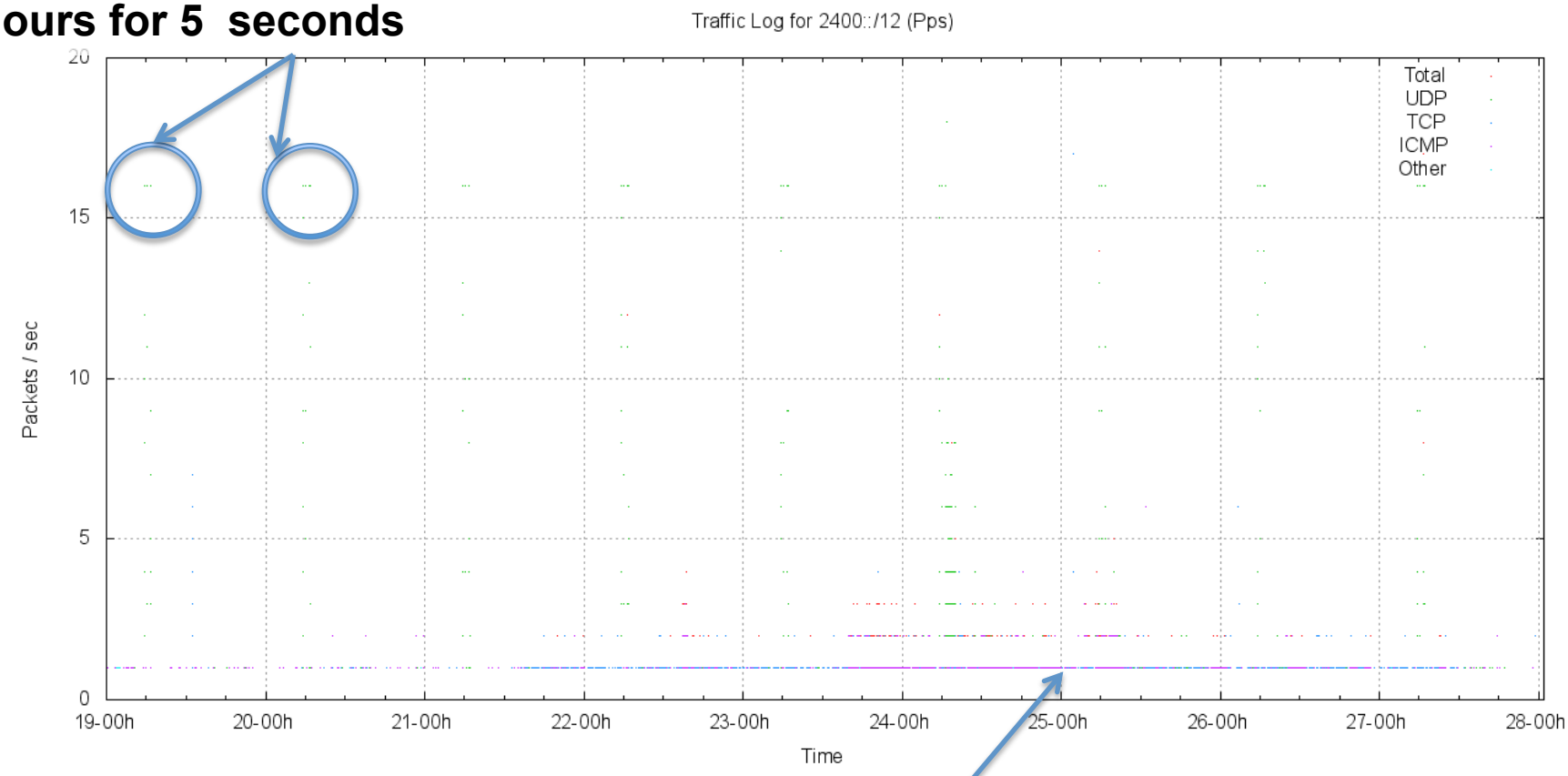
Leaked IPv6 traffic

Dark IPv6 Traffic



Dark IPv6 Traffic

Yes, that's a pattern of 16 UDP packets per second every 24 hours for 5 seconds



less than 1 packet per second of ICMP

Dark IPv6 Traffic Profile

Average Packet Rate:

1 packet per 36.8 seconds for the entire /12

Packet Count: 21,166

ICMP: 7881 (37%)

TCP: 7660 (36%)

UDP: 5609 (26%)

TCP Profile

SYN packets: (possibly probe / scanning traffic)

1126

SYN+ACK packets: (wrong source, local config errors?)

6392

Others (Data packets!):

141

TCP Oddities

Stateless TCP in the DNS?

(no opening handshake visible in the data collection – just the TCP response data!)

DNS TCP Response:

04:47:06.962808 IP6 (hlim 51, next-header TCP (6) payload length: 1351)

2001:468:1802:102::805b:fe01.53 > 2401:1a19::123:108:224:6.49121, Length: 1319 ACK: 1672186592 WIN 49980

Query: A? finlin.wharton.upenn.edu.

Response: finlin.wharton.upenn.edu. A 128.91.91.59

TCP Probing?

13:12:56.528487 IP6 (hlim 44, next-header TCP (6) payload length: 1460) 2001:250:7801:a400::1987:407.33729 > 2402:e968:6000::d27e:4ed:fb5b.2273: ., 3207301626:3207303066(1440) ack 3706857348 win 63916

01:47:00.122909 IP6 (hlim 44, next-header TCP (6) payload length: 20) 2001:250:7801:a400::1987:407.57777 > 2402:2b75:2100:0:42:dc34:e8f3:52a4.3113: ., 272892761:272892761(0) ack 2064800132 win 64800

01:50:47.197265 IP6 (hlim 44, next-header TCP (6) payload length: 20) 2001:250:7801:a400::1987:407.57777 > 2402:2f2a:179:341f:d6:dc34:e8f3:52a4.3113: ., 302360250:302360250(0) ack 2091174988 win 64800

03:44:39.140290 IP6 (hlim 44, next-header TCP (6) payload length: 20) 2001:250:7801:a400::1987:407.57777 > 2402:a236:6000:0:4d8:dc34:e8f3:52a4.3113: ., 829577701:829577701(0) ack 2622550921 win 64800

03:58:23.851708 IP6 (hlim 44, next-header TCP (6) payload length: 20) 2001:250:7801:a400::1987:407.57777 > 2402:9a23:100:2:d6:dc34:e8f3:52a4.3113: .,, 829661294:829661294(0) ack 2702723699 win 64800

05:02:52.568996 IP6 (hlim 44, next-header TCP (6) payload length: 20) 2001:250:7801:a400::1987:407.57777 > 2402:1123:1ba:ec05:ef:f2c6:ce35:c40f.1158: ., 1365702964:1365702964(0) ack 3293642040 win 64800

05:50:43.706430 IP6 (hlim 44, next-header TCP (6) payload length: 20) 2001:250:7801:a400::1987:407.57777 > 2402:76d9:16b:7320:d8:f2c6:ce35:c40f.1158: ., 1409613792:1409613792(0) ack 3600529388 win 64800

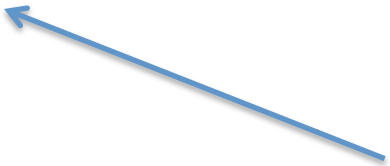
07:20:15.728521 IP6 (hlim 44, next-header TCP (6) payload length: 20) 2001:250:7801:a400::1987:407.57777 > 2402:6219:4100:0:2b0:dc34:e8f3:52a4.3113: .,, 830692465:830692465(0) ack 3672203022 win 64800

08:37:57.505208 IP6 (hlim 44, next-header TCP (6) payload length: 20) 2001:250:7801:a400::1987:407.57777 > 2402:b54e:1cc:e14:52:dc34:e8f3:52a4.3113: .,, 831214068:831214068(0) ack 4169603866 win 64800

Repeated TCP packets, same source addresses and ports, no preceding SYN/ACK TCP handshake, different addresses addresses, small dest port set (1158, 3113, 2273)

TCP Probing, or…?

12:44:54.038234 IP6 2001::4137:9e76:28ae:355f:8417:a083.80 > 240a:f000:1405:6001:1cbc:f191:1384:7cde.1597: Flags [S.], seq 3889176058, ack 2381452531, win 8192, length 0
12:44:54.038358 IP6 2001::4137:9e76:28ae:355f:8417:a083.80 > 240b:f000:1685:6001:1cbc:f191:1384:7cde.1597: Flags [S.], seq 3889176058, ack 2381452531, win 8192, length 0
12:44:54.038613 IP6 2001::4137:9e76:28ae:355f:8417:a083.80 > 240c:f000:1905:6001:1cbc:f191:1384:7cde.1597: Flags [S.], seq 3889176058, ack 2381452531, win 8192, length 0
12:44:54.914216 IP6 2001::4137:9e76:28ae:355f:8417:a083.80 > 240c:f000:1905:6001:1cbc:f191:1384:7cde.1597: Flags [.], seq 1, ack 220, win 17080, length 0
12:44:54.914341 IP6 2001::4137:9e76:28ae:355f:8417:a083.80 > 240a:f000:1405:6001:1cbc:f191:1384:7cde.1597: Flags [.], seq 1, ack 220, win 17080, length 0
12:44:54.914466 IP6 2001::4137:9e76:28ae:355f:8417:a083.80 > 240b:f000:1685:6001:1cbc:f191:1384:7cde.1597: Flags [.], seq 1, ack 220, win 17080, length 0
12:49:52.061661 IP6 2001::4137:9e76:28ae:355f:8417:a083.80 > 240b:f000:1685:af01:b469:173f:8bc8:3411.3991: Flags [.], seq 536162733, ack 2327619384, win 16621, length 0
12:49:52.061785 IP6 2001::4137:9e76:28ae:355f:8417:a083.80 > 240c:f000:1905:af01:b469:173f:8bc8:3411.3991: Flags [.], seq 536162733, ack 2327619384, win 16621, length 0
12:49:52.061915 IP6 2001::4137:9e76:28ae:355f:8417:a083.80 > 240a:f000:1405:af01:b469:173f:8bc8:3411.3991: Flags [.], seq 536162733, ack 2327619384, win 16621, length 0



Same Teredo source address, but varying destination addresses

Self-Misconfiguration

10:56:20.719296 IP6 (hlim 57, next-header TCP (6) payload length: 40) 2001:470:1f04:815::2.25 > 2402:5000::250:56ff:feb0:11aa.37839: S, cksum 0x79db (correct), 2261394238:2261394238(0) ack 2082559012 win 64768 <mss 1420,sackOK,timestamp 128287793 3737661225,nop,wscale 11>

A mail server at he.net is (correctly) responding to a mail client at the (invalid) address 2402:5000::250:56ff:feb0:11aa. There are sequences of 8 packets paced over ~90 seconds with doubling intervals – typical signature of a SYN handshake failure

This single address pair generated a total of 6,284 packets over 9 days (corresponding to 780 sendmail attempts!)

Dark DNS

Queries: 2,892 queries over 7 days

from just 4 source addresses!

Backscattered Responses: 30

All of these look a lot like configuration errors in dual stack environments. These errors go largely unnoticed because of the fallback to V4 in dual stack.

Dark ICMP

echo request packets (ping) – 7,802 packets

93 others – destination unreachables, and malformed packet headers

IPv6 Dark Traffic

- Most of the traffic in the dark space is leakage from private use contexts
  - There is a message here to all "private" networks: they really aren't necessarily all that private!
- And we've seen a small amount of traffic that appears to be a result of poor transcription of IPv6 addresses into system configs and into DNS zone files
- And the use of dual stack makes most of these IPv6 config stuffups go completely unnoticed!

IPv6 Scanning

- What happens in IPv4 does not translate into IPv6 .
- There is no visible evidence of virus scanners attempting to probe into the dark address blocks in IPv6 - yet
- The nature of IPv6 is such that address scanning as a means of virus propagation is highly impractical
  - a /48 contains 2^{80} addresses. Scanning 1 million addresses per second implies a "full" scan will take 2^{60} seconds. That's 36 billion years, or 3 times the estimated life of the universe!
  - That does not mean that IPv6 is magically "secure" – far from it – it just means that virus propagation via +1 "full" address scanning algorithm does not translate from IPv4 into IPv6

Hanlon's Razor:

Never attribute to malice what can equally be explained by stupidity!

Thank You

Questions?