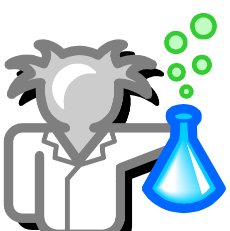
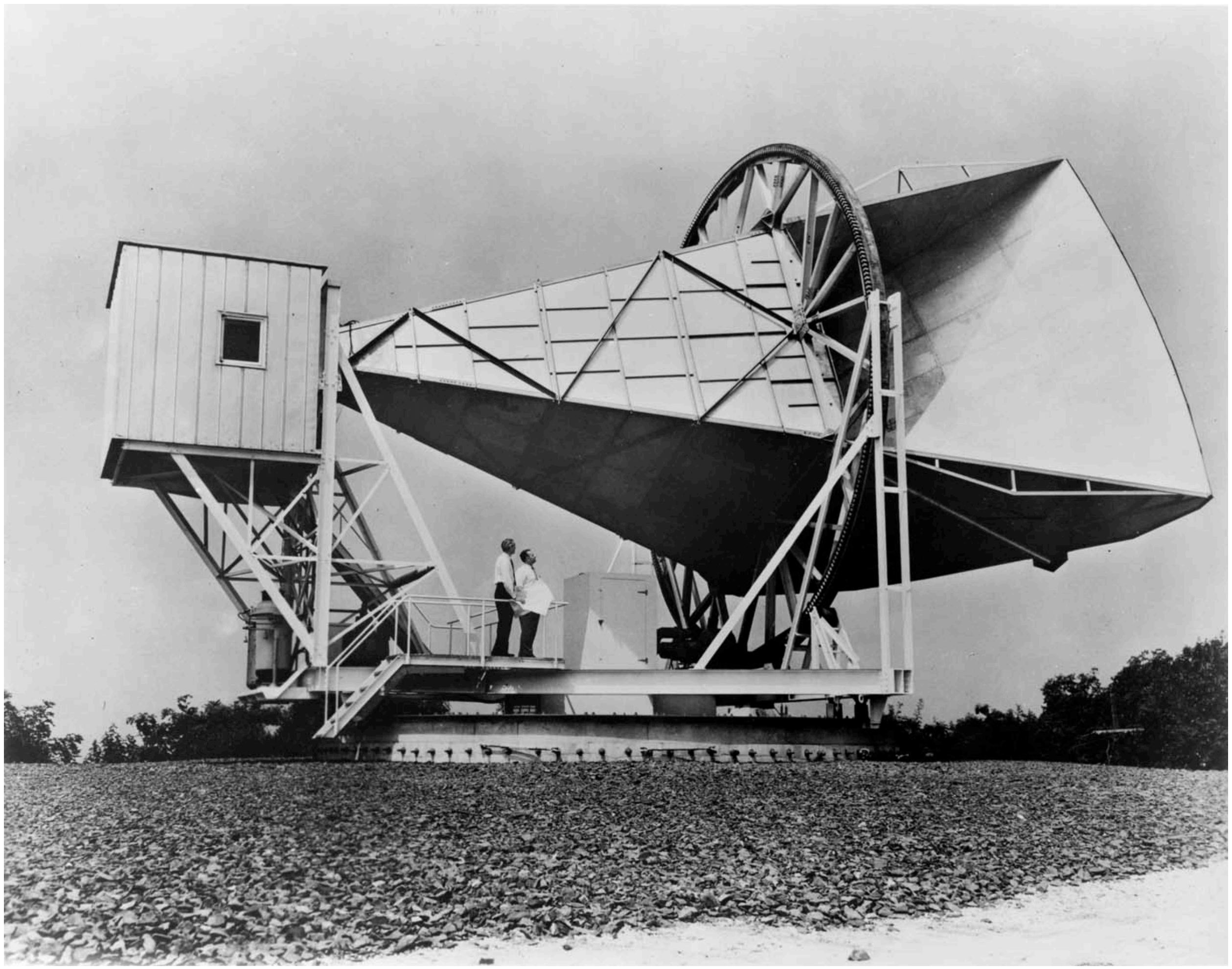
IPv6 Background Radiation

Geoff Huston

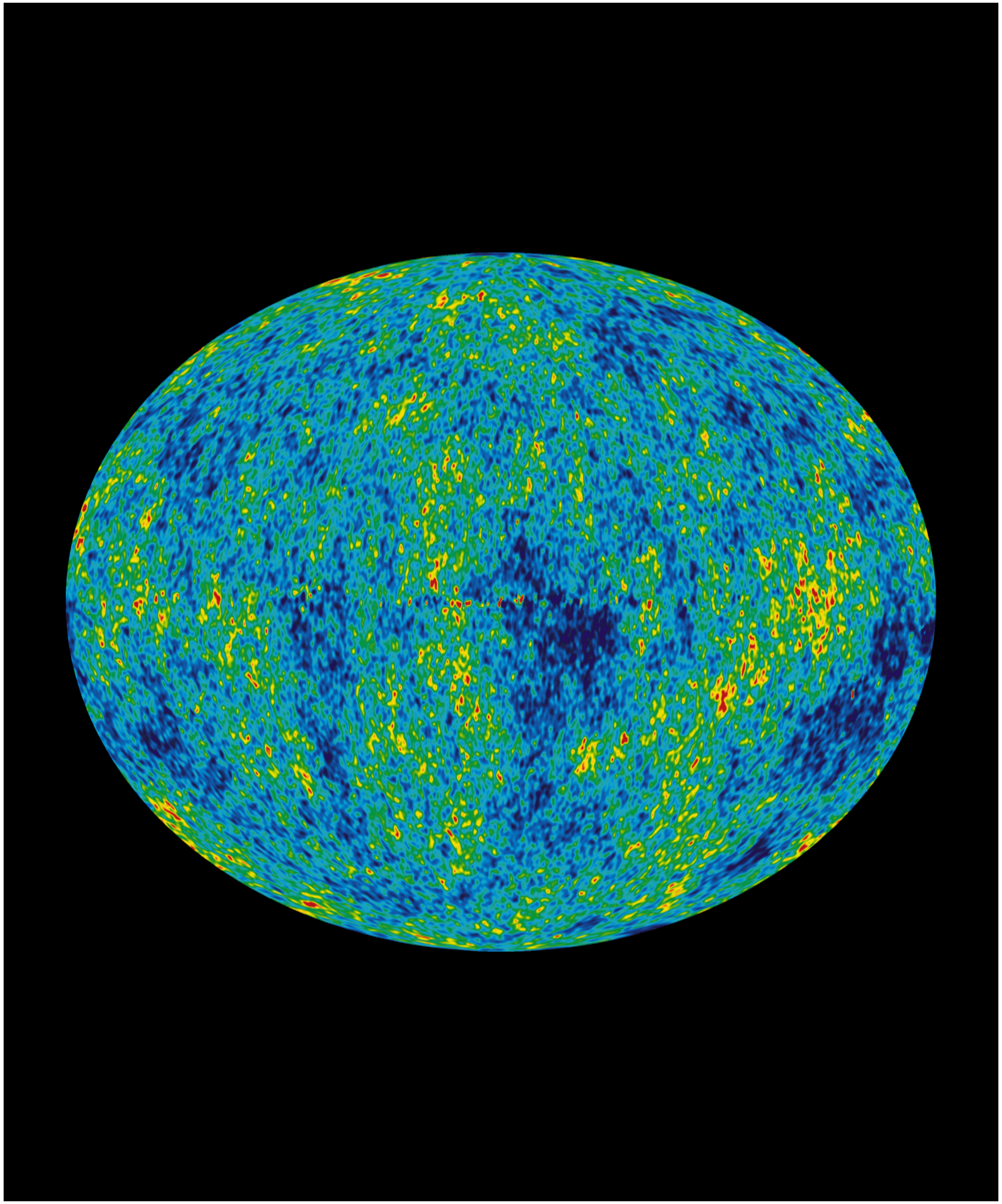
APNIC R&D



Radiation Detection



The Holmdel Horn Antenna, at Bell Labs, on which Penzias and Wilson discovered the cosmic microwave background radiation



The detailed, all-sky picture of the infant universe created from five years of WMAP data. The image reveals 13.7 billion year old temperature fluctuations (shown as color differences) that correspond to the seeds that grew to become the galaxies. The signal from the our Galaxy was subtracted using the multi-frequency data. This image shows a temperature range of ± 200 microKelvin.

Credit: NASA / WMAP Science Team

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, or an average of 1 packet every 3 seconds
  - 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 IPv4 network is 1.1.1.0/24. This prefix attracts some 100Mbps as a constant incoming traffic load

IPv4 vs IPv6

- Darknets in IPv4 have been the subject of numerous studies for many years
- What about IPv6?
  - Previous published findings on IPv6 Darknets
    - Matt Ford et al, 2006; "Initial Results from an Ipv6 Darknet", In Proceedings of International Conference on Internet Surveillance and Protection (ICISP'06)
      - advertised a "dark" /48 for 15 months at UK6x
      - received 12 packets, all ICMPv6
      - < 1ppm (packet per month!) per /48

Does IPv6 Glow in the Dark?

- The IPv4 address scanning approach does not work in IPv6
  - Much of the scanning traffic in IPv4 is seen to perform a +1 incremental “walk” of the IPv4 address space – this is infeasible in IPv6
- Random address selection will not work either
- Reverse walking DNS zones is feasible, but this will not result in traffic directed to dark nets unless the DNS itself includes pointers to dark nets
- So it does appear that IPv6 will not have much background dark traffic
  - Perhaps the 2006 finding of 1 ppm per /48 of dark IPv6 traffic is unexceptional

This Experiment

- Investigates what happens to the IPv6 dark traffic profile when we increase the size of the IPv6 Darknet
- This experiment used a /12 as the basis of the dark traffic measurement

2400::/12

Allocated to APNIC on 3 October 2006

Currently (April 2012) 2400::/12 has:

- 1468 address allocations, spanning a total of:
  - 28,809 /32's
  - 123,733,712,830,464 /64s
  - 2.75% of the total block
- 1,176 route advertisements, spanning a total of:
  - 13,383 /32's
  - 57,480,650,424,330 /64's
  - 1.28% of the /12 block

1.28% of the block is covered by existing more specific advertisements
1.47% of the block is unadvertised allocated address space
97.25% of the block is unadvertised and unallocated

Advertising 2400::/12

Advertised by AS7575 (AARNet)

Passive data collection (no responses generated by the measurement equipment)

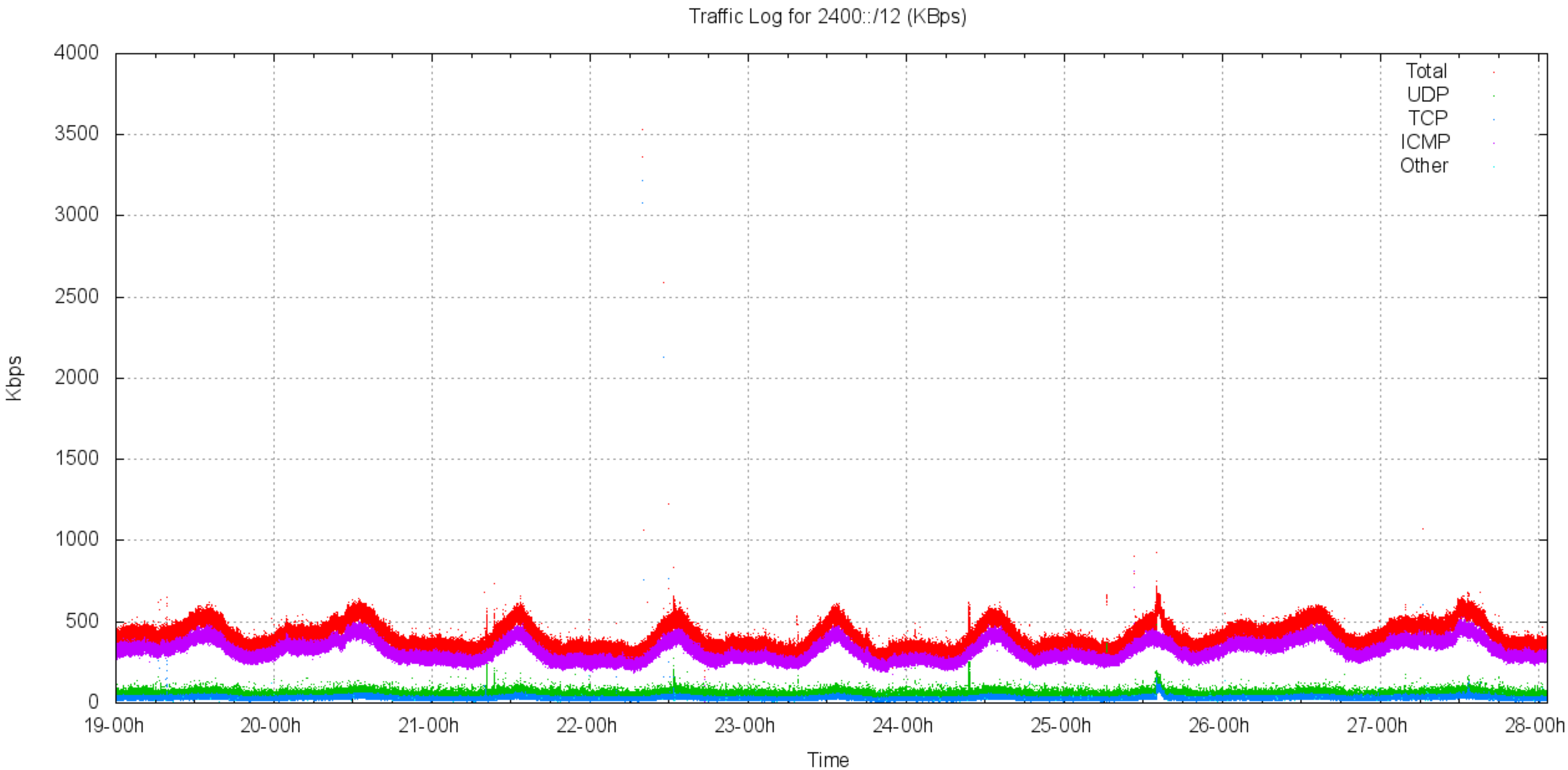
2 Darknet experiments performed (so far):

- 8 days: 19th June 2010 – 27th June 2010
- 107 days: 21st March 2011 – 6th July 2011

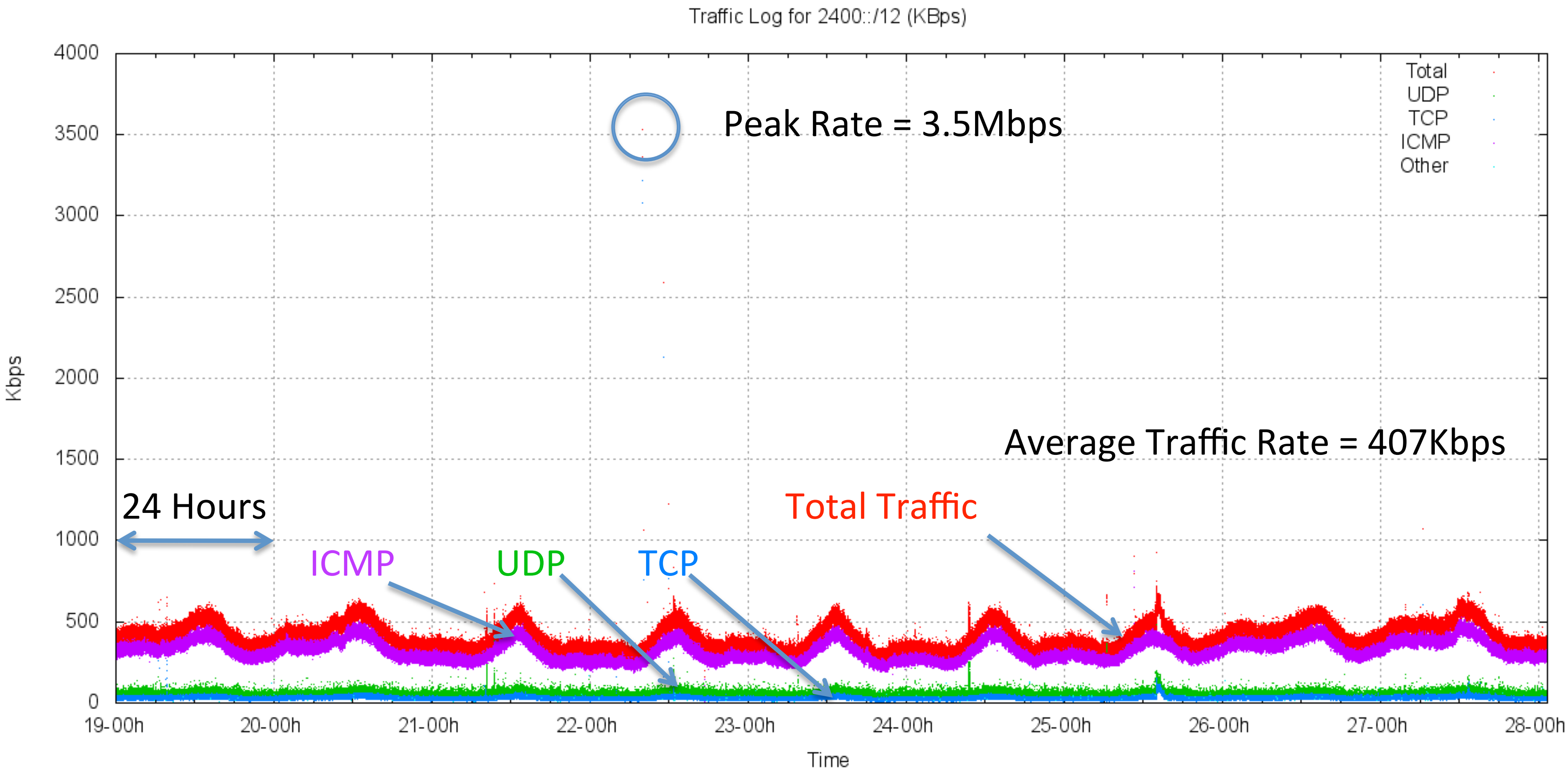
A third experiment, hosted by Sandia, underway

- started 25th April 2012

Traffic Profile 2010



Traffic Profile 2010



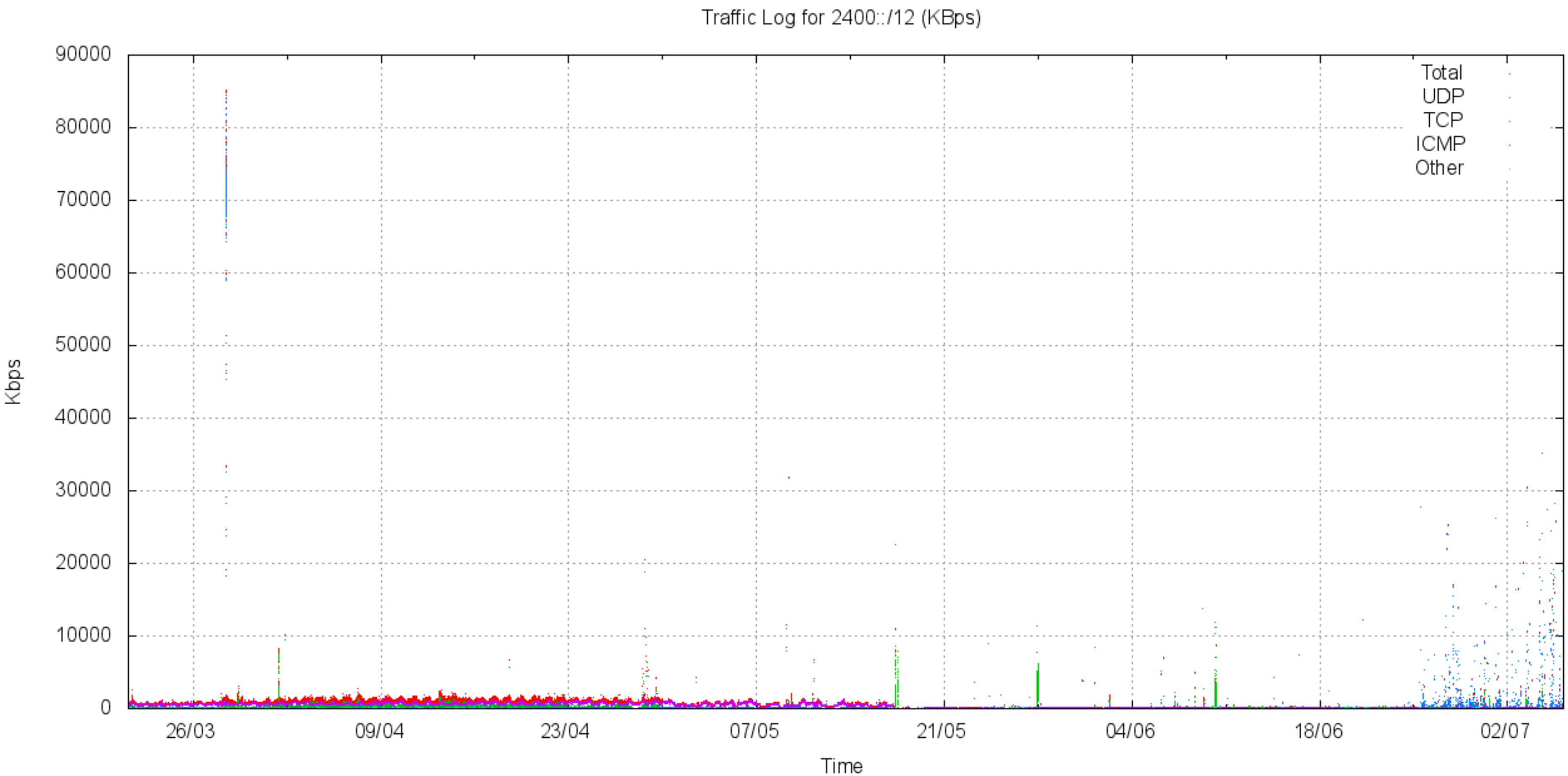
Traffic Profile 2010

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

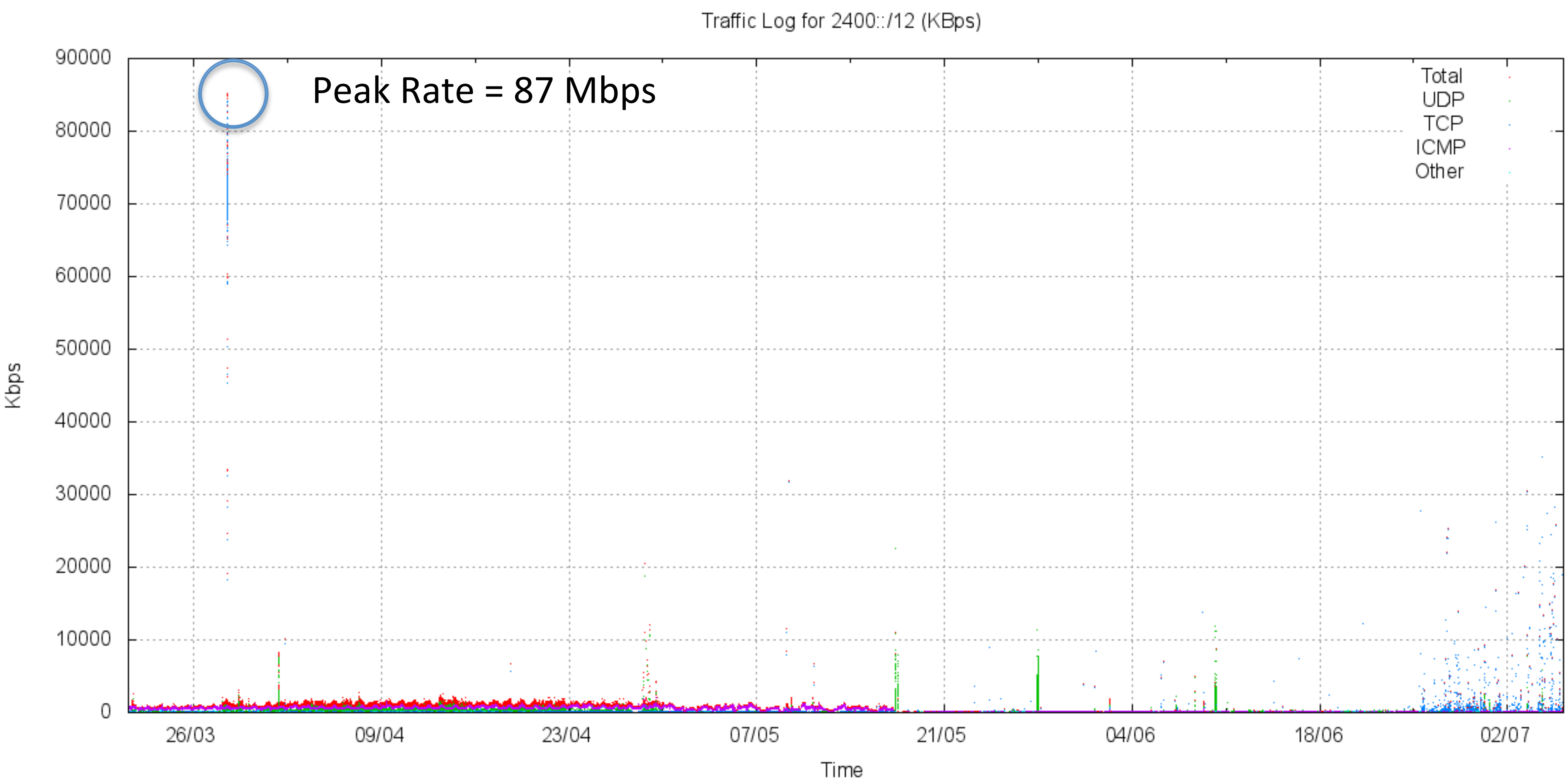
- ICMP: 323 Kbps (611 pps)
- UDP: 54 Kbps (68 pps)
- TCP: 30 Kbps (45 pps)

This is predominately ICMP traffic.

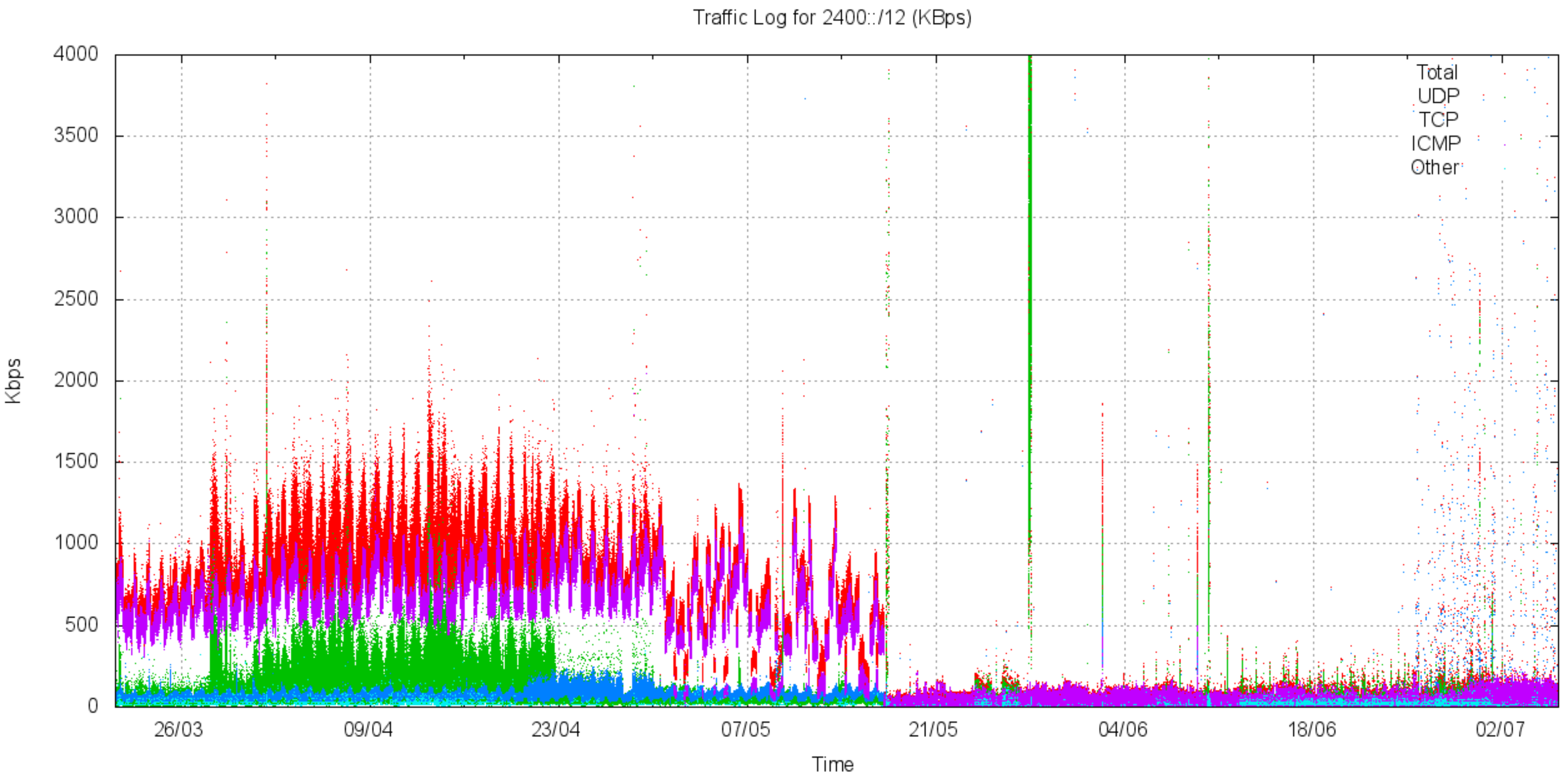
Total Traffic Profile 2011



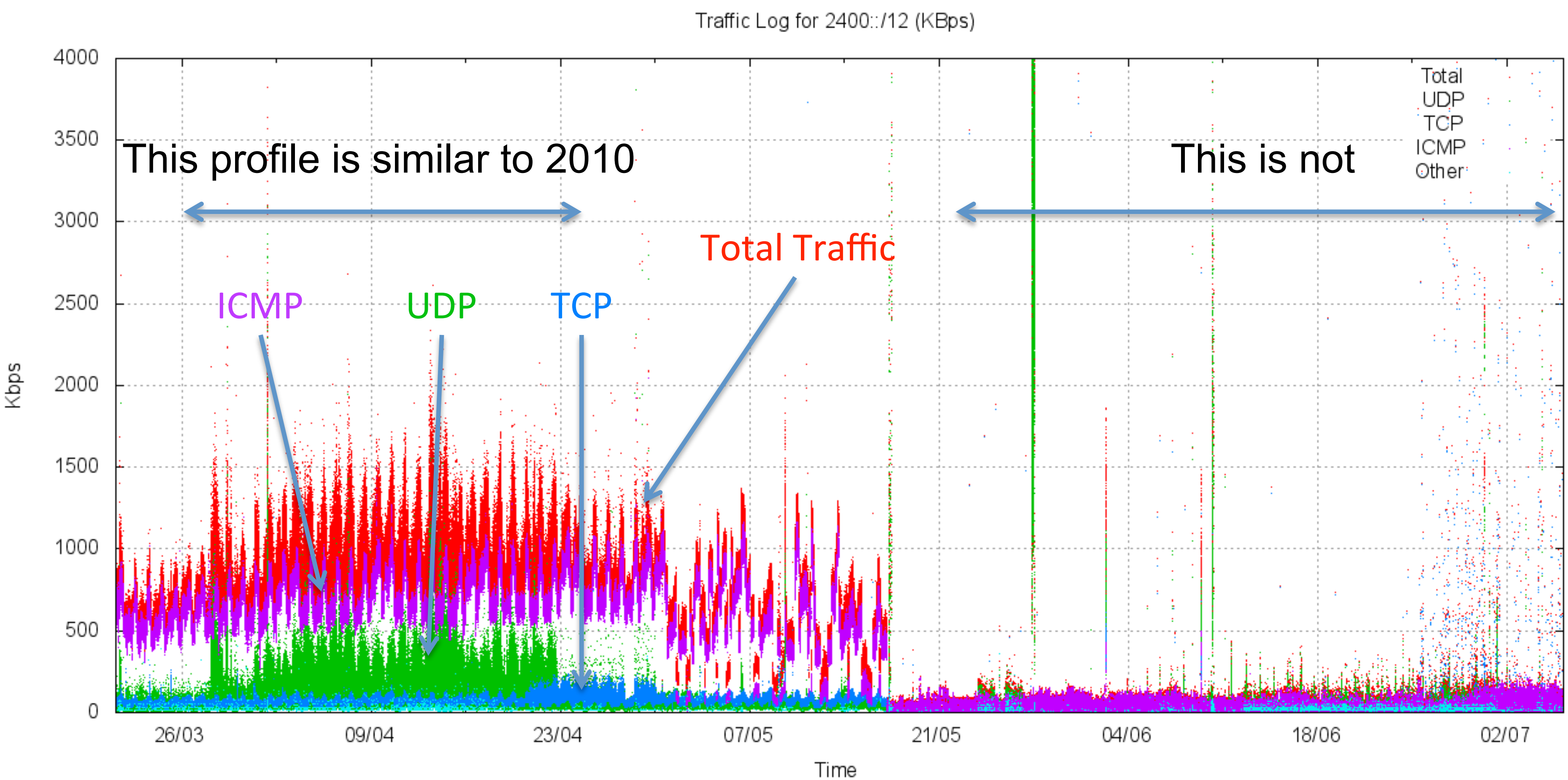
Total Traffic Profile 2011



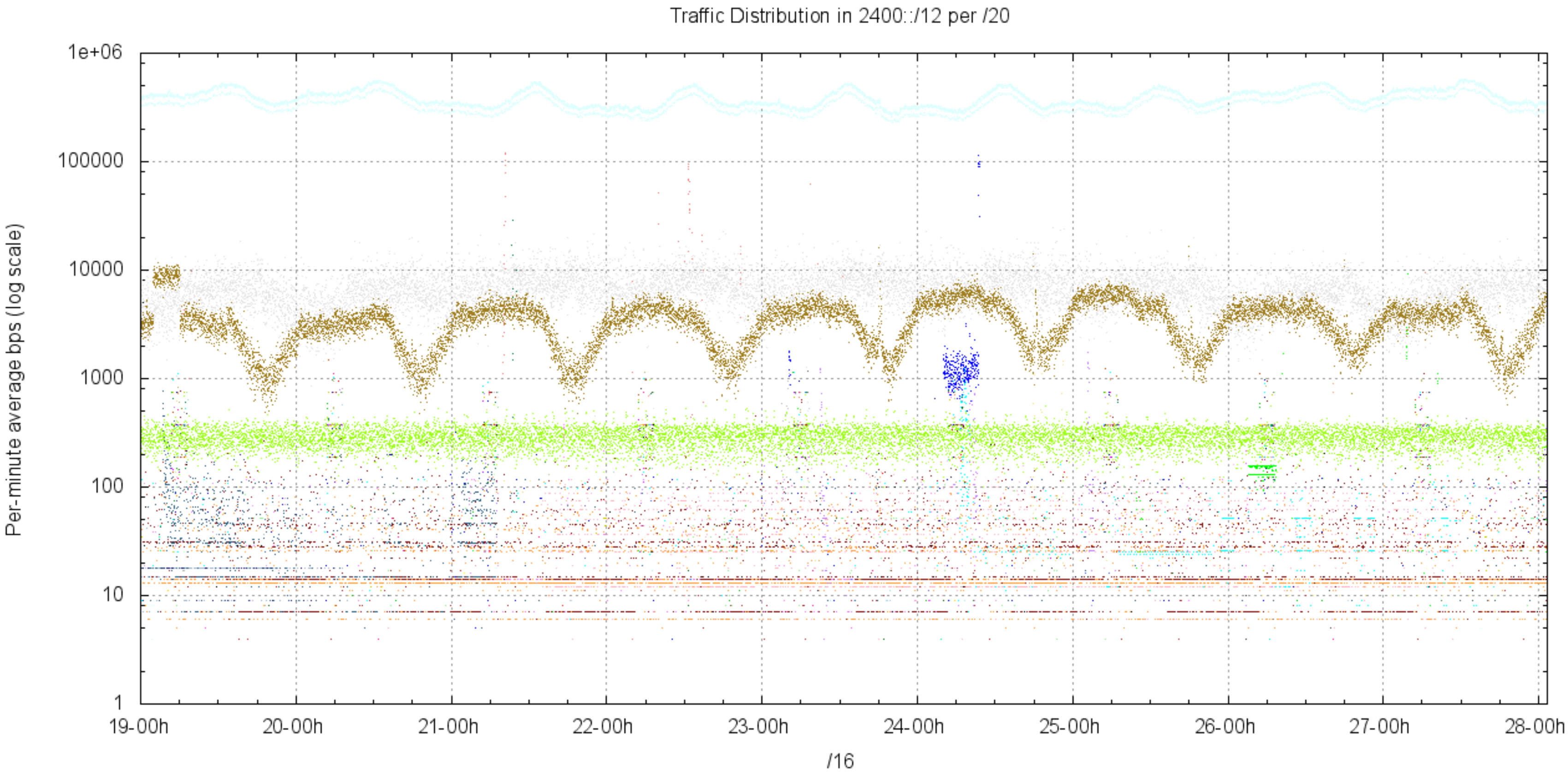
Total Traffic Profile 2011



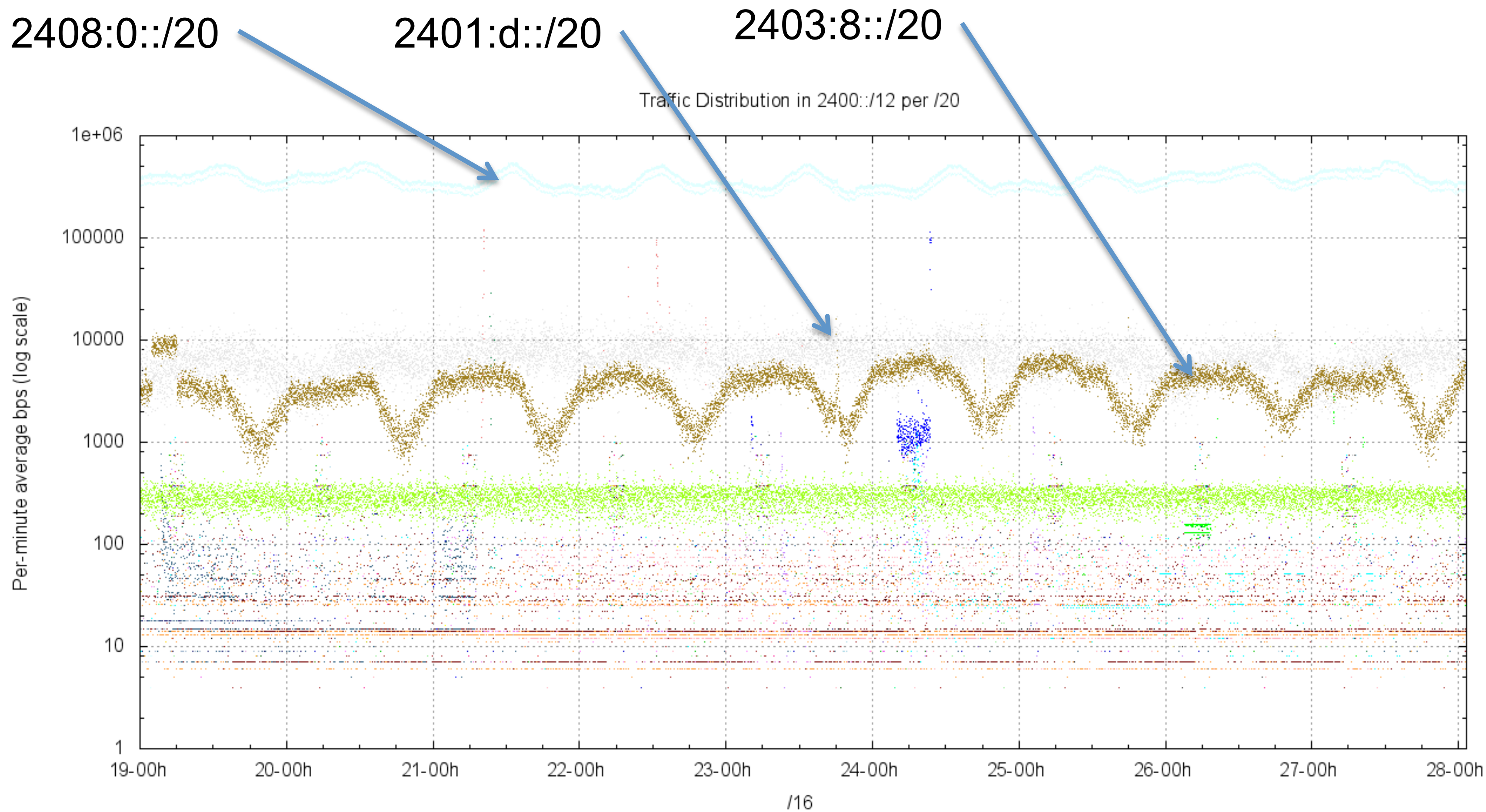
Total Traffic Profile 2011



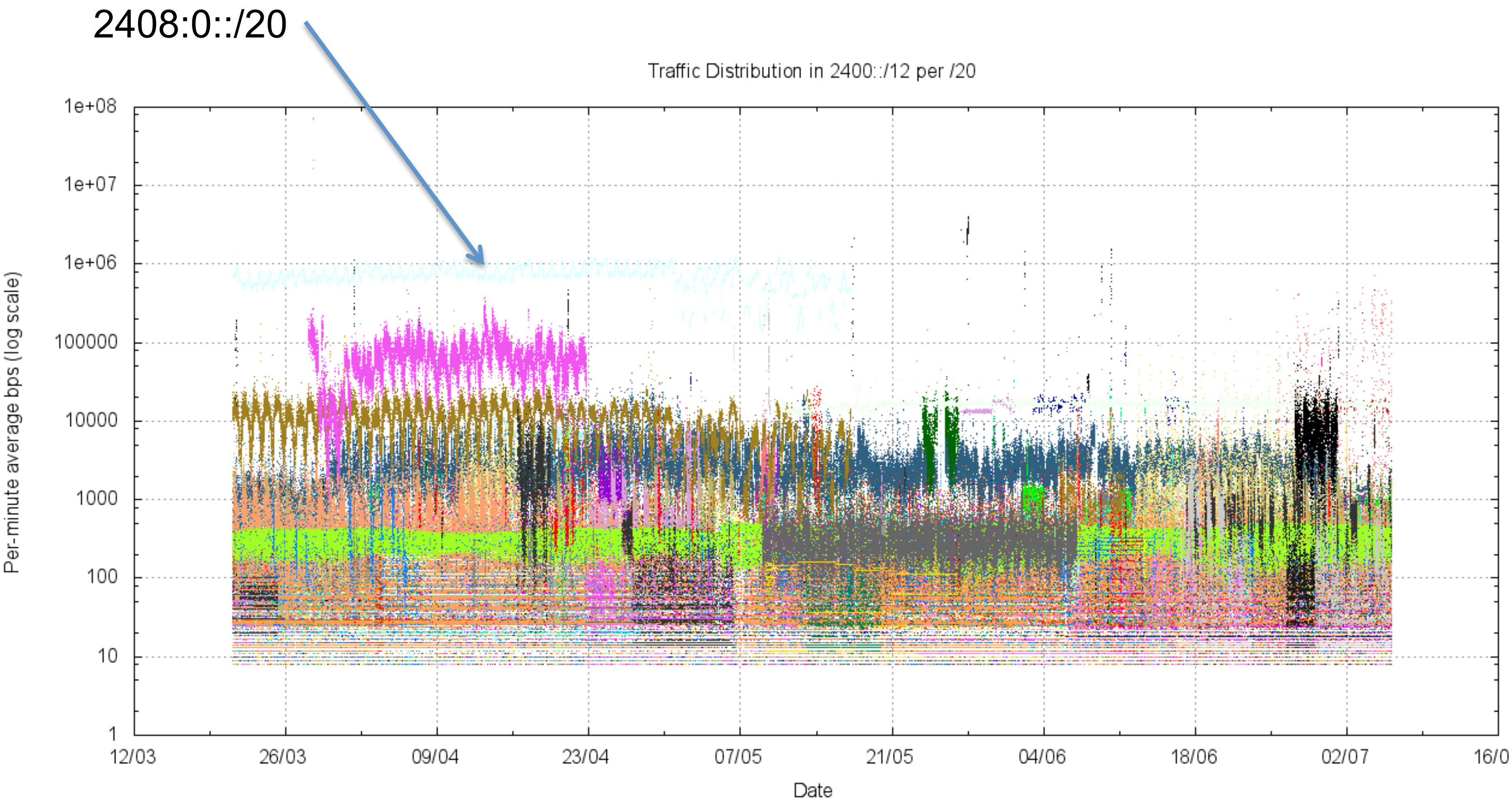
Destination Address Distribution 2010



Destination Address Distribution 2010



Destination Address Distribution 2011



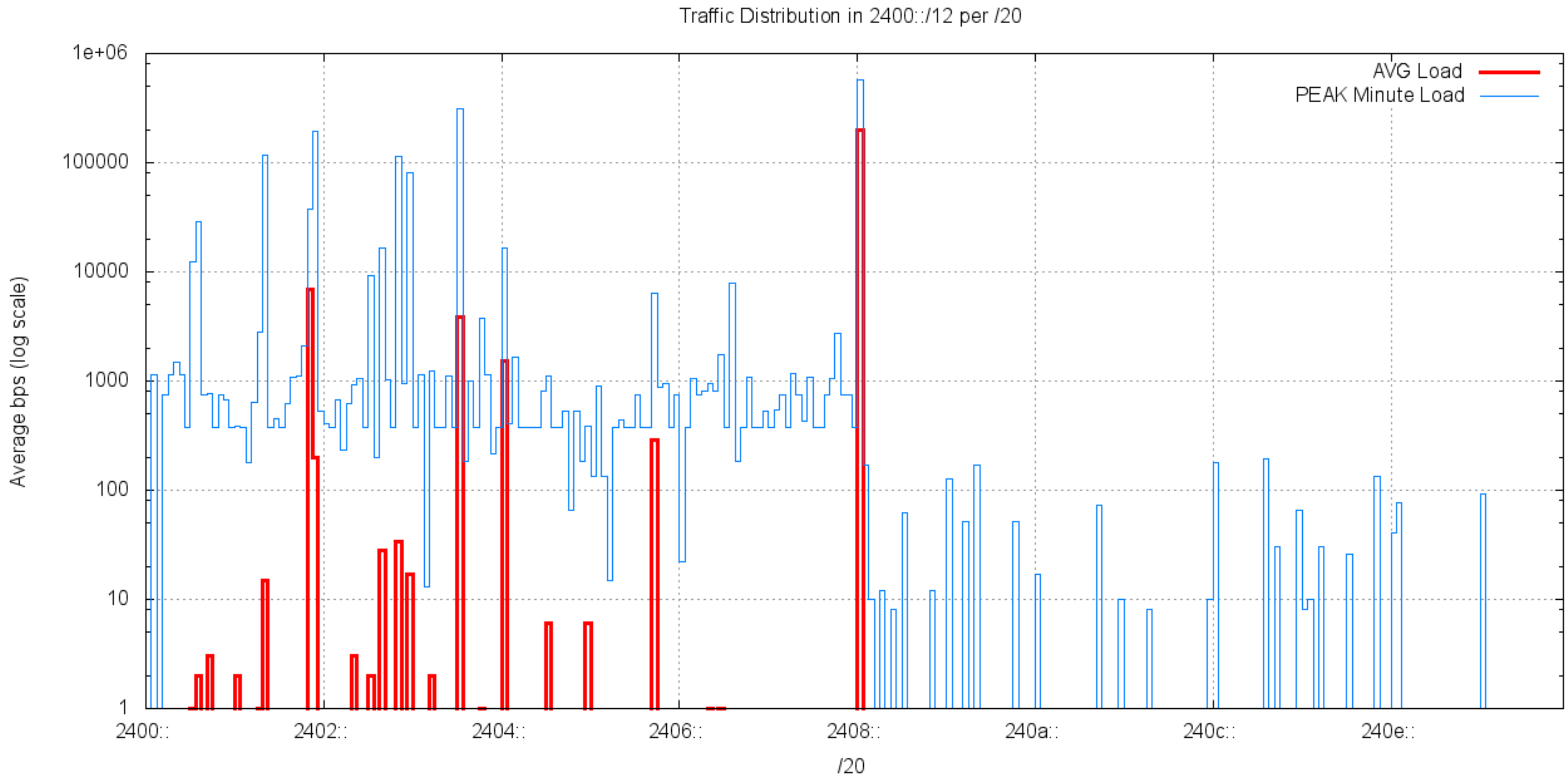
Top 5 /20s in 2400::/12 2010

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

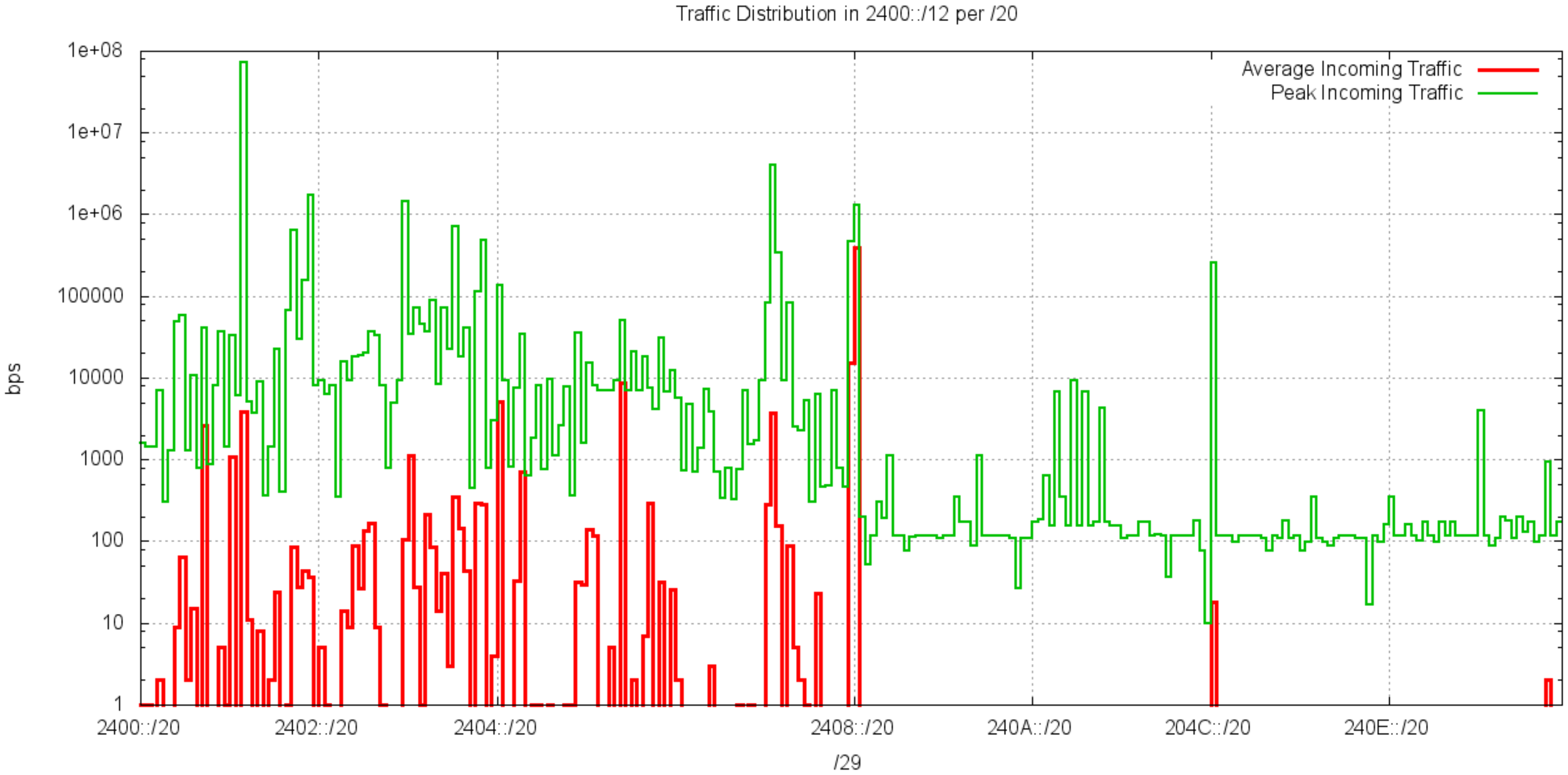
Top 5 /20s in 2400::/12 2011

2408:0000:/20	390Kbps	Allocated: 2408::/22 – NTT East, JP
2407:f000::/20	15Kbps	8 x /32 allocations in this block
2405:6000::/20	9Kbps	8 x /32 allocations in this block
2404:0000::/20	5Kbps	36 allocations in this block
2401:2000::/20	4Kbps	17 x /32 allocations in this block

Destination Address Distribution 2010



Destination Address Distribution 2011



What is this traffic?

Total Packets Captured in 2011: 6,267,034,487

ICMP : 87.89%

TCP: 7.92%

UDP: 4.19%

98.9% of TCP packets were SYN (connection attempt to dark address)

0.4% of TCP packets were SYN+ACK (connection attempt from dark address)

0.7% of TCP packets were TCP data (artificially constructed?)

ICMP

IP6 2001:0:4137:9e76:24ba:fba6:42f3:bce0 > 2408:f1:67a1:0:6967:db0:ca15:ceee: ICMP6, echo request, seq 18334, length 12
IP6 2001:0:4137:9e76:180f:1c01:36cb:2df5 > 2408:b2:a313:0:e041:4cdc:5422:d844: ICMP6, echo request, seq 46648, length 12
IP6 2001:0:5ef5:79fd:28fe:a74:a1d2:cbed > 2408:120:bfff:3e1:d9e4:6c95:211c:121c: ICMP6, echo request, seq 23896, length 12
IP6 2001:0:5ef5:73b8:1045:558:68e2:3432 > 2408:a2:451c:0:217:f2ff:fe02:3ecb: ICMP6, echo request, seq 29301, length 12
IP6 2001:0:5ef5:73b8:343c:2a87:a8c4:9683 > 2408:a6:4d7:0:ec7d:242e:a0bd:f218: ICMP6, echo request, seq 12222, length 12
IP6 2001:0:5ef5:79fd:146e:194a:a78e:ef35 > 2408:82:7fff:554:3e:5c18:a382:614b: ICMP6, echo request, seq 60584, length 12
IP6 2001:0:4137:9e76:cfc:2504:4367:4010 > 2408:27:de:0:80b9:7ed5:66db:4029: ICMP6, echo request, seq 23756, length 12
IP6 2001:0:4137:9e76:2817:11e1:42e1:4422 > 2408:157:3f1:0:198b:9612:572b:6cc: ICMP6, echo request, seq 64546, length 12
IP6 2001:0:4137:9e76:24ad:37e7:8423:3161 > 2408:e2:e39a:0:44a1:8d65:8c05:1005: ICMP6, echo request, seq 29296, length 12
IP6 2001:0:4137:9e76:883:142f:a061:ff0c > 2408:1aa:133:0:40fc:2a73:3fcd:91c3: ICMP6, echo request, seq 58691, length 12
IP6 2001:0:5ef5:79fd:18d9:1a5c:3d81:4bfa > 2408:26:1fff:c24:5c8e:f7d1:5e97:4804: ICMP6, echo request, seq 47237, length 12
IP6 2001:0:4137:9e76:246e:1036:2d38:86a8 > 2408:181:1fff:df:c1e0:3a9b:81f8:f5e9: ICMP6, echo request, seq 53782, length 12
IP6 2001:0:4137:9e76:c61:1d33:81e4:f1dc > 2408:f2:700:0:48db:99cd:9852:9cc0: ICMP6, echo request, seq 10304, length 12

What we appear to be seeing here is Teredo connection attempts, predominately to hosts located in the JP NTT IPv6 network.

The JP NTT IPv6 network is a closed private network, whose edges are configured to return RSTs to outgoing SYN attempts. Until June 18 2011 this network block was unadvertised, so the 2400::/12 collector collected all the backscatter from this network.

However the internal IPv6 addresses leak out (via DHTs?) and others attempt to connect to these hosts' IPv6 addresses using Teredo

Private Addresses in IPv6

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

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

- In IPv6 its conventional to use public IPv6 addresses in private contexts

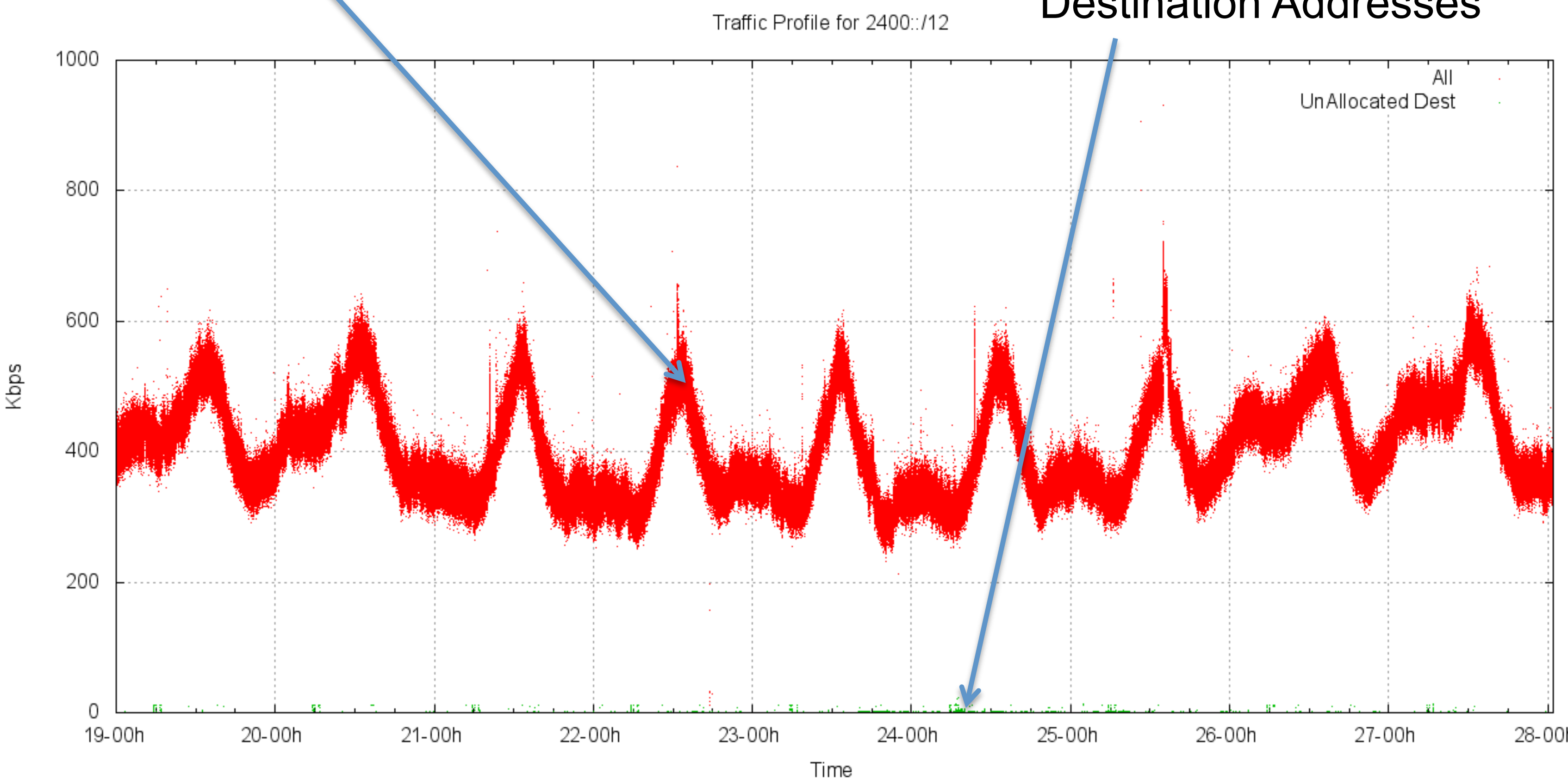
- **How much of this "dark" IPv6 traffic is a result of "leakage" from private contexts into the public network?**

- Lets filter the packets using the allocation data

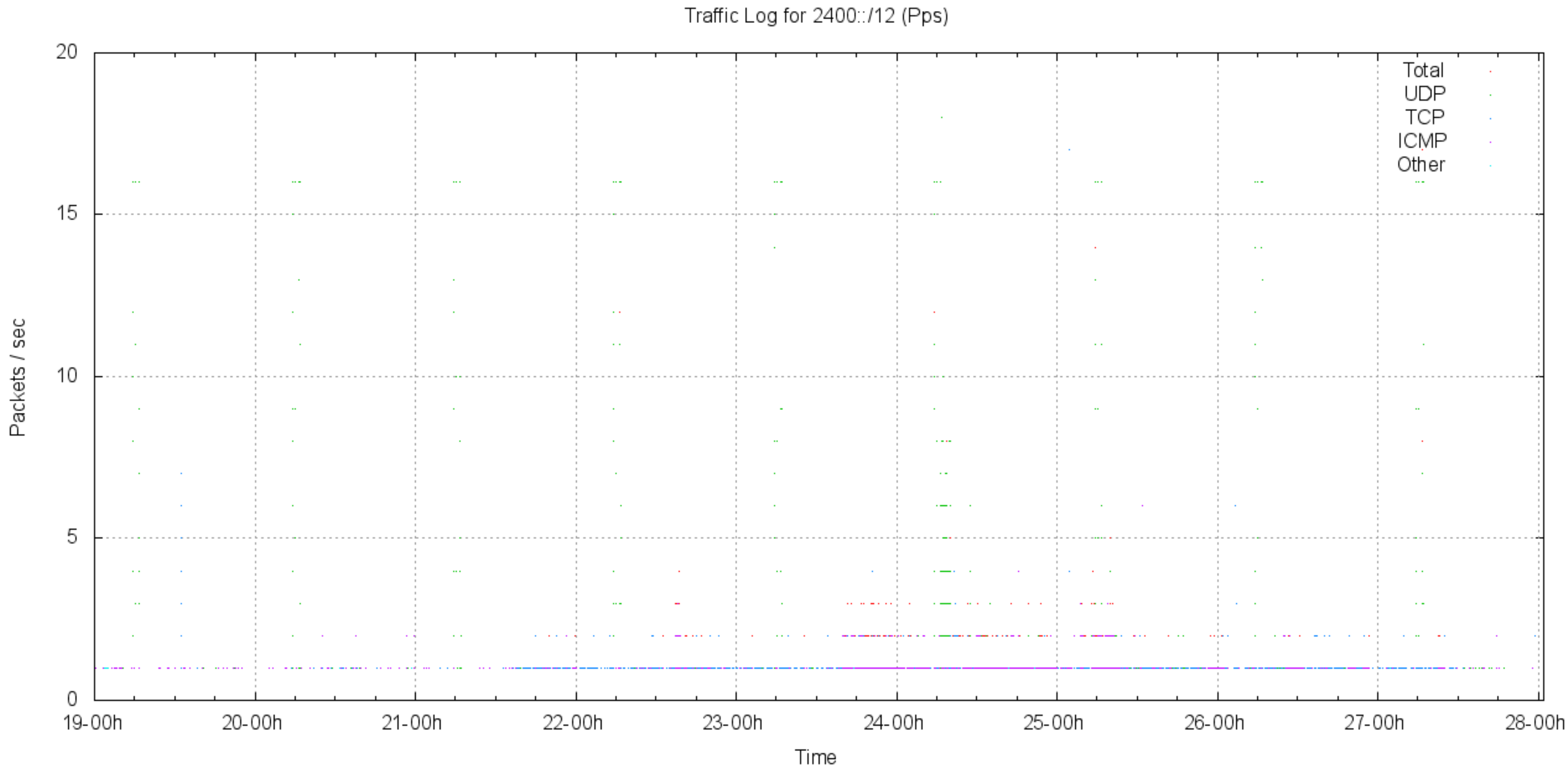
Allocated vs Unallocated Dark Traffic - 2010

All “dark” IPv6 traffic

“dark” traffic to Unallocated Destination Addresses

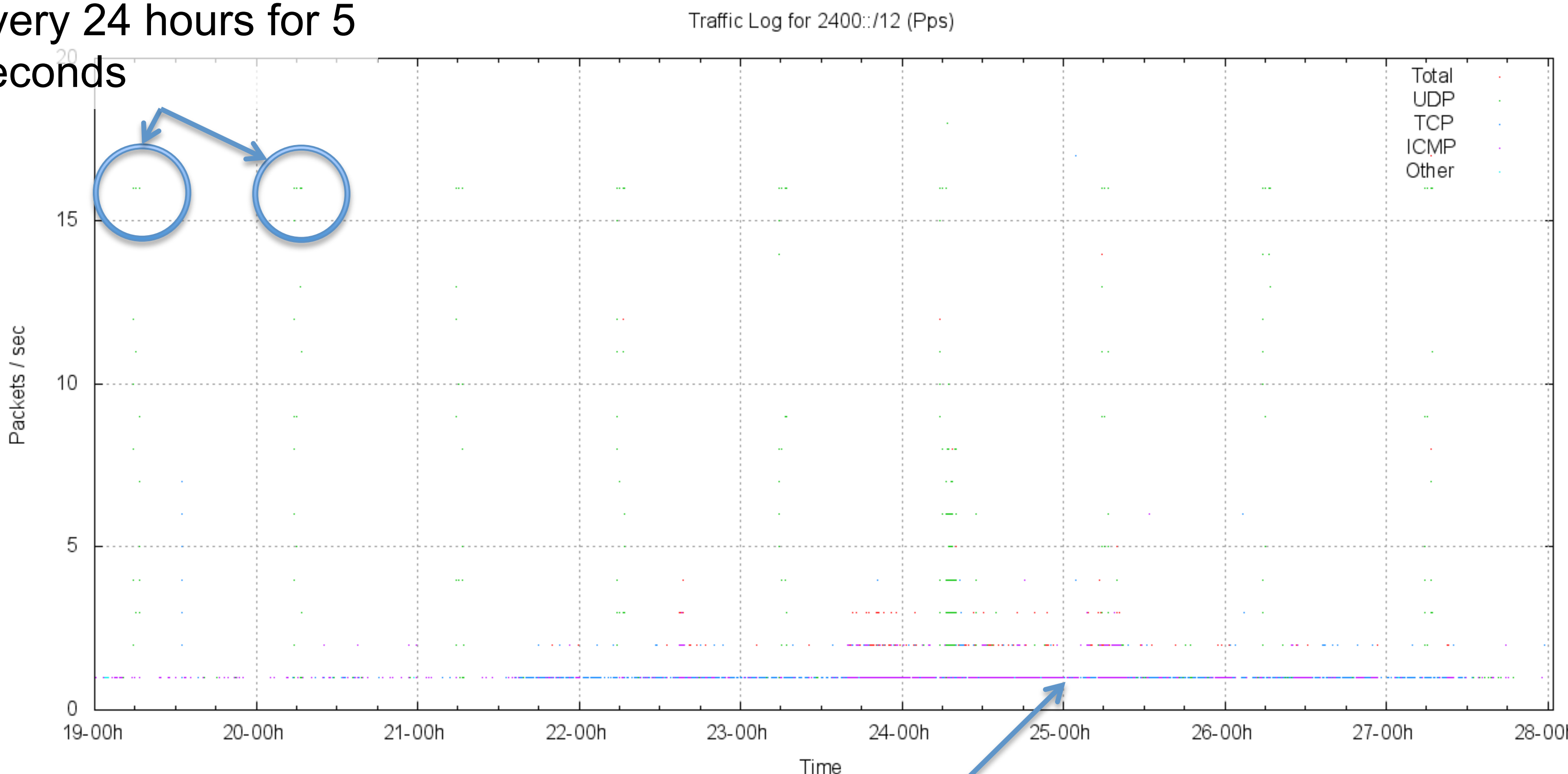


Dark Traffic to Dark Addresses 2010



Dark Traffic to Dark Addresses 2010

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



less than 1 packet per second of ICMP

Dark Traffic Profile

Traffic directed to unallocated IPv6 addresses:

- Collection period: 9 days
- Average Packet Rate: 1 packet per 36.8 seconds
- Packet Count: 21,166
  - ICMP: 7881 (37%)
  - TCP: 7660 (36%)
  - UDP: 5609 (26%)

TCP Profile

SYN packets: (wrong destination, DNS typos?)

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!)

This leakage may have been tickled by this experiment – HE normally filter unallocated address space and the 2400::/12 advertisement would've been blocked by HE

UDP Traceroute6

```
16:42:15.769564 IP6 (hlim 1) 2001:470:9:babe::3.48038 > 2405:a800::1.33464: UDP, length 32
16:42:15.770189 IP6 (hlim 1) 2001:470:9:babe::3.40743 > 2405:a800::1.33465: UDP, length 32
16:42:15.921349 IP6 (hlim 1) 2001:470:9:babe::3.34520 > 2405:a800::1.33466: UDP, length 32
16:42:15.921849 IP6 (hlim 2) 2001:470:9:babe::3.44740 > 2405:a800::1.33467: UDP, length 32
16:42:15.989684 IP6 (hlim 2) 2001:470:9:babe::3.42310 > 2405:a800::1.33468: UDP, length 32
16:42:15.995430 IP6 (hlim 2) 2001:470:9:babe::3.52710 > 2405:a800::1.33469: UDP, length 32
16:42:15.996180 IP6 (hlim 3) 2001:470:9:babe::3.51306 > 2405:a800::1.33470: UDP, length 32
16:42:16.000302 IP6 (hlim 3) 2001:470:9:babe::3.55161 > 2405:a800::1.33471: UDP, length 32
16:42:16.000803 IP6 (hlim 3) 2001:470:9:babe::3.55674 > 2405:a800::1.33472: UDP, length 32

…
```

Source: 2001:470:9:babe::3, testing a path to 2405:a800::1, using UDP ports 33464 through to 33493 in sequence with increasing IPv6 hop limits

Total of 1,883 packets were seen between these two hosts!

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.

DNS Oddities

```
11:01:21.259288 IP6 2001:468:1802:102::805b:fe01 53 > 2407:ed24::113:23:133:101 40288  97.229.175.128.in-addr.arpa. PTR roaming-229-97.nss.udel.
22:50:24.316093 IP6 2607:f470:1003::3:3          53 > 2407:bde7::113:23:133:101 16554  noc3.dccs.upenn.edu. A 128.91.251.158, noc3.dccs.upenn.ed
00:59:40.623590 IP6 2001:468:1802:102::805b:fe01 53 > 2407:df5c::113:23:133:101 47237  knowledge.wharton.upenn.edu. A 128.91.87.103, knowledge.w
06:37:59.021141 IP6 2607:f470:1003::3:3          53 > 2407:cd0d::113:23:133:101 44097: 94.80.91.130.in-addr.arpa. PTR masca7.museum.upenn.edu.
06:55:21.099014 IP6 2001:468:1802:102::805b:fe01 53 > 2407:29ca::113:23:133:101 47145: dns2.udel.edu. A 128.175.13.17
04:53:08.631077 IP6 2001:468:1802:102::805b:fe01 53 > 2407:f0e1::113:23:133:101 29201: noc3.dccs.upenn.edu. A 128.91.251.158, noc3.dccs.upenn.ed
20:04:03.879610 IP6 2001:468:1802:102::805b:fe01 53 > 2407:72c4::113:23:133:101 53336: 58.140.175.128.in-addr.arpa. PTR mbna58.be.udel.edu.
22:55:02.029732 IP6 2607:f470:1003::3:3          53 > 2407:6a85::113:23:133:101 40444: noc2.dccs.upenn.edu. A 128.91.254.1, noc2.dccs.upenn.edu.
```

This looks like some form of backscatter from source address spoofing.

What's Left in dark UDP?

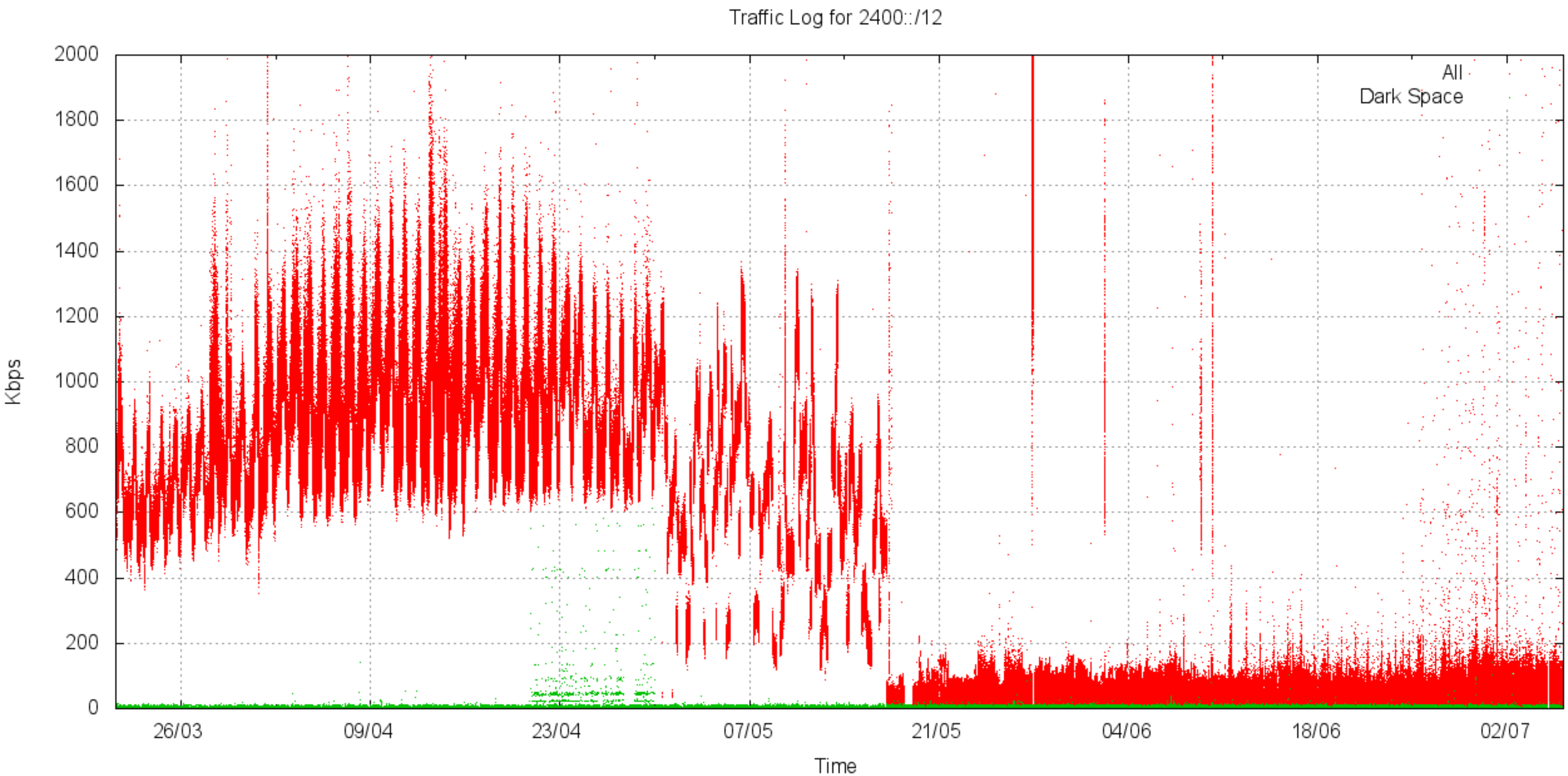
803 packets from 68 distinct sources, 45 of which are 6to4 source addresses

A lot of this looks like leakage from private contexts

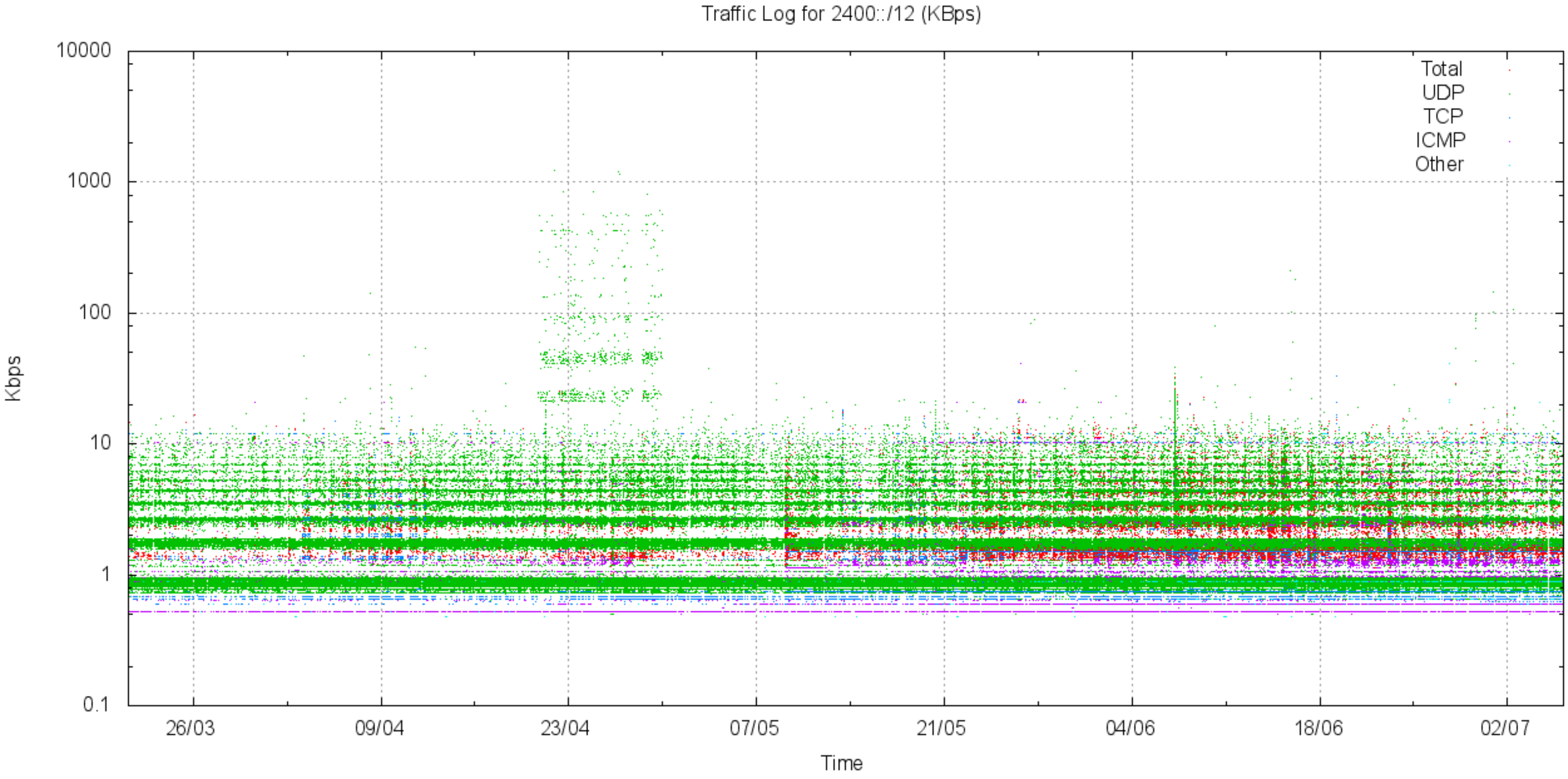
Dark ICMP

- echo request packets (ping) – 7,802 packets
- 93 others – destination unreachables, and malformed packet headers

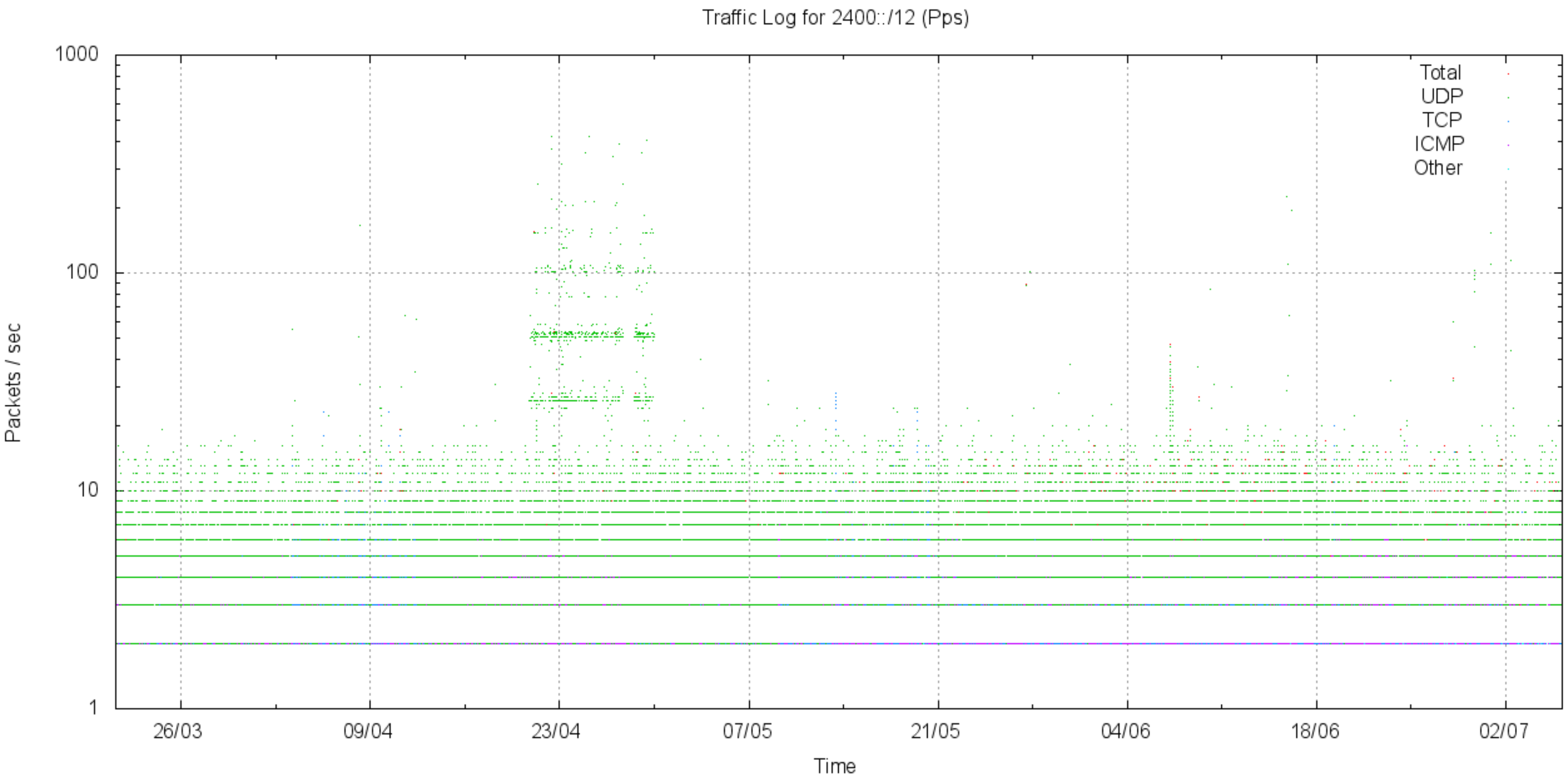
>> to 2011 – All vs Dark



2011 – Dark Space



2011 – Dark Space – Packets/Sec



Traffic Profile

Traffic directed to unallocated IPv6 addresses:

- Collection period: 107 days
- Average Packet Rate: 1 packet per 4.9 seconds
- Packet Count: 1,850,318
  - ICMP: 111,959 (6%)
  - TCP: 310,319 (17%)
  - UDP: 1,423,116 (77%)

TCP

SYN: 96% (297,063 packets) – attempting to connect to a dark address

804 unique destinations

- 96 destinations using port 25
- 139 destinations using port 80
- 16 destinations using port 443

SYN+ACK: 3% (9,724 packets) – attempting to connect from a dark address

53 unique destinations

72 unique sources

- 37 sources were on port 80
- 4 sources were on port 443
- 1 source on port 53

DATA: 1% (3,337 packets) – ?

2,272 with length 0 (ACK)

- 1413 unique sources
- 1528 unique desatinations

UDP

DNS queries: 1,386,648

310 unique destinations

DNS responses: 6,057

8 unique sources

Other UDP packets: 22,604

from just 986 unique source addresses

of which just 561 are non-6to4!

most of which are sequences of ascending destination port numbers – UDP traceroute

ICMP

TEREDO Connect ICMP: 72% (81,125)

ICMP6 Destination Unreachable: 7.5% (8,367)

ICMP6 time exceeded: 1% (1,052)

ICMP6 ping (echo req): 18% (20,720)

- 82 unique sources
- 1,101 unique destinations

My Award for the most broken IPv6 packet I've seen so far!

IP6 2001:67c:104:120a::81:1 > 2406:1e33:dead:145a:250:56ff:feaa:714a: ICMP6, destination unreachable[|icmp6]

Let's see what this means:

2406:1e33:dead:145a:250:56ff:feaa:714a is sending a packet to an unreachable address

2001:67c:104:120a::81:1 is saying back: you can't get there from here

but 2001:67c:104:120a::81:1 is also a dark (unallocated address)

So its a dark router telling a dark host that it is sending a packet to a dark destination!

And there were another 1063 packets just like this!

IPv6 Radiation - Malign or Benign?

- What happens in IPv4 malware does not translate into IPv6 .
- The nature of IPv6 is such that address scanning as a means of virus propagation is highly impractical
  - We may have seen some small number of guessing probes directed at ::1 and ::2 source addresses, but nothing else
- Walking the DNS for pointers to viable IPv6 addresses should be expected
  - but we did not see any of that form of behaviour in our data
- We've found no visible evidence of virus scanners attempting to probe into private use and dark address blocks in IPv6 – yet!

IPv6 Leaks

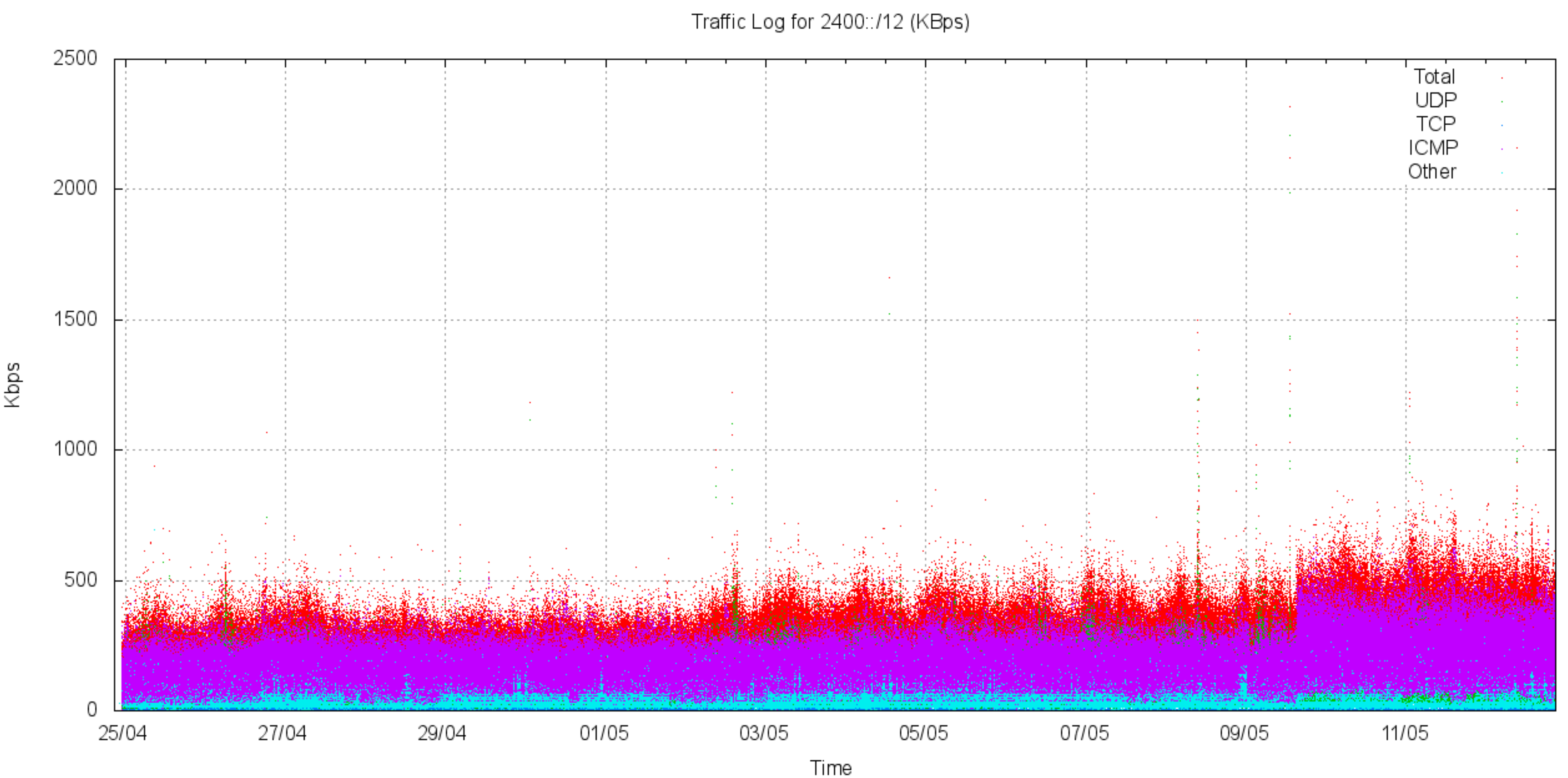
- There is no counterpart to RFC1918 private space
- Most of the traffic in the dark space is leakage from private use contexts
  – There is a message here to all “private” networks: they really aren’t necessarily all that private!

IPv6:: Misconfiguration Rules!

There are increasing levels of dark IPv6 traffic that appears to be a result of poor transcription of IPv6 addresses into system configs and into DNS zone files

- And for the moment the dual stack environment masks this because of auto-failback to IPv4

2012 - first results



2012 Profile

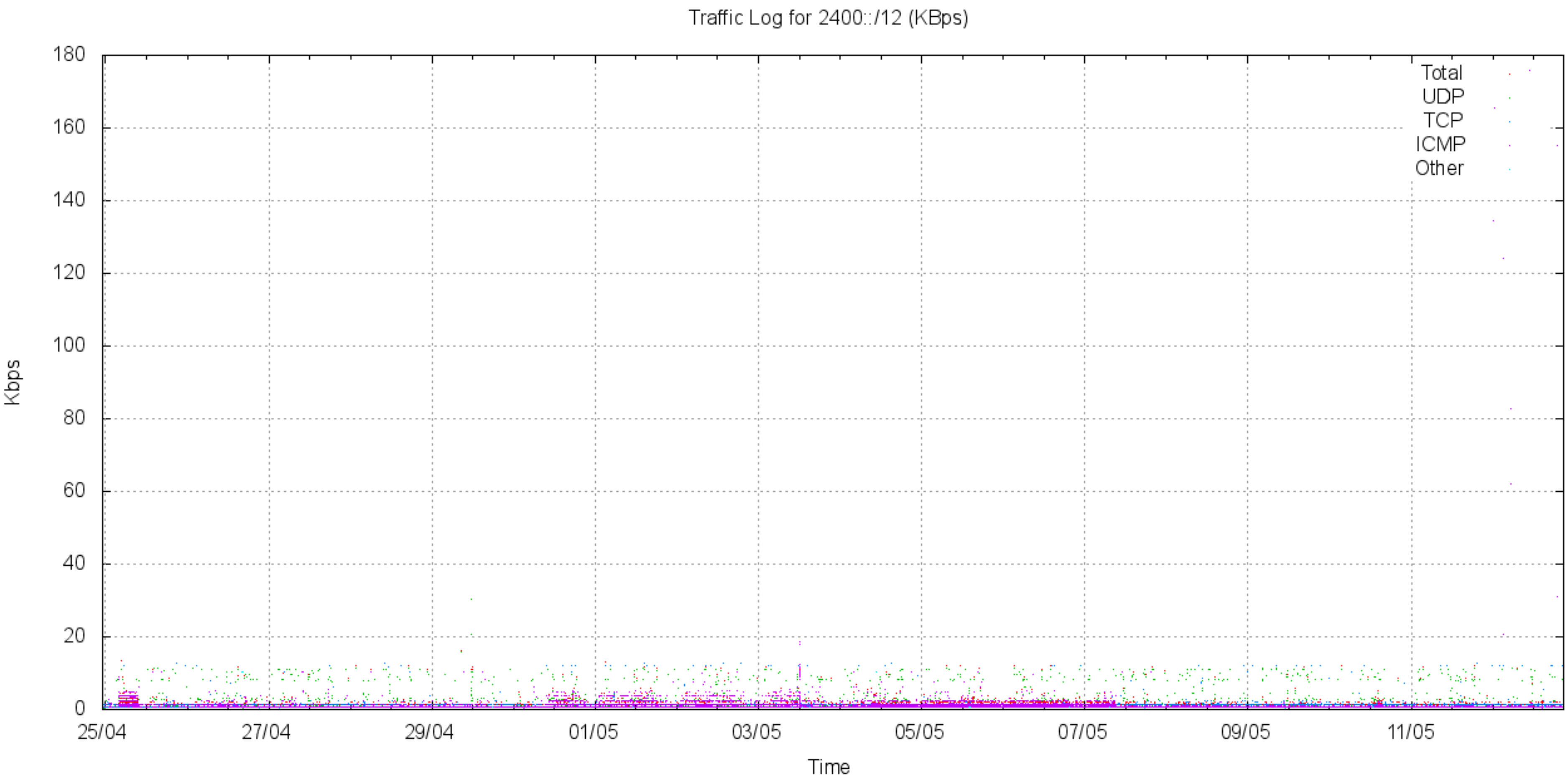
Rank	ICMP		TCP				UDP			
	Type	Count	Source	Count	Dest	%	Source	Count	Dest	Count
0	128	51,125,688	80	298,631	80	656,502	53	36,727,642	53	8,977,046
1	129	20,574,495	53	293,522	179	656,302	44000	24,794	32769	6,428,615
2	1	914,858	443	30,185	443	631,490	500	17,335	54053	6,182,605
3	3	308,772	6667	13,832	6697	207,246	39246	13,949	53700	4,412,492
REST		454		2,901,603		1,386,233		9,350,390		20,133,352
		72,924,267		3,537,773		3,537,773		46,134,110		46,134,110

128 -> Echo Request
129 -> Echo Reply
1 -> Dest Unreachable
3 -> TTL Exceeded

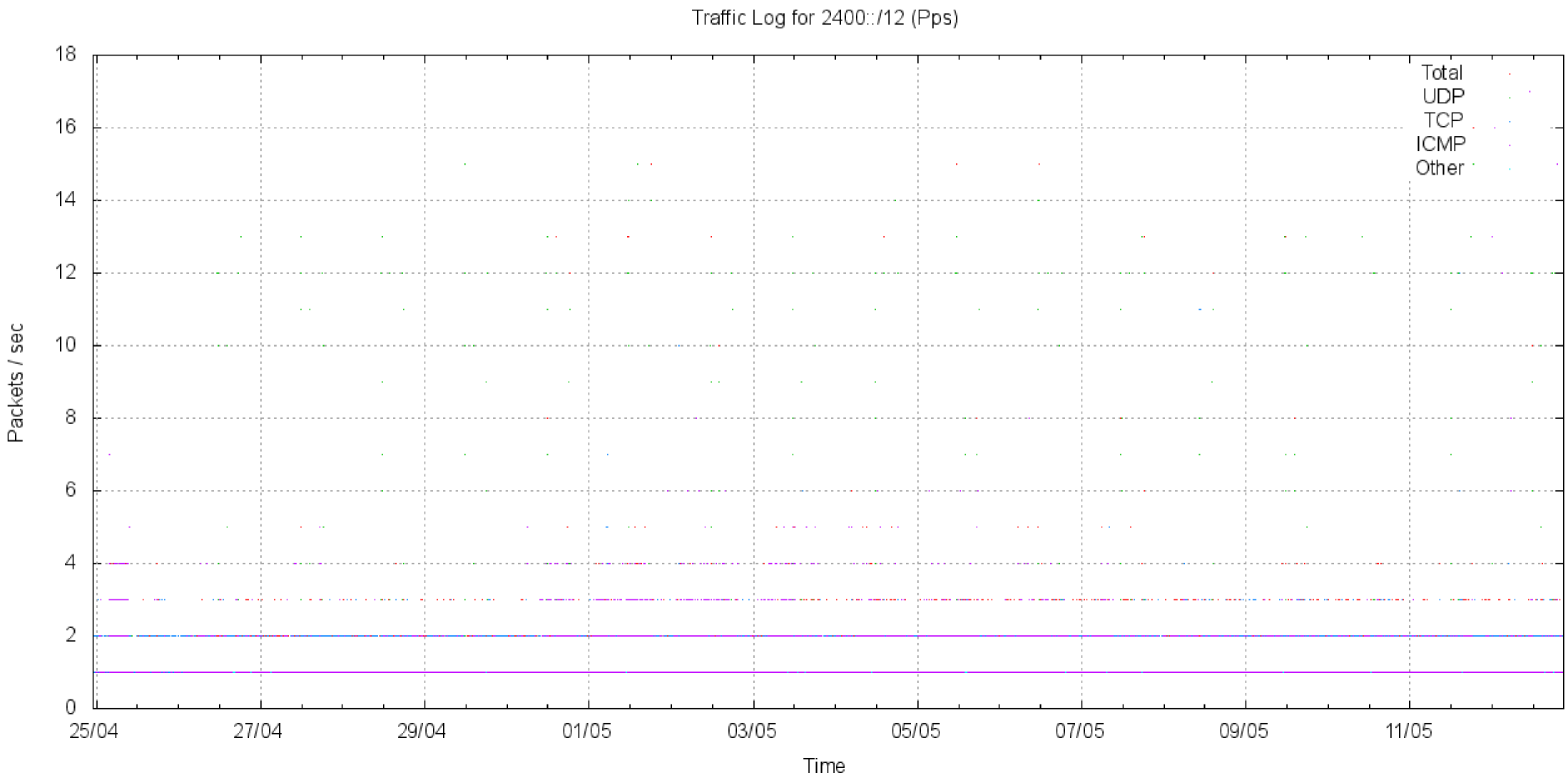
80 -> HTTP
53 -> DNS
179 -> BGP
443 -> HTTPS

53 -> DNS
500-> iSAKMP

2012 - filtered dark



2012 - filtered dark



2012 Profile - filtered dark

Rank	ICMP Type	Count	TCP Source	Count	Dest	Count	UDP Source	Count	Dest	Count
0	128	61479	80	42	80	126368	53	629	53	458
1	1	15022	34676	36	443	293	63000	186	33483	116
2	129	1282	53439	34	30965	132	35691	46	33487	116
3	3	252	47342	30	59280	100	32100	23	33488	116
REST		226		130723		3972		3118		3196
		78,261		130,865		130,865		4,002		4,002

128 -> Echo Request
129 -> Echo Reply
1 -> Dest Unreachable
3 -> TTL Exceeded

80 -> HTTP
443 -> HTTPS

53 -> DNS

Thank You

Questions?