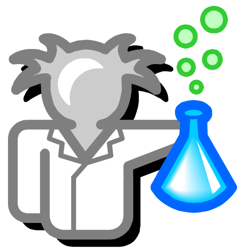
IPv6 Background Radiation

Geoff Huston

APNIC R&D



IPv4 Background Radiation

- We understand that the IPv4 address space is now heavily polluted with toxic background traffic
  - Most of this traffic is directly attributable to infected hosts performing address and port scanning over the entire IPv4 address range
  - Average background traffic level in IPv4 is ~5.5Gbps across the Internet, or around 300 – 600 bps per /24, or an average of 1 packet every 2 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?
- Does IPv6 glow in the dark with toxic radiation yet?

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

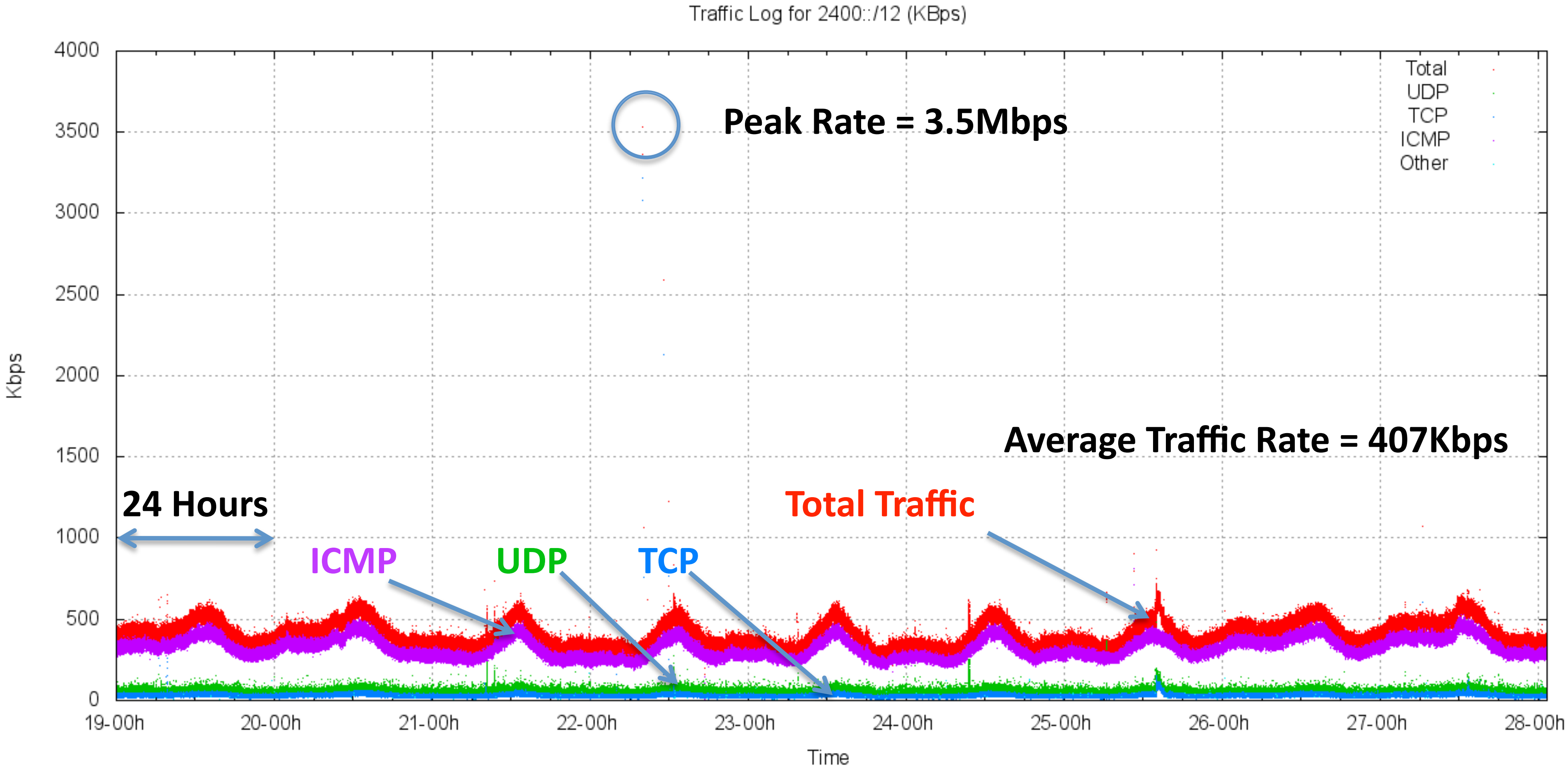
98.41% of the block is unadvertised and unallocated

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



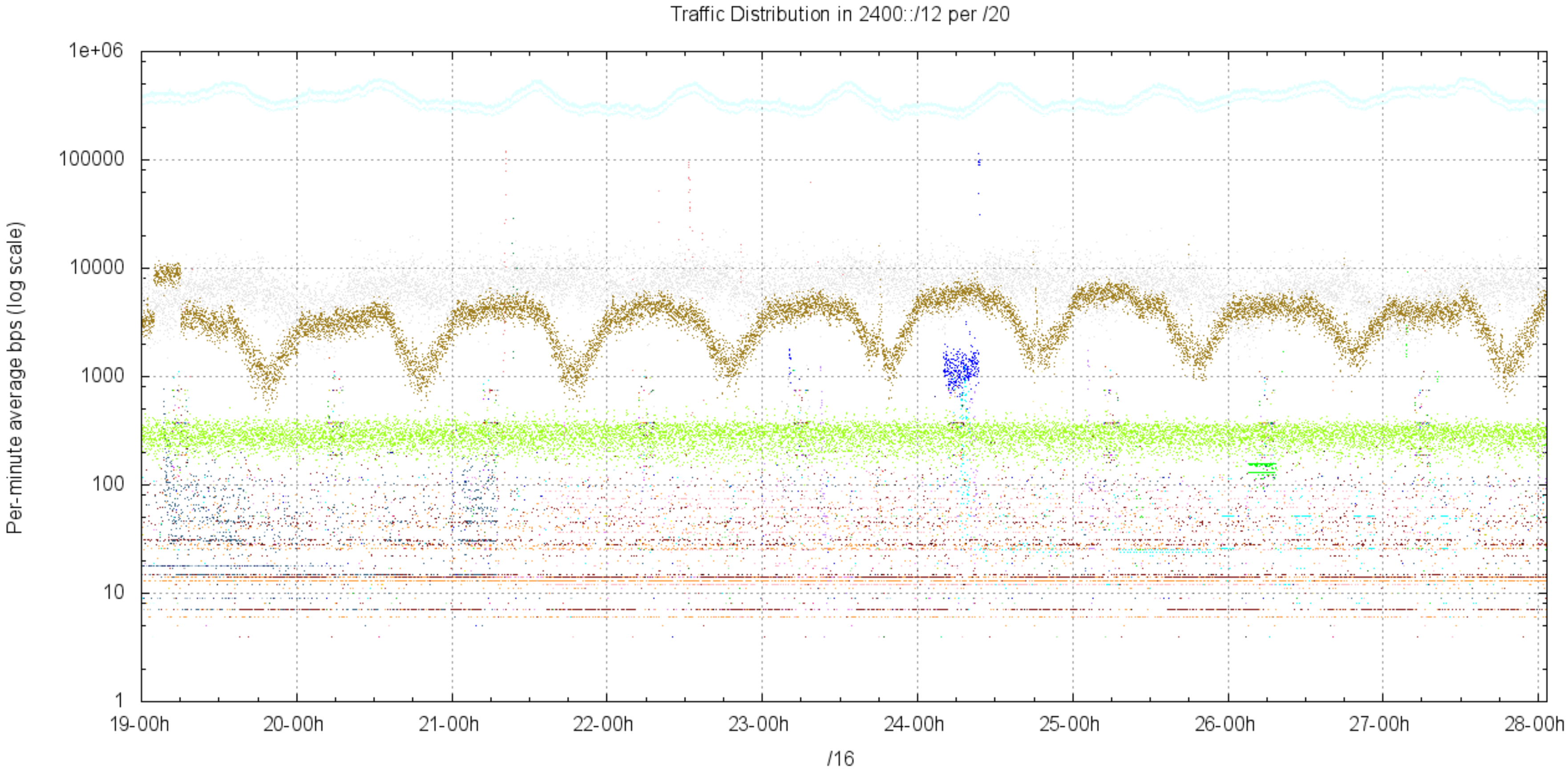
Traffic Profile

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

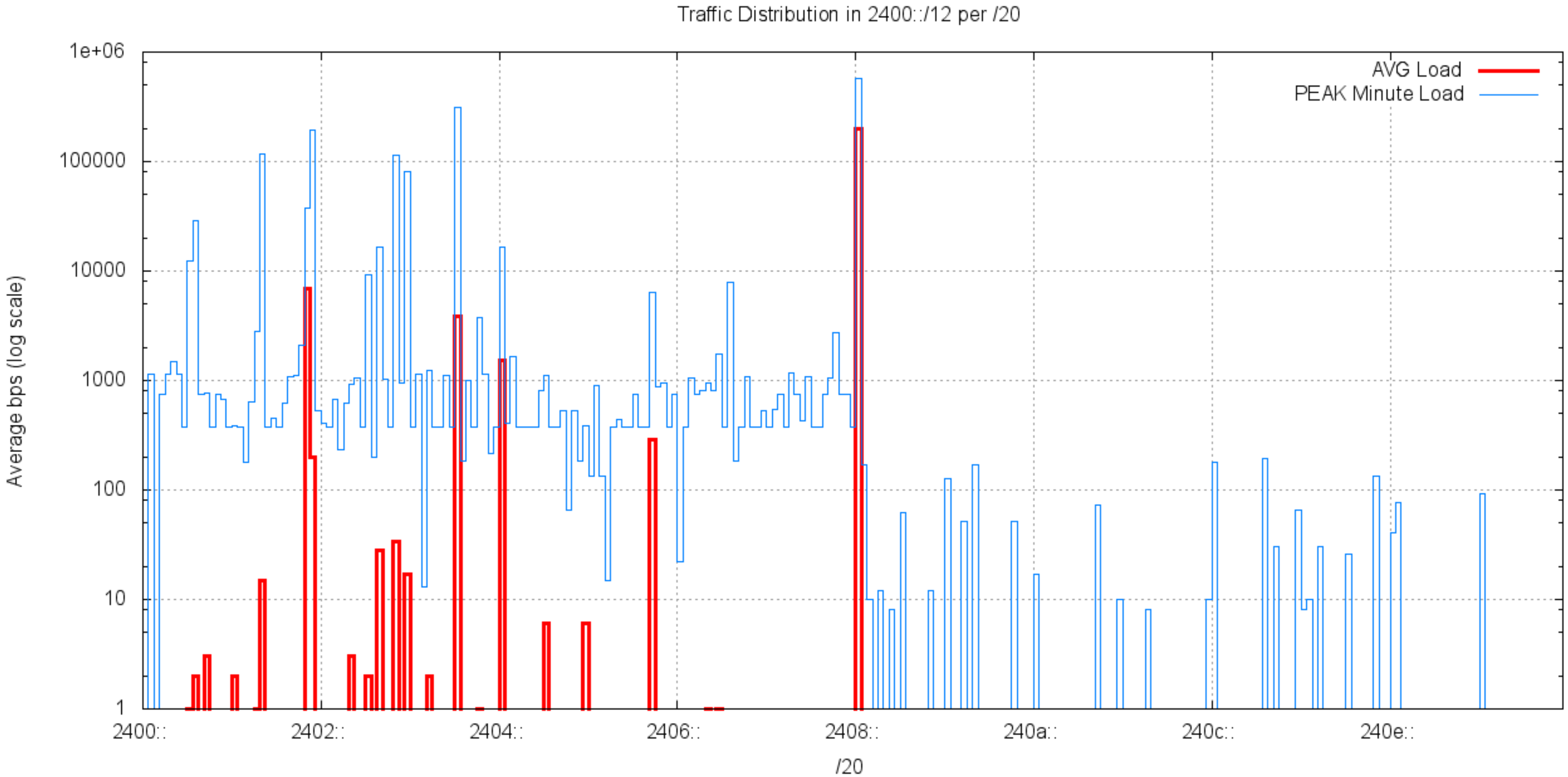
- ICMP: 323 Kbps (611 pps)
- UDP: 54 Kbps (68 pps)
- TCP: 30 Kbps (45 pps)

This is predominately ICMP traffic (destination unreachables being sent to dud addresses – i.e. a double misconfig of both source AND destination).

Destination Address Distribution



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

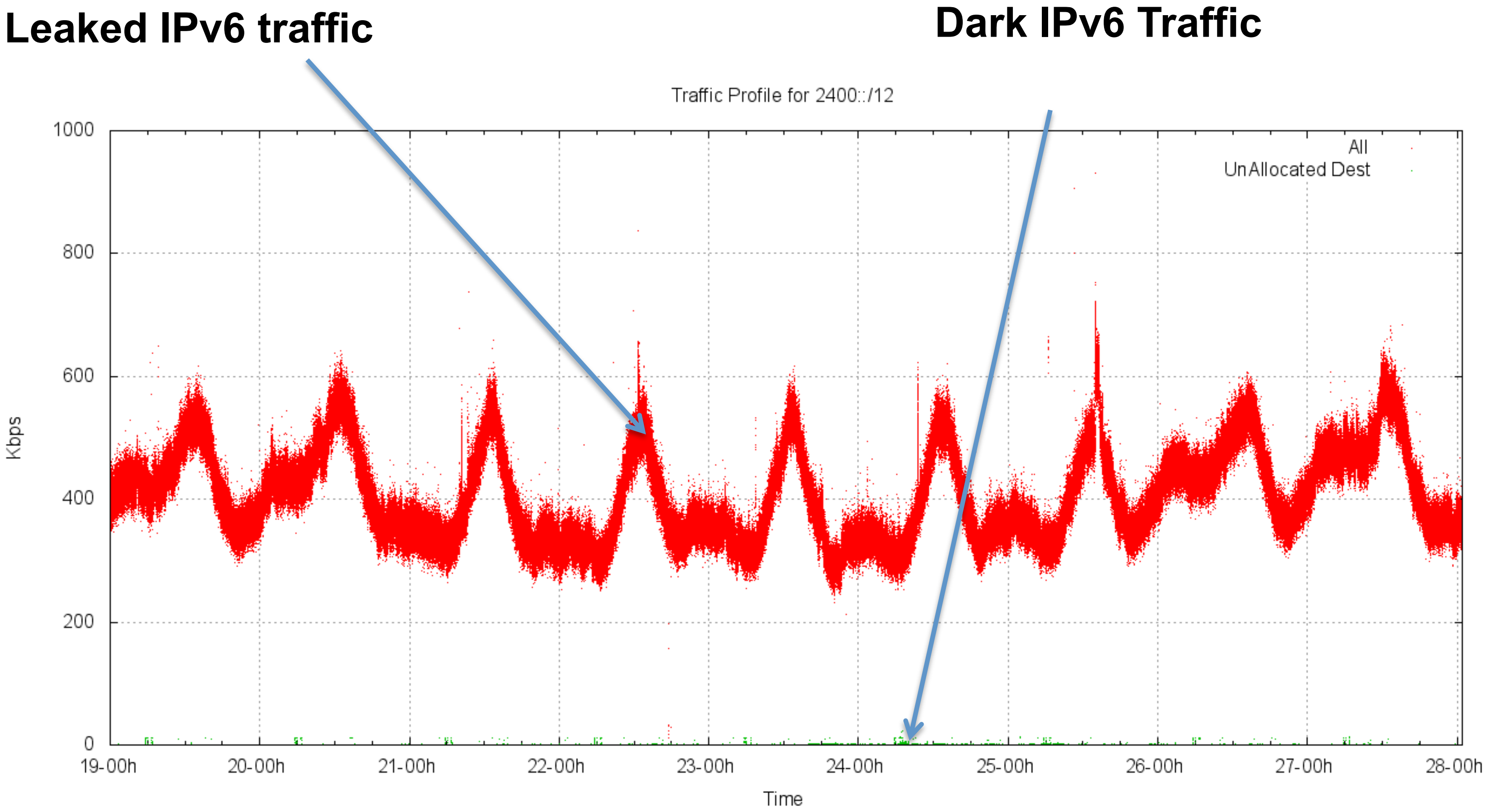
  (well, there are ULAs, but they are slightly different!)

- 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?**

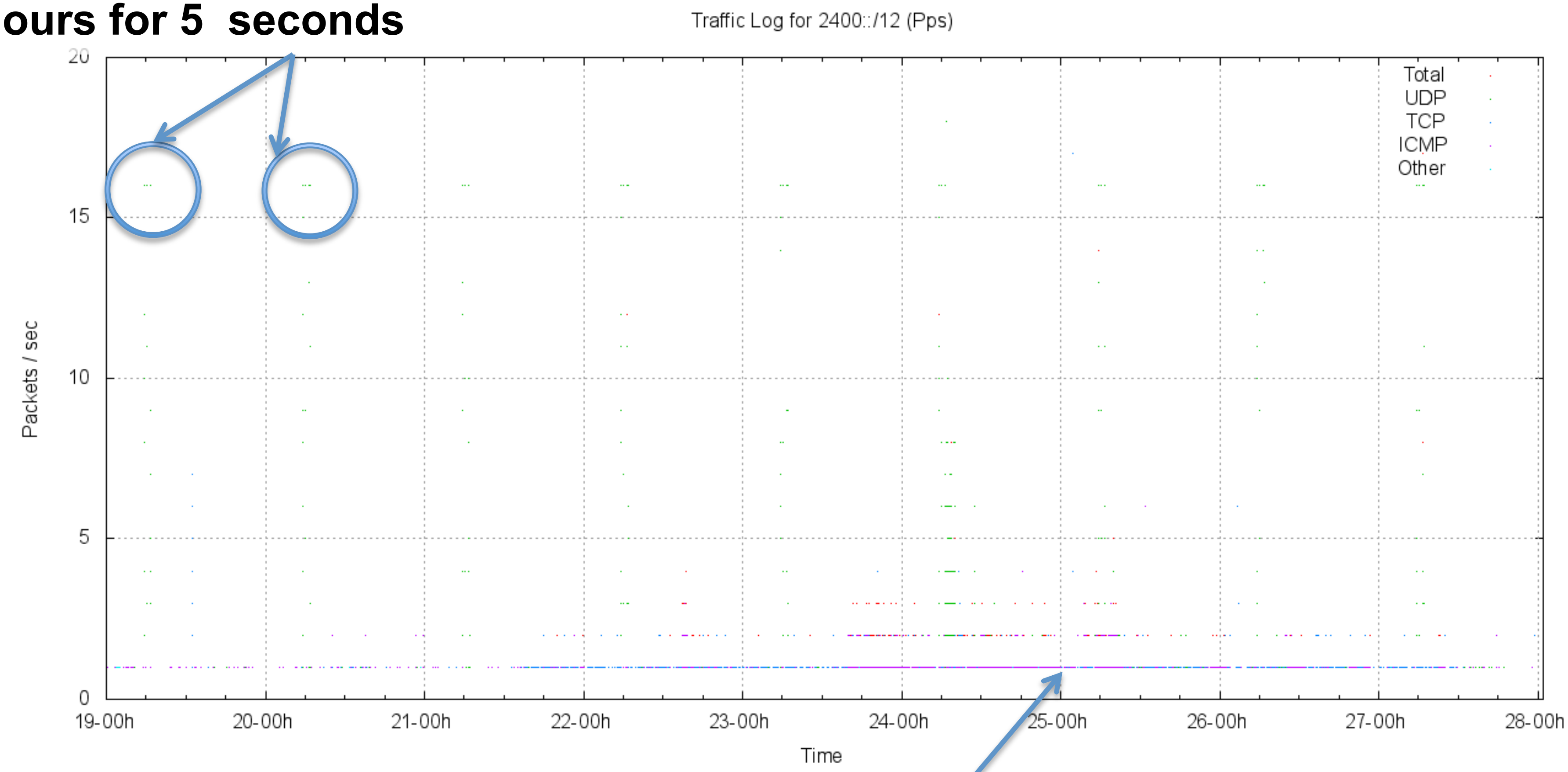
- Flter the captured packets using the address allocation data

Allocated vs Unallocated Dark 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 a 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 private use and dark address blocks in IPv6
- The nature of IPv6 is such that address scanning as a means of virus propagation is highly impractical
  - That does not mean that IPv6 is magically “secure” – far from it – it just means that virus propagation via address scanning does not translate from IPv4 into IPv6

Thank You