IPv6 Background Radiation

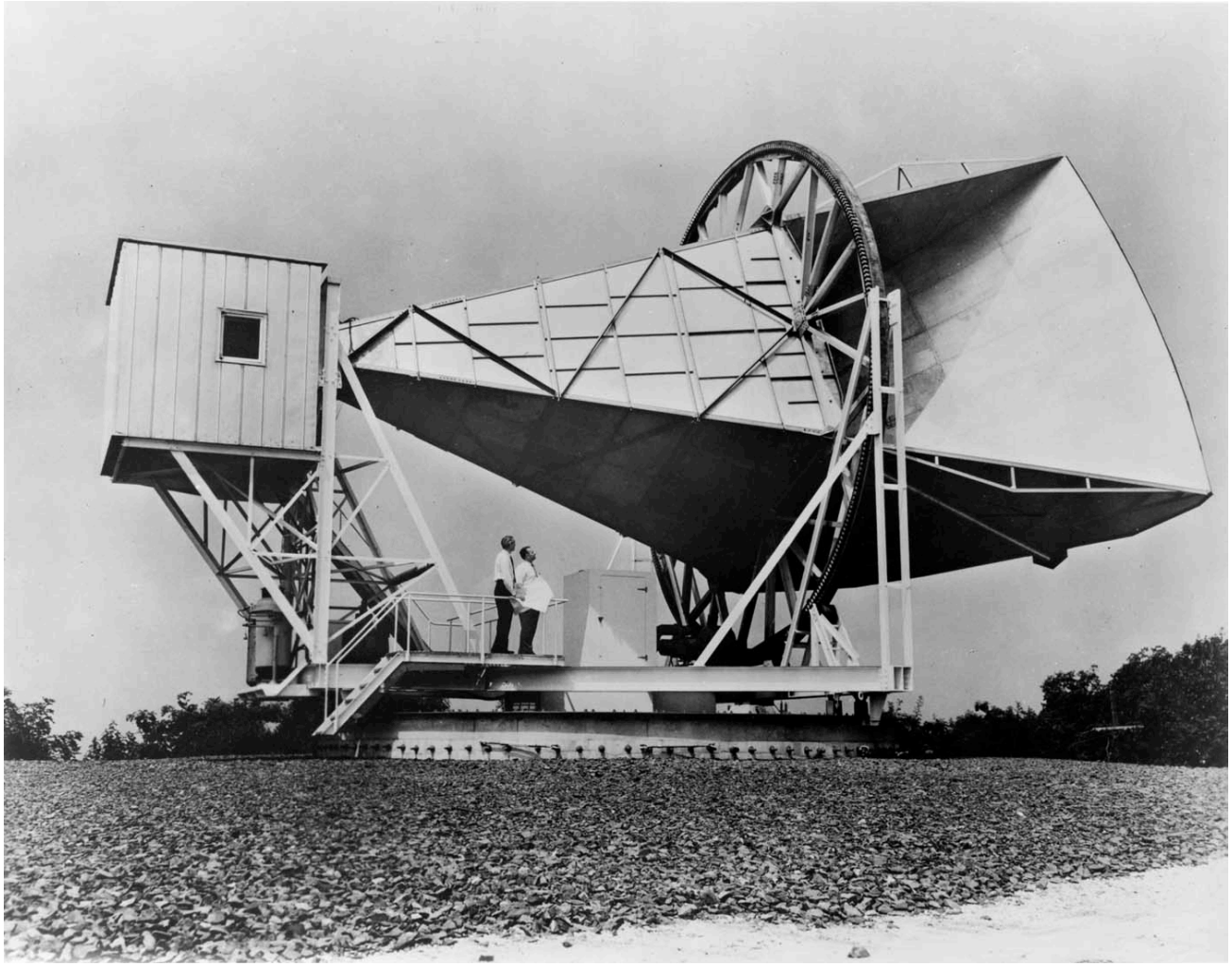
Geoff Huston

APNIC R&D

Network “Background Radiation”

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

Radiation Detection



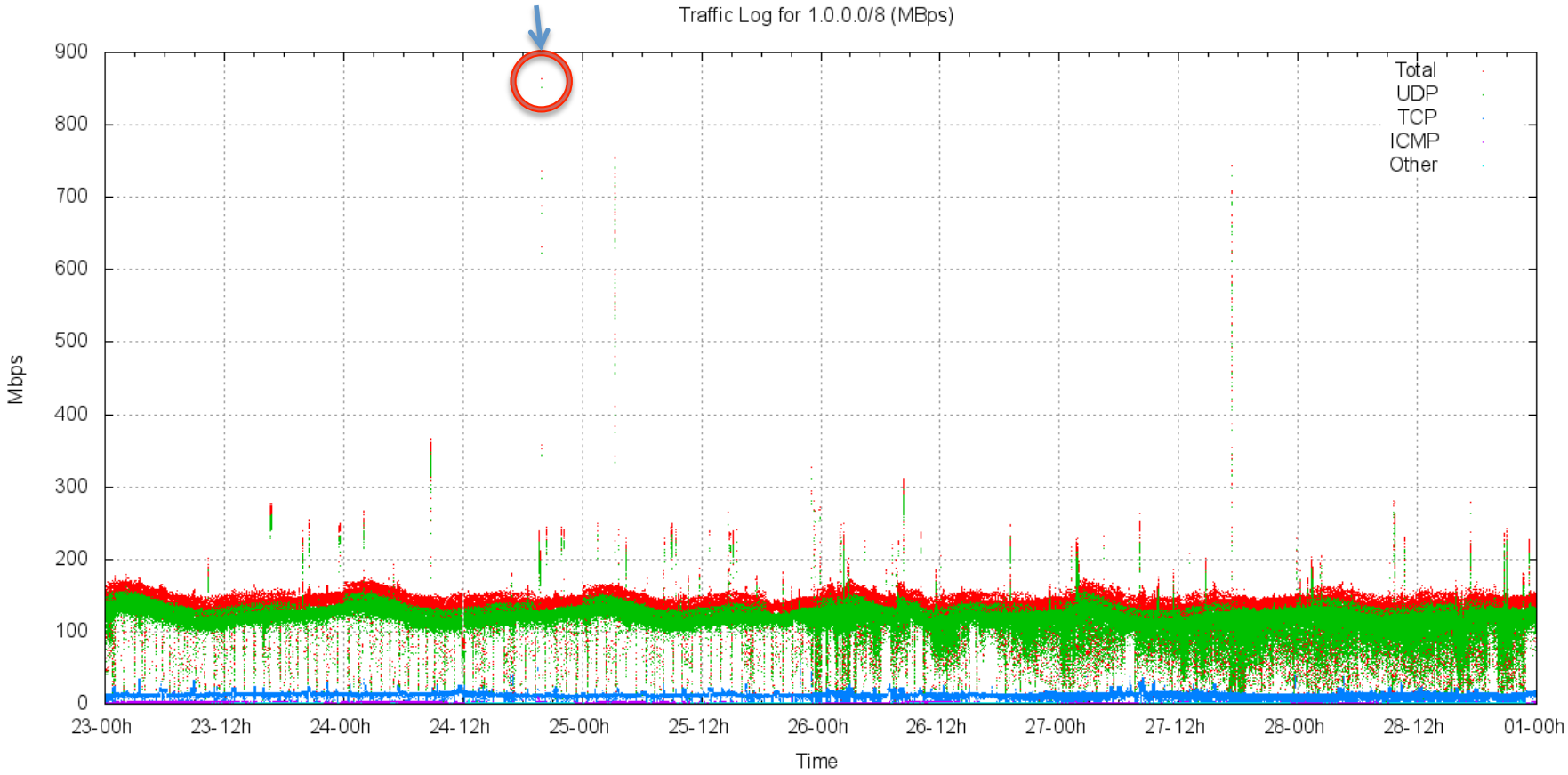
The Holmdel Horn Antenna, at Bell Labs, on which Penzias and Wilson discovered the cosmic microwave background radiation

IPv4 Background Radiation

- We understand that the IPv4 address space is now heavily polluted with toxic background traffic

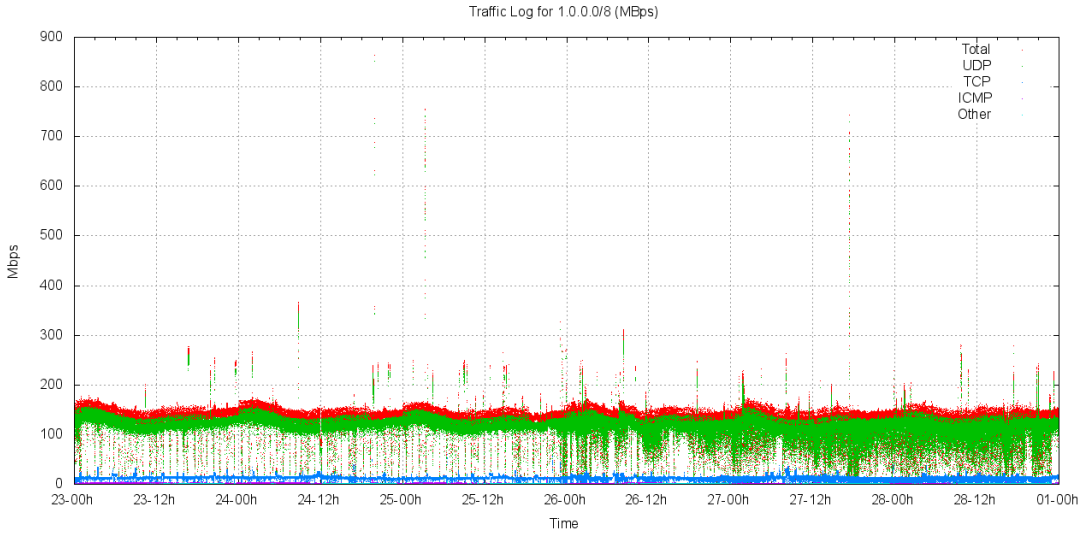
IPv4 – Traffic in network 1/8

Peak Traffic rate
850Mbps

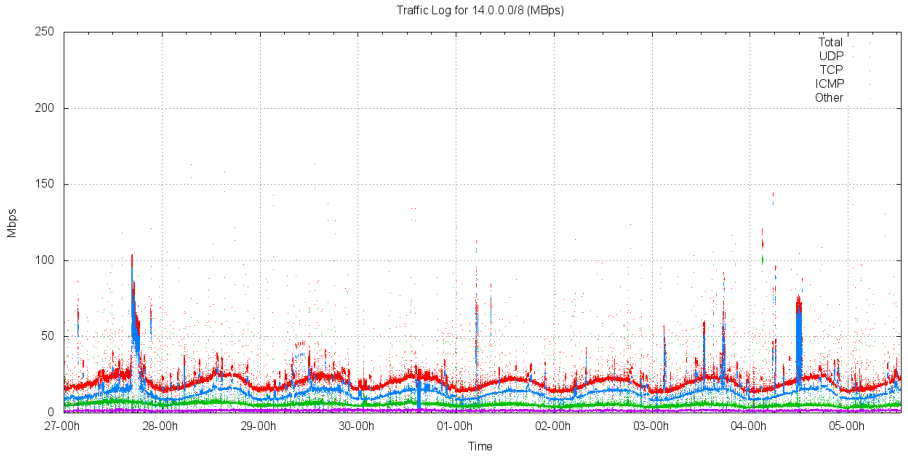


Most of the traffic is RTP directed to 1.1.1.1 – malconfigured SIP phones!

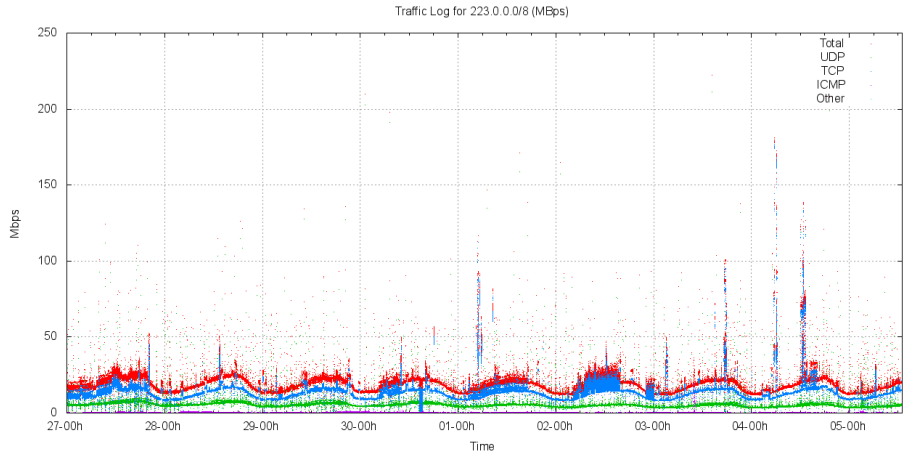
Traffic profile of 1/8



What's "normal" in IPv4?

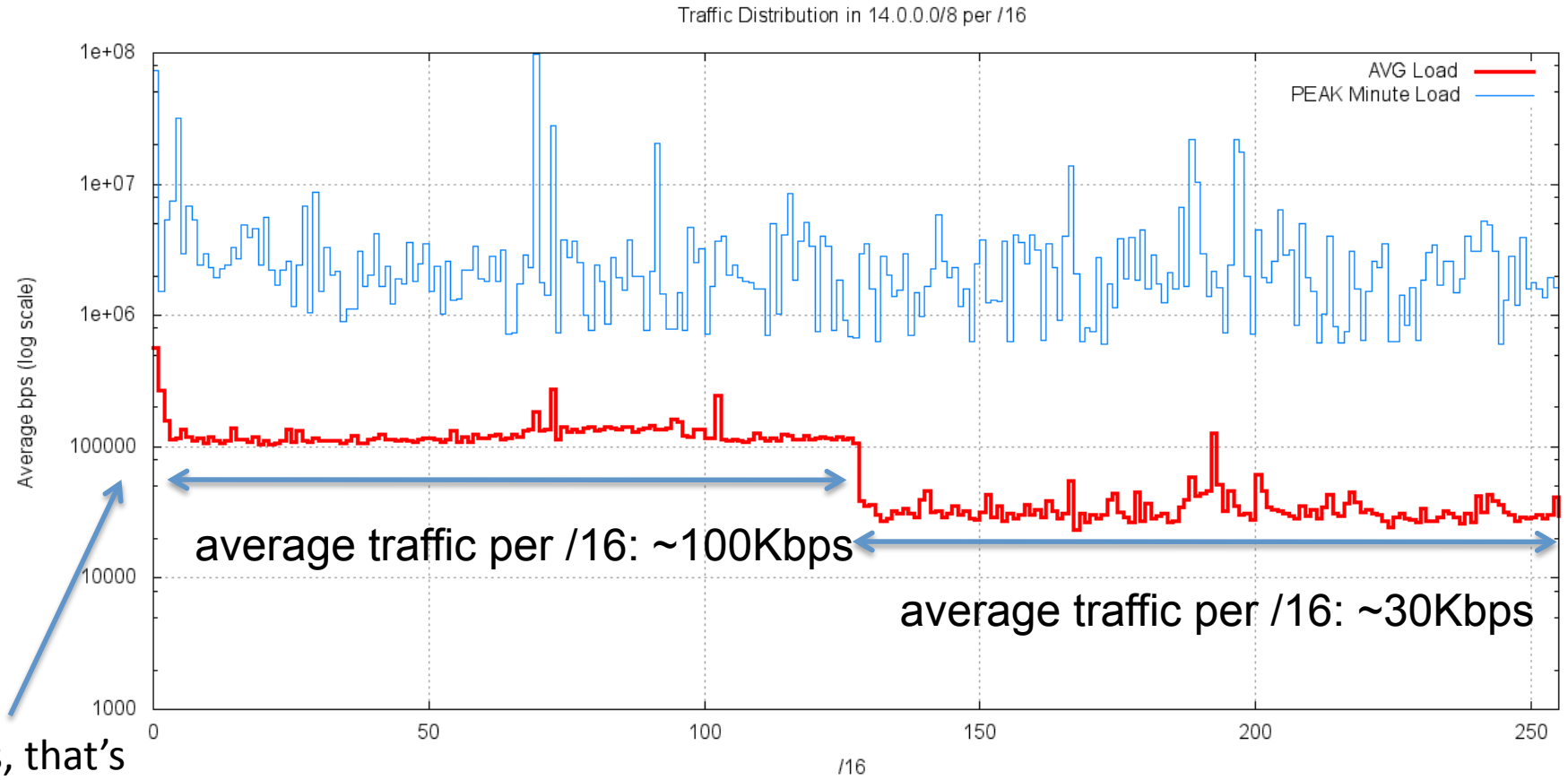


Traffic profile of 14/8



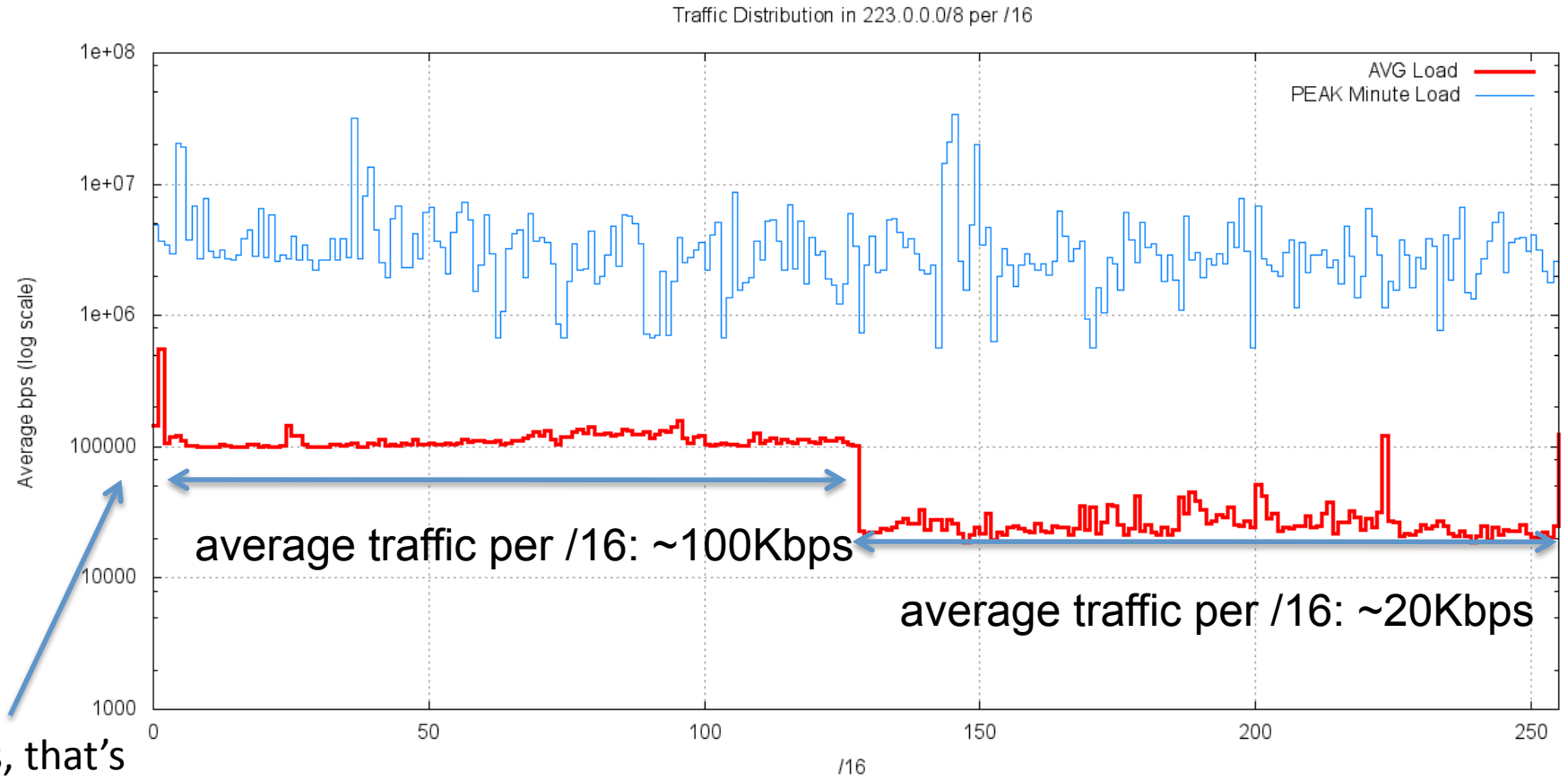
Traffic profile of 223/8

14.0.0.0/8
Horizontal Profile per /16



Yes, that's
a Log Scale!

223.0.0.0/8
Horizontal Profile per /16



Yes, that's
a Log Scale!

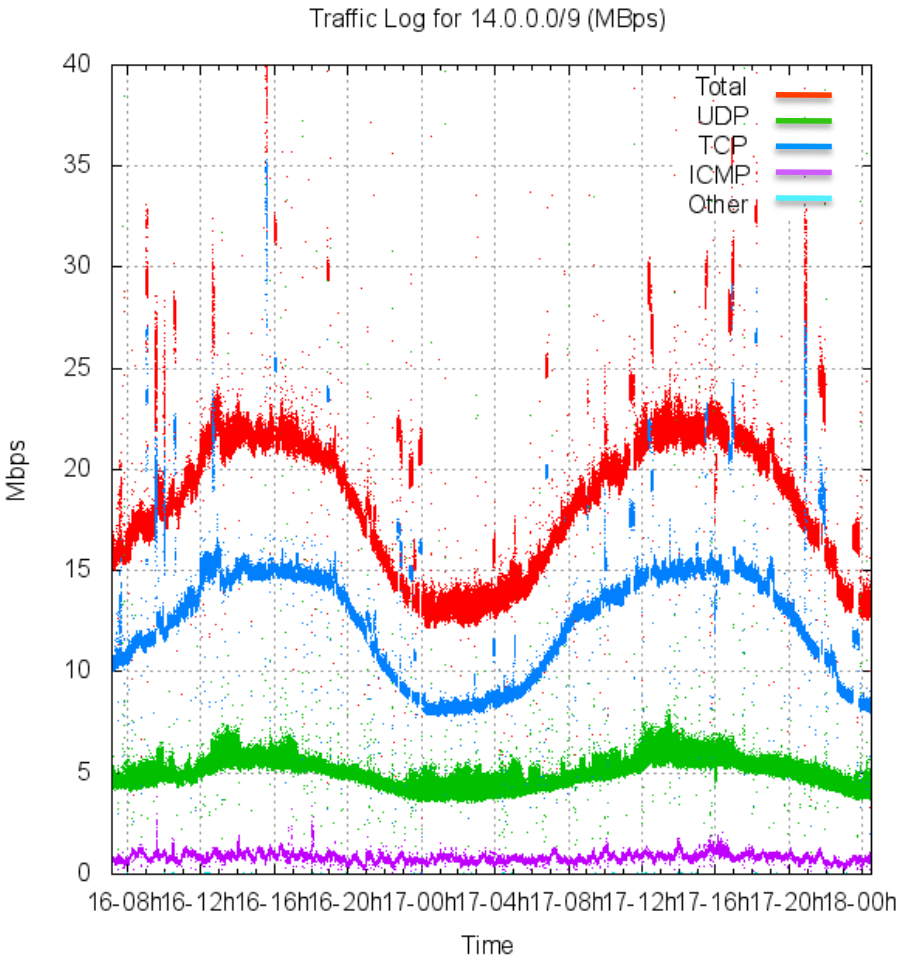
What's in the low half?

Conficker!

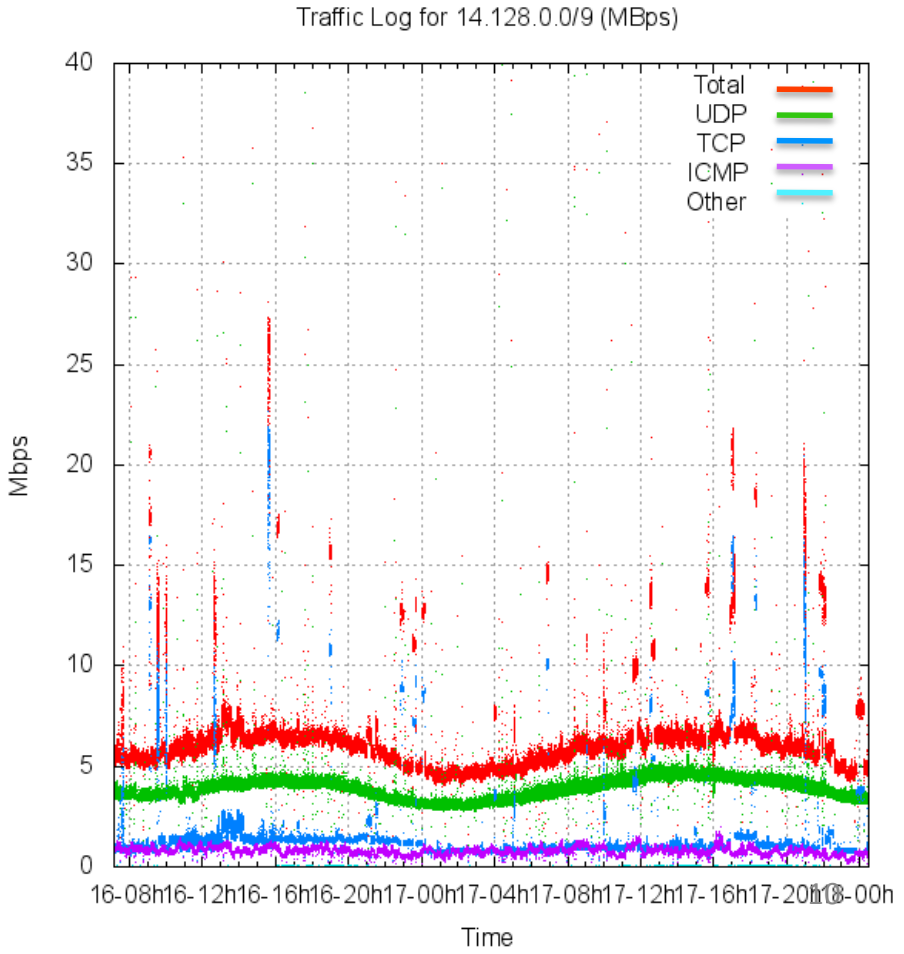
- Conficker will not scan addresses with bit 9 set
- the "low" half of the /8 is scanned by conficker at a rate of ~24,000 packets per second

comparing /9s in 14/8

Low Half



High Half



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.

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

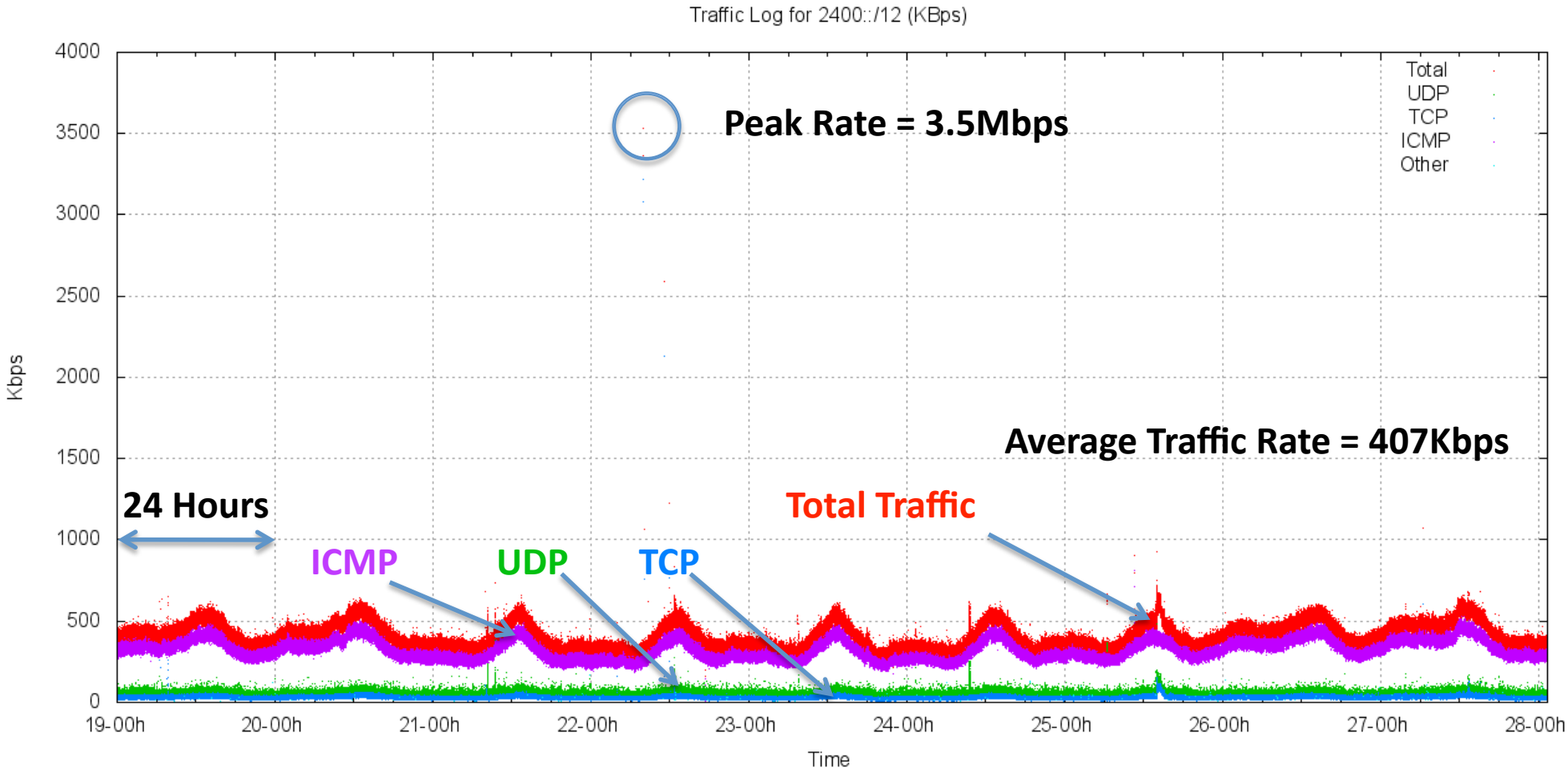
98.41% of the block is unadvertised and unallocated

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 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 ping traffic:

That's a lot of 2002:: 6to4 source addresses

Some of these 2002:: sources are 6to4 cpe, and some are windows end systems

There are also a lot of Teredo 2001:0: sources

And remarkably little unicast IPv6 source addresses

And the destinations are predominately in 2408::/16

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 …

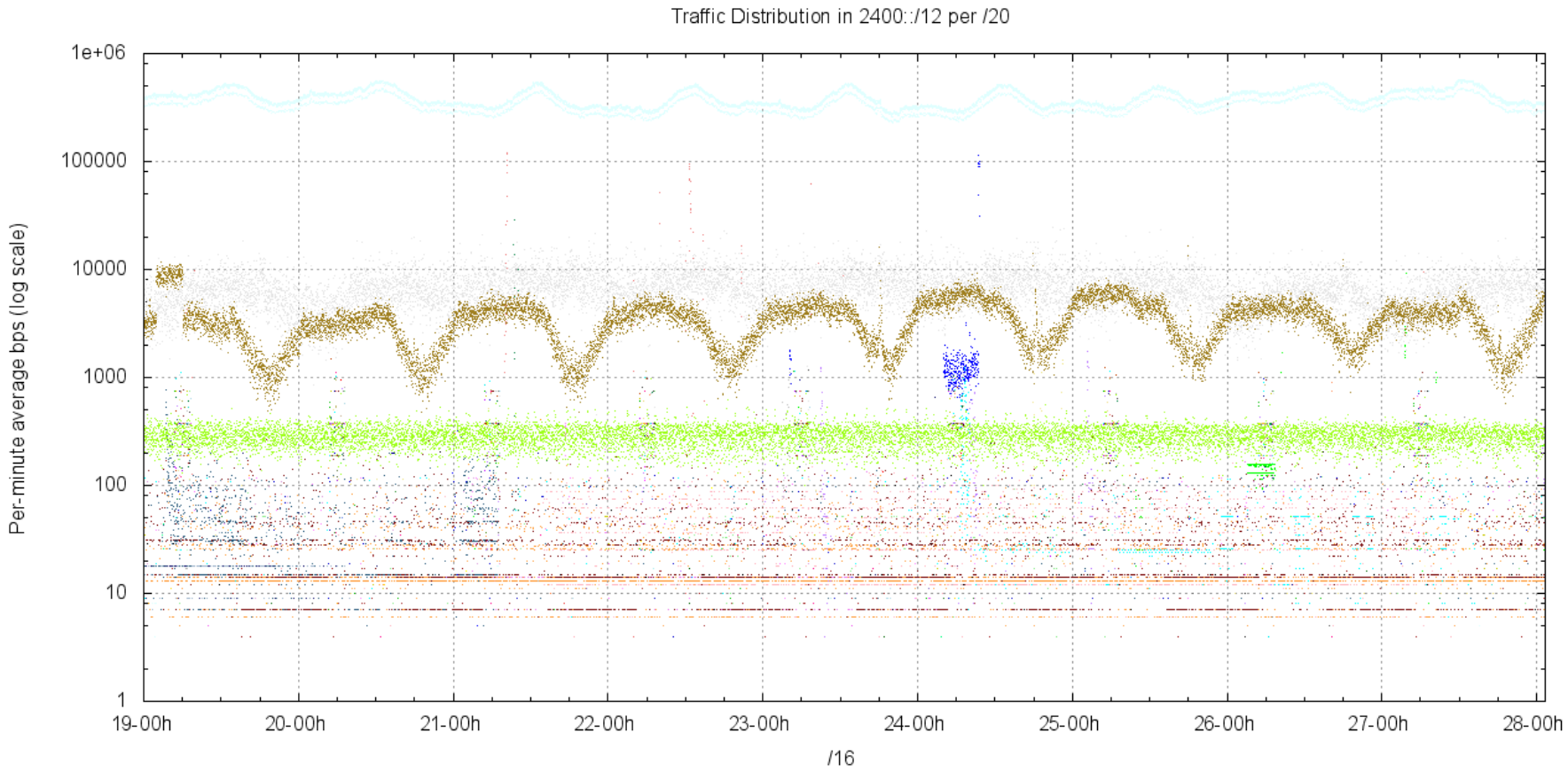
ICMP destination unreachable messages…

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

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

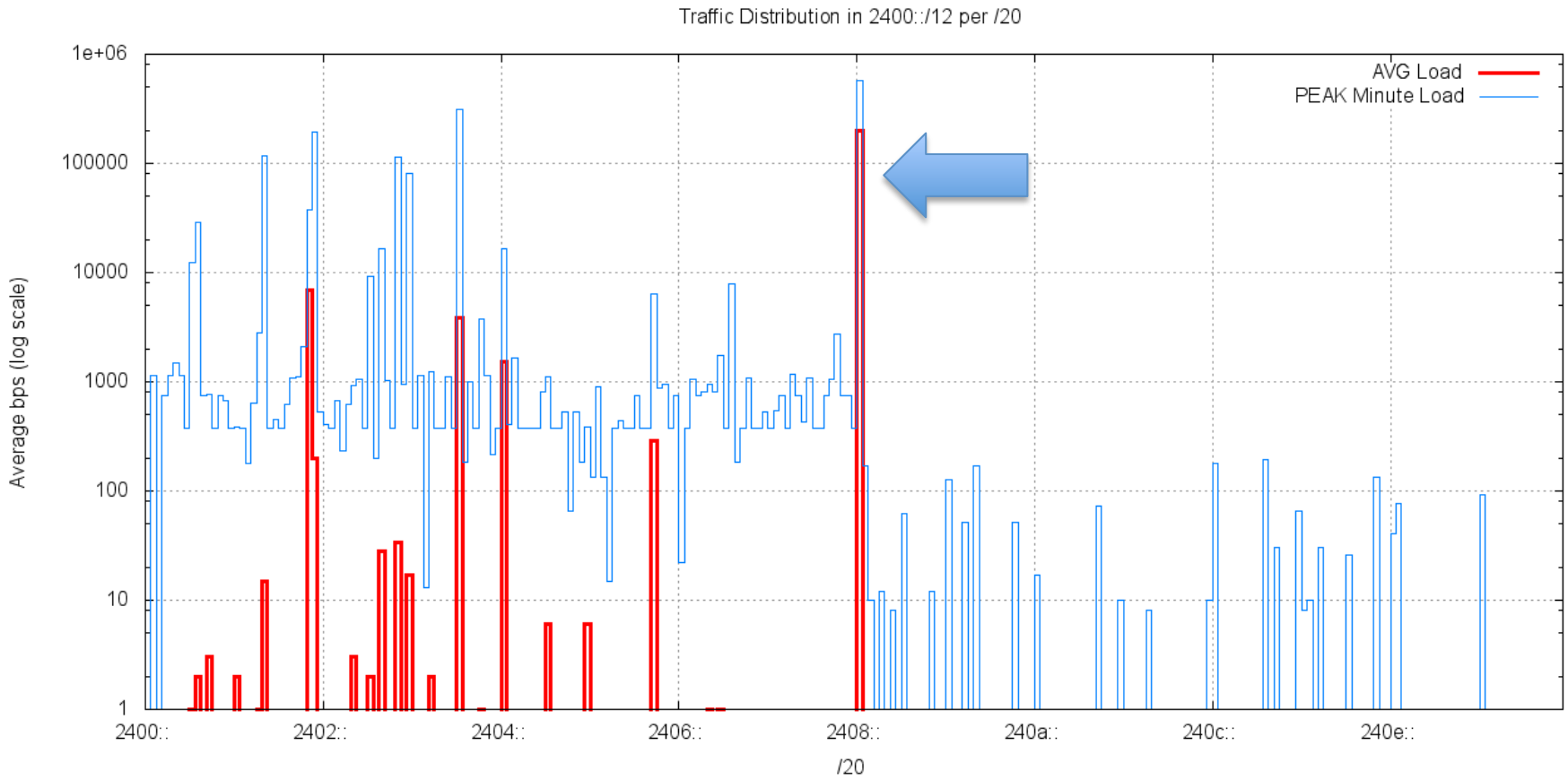
That's a double misconfig of both source AND destination addresses! well done!

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

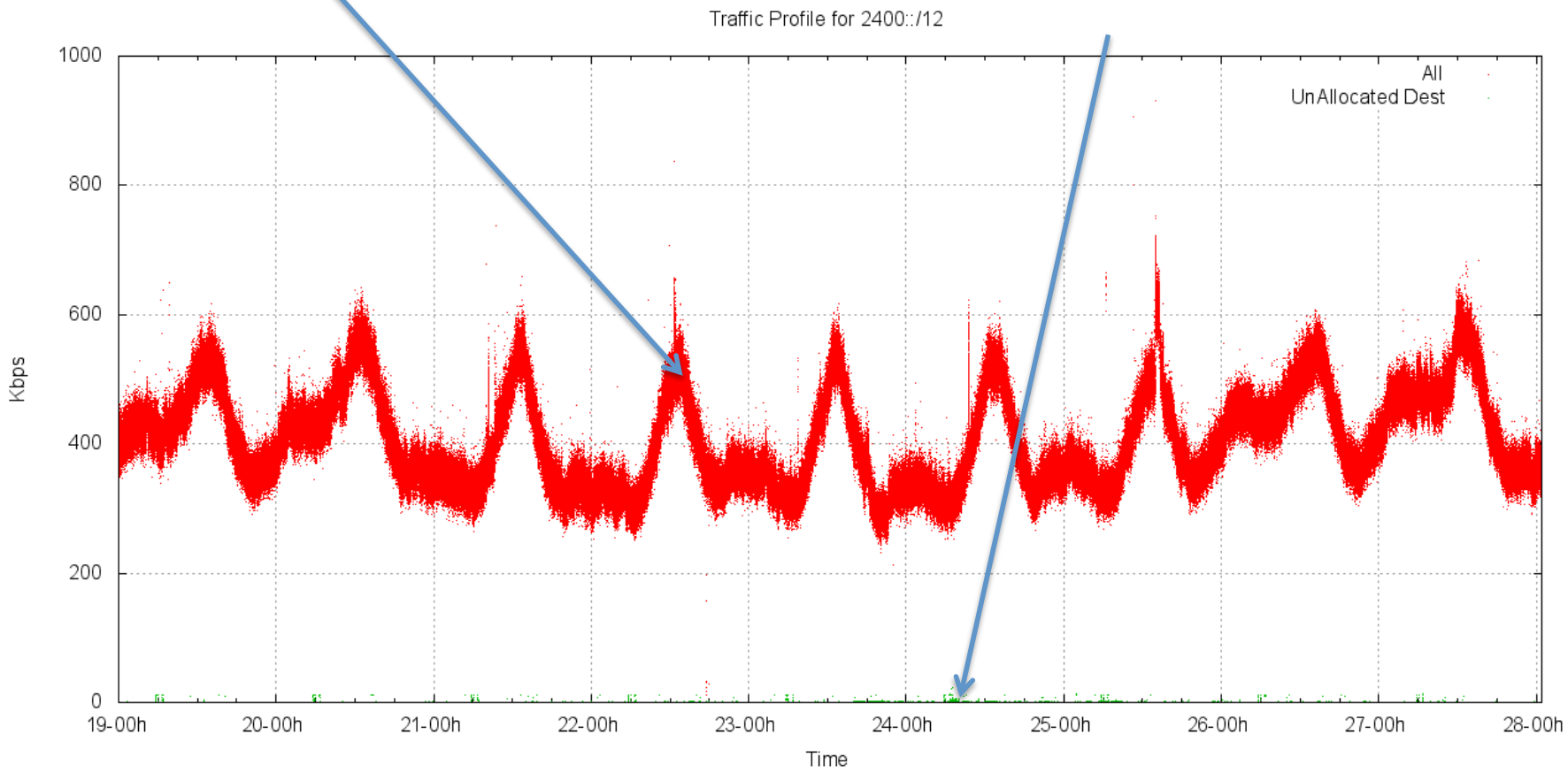
- **How much of this "dark" IPv6 traffic is a result of "leakage" from private contexts into the public network?**

- Filter the captured packets using the address allocation data

Allocated vs Unallocated Dark Traffic

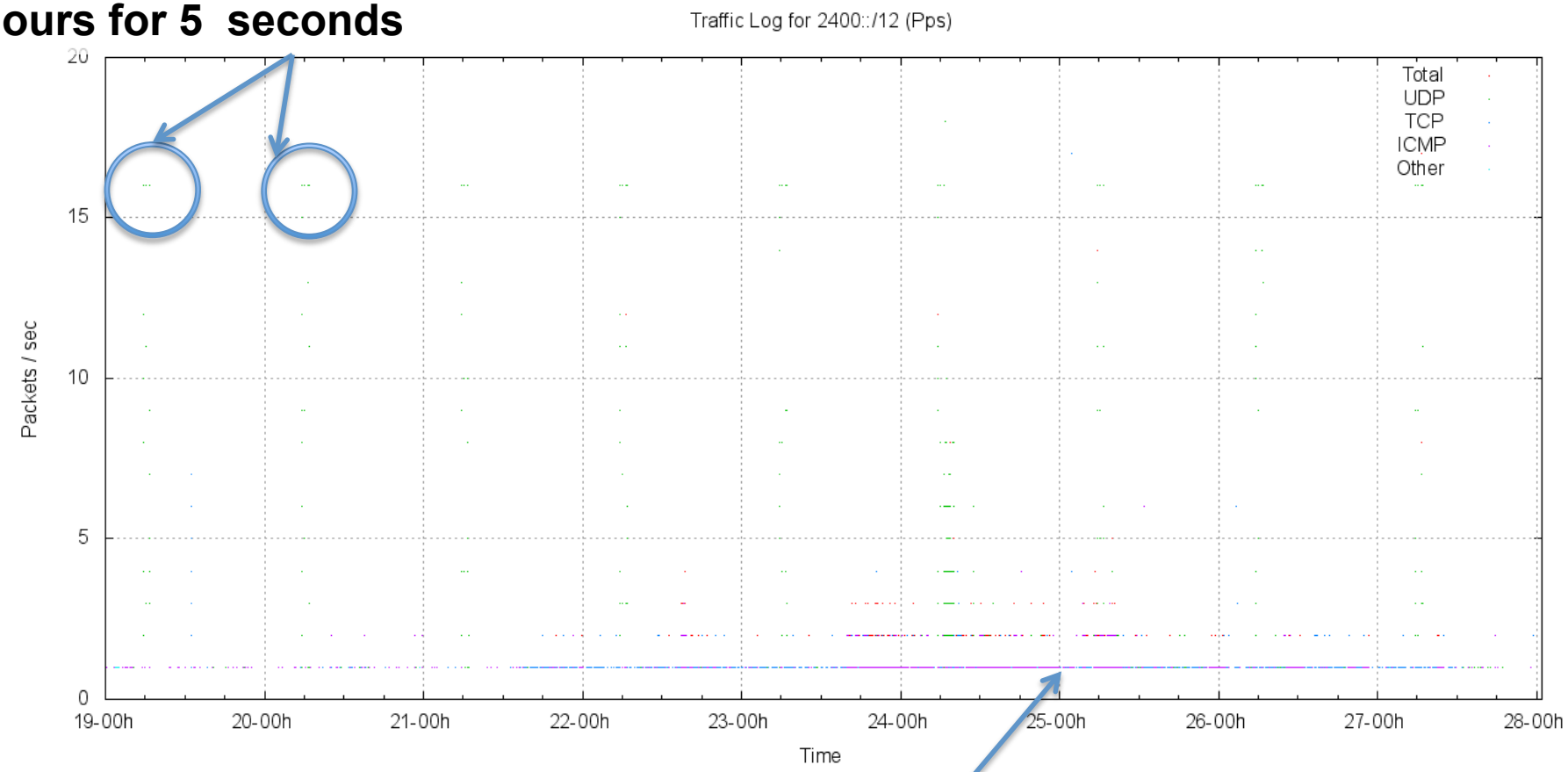
Leaked IPv6 traffic

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

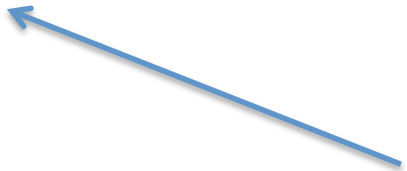
07:20:15.728521 IP6 (hlim 44, next-header TCP (6) payload length: 20) 2001:250:7801:a400::1987:407.57777 > 2402:6219:4100:0:2b0:dc34:e8f3:52a4.3113: .,, 830692465:830692465(0) ack 3672203022 win 64800

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 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 the dark address blocks in IPv6
- 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 billions 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 does not translate from IPv4 into IPv6

Hanlon's Razor:

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

Thank You