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
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
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: 19\textsuperscript{th} June 2010 – 27\textsuperscript{th} June 2010
  107 days: 21\textsuperscript{st} March 2011 – 6\textsuperscript{th} July 2011

A third experiment, hosted by Sandia, underway started 25\textsuperscript{th} April 2012
Traffic Profile 2010

Traffic Log for 2400::/12 (Kbps)
Traffic Profile 2010

Traffic Log for 2400::/12 (Kbps)

Peak Rate = 3.5Mbps

Average Traffic Rate = 407Kbps

24 Hours

Total Traffic

ICMP  UDP  TCP

0  500  1000  1500  2000  2500  3000  3500  4000

Time

19-00h  20-00h  21-00h  22-00h  23-00h  24-00h  25-00h  26-00h  27-00h  28-00h
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

Traffic Log for 2400/12 (KBps)

Peak Rate = 87 Mbps
Total Traffic Profile 2011
Total Traffic Profile 2011

This profile is similar to 2010

Traffic Log for 2400 /12 (KBps)

ICMP, UDP, TCP

Total Traffic

This is not
Destination Address Distribution
2010

Traffic Distribution in 2400::/12 per /20

Per-minute average bps (log scale)
Destination Address Distribution

2010

2408:0::/20  
2401:d::/20  
2403:8::/20

Traffic Distribution in 2400::/12 per /20
Destination Address Distribution 2011

2408:0::/20

Traffic Distribution in 2400::/12 per /20

Per-minute average bps (log scale)
<table>
<thead>
<tr>
<th>Network</th>
<th>Bandwidth</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>2408:0000::/20</td>
<td>197Kbps</td>
<td>Allocated: 2408::/22 – NTT East, JP</td>
</tr>
<tr>
<td>2401:d000::/20</td>
<td>7Kbps</td>
<td>8 x /32 allocations in this block</td>
</tr>
<tr>
<td>2403:8000::/20</td>
<td>4Kbps</td>
<td>4 x /32 allocations in this block</td>
</tr>
<tr>
<td>2404:0000::/20</td>
<td>1Kbps</td>
<td>29 allocations in this block</td>
</tr>
<tr>
<td>2405:b000::/20</td>
<td>0.3Kbps</td>
<td>4 x /32 allocations in this block</td>
</tr>
</tbody>
</table>
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

Traffic Distribution in 2400:/12 per /20

Average bps (log scale)

AVG Load
PEAK Minute Load

2400:: 2402:: 2404:: 2406:: 2408:: 240a:: 240c:: 240e::
Destination Address Distribution
2011

Traffic Distribution in 2400: /12 per /20

Average Incoming Traffic
Peak Incoming Traffic
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?)
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 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?

• Let's filter the packets using the allocation data
Allocated vs Unallocated Dark Traffic - 2010

All “dark” IPv6 traffic

“dark” traffic to Unallocated Destination Addresses

Traffic Profile for 2400:/12
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)
Response: finlin.wharton.upenn.edu. A 128.91.91.59
TCP Probing?

05:02:52.568966 IP6 (hlim 44, next-header TCP (6) payload length: 20) 2001:250:7801:a400::1987:57777 > 2402:1123:1ba:ec05:ef:f2c6:ce35:c40f.1158: ,, 1365702964:1365702964(0) ack 3293642040 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…?

Same Teredo source address, but varying destination addresses
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

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

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 unreachable, and malformed packet headers
>> to 2011 – All vs Dark

Traffic Log for 2400::/12

Kbps

Time

02/07 18/06 04/06 21/05 07/05 23/04 09/04 26/03

0 200 400 600 800 1000 1200 1400 1600 1800 2000
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 destinations
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!


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

Traffic Log for 2400../12 (Kbps)

Time

Kbps
## 2012 Profile

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

128 -> Echo Request  
129 -> Echo Reply  
1 -> Dest Unreachable  
3 -> TTL Exceeded  
80 -> HTTP  
53 -> DNS  
500 -> ISAKMP  
179 -> BGP  
443 -> HTTPS
Traffic Log for 2400:/12 (KBps)
Traffic Log for 2400:/12 (Pps)

- Total
- UDP
- TCP
- ICMP
- Other
<table>
<thead>
<tr>
<th>Rank</th>
<th>ICMP Type</th>
<th>Count</th>
<th>TCP Source</th>
<th>Count</th>
<th>Dest</th>
<th>Count</th>
<th>UDP Source</th>
<th>Count</th>
<th>Dest</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>128</td>
<td>61479</td>
<td>80</td>
<td>42</td>
<td>80</td>
<td>126368</td>
<td>53</td>
<td>629</td>
<td>53</td>
<td>458</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>15022</td>
<td>34676</td>
<td>36</td>
<td>443</td>
<td>293</td>
<td>63000</td>
<td>186</td>
<td>33483</td>
<td>116</td>
</tr>
<tr>
<td>2</td>
<td>129</td>
<td>1282</td>
<td>53439</td>
<td>34</td>
<td>30965</td>
<td>132</td>
<td>35691</td>
<td>46</td>
<td>33487</td>
<td>116</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>252</td>
<td>47342</td>
<td>30</td>
<td>59280</td>
<td>100</td>
<td>32100</td>
<td>23</td>
<td>33488</td>
<td>116</td>
</tr>
<tr>
<td>REST</td>
<td></td>
<td>226</td>
<td>130723</td>
<td></td>
<td>3972</td>
<td></td>
<td>3118</td>
<td></td>
<td>3196</td>
<td></td>
</tr>
</tbody>
</table>

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

- 80  -> HTTP
- 443 -> HTTPS
- 53  -> DNS
Thank You

Questions?