Traffic on TCP port 53 and DNS Response Sizes at U Auckland

CAIDA/WIDE Workshop, March 2006

Nevil Brownlee
Why look at TCP port 53?

- Recent reports [Randy, Daniel] suggest that
  - Successive DNS requests can go to different anycast root servers
  - Routes can be unstable – they can switch quickly
- UDP can cope with such switches, TCP would not cope well
- So .. how much *DNS over TCP* traffic is there?
  - Expect to see zone transfers,
  - and a few name lookups
- Used *NeTraMet* to collect data at Auckland
NeTraMet meter setup at Auckland

- Meter observes all Internet traffic in/out
- Meter can run SRL rulesets run to produce
  - DNS root/gTLD RTTs
  - Other rulesets, as needed from time to time
- Reworked NeTraMet’s *Turnaround Time* code to handle DNS over TCP
  - NeTraMet uses the timestamps for the packets that carry the first \( n \) bytes of the DNS request and response
- Ran ruleset to observe flows on TCP port 53
  - Ruleset tries to use first packet as source of flow
- Also ran tcpdump to gather headers of TCP 53 packets
## NeTraMet v5.1: -c900 -r dns-tcp-wire.rules localhost eth3
10000 flows starting at 17:32:23 Thu 22 Dec 2005

### Format: flowruleset flowindex firsttime sourcepeertype sourcetransertype
sourcepeeraddress destpeeraddress d_tooctets d_fromoctets 

d_topdus d_frompdu d_tolostpdu d_fromlostpdu (d_toturnaroundtime)

### Time: 21:15:00 Thu 22 Dec 2005 localhost Flows from 1246168 to 1336150

<table>
<thead>
<tr>
<th>Time</th>
<th>Flowindex</th>
<th>Firsttime</th>
<th>Sourcepeertype</th>
<th>Sourcepeertype</th>
<th>Sourcepeeraddress</th>
<th>Destpeeraddress</th>
<th>D_toOctets</th>
<th>D_fromOctets</th>
<th>D_topDUs</th>
<th>D_fromDUs</th>
<th>D_toLostPDU</th>
<th>D_fromLostPDU</th>
<th>(D_toTurnaroundTime)</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 11</td>
<td>94590</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>130.216.1.2</td>
<td>67.15.35.19</td>
<td>176</td>
<td>74</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>20 30</td>
<td>234963</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>130.216.1.1</td>
<td>216.26.160.5</td>
<td>74</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>20 77</td>
<td>1247060</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>130.216.1.1</td>
<td>204.152.184.64</td>
<td>37034</td>
<td>1659476</td>
<td>561</td>
<td>1098</td>
<td>0</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>20 78</td>
<td>1276973</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>218.25.41.136</td>
<td>130.216.112.11</td>
<td>156</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0 (0)</td>
</tr>
<tr>
<td>20 79</td>
<td>1292934</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>130.216.1.1</td>
<td>205.171.14.195</td>
<td>386</td>
<td>4620</td>
<td>5</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>(1982)</td>
</tr>
<tr>
<td>20 80</td>
<td>1292989</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>130.216.1.2</td>
<td>205.171.9.242</td>
<td>452</td>
<td>4752</td>
<td>6</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>(2996)</td>
</tr>
<tr>
<td>20 81</td>
<td>1299794</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>130.216.1.1</td>
<td>194.30.63.66</td>
<td>0</td>
<td>60</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>20 82</td>
<td>1330338</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>130.216.1.1</td>
<td>62.45.94.136</td>
<td>176</td>
<td>74</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>20 83</td>
<td>1331230</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>202.108.12.66</td>
<td>130.216.35.35</td>
<td>318</td>
<td>300</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>(0)</td>
</tr>
</tbody>
</table>

# EndData: localhost

- However ..
- What are all the other flows?
- What can we infer from the To/From PDU counts?
Successful DNS transactions: To/From pdu counts

Example TCP connection:
- 5 packets To, 3 packets From

Actual connections depend on behaviour of nameserver and TCP stack. We often see . .
- Length (2 bytes) sent as separate packet (before request or response)
- Some TCP stacks ACK responses quickly, i.e. not piggybacked with FINs
- (We never see the request piggybacked with the handshake ACK)

Summary: successful transactions are just normal TCP connections
These flows looked odd because their times are so small, only around $0.8ms$. They are a sequence of requests from 132.205.96.87—a nameserver outside U Auckland, to our nameservers, 130.216.1.2 and 130.216.1.1. For each of the two flows’ 53 transactions, 6 packets were sent and 5 received. What we’re observing here is the time for our servers to respond to incoming requests.
Unusual successful flows (2)

This flow had 33 transactions, each taking about 161 ms

130.216.165.190 is not one of our local caching nameservers
It appears to be a (misconfigured?) user machine

192.175.48.1 is prisoner.iana.org.
prisoner is one of IANA’s ‘blackhole’ servers
Those servers respond to inverse lookups of RFC 1918 addresses
And now, *unsuccessful* flows

- Lots of requests are simply ignored
  - They’re the ones that get 0 packets *From* their destination hosts

- Others exchange packets, but don’t get matching requests/responses
  - They have to/from counts like 8 6 and 7 5
  - Needed to look their packet headers with tcpdump ..
This example shows a host scan through our network, 130.216/16

SRL ruleset incorrectly gives 217.172.172.67 as the flow’s destination

That’s because the ruleset looks for destination port 53,

but these packets use port 53 as their source

We see address scans like this every few days
DDoS attack (1)

Remote host is trying to open TCP connections

• Three connection attempts, using ports 2347, 2372 and 2394
• External host sends SYN, we respond with SYN+ACK
• External host terminates connection with RST
• Meter is outside firewall – we retry the SYN+ACK four times
• 6 packets sent, 5 received, × 3 ports ⇒ 18 15

• Looks like a DDoS attack (source address spoofed)
• We reply to the spoofed address, it responds with RST
These attacks keep happening, every 1/4 to 3 hours

Most – if not all – of them come from addresses within Chinese ISP address ranges

They’re part of the Internet ‘background noise’
Traffic on TCP port 53: Conclusion

- At Auckland we see:
  - a steady trickle of DNS requests over TCP
  - a few zone transfers at scheduled intervals
  - a few common attack patterns

- Now we need to categorise the patterns so as to recognise and count them over a long period

- We want to track TCP port 53 usage so as to discover whether DNS over TCP is increasing over time

Comment: RFC 2671 (EDNSO) allows DNS record sizes up to 65535, with or without fragmentation
  - We see lots of responses with $> 512$ bytes
  - Maybe a nameserver could send back a large response as a set of IPv4 fragments?
DNS record size distributions

DNS request/response sizes at Auckland in March 2006

Record size (B)
DNS sizes, 2005 and 2006

DNS reply size distributions at Auckland, Aug 05 and Mar 06

% replies in 2006
% replies in 2005

Record size (B)