Combining Active and Passive Monitoring

Mohit Lad
CEO, ThousandEyes
mohit@thousandeyes.com
Basics

» Passive Monitoring
  » Capture traffic from the network by generating a copy of the traffic usually via a span port, mirror port or network tap
  » Typical Use: Discover what is going on

» Active Probing
  » Generating a synthetic probe that will discover information and report back
  » Examples: ping, traceroute
  » Typical Use: Find the root cause
Example: Google does not load
Example: Google does not load: Step 1 DNS resolution

Local DNS resolver

Name Server for .com

Authoritative DNS for Google.com

google.com?

1.2.3.4
Probing for DNS issues

- Tcpdump on client -> tells us if we get a DNS reply or not
- What if we don’t get a reply?
  - Check for resolver, returns replies to other domains
  - Troubleshoot DNS from resolver to Google
- If we get a reply, is DNS working?
Buenos Aires cannot resolve DNS

**Worldwide Averages for**

<table>
<thead>
<tr>
<th>Availability</th>
<th>Resolution Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>97.62%</td>
<td>104 ms</td>
</tr>
</tbody>
</table>

**Active Alerts**

- **DNS outage 1 or more locations**

<table>
<thead>
<tr>
<th>Agent</th>
<th>Date</th>
<th>Mappings</th>
<th>Error Details</th>
<th>Resolution Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buenos Aires, Argentina</td>
<td>2014-10-09 20:21:56</td>
<td></td>
<td>Could not reach name server</td>
<td></td>
</tr>
</tbody>
</table>
Domain in question is anycasted
How do we know it’s anycast?

10 ms from Paris

55 ms from Sao Paulo
Identifying the problematic Anycast instance
So is everything ok if we get a DNS reply? Let's look at Facebook NS.

Facebook NS gets “no mapping” in China.
Facebook.com A record is 100% available in China
Most of the world maps facebook.com to 173.252.120.6
Who owns 173.252.120.6

<table>
<thead>
<tr>
<th>NetRange</th>
<th>173.252.64.0 - 173.252.127.255</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIDR</td>
<td>173.252.64.0/18</td>
</tr>
<tr>
<td>OriginAS</td>
<td>AS32934</td>
</tr>
<tr>
<td>NetName</td>
<td>FACEBOOK-INC</td>
</tr>
<tr>
<td>NetHandle</td>
<td>NET-173-252-64-0-1</td>
</tr>
<tr>
<td>Parent</td>
<td>NET-173-0-0-0-0</td>
</tr>
<tr>
<td>NetType</td>
<td>Direct Assignment</td>
</tr>
<tr>
<td>RegDate</td>
<td>2011-02-28</td>
</tr>
<tr>
<td>Updated</td>
<td>2012-02-24</td>
</tr>
<tr>
<td>Ref</td>
<td><a href="http://whois.arin.net/rest/net/NET-173-252-64-0-1">http://whois.arin.net/rest/net/NET-173-252-64-0-1</a></td>
</tr>
</tbody>
</table>
72% of China sees a different IP 37.61.54.158
Who owns 37.61.54.158?

Azerbaijan
Traceroute

» Protocol used can make a big difference, TCP, UDP or ICMP
» Load balancing can distort discovered routes
» Hard to distinguish between muted interfaces and real loss
» Multiple routes exist, need several probes
» MPLS can distort delays
Country Financial Outage

Country Financial
https://www.countryfinancial.com/SiteController?url=/custo...

Agent: All agents

Metric: Availability, Response Time, Throughput

Date: SEP 04 17:30 UTC (35 Days Ago)

Errors by Type:
- DNS: 0
- Connect: 7
- SSL: 0
- Send: 0
- Receive: 0
- HTTP: 0

Click on an agent to select it, click on the background to deselect.
Looking at the network

Network – Path Visualization

www.countryfinancial.com:443
Country Financial

Agents
All agents visible
Group by continent

Metric
Loss
Latency
Jitter
Bandwidth

Date
SEP 04
17:35 UTC
(35 Days Ago)

Quick Selection
5 nodes with forwarding loss > 0%
5 links are part of an MPLS tunnel
3 agents with failed path MTU discovery

5 nodes selected
Deselect All

Average Loss

Source
Destination
Show 0 hops
Show 3 hops

Mark nodes with loss > 0%
Color links with delay > 100 ms

North America

Atlanta, GA
Las Vegas, NV
Newark, NJ
San Diego, CA
Philadelphia, PA

208.74.228.151

ThousandEyes
Looking at the network

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Prefix</th>
<th>Network</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>be2005.ccr21.ord03.atlas.cogentco.com</td>
<td>66.28.4.74</td>
<td>66.28.0.0/16</td>
<td>Cogent Communications (AS 174)</td>
<td>United States</td>
</tr>
<tr>
<td>173.249.64.245</td>
<td>173.249.64.245</td>
<td>173.249.64.0/20</td>
<td>Access2Go, Inc. (AS 4094B)</td>
<td>United States</td>
</tr>
<tr>
<td>be2003.ccr21.ord03.atlas.cogentco.com</td>
<td>154.54.29.22</td>
<td>154.48.0.0/12</td>
<td>Cogent Communications (AS 174)</td>
<td>United States</td>
</tr>
<tr>
<td>208.74.228.191</td>
<td>208.74.228.191</td>
<td>208.74.228.0/24</td>
<td>CC Services, Inc (AS 10511)</td>
<td>United States</td>
</tr>
<tr>
<td>be2114.ccr41.ord01.atlas.cogentco.com</td>
<td>66.28.4.202</td>
<td>66.28.0.0/16</td>
<td>Cogent Communications (AS 174)</td>
<td>United States</td>
</tr>
</tbody>
</table>
Diving deeper into BGP
After things are stable
Let's look at a DDoS attack
Network View shows congested Nodes in Upstream ISPs

Nodes with >25% packet loss

High packet loss from all testing points

Packet loss in upstream ISPs Verizon and AT&T

HSBC bank website under attack
DDoS Attack: Mitigation Handoff Using BGP

Prior Autonomous System (HSBC)

New Autonomous System (VeriSign)

Withdrawn routes

New routes

HSBC prefix
Paypal Issues

Errors by Type

- DNS: 0
- Connect: 1
- SSL: 0
- Send: 0
- Receive: 0
- HTTP: 0

Click on an agent to select it, click on the background to deselect.
Let's look at the network
Akamai advertising address block
Indosat advertising the same prefix block
Thanks!

mohit@thousandeyes.com