Linux Networking: traceroute

David Morgan

ping

- Basic connectivity test
  - do I have a connection?
  - how long is the roundtrip?
- Same concept can be extended
  - find the hop by hop route to destination
  - approximate the bandwidth of the connection
ping

sequence number

hop countdown  trip time

traceroute

● If ping fails to make an end to end the next step is usually traceroute
● reports step by step progress through the route
● uses UDP frames manipulating the TTL field to get all the routers to identify themselves
IP Header

Following the 14 byte Ethernet Header is a 20 byte IP header (there are packets other than IP too)

We'll look at the IP header in more detail later but right now we want to focus on the IP addresses and the Time To Live or TTL field
**IP’s TTL rules**

- TTL field acts as a packet timer
- Prevents misrouted packets from circling the internet forever
- Every routing hop decrements the TTL field by one
- Only layer 3 devices (routers) can decrement the TTL
  - Why can't a switch or hub decrement???

**TTL = 0**

When the TTL reaches zero the packet must be thrown away....

your packet ==> … by any router that sees it.
TTL = 0

.....but router has to tell the sender so.

To sender @ 192.168.100.23

Kiss your packet bye-bye

From router @ 10.100.13.1

...your ICMP
"Postcard from the Edge"

The router that throws my TTL=0 packet away sends me a message with its IP

If I set my TTL to 1, the packet would get thrown away and I would be notified by the first router in the path

If I set the TTL in the next packet to 2, it would get tossed and I would be notified by the second router in the path

I could find the ID of every router in the path this way
traceroute - the pathfinder

the router that threw #1 away
When-to-quit FAQ

Q. *How do you know when to stop?*
A. When you reach the target

Q. *How do you know when you reach the target?*
A. Get it to tell you so:
   
   Send UDP to an unused port and an ICMP “destination unreachable” should come back

   or

   Send ICMP “echo request” and an ICMP “echo reply” should come back.
Getting a rise out of ‘em

<table>
<thead>
<tr>
<th>intermediate router tweak</th>
<th>end-target tweaks</th>
</tr>
</thead>
<tbody>
<tr>
<td>time exceeded</td>
<td>dest unreachable</td>
</tr>
<tr>
<td>code 11</td>
<td>echo reply</td>
</tr>
</tbody>
</table>

Type 0:
- Code 0 = timeout exceeded in transit;
- 1 = fragment reassembly time exceeded

Type 3:
- Code 0 = net unreachable;
- 1 = host unreachable;
- 2 = protocol unreachable;
- 3 = port unreachable;
- 4 = fragmentation needed;
- 5 = source route failed.

traceroute report — we made em all answer
**traceroute – using UDP**

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-49</td>
<td>127.0.0.1</td>
<td>192.168.1</td>
<td>ICMP</td>
<td>Time-to-Live expired</td>
</tr>
<tr>
<td>49-98</td>
<td>192.168.1</td>
<td>127.0.0.1</td>
<td>UDP</td>
<td>Source port 443, destination port 123456</td>
</tr>
<tr>
<td>98-147</td>
<td>127.0.0.1</td>
<td>192.168.1</td>
<td>UDP</td>
<td>Source port 443, destination port 123456</td>
</tr>
<tr>
<td>147-196</td>
<td>192.168.1</td>
<td>127.0.0.1</td>
<td>UDP</td>
<td>Source port 443, destination port 123456</td>
</tr>
<tr>
<td>196-246</td>
<td>127.0.0.1</td>
<td>192.168.1</td>
<td>UDP</td>
<td>Source port 443, destination port 123456</td>
</tr>
<tr>
<td>246-296</td>
<td>192.168.1</td>
<td>127.0.0.1</td>
<td>UDP</td>
<td>Source port 443, destination port 123456</td>
</tr>
</tbody>
</table>

**traceroute – using ICMP**

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-49</td>
<td>127.0.0.1</td>
<td>192.168.1</td>
<td>ICMP</td>
<td>Time-to-Live expired</td>
</tr>
<tr>
<td>49-98</td>
<td>192.168.1</td>
<td>127.0.0.1</td>
<td>UDP</td>
<td>Source port 443, destination port 123456</td>
</tr>
<tr>
<td>98-147</td>
<td>127.0.0.1</td>
<td>192.168.1</td>
<td>UDP</td>
<td>Source port 443, destination port 123456</td>
</tr>
<tr>
<td>147-196</td>
<td>192.168.1</td>
<td>127.0.0.1</td>
<td>UDP</td>
<td>Source port 443, destination port 123456</td>
</tr>
<tr>
<td>196-246</td>
<td>127.0.0.1</td>
<td>192.168.1</td>
<td>UDP</td>
<td>Source port 443, destination port 123456</td>
</tr>
<tr>
<td>246-296</td>
<td>192.168.1</td>
<td>127.0.0.1</td>
<td>UDP</td>
<td>Source port 443, destination port 123456</td>
</tr>
</tbody>
</table>

traceroute uses port numbers that are unlikely & varying to assure hitting an unused one.
Expect it not to be too consistent

- different routes at different times
- different timings
- different routes to-and-fro
- different representation (addressing) of route to-and-fro even if same route

Some options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p</td>
<td>set port number for UDP probe packets (default 33434 and up)</td>
</tr>
<tr>
<td>-f</td>
<td>set initial probe packet’s ttl value (default 1)</td>
</tr>
<tr>
<td>-q</td>
<td>set number of probes sent at each ttl setting (default 3)</td>
</tr>
<tr>
<td>-m</td>
<td>set max ttl setting used (default 30)</td>
</tr>
<tr>
<td>-I</td>
<td>use ICMP (default UDP)</td>
</tr>
<tr>
<td>-n</td>
<td>print addresses numerically, don’t resolve to names</td>
</tr>
</tbody>
</table>
Some far-away destinations

- Armenia 195.250.64.38
- New Delhi 202.41.110.89
- Bangalore 144.16.64.2
- Kirghizstan 212.42.96.2
- Nairobi 62.56.157.11