TNE30019/TNE80014 – Unix for Telecommunications

Network and Traffic Analysis Tools – ping, traceroute and tracepath

Dr. Jason But

Swinburne University

Outline

- Basic Network analysis tools
  - `ping` – test connectivity
  - `traceroute` – `ping` plus network path discovery
  - `tracepath` – replacement for `traceroute`

`ping`

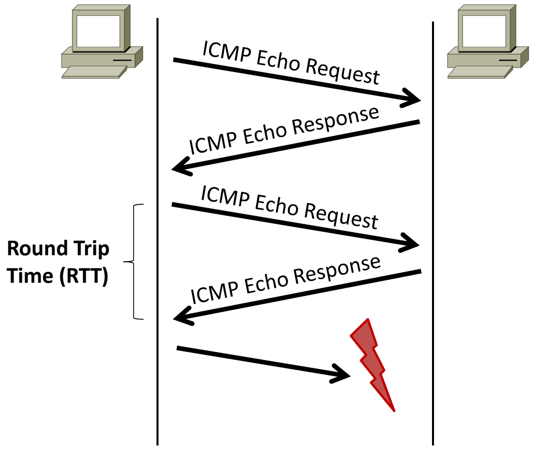
- Traditional network testing tool
- Sends ICMP[1] echo request packets to specified host
- Host responds with ICMP echo replies
- Ping calculates Δt for each request/reply pair and displays this as ping Round Trip Time (RTT)

Uses

- Test whether pinged host is active
- Measure network “distance” to pinged host
- Test network responsiveness to different sized packets
- Broadcast ping
  - Locate all connected hosts in subnet
  - Hosts will only respond if programmed to (in kernel)

[1] J.Postel, *“Internet Control Message Protocol”*, IETF Request For Commant (RFC 777), `http://www.ietf.org/rfc`

`ping` – Message Exchange



ping – Example Output

```
> ping 136.186.229.1
PING 136.186.229.1 (136.186.229.1) 56(84) bytes of data.
64 bytes from 136.186.229.1: icmp_seq=1 ttl=255 time=0.288 ms
64 bytes from 136.186.229.1: icmp_seq=2 ttl=255 time=0.287 ms
64 bytes from 136.186.229.1: icmp_seq=3 ttl=255 time=0.308 ms
64 bytes from 136.186.229.1: icmp_seq=4 ttl=255 time=0.281 ms
```

traceroute

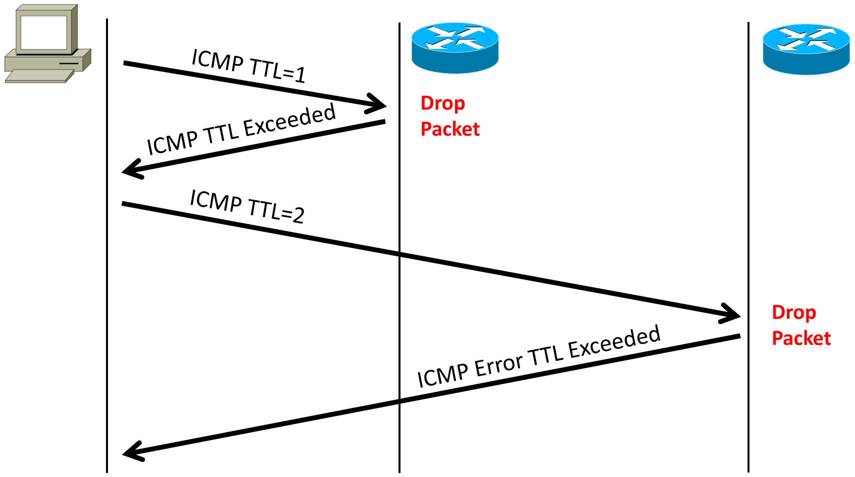
IP Time-to-live (TTL) field

- Field in IP header
- Set to initial TTL value by sender of packet
- Decremented by one by each router
- If TTL=0 router will drop packet and send error

traceroute

- Sends sequence of ICMP echo requests with increasing TTL
- Prints list of all routers on path to specified host
- Estimated RTT to each router is also calculated
- Routing can change, so path may be different each time
- Will reverse resolve DNS names of each router – can give hints to location

traceroute – Message Exchange



and so on...

traceroute – Example Output

```
> traceroute ruleprimary1.caia.swin.edu.au
traceroute to ruleprimary1.caia.swin.edu.au (136.186.230.16), 64 hops max,
   52 byte packets
 1  136.186.229.4 (136.186.229.4)  0.301 ms  0.298 ms  0.290 ms
 2  136.186.107.77 (136.186.107.77)  0.279 ms  14.254 ms  0.592 ms
 3  136.186.251.146 (136.186.251.146)  0.443 ms
    136.186.251.170 (136.186.251.170)  0.353 ms  0.335 ms
 4  vpn252-186.cc.swin.edu.au (136.186.252.186)  0.897 ms  0.796 ms  0.756 ms
 5  vpn252-225.cc.swin.edu.au (136.186.252.225)  1.341 ms  1.030 ms  0.925 ms
 6  136.186.254.82 (136.186.254.82)  1.844 ms  1.706 ms  2.423 ms
 7  136.186.13.10 (136.186.13.10)  2.685 ms  1.881 ms  1.956 ms
 8  136.186.251.213 (136.186.251.213)  2.217 ms  2.031 ms
    136.186.251.245 (136.186.251.245)  2.075 ms
 9  136.186.104.78 (136.186.104.78)  1.822 ms  1.767 ms  1.757 ms
10  ruleprimary1 (136.186.230.16)  2.195 ms  1.786 ms  1.749 ms
```

tracepath

- Uses same probing technique as `traceroute`
- Uses UDP packets rather than ICMP
  - Some firewalls drop ICMP
  - Routers handle ICMP in slow path (can affect RTT)
- Newer traceroute versions also use UDP by default, but can be instructed to use ICMP
- Measures and reports path Maximum Transfer Unit (MTU)