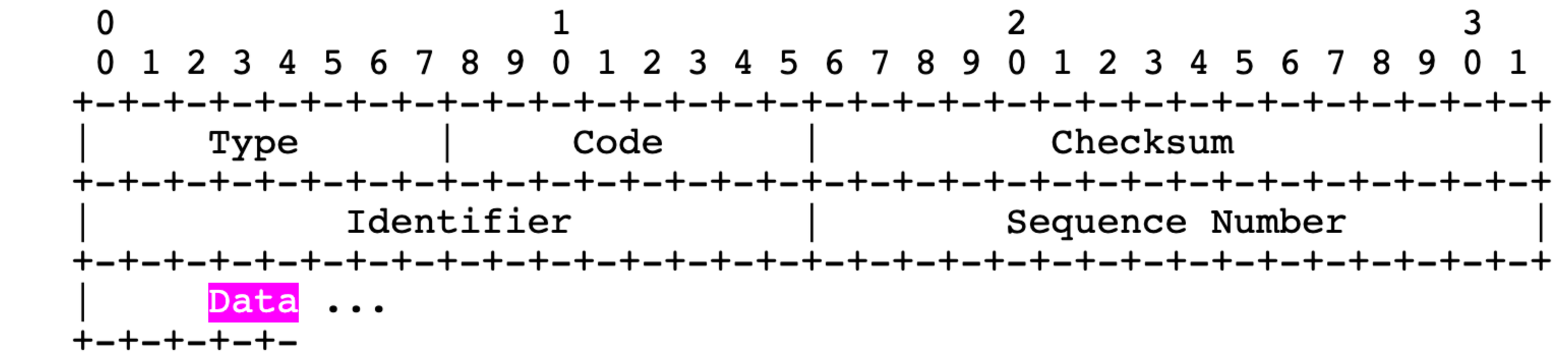
System Administration

Week 06, Segment 4
Networking II: ICMP

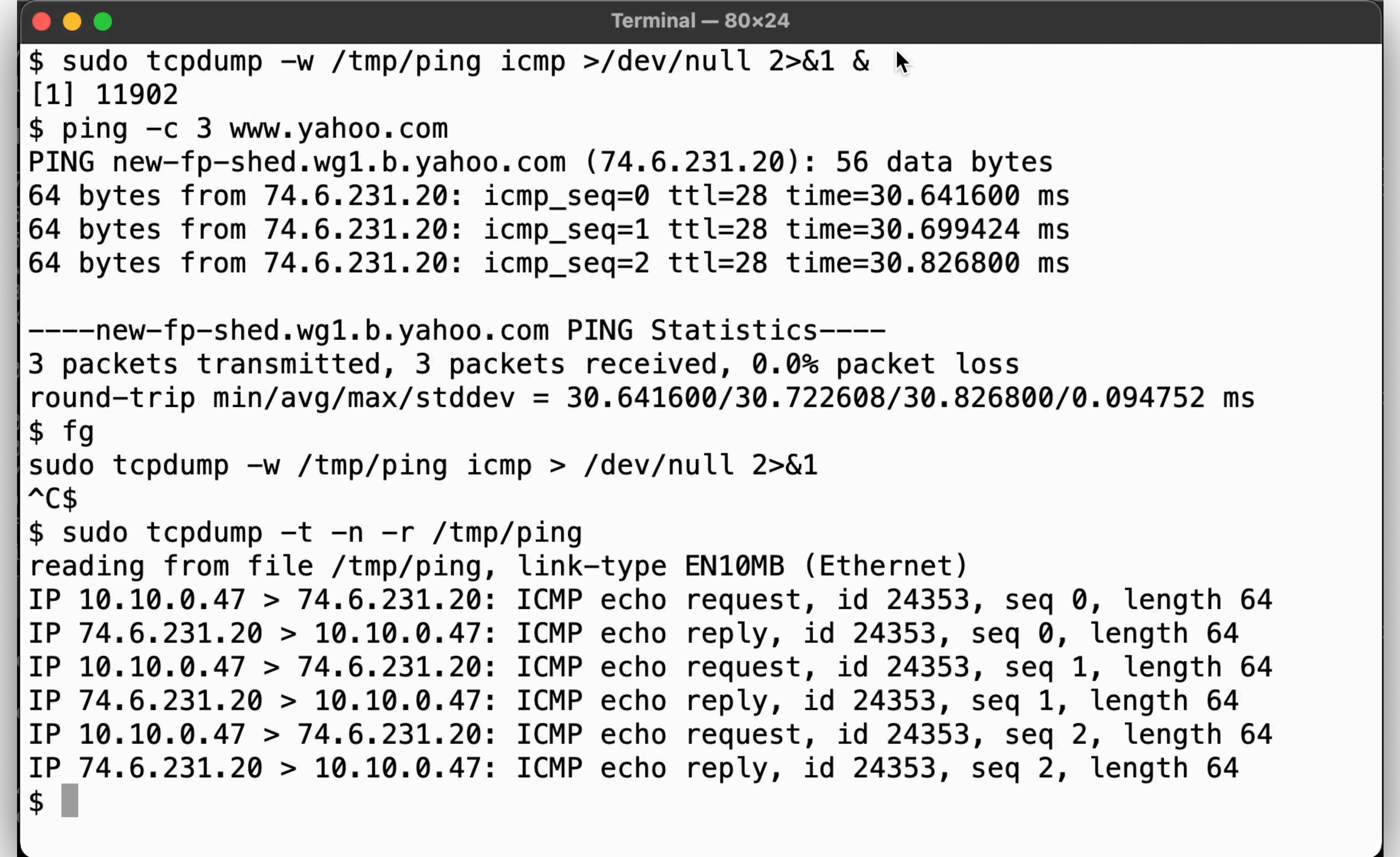
Department of Computer Science
Stevens Institute of Technology

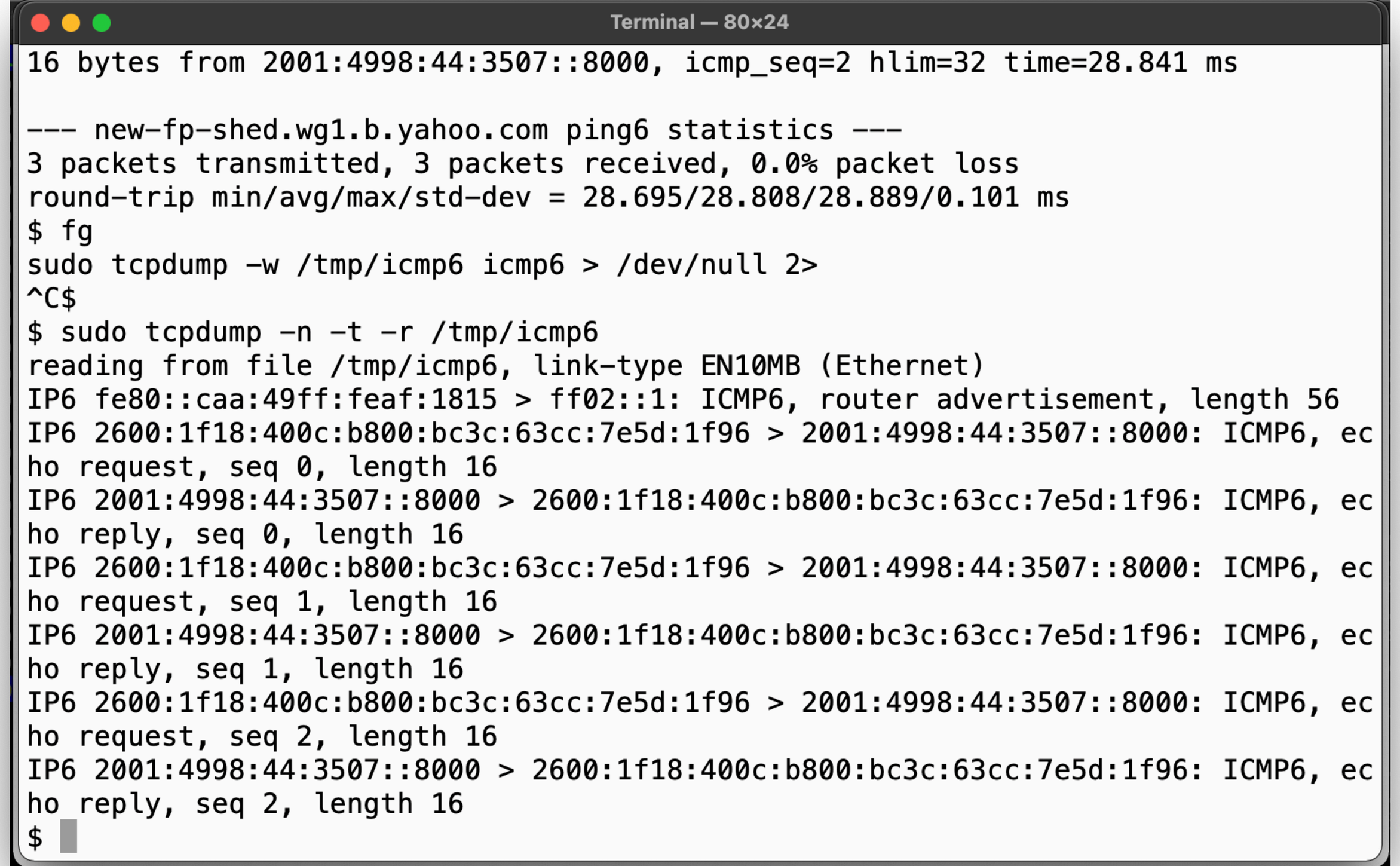
Jan Schaumann
jschauma@stevens.edu
https://stevens.netmeister.org/615/

Echo or Echo Reply Message

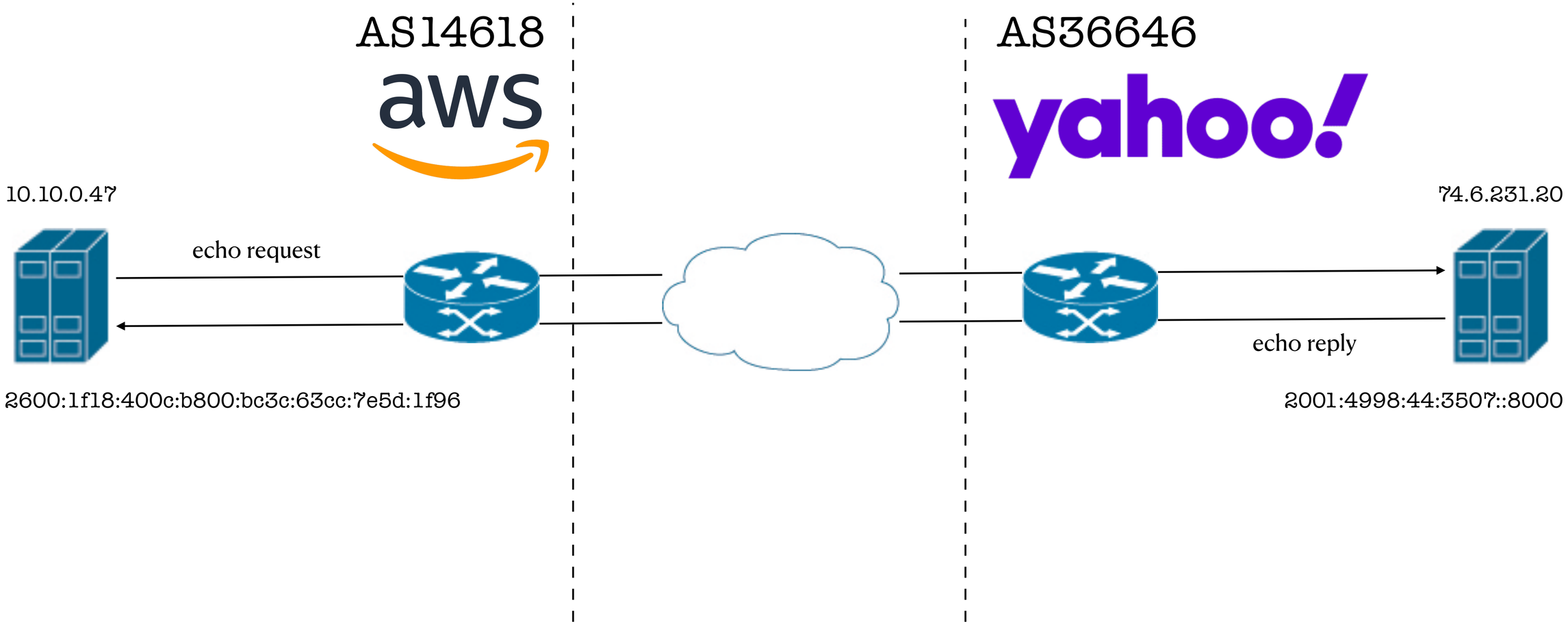


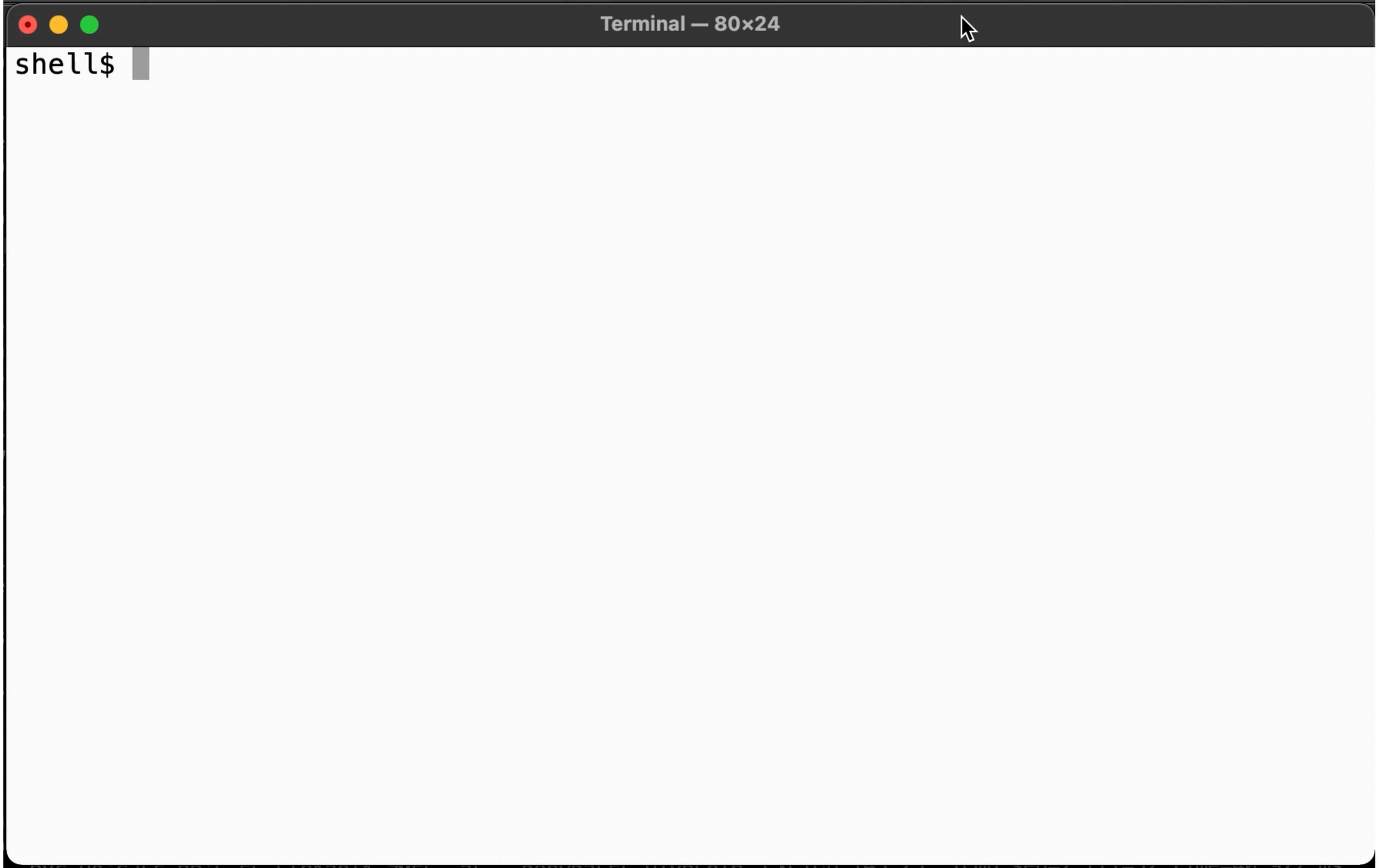

```
sudo tcpdump -w /tmp/ping icmp > /dev/null 2>&1
^C$
$ sudo tcpdump -t -n -r /tmp/ping
reading from file /tmp/ping, link-type EN10MB (Ethernet)
IP 10.10.0.47 > 74.6.143.26: ICMP echo request, id 7296, seq 0, length 64
IP 74.6.143.26 > 10.10.0.47: ICMP echo reply, id 7296, seq 0, length 64
IP 10.10.0.47 > 74.6.143.26: ICMP echo request, id 7296, seq 1, length 64
IP 74.6.143.26 > 10.10.0.47: ICMP echo reply, id 7296, seq 1, length 64
IP 10.10.0.47 > 74.6.143.26: ICMP echo request, id 7296, seq 2, length 64
IP 74.6.143.26 > 10.10.0.47: ICMP echo reply, id 7296, seq 2, length 64
$
```

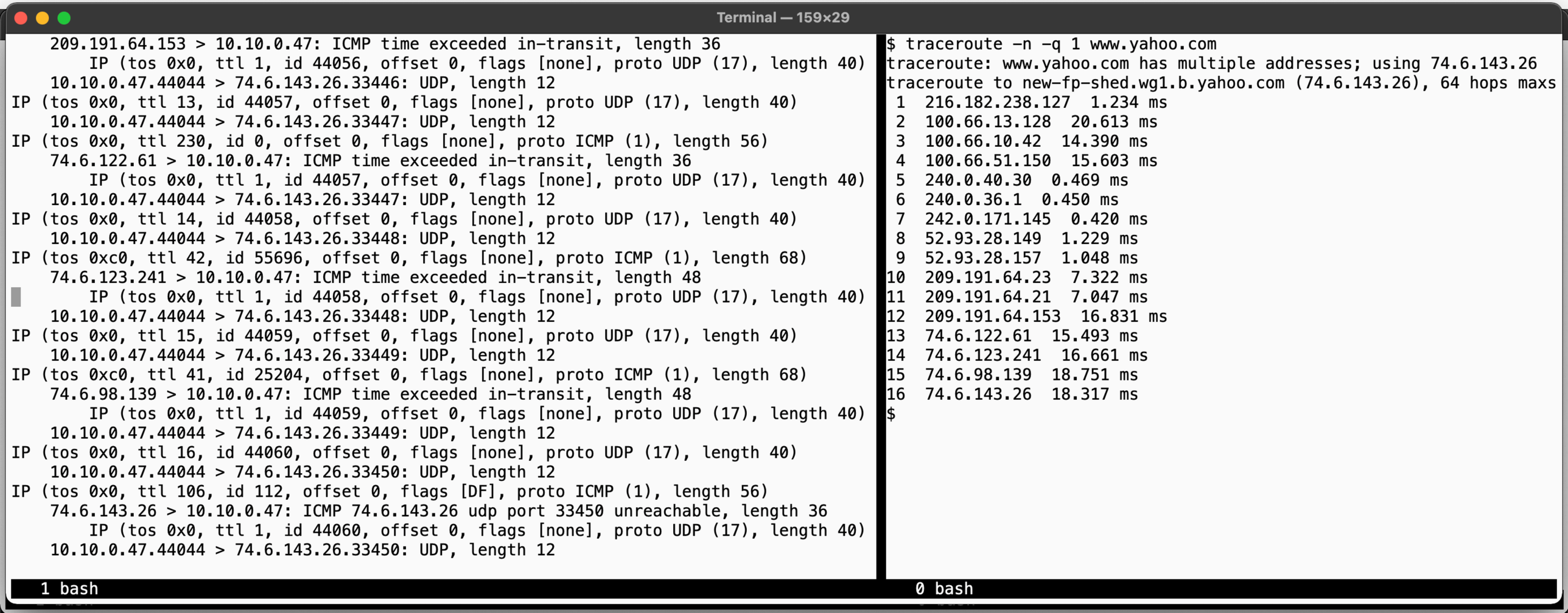

Terminal — 80×24
$ sudo tcpdump -w /tmp/ping icmp >/dev/null 2>&1 &
[1] 11902
$ ping -c 3 www.yahoo.com
PING new-fp-shed.wg1.b.yahoo.com (74.6.231.20): 56 data bytes
64 bytes from 74.6.231.20: icmp_seq=0 ttl=28 time=30.641600 ms
64 bytes from 74.6.231.20: icmp_seq=1 ttl=28 time=30.699424 ms
64 bytes from 74.6.231.20: icmp_seq=2 ttl=28 time=30.826800 ms
----new-fp-shed.wg1.b.yahoo.com PING Statistics----
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 30.641600/30.722608/30.826800/0.094752 ms
$ fg
sudo tcpdump -w /tmp/ping icmp > /dev/null 2>&1
^C$
$ sudo tcpdump -t -n -r /tmp/ping
reading from file /tmp/ping, link-type EN10MB (Ethernet)
IP 10.10.0.47 > 74.6.231.20: ICMP echo request, id 24353, seq 0, length 64
IP 74.6.231.20 > 10.10.0.47: ICMP echo reply, id 24353, seq 0, length 64
IP 10.10.0.47 > 74.6.231.20: ICMP echo request, id 24353, seq 1, length 64
IP 74.6.231.20 > 10.10.0.47: ICMP echo reply, id 24353, seq 1, length 64
IP 10.10.0.47 > 74.6.231.20: ICMP echo request, id 24353, seq 2, length 64
IP 74.6.231.20 > 10.10.0.47: ICMP echo reply, id 24353, seq 2, length 64
$

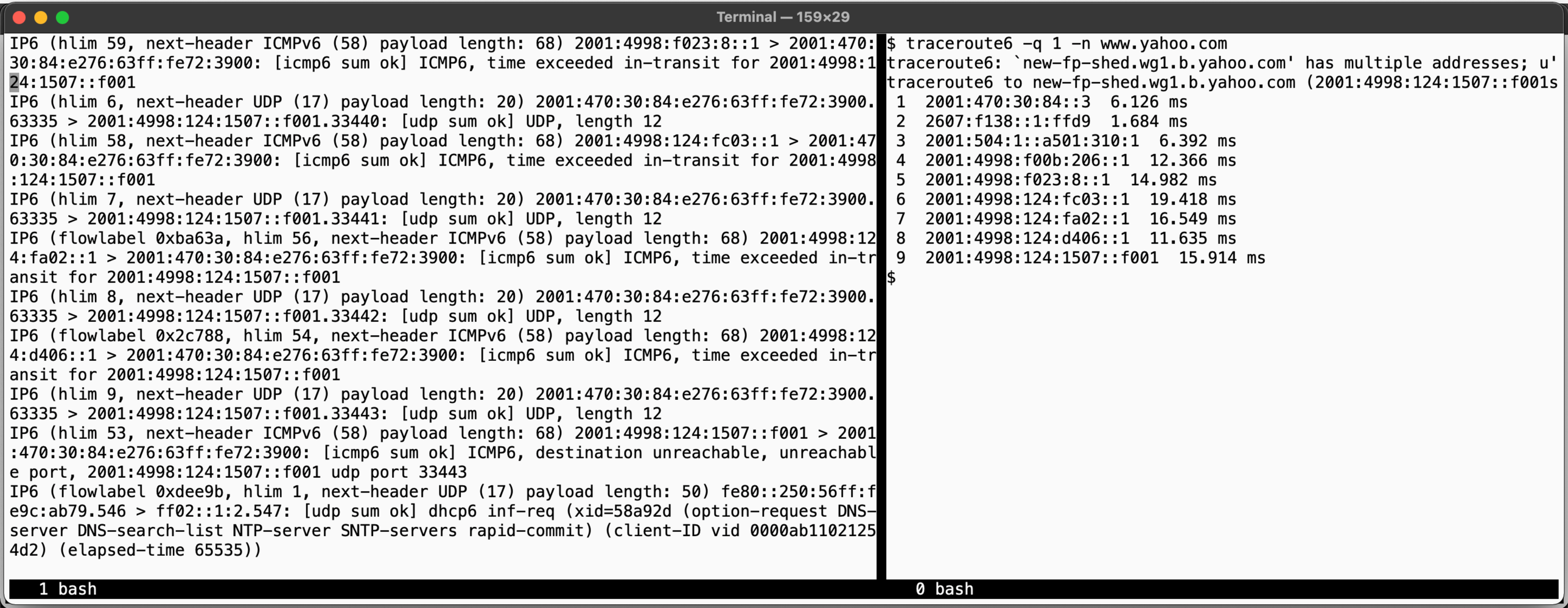

Terminal — 80×24
16 bytes from 2001:4998:44:3507::8000, icmp_seq=2 hlim=32 time=28.841 ms
--- new-fp-shed.wg1.b.yahoo.com ping6 statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 28.695/28.808/28.889/0.101 ms
$ fg
sudo tcpdump -w /tmp/icmp6 icmp6 > /dev/null 2>
^C$
$ sudo tcpdump -n -t -r /tmp/icmp6
reading from file /tmp/icmp6, link-type EN10MB (Ethernet)
IP6 fe80::caa:49ff:feaf:1815 > ff02::1: ICMP6, router advertisement, length 56
IP6 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96 > 2001:4998:44:3507::8000: ICMP6, ec
ho request, seq 0, length 16
IP6 2001:4998:44:3507::8000 > 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96: ICMP6, ec
ho reply, seq 0, length 16
IP6 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96 > 2001:4998:44:3507::8000: ICMP6, ec
ho request, seq 1, length 16
IP6 2001:4998:44:3507::8000 > 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96: ICMP6, ec
ho reply, seq 1, length 16
IP6 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96 > 2001:4998:44:3507::8000: ICMP6, ec
ho request, seq 2, length 16
IP6 2001:4998:44:3507::8000 > 2600:1f18:400c:b800:bc3c:63cc:7e5d:1f96: ICMP6, ec
ho reply, seq 2, length 16
$

ICMP (RFC792) / ICMPv6 (RFC4443)




Terminal — 80×24
shell$


Terminal — 159×29
209.191.64.153 > 10.10.0.47: ICMP time exceeded in-transit, length 36
IP (tos 0x0, ttl 1, id 44056, offset 0, flags [none], proto UDP (17), length 40)
10.10.0.47.44044 > 74.6.143.26.33446: UDP, length 12
IP (tos 0x0, ttl 13, id 44057, offset 0, flags [none], proto UDP (17), length 40)
10.10.0.47.44044 > 74.6.143.26.33447: UDP, length 12
IP (tos 0x0, ttl 230, id 0, offset 0, flags [none], proto ICMP (1), length 56)
74.6.122.61 > 10.10.0.47: ICMP time exceeded in-transit, length 36
IP (tos 0x0, ttl 1, id 44057, offset 0, flags [none], proto UDP (17), length 40)
10.10.0.47.44044 > 74.6.143.26.33447: UDP, length 12
IP (tos 0x0, ttl 14, id 44058, offset 0, flags [none], proto UDP (17), length 40)
10.10.0.47.44044 > 74.6.143.26.33448: UDP, length 12
IP (tos 0xc0, ttl 42, id 55696, offset 0, flags [none], proto ICMP (1), length 68)
74.6.123.241 > 10.10.0.47: ICMP time exceeded in-transit, length 48
IP (tos 0x0, ttl 1, id 44058, offset 0, flags [none], proto UDP (17), length 40)
10.10.0.47.44044 > 74.6.143.26.33448: UDP, length 12
IP (tos 0x0, ttl 15, id 44059, offset 0, flags [none], proto UDP (17), length 40)
10.10.0.47.44044 > 74.6.143.26.33449: UDP, length 12
IP (tos 0xc0, ttl 41, id 25204, offset 0, flags [none], proto ICMP (1), length 68)
74.6.98.139 > 10.10.0.47: ICMP time exceeded in-transit, length 48
IP (tos 0x0, ttl 1, id 44059, offset 0, flags [none], proto UDP (17), length 40)
10.10.0.47.44044 > 74.6.143.26.33449: UDP, length 12
IP (tos 0x0, ttl 16, id 44060, offset 0, flags [none], proto UDP (17), length 40)
10.10.0.47.44044 > 74.6.143.26.33450: UDP, length 12
IP (tos 0x0, ttl 106, id 112, offset 0, flags [DF], proto ICMP (1), length 56)
74.6.143.26 > 10.10.0.47: ICMP 74.6.143.26 udp port 33450 unreachable, length 36
IP (tos 0x0, ttl 1, id 44060, offset 0, flags [none], proto UDP (17), length 40)
10.10.0.47.44044 > 74.6.143.26.33450: UDP, length 12
1 bash
$ traceroute -n -q 1 www.yahoo.com
traceroute: www.yahoo.com has multiple addresses; using 74.6.143.26
traceroute to new-fp-shed.wg1.b.yahoo.com (74.6.143.26), 64 hops maxs
1 216.182.238.127 1.234 ms
2 100.66.13.128 20.613 ms
3 100.66.10.42 14.390 ms
4 100.66.51.150 15.603 ms
5 240.0.40.30 0.469 ms
6 240.0.36.1 0.450 ms
7 242.0.171.145 0.420 ms
8 52.93.28.149 1.229 ms
9 52.93.28.157 1.048 ms
10 209.191.64.23 7.322 ms
11 209.191.64.21 7.047 ms
12 209.191.64.153 16.831 ms
13 74.6.122.61 15.493 ms
14 74.6.123.241 16.661 ms
15 74.6.98.139 18.751 ms
16 74.6.143.26 18.317 ms
$
0 bash


Terminal — 159×29
IP6 (hlim 59, next-header ICMPv6 (58) payload length: 68) 2001:4998:f023:8::1 > 2001:470:
30:84:e276:63ff:fe72:3900: [icmp6 sum ok] ICMP6, time exceeded in-transit for 2001:4998:1
24:1507::f001
IP6 (hlim 6, next-header UDP (17) payload length: 20) 2001:470:30:84:e276:63ff:fe72:3900.
63335 > 2001:4998:124:1507::f001.33440: [udp sum ok] UDP, length 12
IP6 (hlim 58, next-header ICMPv6 (58) payload length: 68) 2001:4998:124:fc03::1 > 2001:47
0:30:84:e276:63ff:fe72:3900: [icmp6 sum ok] ICMP6, time exceeded in-transit for 2001:4998
:124:1507::f001
IP6 (hlim 7, next-header UDP (17) payload length: 20) 2001:470:30:84:e276:63ff:fe72:3900.
63335 > 2001:4998:124:1507::f001.33441: [udp sum ok] UDP, length 12
IP6 (flowlabel 0xba63a, hlim 56, next-header ICMPv6 (58) payload length: 68) 2001:4998:12
4:fa02::1 > 2001:470:30:84:e276:63ff:fe72:3900: [icmp6 sum ok] ICMP6, time exceeded in-tr
ansit for 2001:4998:124:1507::f001
IP6 (hlim 8, next-header UDP (17) payload length: 20) 2001:470:30:84:e276:63ff:fe72:3900.
63335 > 2001:4998:124:1507::f001.33442: [udp sum ok] UDP, length 12
IP6 (flowlabel 0x2c788, hlim 54, next-header ICMPv6 (58) payload length: 68) 2001:4998:12
4:d406::1 > 2001:470:30:84:e276:63ff:fe72:3900: [icmp6 sum ok] ICMP6, time exceeded in-tr
ansit for 2001:4998:124:1507::f001
IP6 (hlim 9, next-header UDP (17) payload length: 20) 2001:470:30:84:e276:63ff:fe72:3900.
63335 > 2001:4998:124:1507::f001.33443: [udp sum ok] UDP, length 12
IP6 (hlim 53, next-header ICMPv6 (58) payload length: 68) 2001:4998:124:1507::f001 > 2001
:470:30:84:e276:63ff:fe72:3900: [icmp6 sum ok] ICMP6, destination unreachable, unreachabl
e port, 2001:4998:124:1507::f001 udp port 33443
IP6 (flowlabel 0xdee9b, hlim 1, next-header UDP (17) payload length: 50) fe80::250:56ff:f
e9c:ab79.546 > ff02::1:2.547: [udp sum ok] dhcp6 inf-req (xid=58a92d (option-request DNS-
server DNS-search-list NTP-server SNTP-servers rapid-commit) (client-ID vid 0000ab1102125
4d2) (elapsed-time 65535))
$ traceroute6 -q 1 -n www.yahoo.com
traceroute6: `new-fp-shed.wg1.b.yahoo.com' has multiple addresses; u'
traceroute6 to new-fp-shed.wg1.b.yahoo.com (2001:4998:124:1507::f001s
1 2001:470:30:84::3 6.126 ms
2 2607:f138::1:ffd9 1.684 ms
3 2001:504:1::a501:310:1 6.392 ms
4 2001:4998:f00b:206::1 12.366 ms
5 2001:4998:f023:8::1 14.982 ms
6 2001:4998:124:fc03::1 19.418 ms
7 2001:4998:124:fa02::1 16.549 ms
8 2001:4998:124:d406::1 11.635 ms
9 2001:4998:124:1507::f001 15.914 ms
$
1 bash
0 bash

UDP: 33435; HLIM=1

ICMP6: TIME EXCEEDED

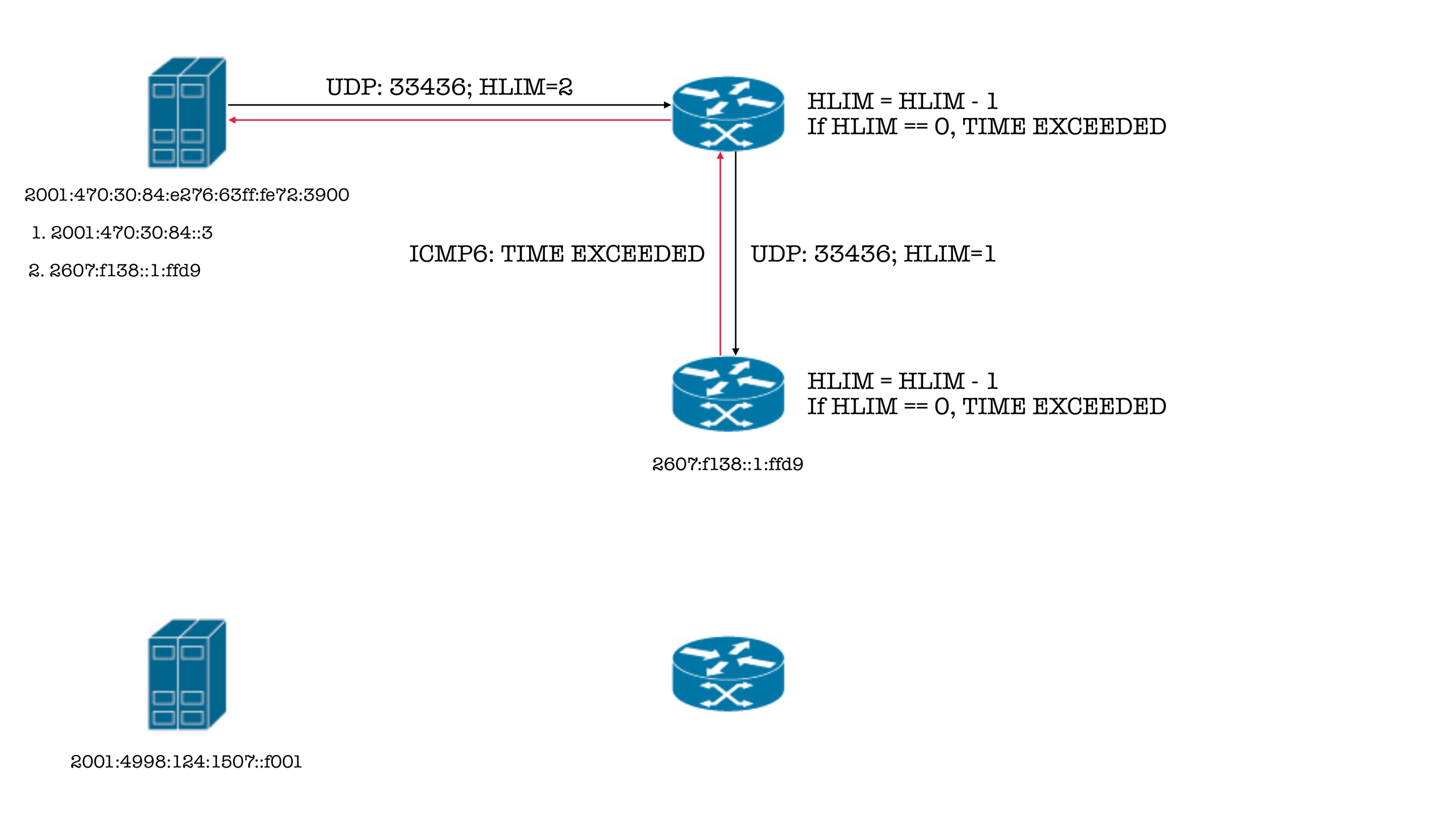
HLIM = HLIM - 1
If HLIM == 0, TIME EXCEEDED

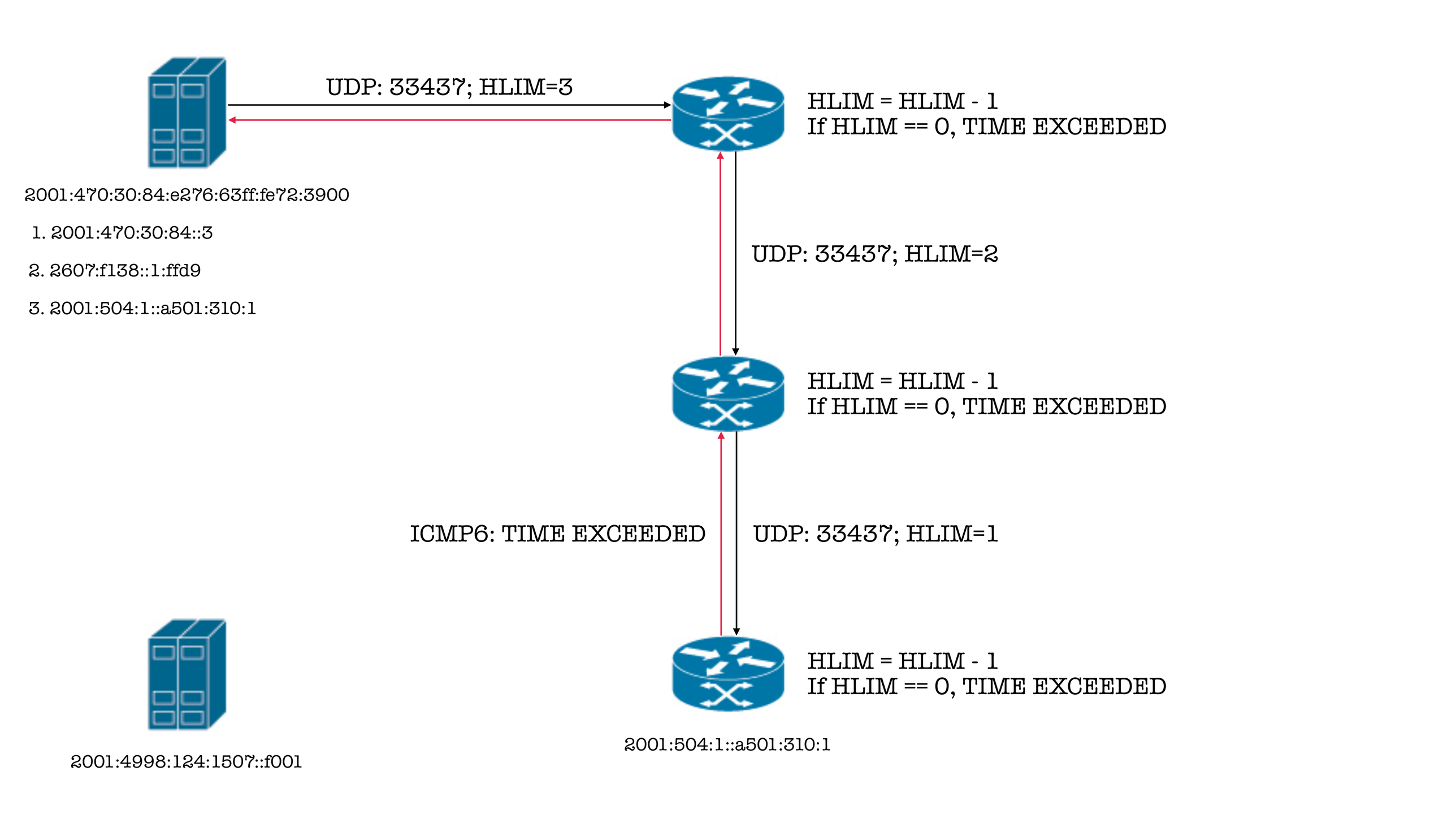
2001:470:30:84:e276:63ff:fe72:3900

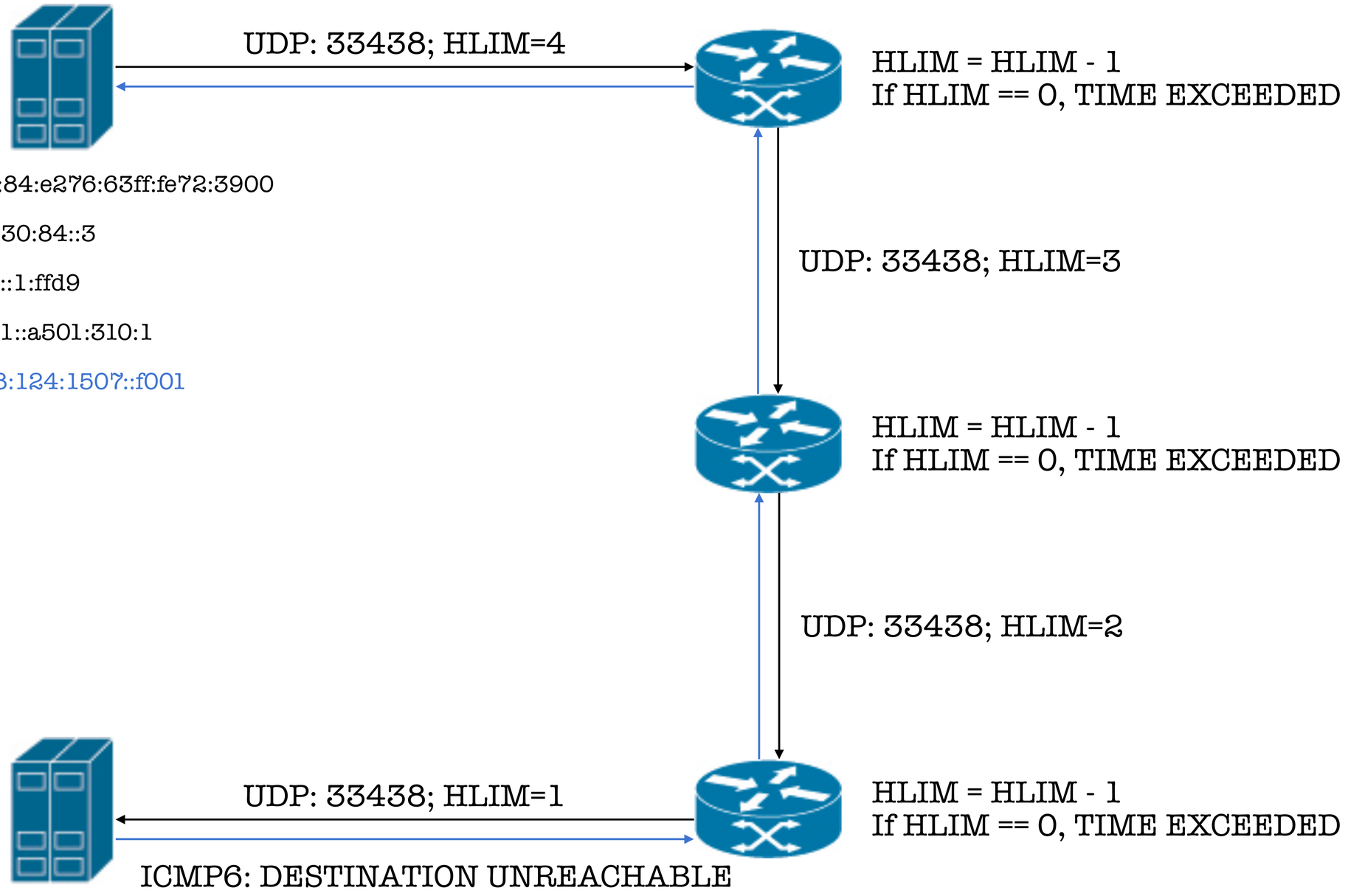
2001:470:30:84::3

1. 2001:470:30:84::3

2001:4998:124:1507::f001


UDP: 33436; HLIM=2
HLIM = HLIM - 1
If HLIM == 0, TIME EXCEEDED
2001:470:30:84:e276:63ff:fe72:3900
1. 2001:470:30:84::3
2. 2607:f138::1:ffd9
ICMP6: TIME EXCEEDED
UDP: 33436; HLIM=1
HLIM = HLIM - 1
If HLIM == 0, TIME EXCEEDED
2607:f138::1:ffd9
2001:4998:124:1507::f001


UDP: 33437; HLIM=3
HLIM = HLIM - 1
If HLIM == 0, TIME EXCEEDED
2001:470:30:84:e276:63ff:fe72:3900
1. 2001:470:30:84::3
2. 2607:f138::1:ffd9
3. 2001:504:1::a501:310:1
UDP: 33437; HLIM=2
HLIM = HLIM - 1
If HLIM == 0, TIME EXCEEDED
ICMP6: TIME EXCEEDED
UDP: 33437; HLIM=1
HLIM = HLIM - 1
If HLIM == 0, TIME EXCEEDED
2001:504:1::a501:310:1
2001:4998:124:1507::f001


UDP: 33438; HLIM=4
HLIM = HLIM - 1
If HLIM == 0, TIME EXCEEDED
2001:470:30:84:e276:63ff:fe72:3900
1. 2001:470:30:84::3
2. 2607:f138::1:ffd9
3. 2001:504:1::a501:310:1
4. 2001:4998:124:1507::f001
UDP: 33438; HLIM=3
HLIM = HLIM - 1
If HLIM == 0, TIME EXCEEDED
UDP: 33438; HLIM=2
UDP: 33438; HLIM=1
HLIM = HLIM - 1
If HLIM == 0, TIME EXCEEDED
ICMP6: DESTINATION UNREACHABLE
2001:4998:124:1507::f001

Summary

ICMP (RFC792) / ICMPv6 (RFC4443)

- `ping(1)`: echo-request / echo-reply
- `traceroute(1)`:
  - UDP to random part with increasing TTL/HLIM
  - routers generate `TIME EXCEEDED`
  - destination generates `DESTIONATION UNREACHABLE`
  - can use ICMP or TCP instead of UDP
- IPv4 PATH MTU Discovery works just like `traceroute(1)`.

Exercises

- What other ICMP types are there, and when would you use them?
- Some traceroute output generates ‘*’ for some hops — why is that?
- Look up AS numbers when doing a `traceroute` from your EC2 instance:

What’s up with that?