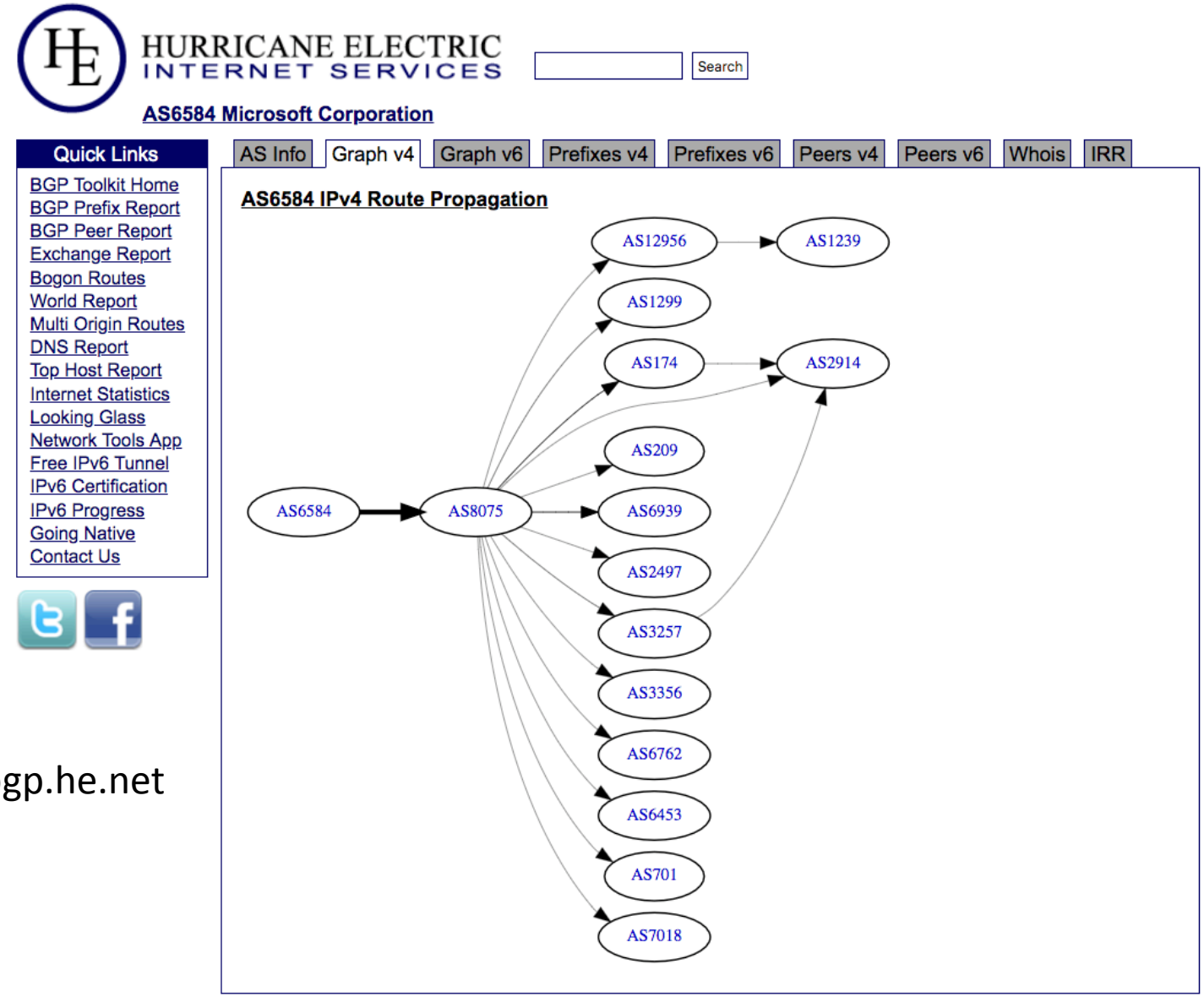
Internet Measurement
& Analysis (IMA)

Internet Topology: Part II

Internet Topology Discovery with Active Measurements

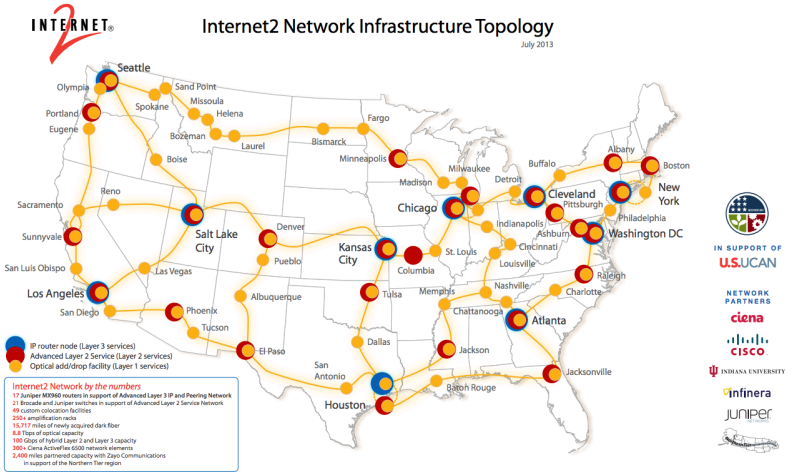
Prof. Georgios Smaragdakis, Ph.D.

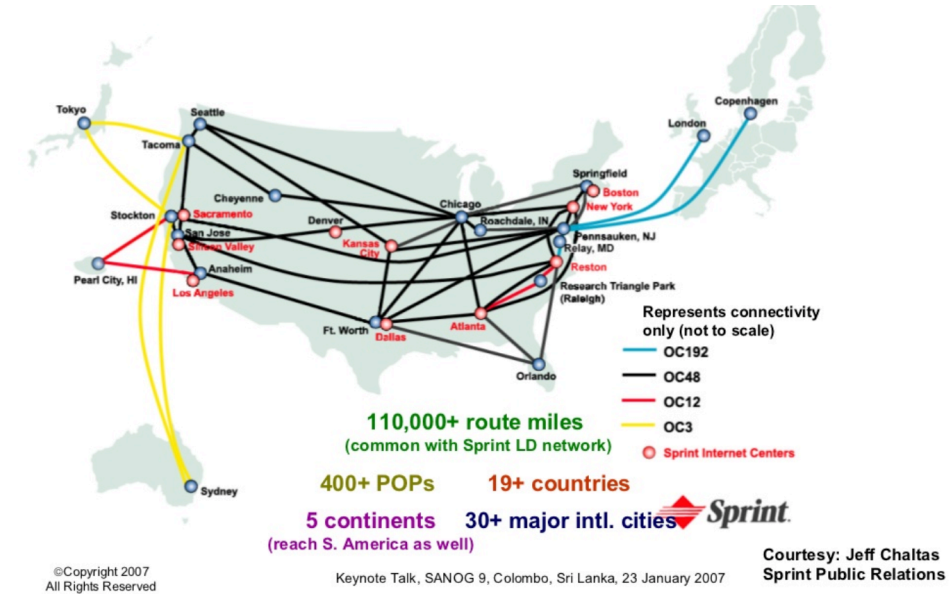
Topologies at the AS Level (logical level)



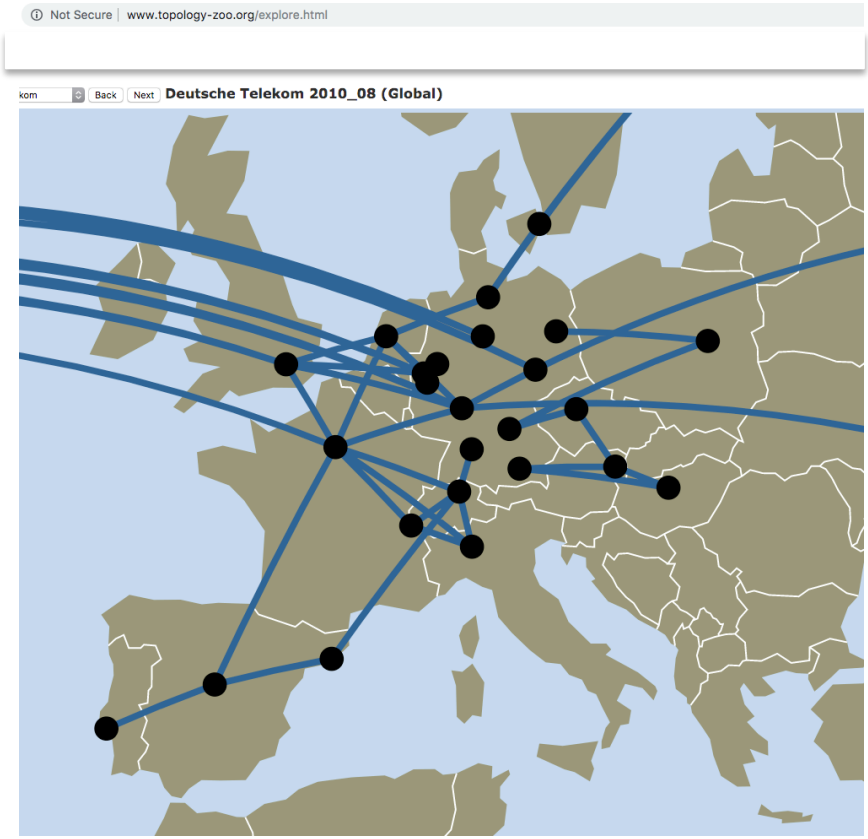
https://bgp.he.net

Topologies at the Router Level

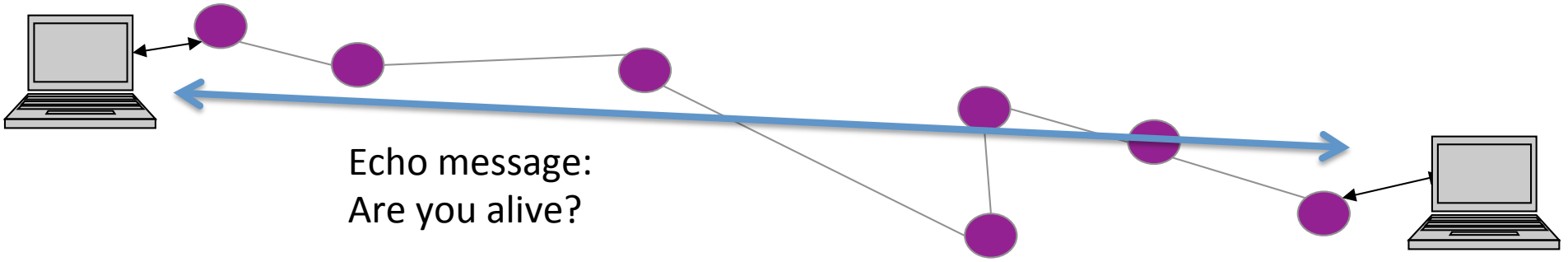




www.topology-zoo.org

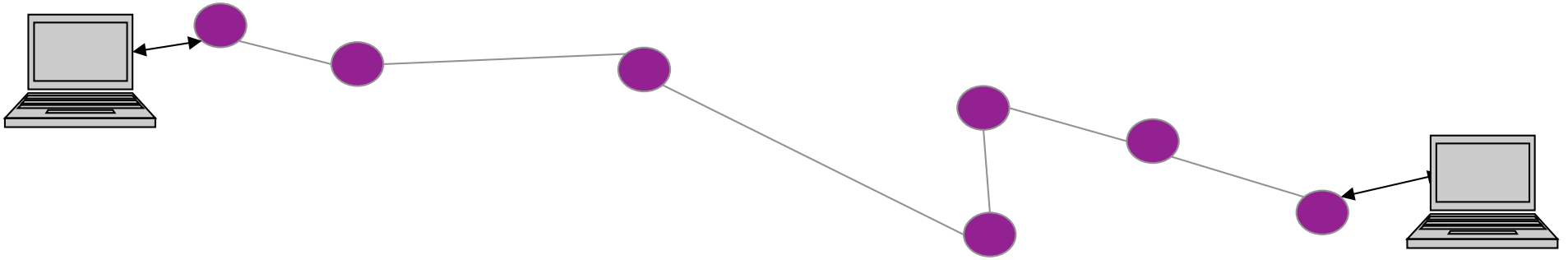


Ping



- Tool that is used to test the reachability of a host
- Uses ICMP messages (part of the Internet suite)
- Uses ICMP ECHO_REQUEST to elicit an ICMP ECHO_RESPONSE, as ping does.
- Sends packets with a maximum TTL (time to live; OS-dependent; configurable) Value. Typical packet length: 8B headed + 56B data
- The TTL value is reduced at each hop until the destination is reached

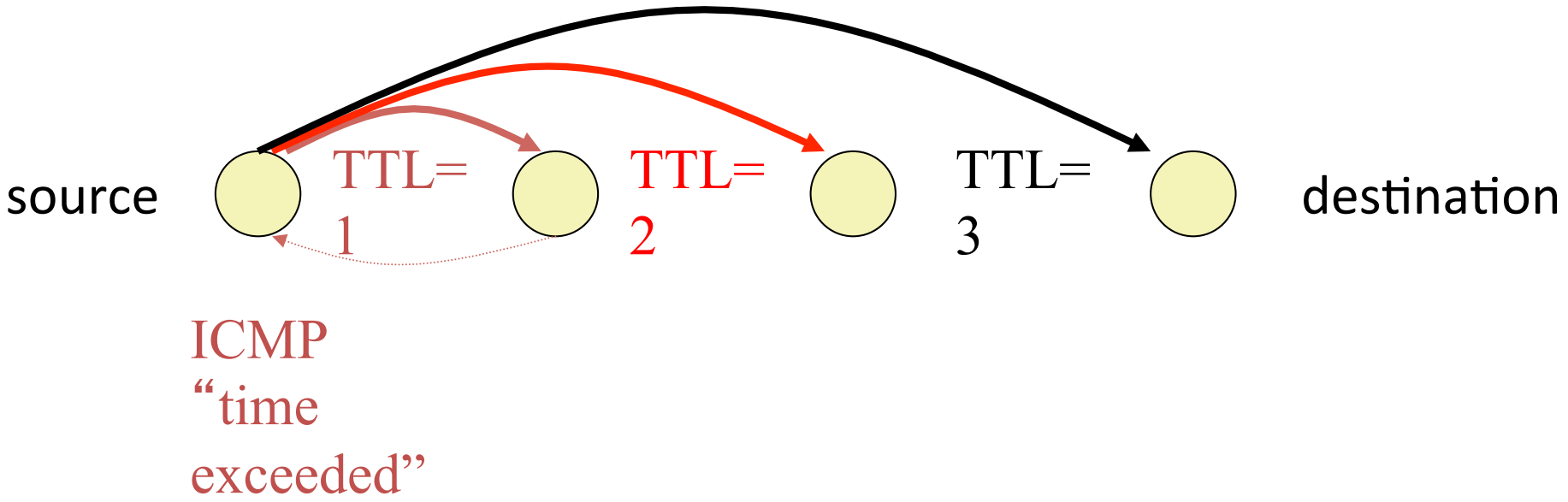
Traceroute



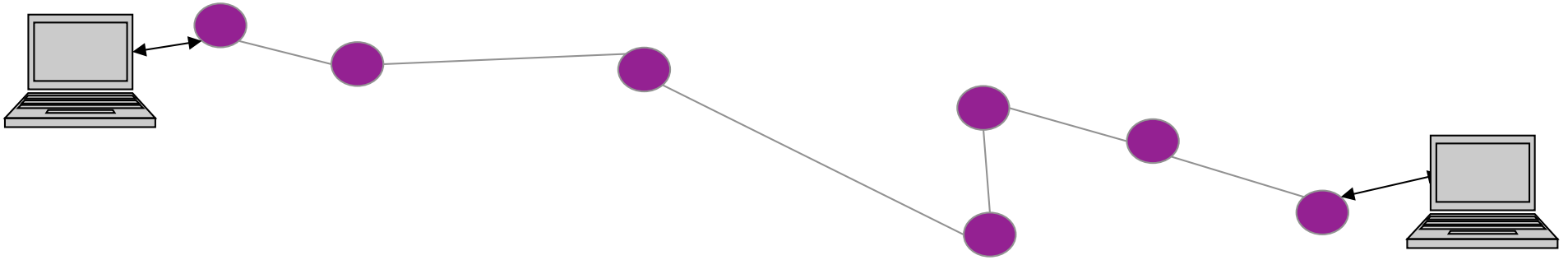
- Traceroute discovers *compliant* (i.e., IP) routers along path between selected network host computers
- It can not measure layer-2 topologies
- With Traceroute we can find paths not visible in BGP and vice versa!
  - Not seen the BGP announcement
  - Load balancing
  - Tunneling

Traceroute

- Uses ICMP ECHO_REQUEST to elicit an ICMP ECHO_RESPONSE, as ping does.
- Send packets with increasing TTL Values



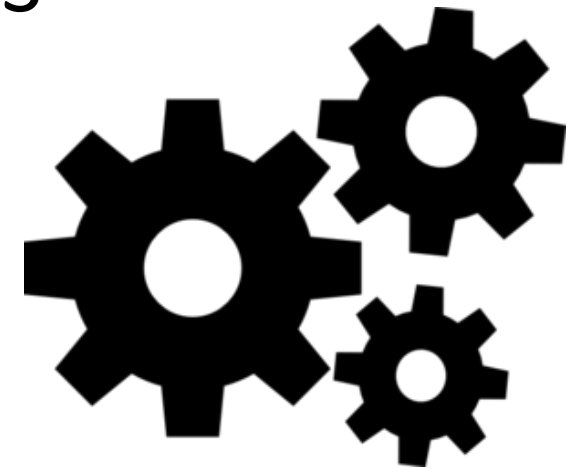
Traceroute



- It uses ICMP messages
  - there are versions using UDP; send a UDP packet to an invalid destination port value: 33434 to 33534
    - Up to 40% of the routers may not reply! (“Beyond Counting: New Perspectives on the Active IPv4 Address Space”, IMC 2016)
  - TCP Traceroute (to port 80) also exists to bypass firewalls

Hands-on Exercise

Traceroute from Berlin to Google without and with IP-to-AS Mapping



TU Berlin-Google

$ traceroute www.google.com

traceroute to www.google.com (172.217.19.196), 64 hops max, 52 byte packets
1 192.168.102.254 (192.168.102.254) 1.390 ms 1.143 ms 1.098 ms
2 ta-inet.gate.tu-berlin.de (130.149.235.193) 1.593 ms 1.460 ms 1.519 ms
3 e-n-hft.gate.tu-berlin.de (130.149.126.57) 2.031 ms 1.909 ms 1.421 ms
4 cr-tub2-te0-0-0-7-5.x-win.dfn.de (188.1.235.117) 1.481 ms 1.963 ms 2.826 ms
5 google.bcix.de (193.178.185.100) 16.246 ms 15.706 ms 15.591 ms
6 108.170.241.193 (108.170.241.193) 15.819 ms 17.410 ms 15.951 ms
7 72.14.238.245 (72.14.238.245) 15.800 ms 16.702 ms 16.558 ms
8 ams16s31-in-f4.1e100.net (172.217.19.196) 15.762 ms 16.281 ms 15.881 ms

Traceroute TU Berlin to Google

$ traceroute www.google.com

traceroute to www.google.com (172.217.19.196), 64 hops max, 52 byte packets
1 192.168.102.254 (192.168.102.254) 1.390 ms 1.143 ms 1.098 ms
2 ta-inet.gate.tu-berlin.de (130.149.235.193) 1.593 ms 1.460 ms 1.519 ms
3 e-n-hft.gate.tu-berlin.de (130.149.126.57) 2.031 ms 1.909 ms 1.421 ms
4 cr-tub2-te0-0-0-7-5.x-win.dfn.de (188.1.235.117) 1.481 ms 1.963 ms 2.826 ms
5 google.bcix.de (193.178.185.100) 16.246 ms 15.706 ms 15.591 ms
6 108.170.241.193 (108.170.241.193) 15.819 ms 17.410 ms 15.951 ms
7 72.14.238.245 (72.14.238.245) 15.800 ms 16.702 ms 16.558 ms
8 ams16s31-in-f4.1e100.net (172.217.19.196) 15.762 ms 16.281 ms 15.881 ms

Traceroute to www.yahoo.com

$traceroute www.yahoo.com

```
traceroute: Warning: www.yahoo.com has multiple addresses; using 87.248.98.7
traceroute to atsv2-fp-shed.wg1.b.yahoo.com (87.248.98.7), 64 hops max, 52 byte packets
 1  192.168.102.254 (192.168.102.254)  1.703 ms  1.283 ms  1.514 ms
 2  ta-inet.gate.tu-berlin.de (130.149.235.193)  1.653 ms  1.536 ms  1.649 ms
 3  e-n-hft.gate.tu-berlin.de (130.149.126.57)  1.729 ms  1.620 ms  1.751 ms
 4  cr-tub2-te0-0-0-7-5.x-win.dfn.de (188.1.235.117)  2.177 ms  2.345 ms  2.024 ms
 5  cr-erl2-be7.x-win.dfn.de (188.1.146.209)  12.463 ms  12.634 ms  12.397 ms
 6  ge-1-3-0.pat1.dee.yahoo.com (80.81.192.115)  18.258 ms  19.083 ms  18.586 ms
 7  unknown-66-196-65-x.yahoo.com (66.196.65.218)  27.225 ms  27.309 ms  27.863 ms
 8  unknown-66-196-65-x.yahoo.com (66.196.65.217)  51.165 ms  46.338 ms  49.013 ms
 9  ge-0-3-9-d104.pat1.the.yahoo.com (66.196.65.21)  46.148 ms
    et-1-1-0.msr1.ir2.yahoo.com (66.196.65.19)  43.678 ms
    ge-0-3-9-d104.pat1.the.yahoo.com (66.196.65.21)  47.566 ms
10  eth-2-5.bas2-1-prd.ir2.yahoo.com (217.146.186.95)  46.415 ms
    eth-1-5.bas2-1-prd.ir2.yahoo.com (217.146.185.180)  43.824 ms
    eth-2-5.bas1-1-prd.ir2.yahoo.com (217.146.186.79)  43.947 ms
11  media-router-fp1.prod1.media.vip.ir2.yahoo.com (87.248.98.7)  43.484 ms  43.322 ms  44.034 ms
```

Traceroute to www.microsoft.com

$traceroute www.microsoft.com

traceroute to e13678.dspb.akamaiedge.net (23.58.217.29), 64 hops max, 52 byte packets

1 192.168.102.254 (192.168.102.254) 1.503 ms 1.293 ms 2.344 ms

2 ta-inet.gate.tu-berlin.de (130.149.235.193) 1.451 ms 1.453 ms 1.462 ms

3 e-n-hft.gate.tu-berlin.de (130.149.126.57) 1.955 ms 3.241 ms 1.416 ms

4 cr-tub2-te0-0-0-7-5.x-win.dfn.de (188.1.235.117) 1.664 ms 1.871 ms 1.577 ms

5 akamai.bcix.de (193.178.185.22) 6.317 ms 7.404 ms 8.285 ms

6 * * *

7 * * *

8 * * *

9 * * *

Different Types of Traceroutes (Linux syntax)

- ICMP:

traceroute -I www.google.com

- UDP:

traceroute -U www.google.com

- TCP:

Traceroute -T -p 80 www.google.com

TU Berlin (2nd vantage point)- Google

$ traceroute -A www.google.com

traceroute to www.google.com (172.217.17.36), 30 hops max, 60 byte packets

1 enwall.net.t-labs.tu-berlin.de (130.149.152.129) [AS680/AS1275] 0.130 ms 0.140 ms 0.126 ms

2 e-n-inet.gate.tu-berlin.de (130.149.235.241) [AS680/AS1275] 75.772 ms 75.801 ms 76.006 ms

3 cr-tub2-te0-0-0-7-5.x-win.dfn.de (188.1.235.117) [AS680] 0.916 ms 0.927 ms 0.902 ms

4 google.bcix.de (193.178.185.100) [AS16374] 15.416 ms 15.367 ms 15.389 ms

5 108.170.241.225 (108.170.241.225) [AS15169] 15.777 ms 108.170.241.193 (108.170.241.193) [AS15169] 14.831 ms 108.170.241.225 (108.170.241.225) [AS15169] 15.778 ms

6 108.170.236.135 (108.170.236.135) [AS15169] 14.776 ms 14.751 ms 14.734 ms

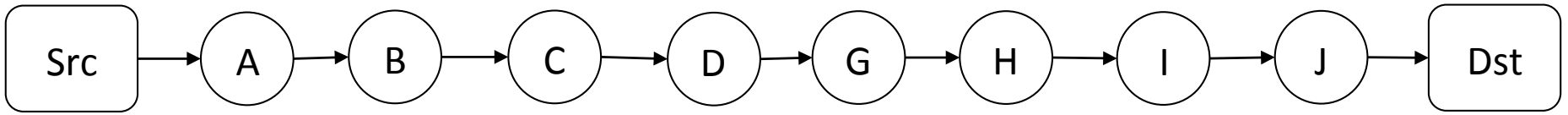
7 ams16s29-in-f36.1e100.net (172.217.17.36) [AS15169] 14.723 ms 14.691 ms 14.671 ms

Mapping IPs to ASes

- It is a difficult problem!
- Reverse DNS can be helpful, but can also be misleading (dig -x IP)
- Origin AS in BGP, but can be re-announced or hijacked!
- Whois databases can be useful, but maybe not updated! (whois -h whois.radb.net IP)
  - You can also get all the prefixes of a network, e.g., for Google: whois -h whois.radb.net -- '-i origin AS15169'

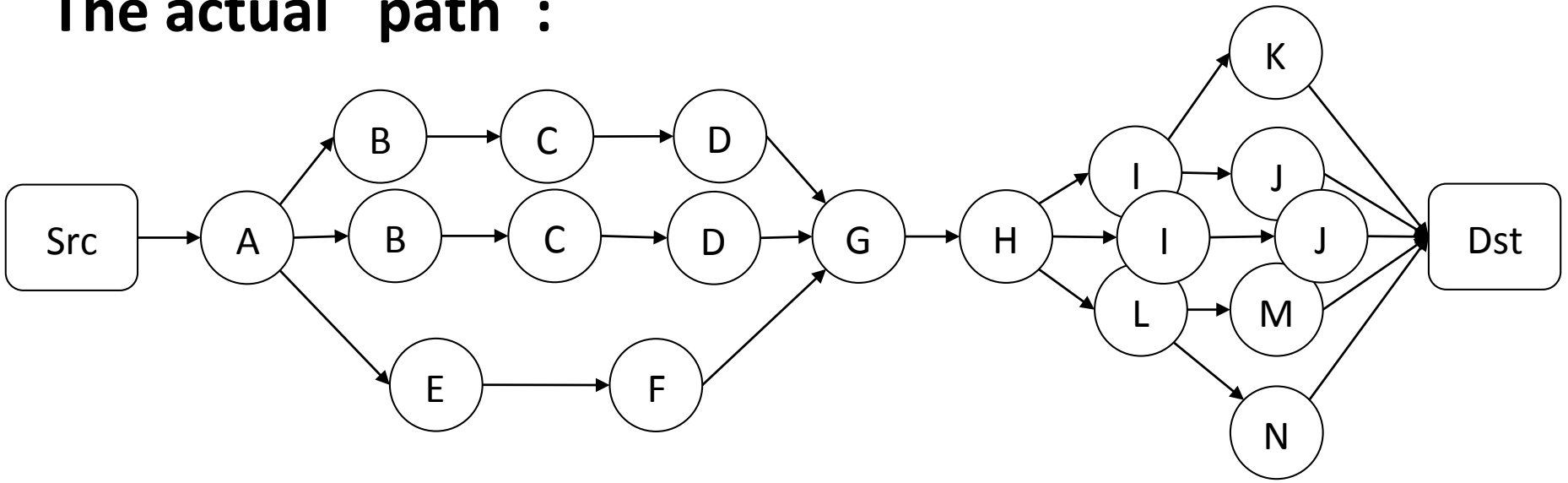
Issues with Traceroutes

The traditional model:

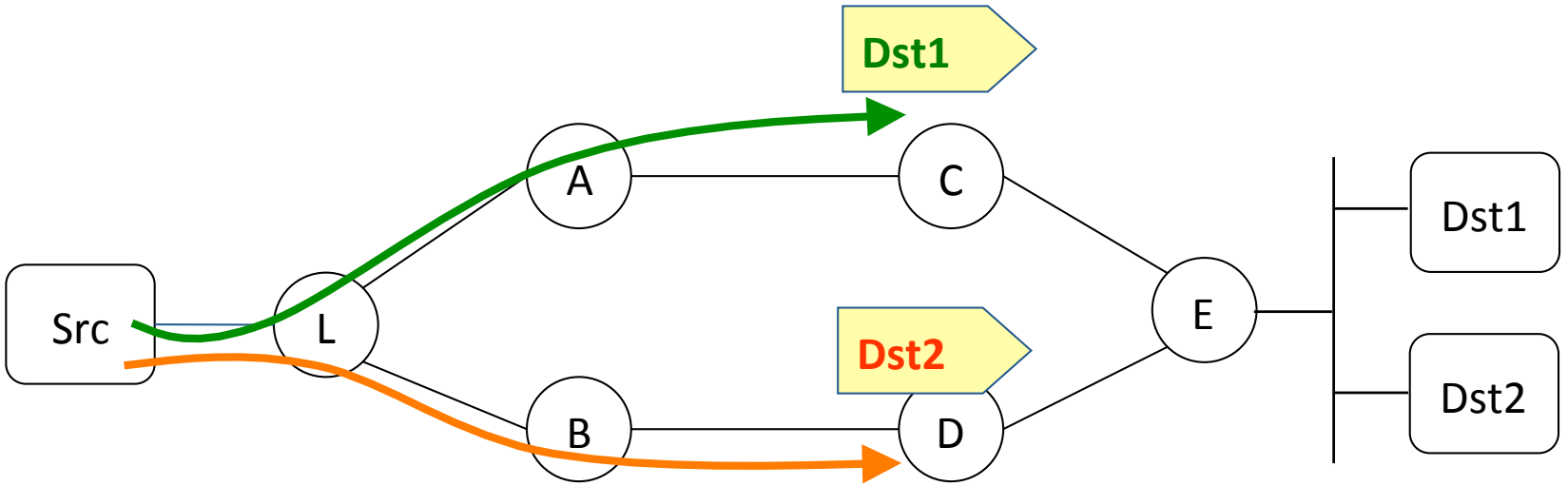


Issues with Traceroutes

The actual "path":

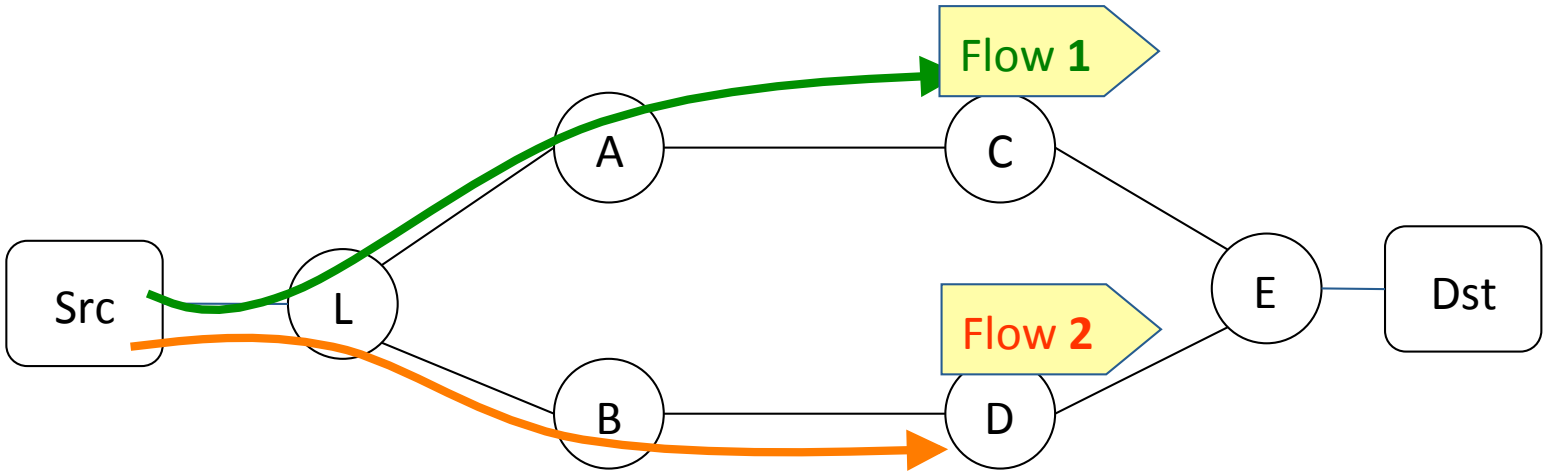


Per Destination Load Balancing



- Different Dsts in a prefix, different paths
- Different flows to same Dst, same path

Per Flow Load Balancing

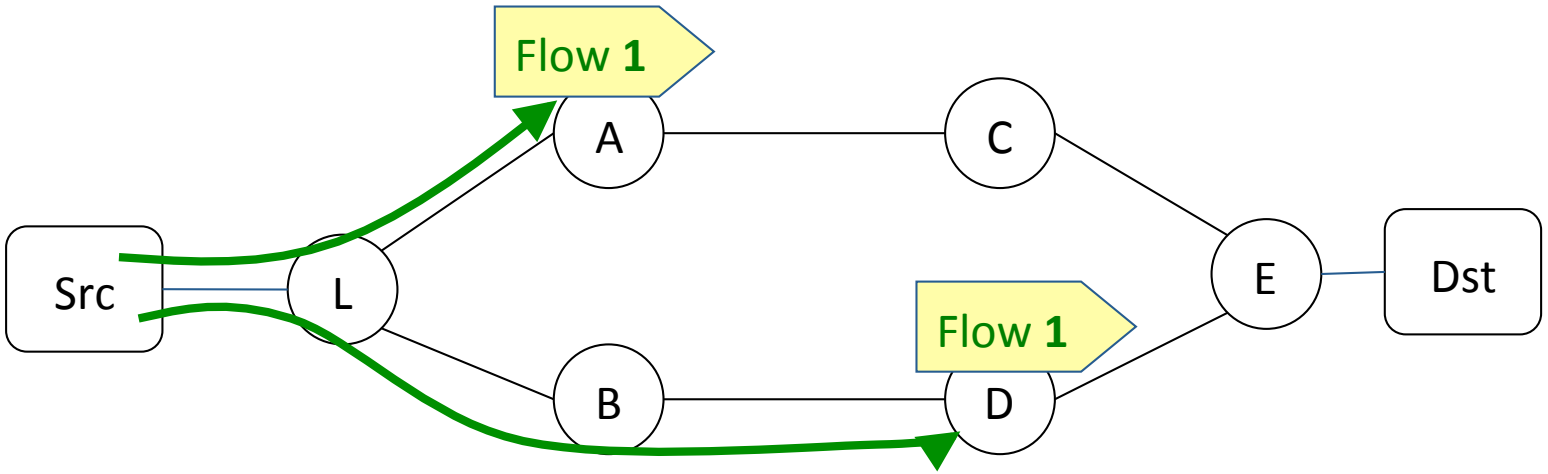


- A flow = 5-tuple

  <src IP, dst IP, src port, dst port, protocol>

- All packets in a flow take the same path

Per Packet Load Balancing

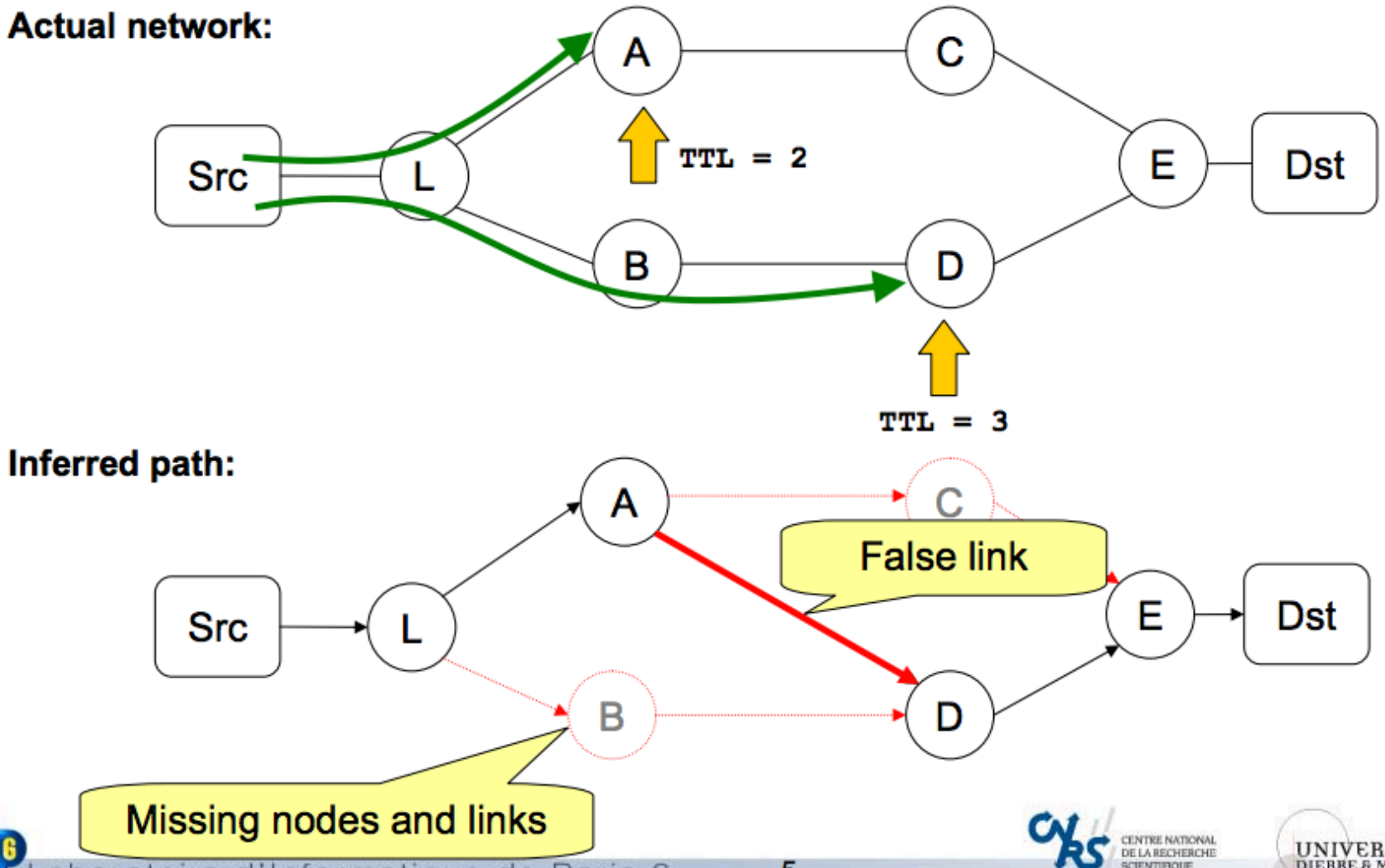


- Packets to a host may take different paths
  - Even if they belong to the same flow

Limitations

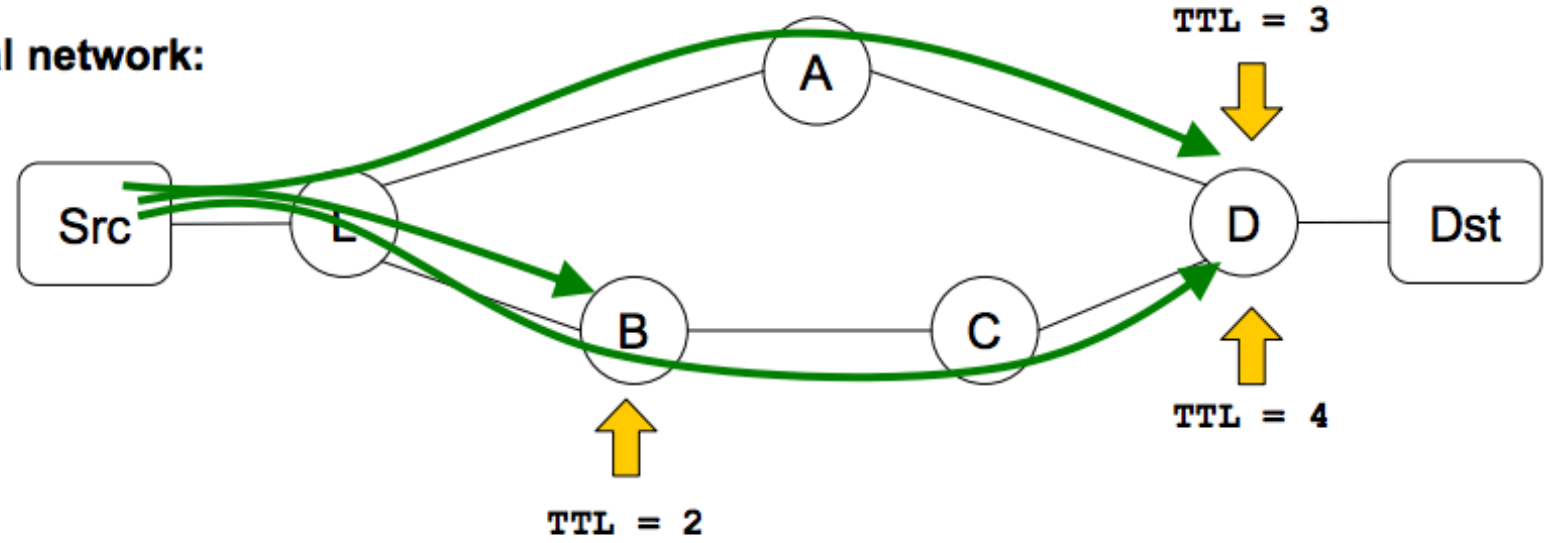
- It is possible to explore multiple paths without even knowing it
- It is possible to add artificial routes
- The Internet is asymmetric! Request and Response may follow a different path!

Traceroute under load balancing

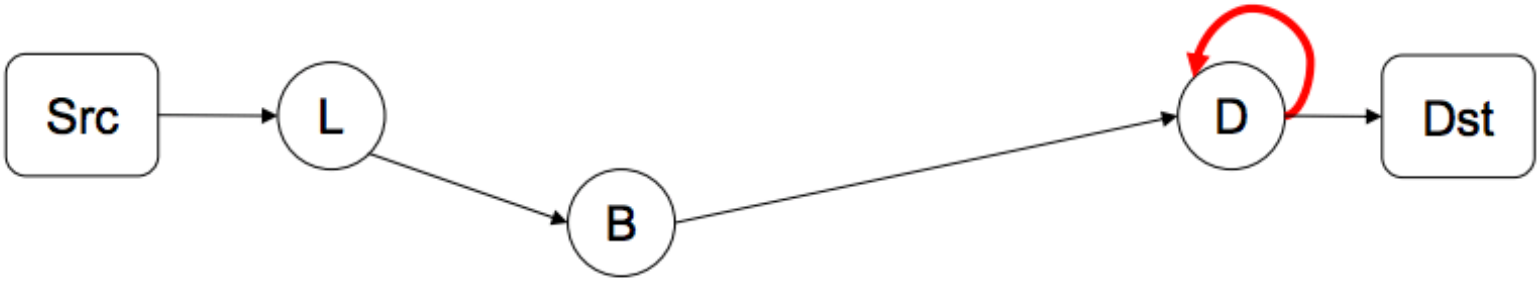


Hard to diagnose aberrant paths

Actual network:

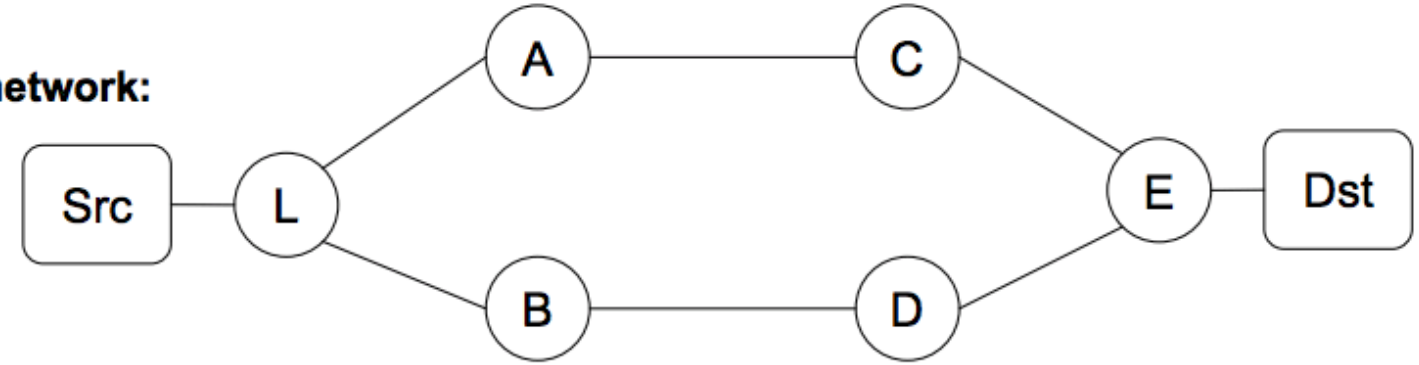


Inferred path:

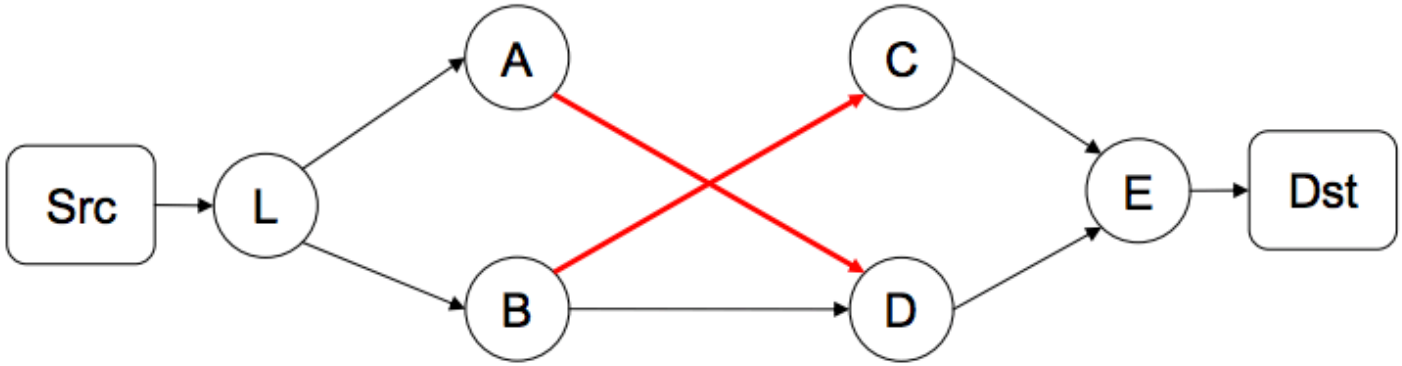


Hard to diagnose unstable paths

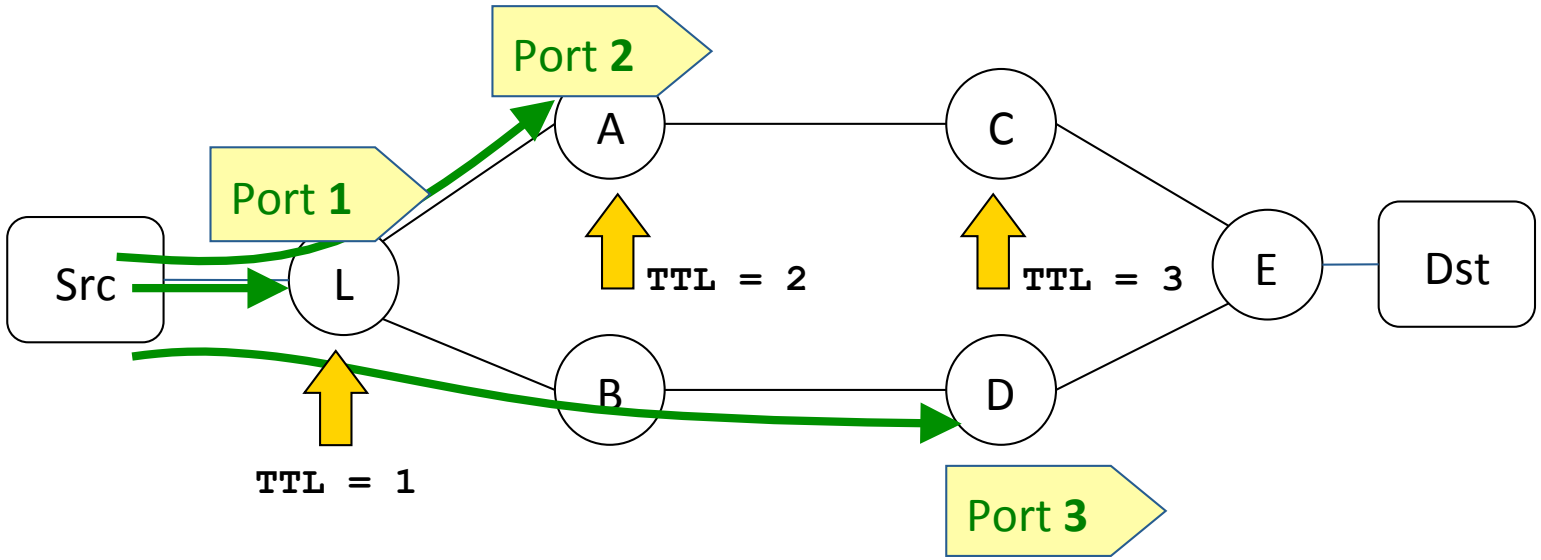
Actual network:



Inferred path:



Traceroute Issues



- Traceroute uses the destination port as identifier
- Per flow load balancers use the destination port as part of the flow identifier

Paris Traceroute: Identifying the probes

IP

Version	IHL	TOS	Total Length	
Identification (+)			Flags	Fragment Offset
TTL		Protocol	Header Checksum	
Source Address				
Destination Address				
Options and Padding				

UDP

Source Port	Destination Port (#)
Length	Checksum (#,*)

ICMP Echo

Type	Code	Checksum (#)
Identifier (*)		Sequence Number (#,*)

TCP

Source Port				Destination Port
Sequence Number (*)				
Acknowledgment Number				
Data Offset	Resvd.	ECN	Control Bits	Window
Checksum				Urgent Pointer
Options and Padding				

Key

Used for per–flow load balancing

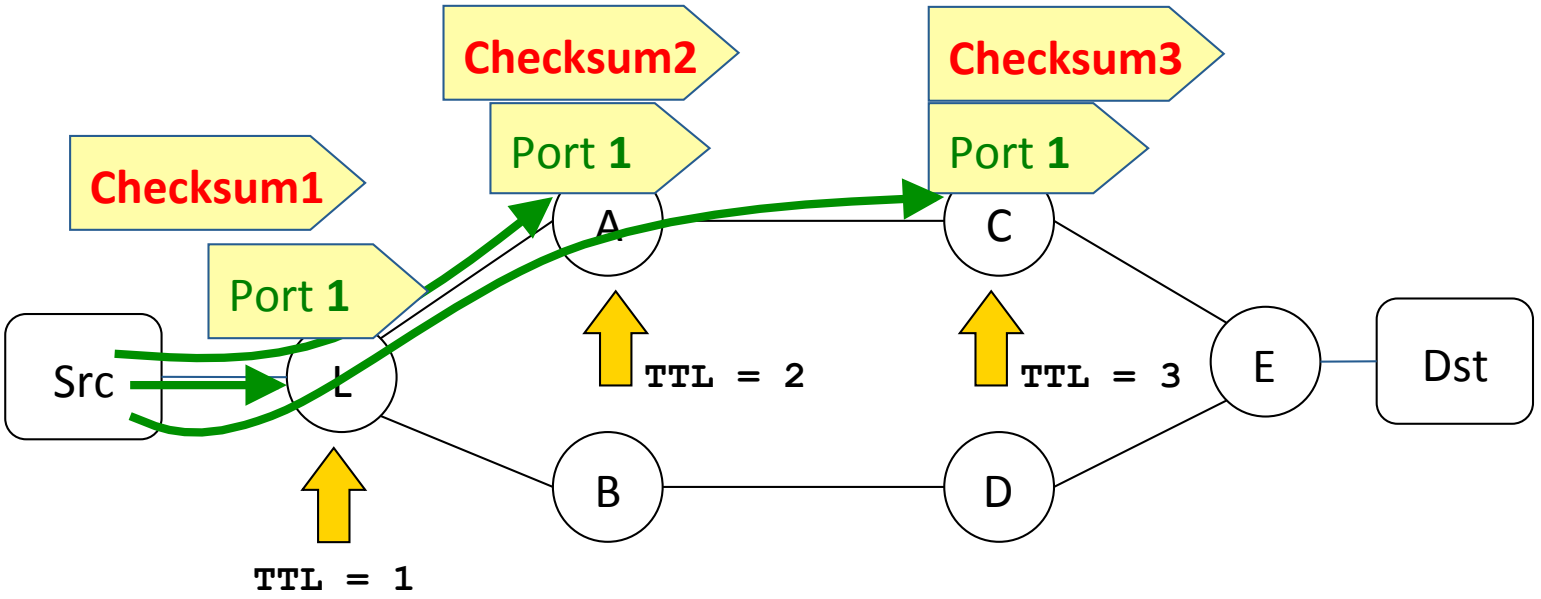
Not encapsulated in ICMP Time Exceeded packets

\# Varied by classic traceroute

\+ Varied by tcptraceroute

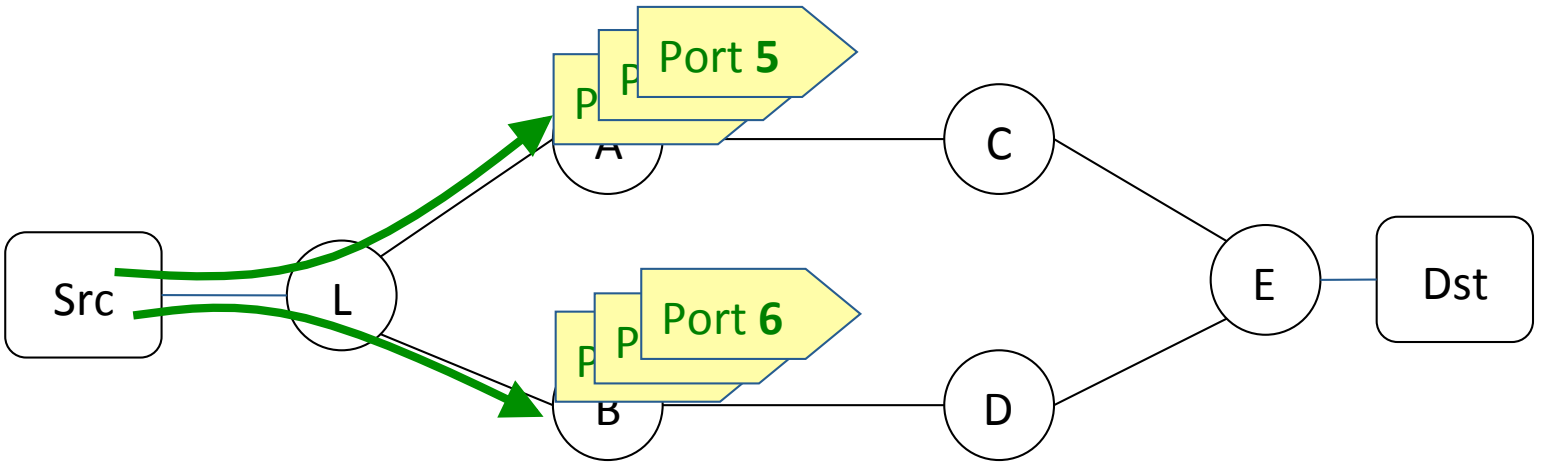
* Varied by Paris traceroute

Paris Traceroute



- Solves the problem with per flow load balancing
  - Probes to a destination belong to the same flow
- How it identifies probes?
  - Use the UDP checksum

Paris Traceroute: tracing all paths



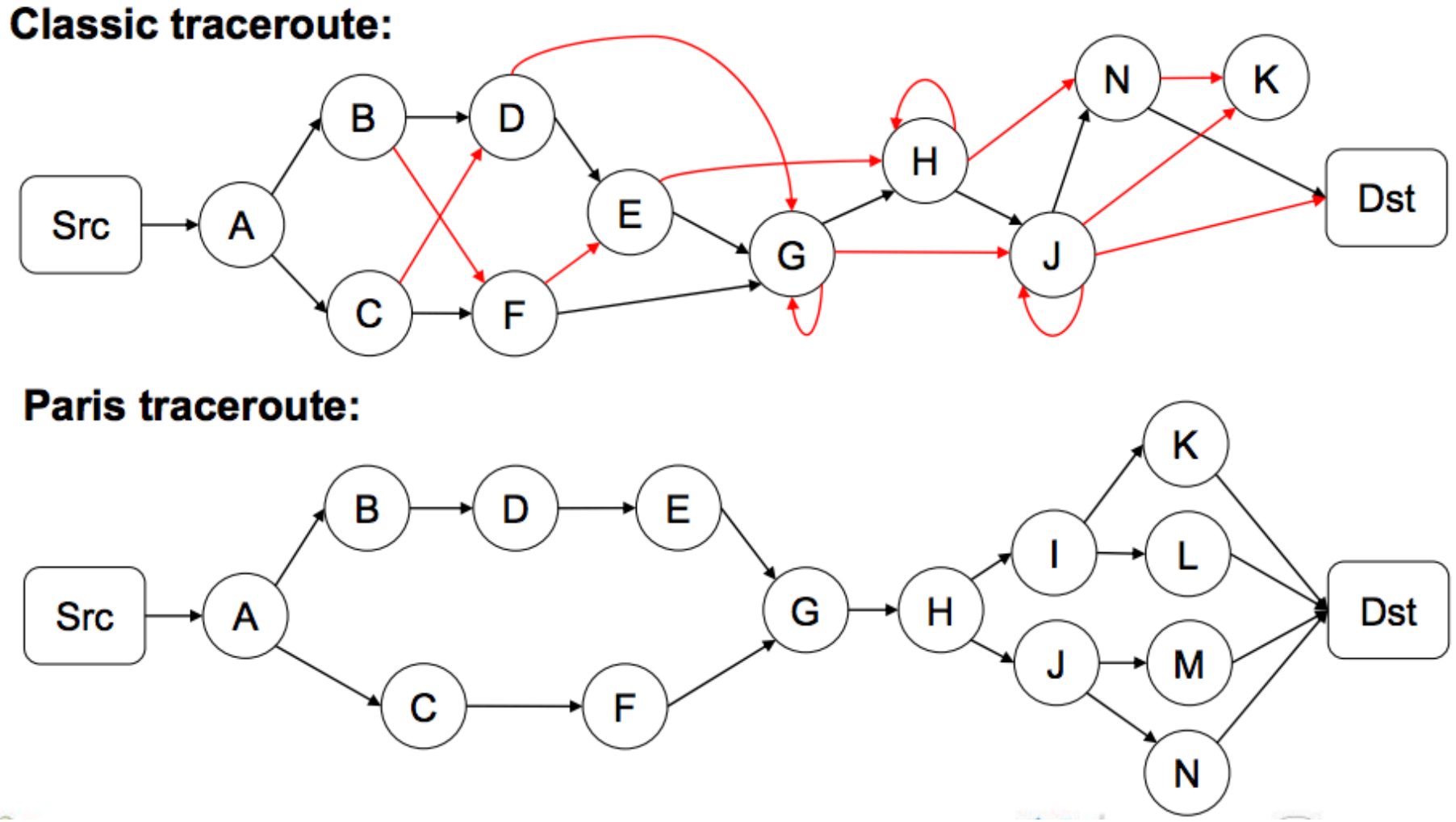
1. Discover the load balancers

- Vary the flow identifier of probes

2. Classify them according to their types

- Maintain the flow identifier

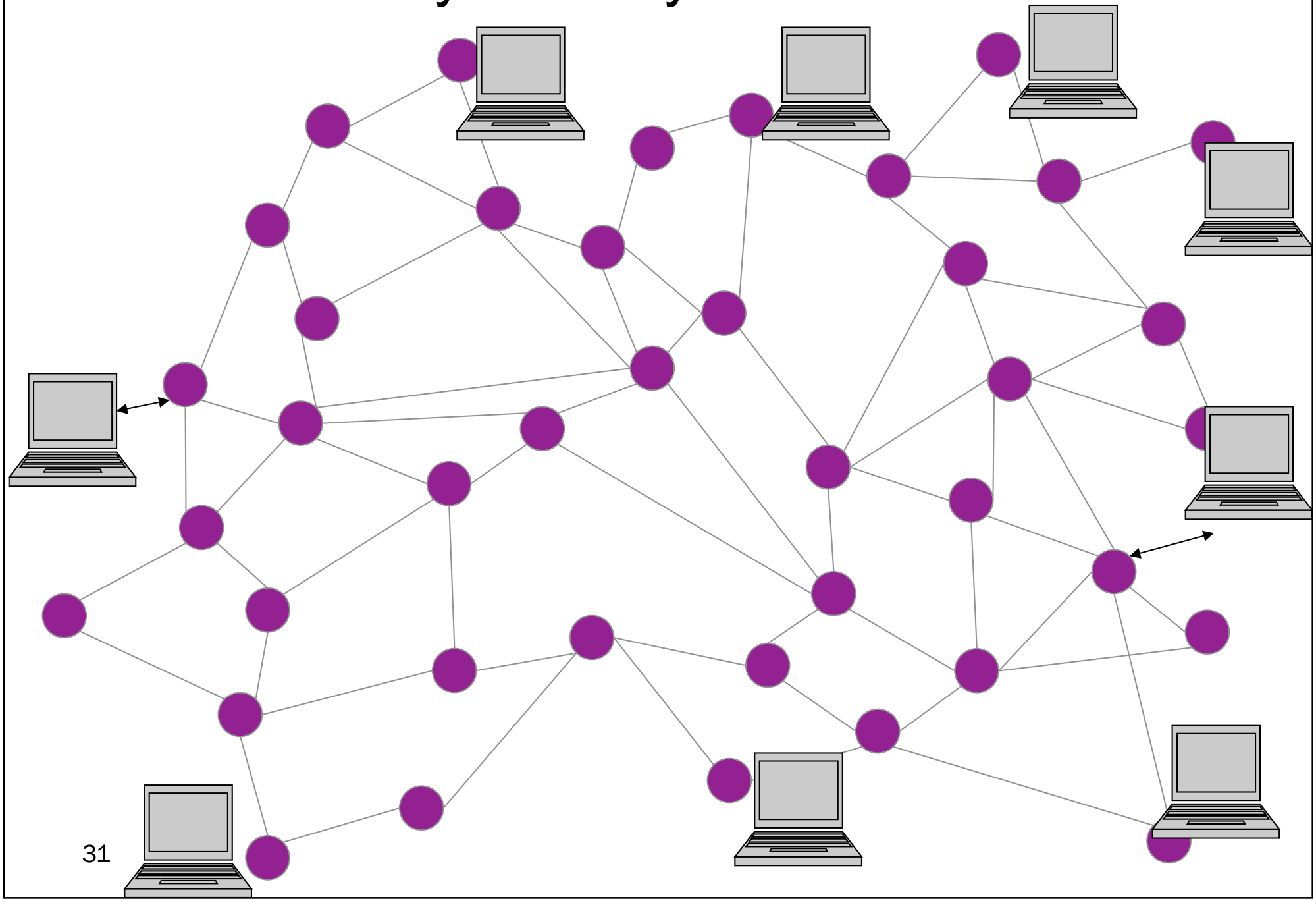
Paris Traceroute



Paris Traceroute

- It can address quite well the per destination and per flow load balancer
- It does not solve the per packet load balancing (random selection)

Many-to-Many Traceroute



Marginal Utility

- It is better to add destination that sources, when you perform large-scale experiment

("On the marginal utility of network topology measurements" IMC 2001)

- However, in many cases routers are configured not to reply to ICMP messages!
- Finding sources in networks that peer or are customers of networks you want to measure can be useful.

Asymmetry

- Internet routes are not symmetric
  - Try Traceroutes from two end points and you will see that most routes are not symmetric
- Reasons:
  - Hot Potato Routing: send the traffic to another network to route as soon as possible
  - Policy Routing: multihoming, business arrangements, etc.

Reading

“Avoiding Traceroute Anomalies with Paris Traceroute”,

Brice Augustin, Xavier Cuvellier, Benjamin Orgogozo, Fabien Viger, Timur Friedman, Matthieu Latapy, Clémence Magnien, Renata Teixeira,

In the Proceedings of IMC 2006