# COMP90007 Internet Technology

Week5

Yiran (Scott) Ruan

Email: yrrua@unimelb.edu.au

Web Page: https://yiranruan.github.io

# Device

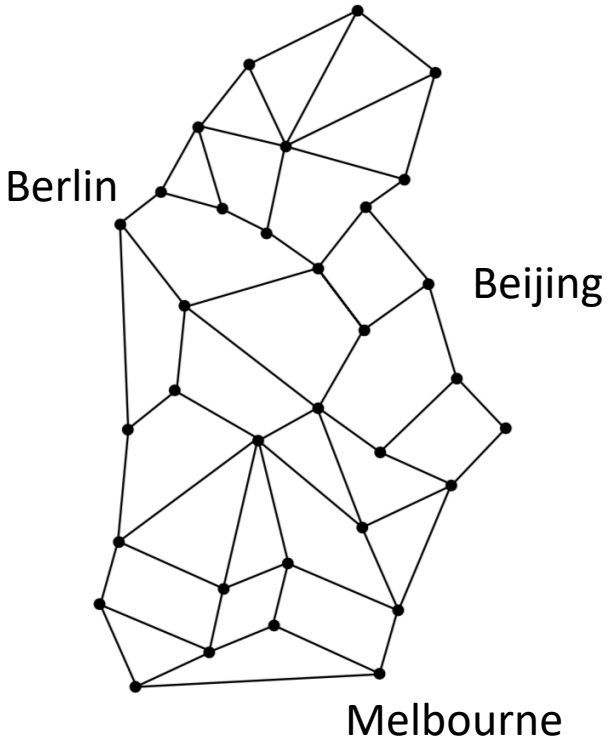
- Of course you are welcome to use your laptop
- We are provided you two servers
  - ssh username@digitalis.eng.unimelb.edu.au
  - ssh username@digitalis2.eng.unimelb.edu.au

# Notice

- Please read your Project documentation carefully for more details about your experiments. This slide is just for a better preparation and understanding.

# Measuring the hop count

- When we send a packet from our source host to the target, there are lots of intermediate hosts in the route.



# traceroute/tracert

- To count the hops number between source and target
  - Mac: traceroute –nw1 cis.unimelb.edu.au
  - Linux: traceroute –nw 1 cis.unimelb.edu.au
  - Win: tracert –dw1 cis.unimelb.edu.au

# Traceroute

- Command statement: traceroute hostname
- Using the TTL field in the header of IP (Internet Protocol) and ICMP (Internet Control Message Protocol) message carried in IP packet.

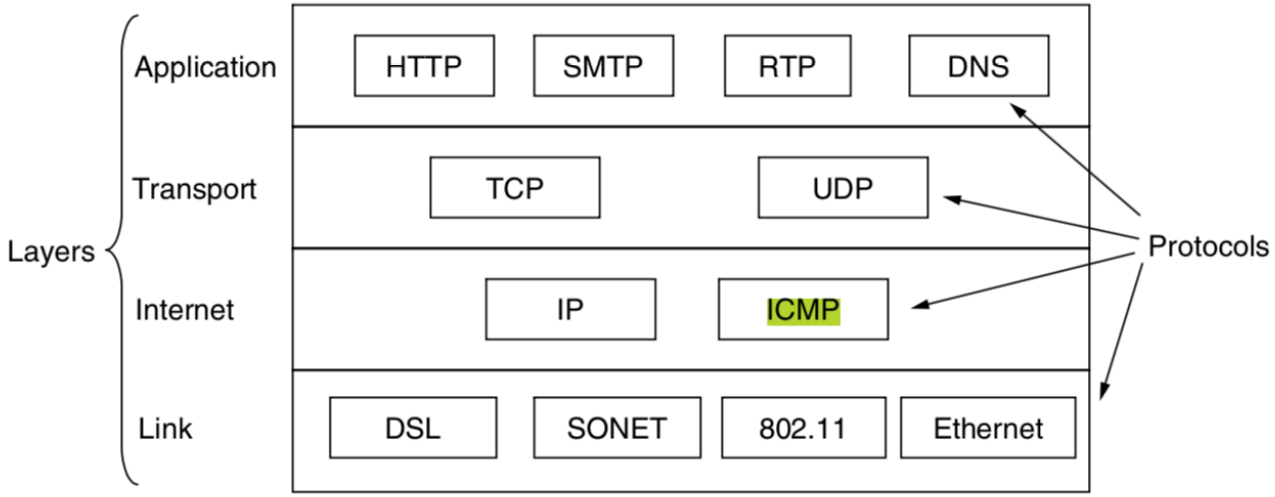



**Figure 1-22.** The TCP/IP model with some protocols we will study.

*Computer Network Page 48

# IPv4 header

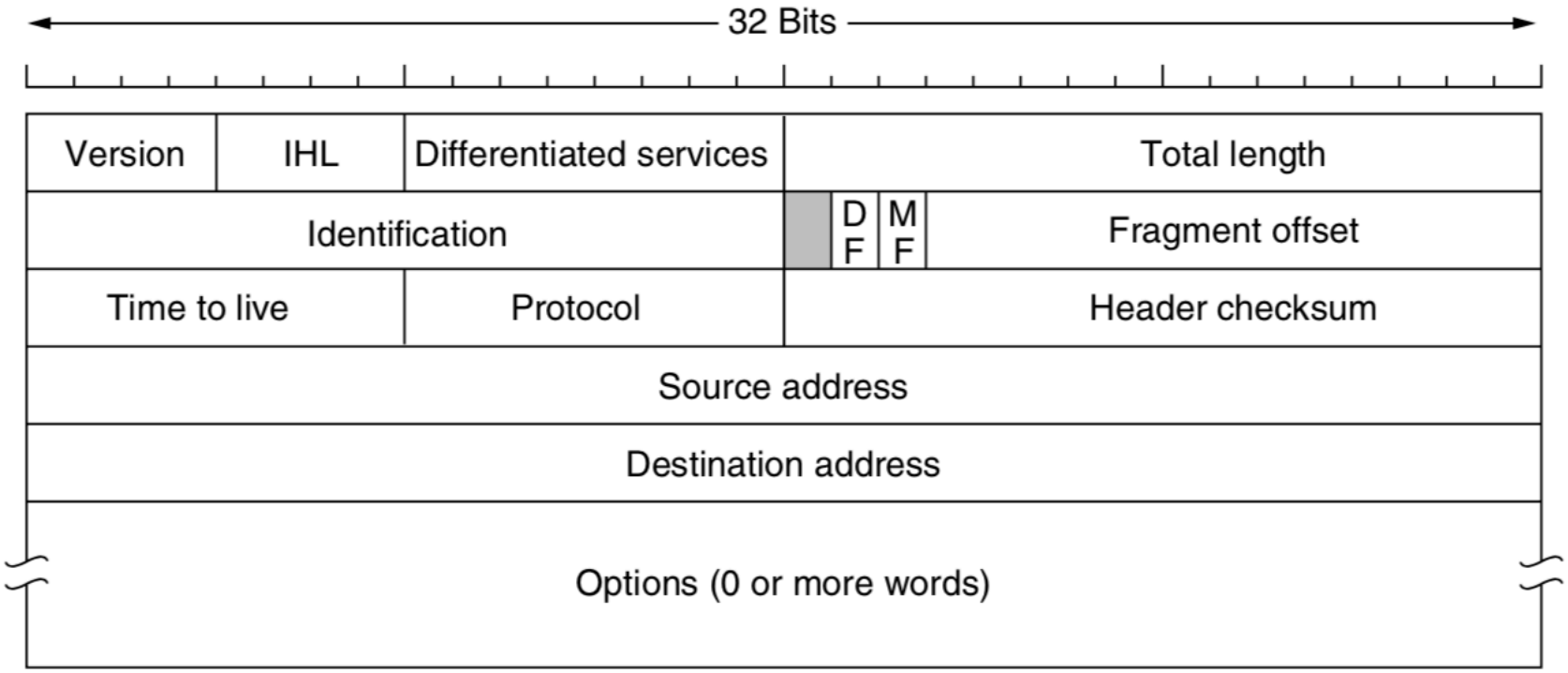
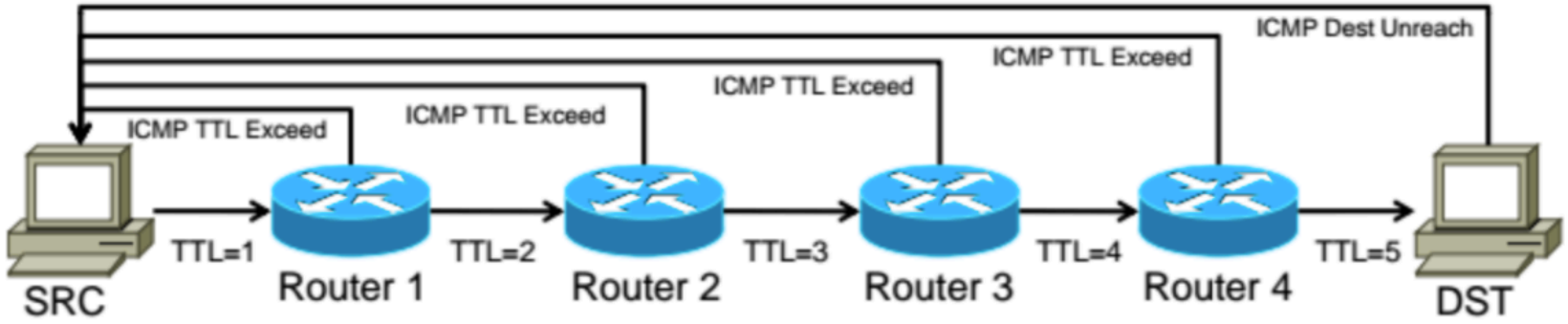



**Figure 5-46.** The IPv4 (Internet Protocol) header.

*Computer Network Page 48

# TTL field

- The *TtL (Time to live)* field is a counter used to limit packet lifetimes. It was originally supposed to count time in seconds, allowing a maximum lifetime of 255 sec. It must be decremented on each hop and is supposed to be decremented multiple times when a packet is queued for a long time in a router. In practice, it just counts hops. When it **hits zero**, the packet is discarded and a warning packet is sent back to the source host.




*Computer Network Page 48

# ICMP

- ICMP could be used to test the Internet. About a dozen types of ICMP messages are defined. Each ICMP message type is carried encapsulated in an IP packet.

| Message type | Description |
|---|---|
| Destination unreachable | Packet could not be delivered |
| Time exceeded | Time to live field hit 0 |
| Parameter problem | Invalid header field |
| Source quench | Choke packet |
| Redirect | Teach a router about geography |
| Echo and echo reply | Check if a machine is alive |
| Timestamp request/reply | Same as Echo, but with timestamp |
| Router advertisement/solicitation | Find a nearby router |

**Figure 5-60.** The principal ICMP message types.

*Computer Network Page 48

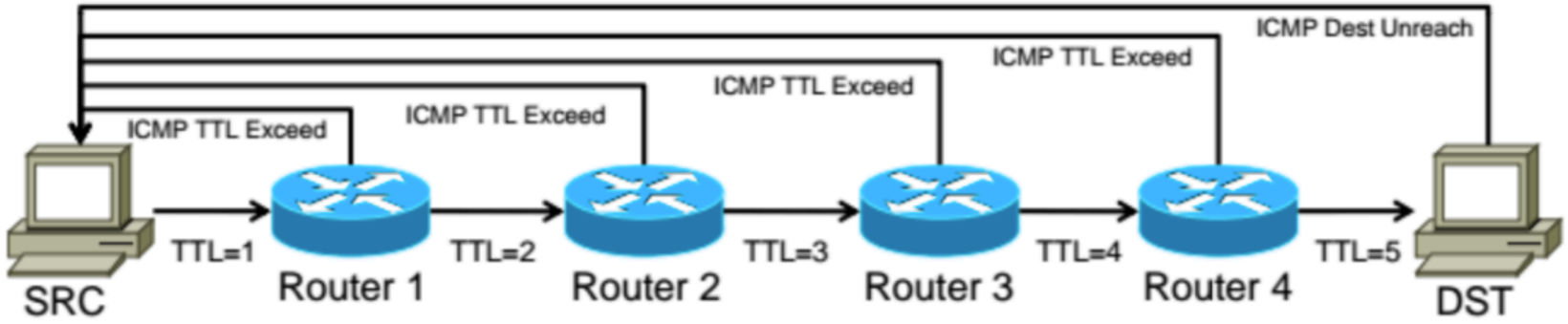
# ICMP – TIME EXCEEDED

- The ***TIME EXCEEDED*** message is sent when a packet is dropped because its *TtL (Time to live)* counter has reached zero. This event is a symptom that packets are looping, or that the counter values are being set too low.

*Computer Network Page 48

# traceroute

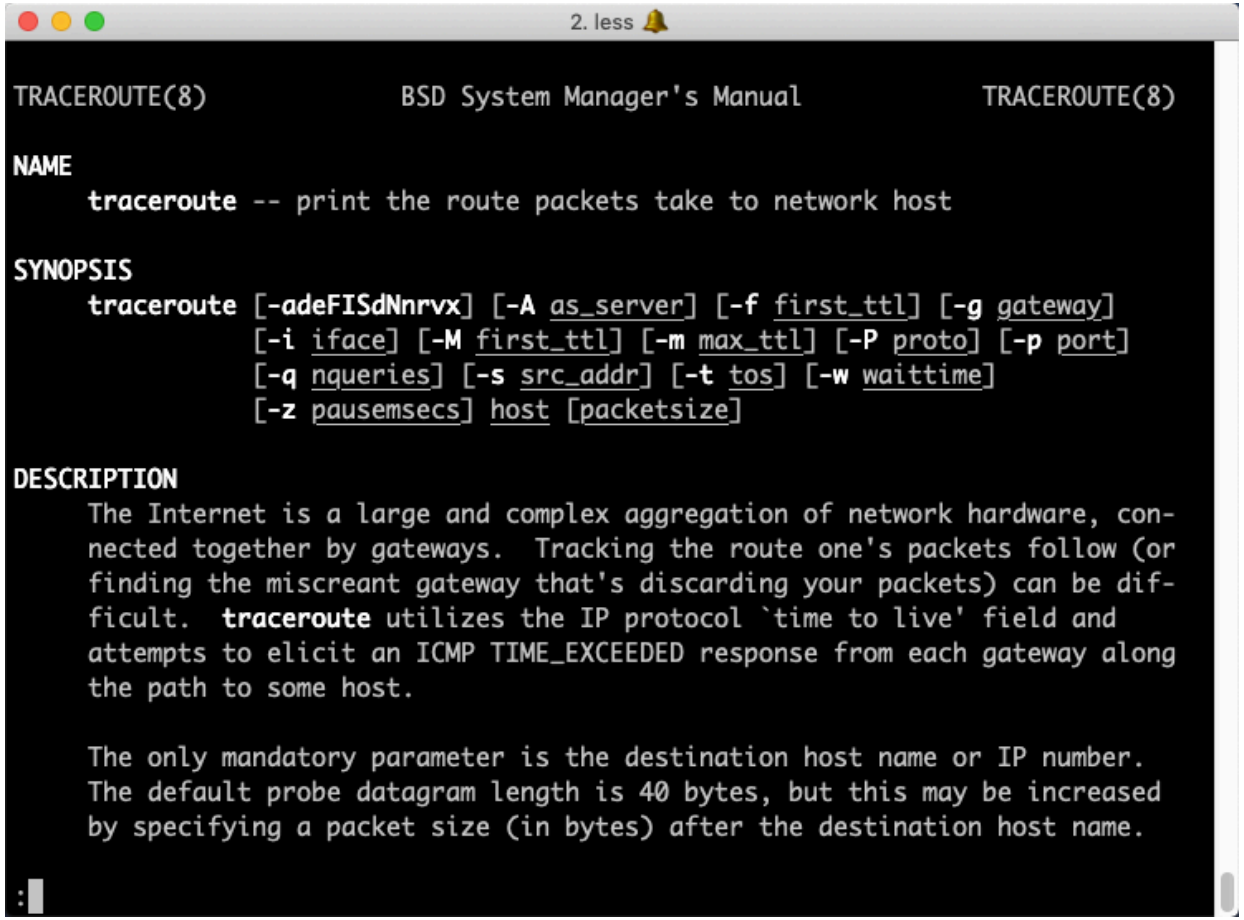
- 1. Send three IP **datagrams** (40 bytes, include source address, target address and sending time label) with TTL = 1
- 2. router: decrease TTL by 1.
  - If TTL = 0, drop this datagram and send back a “ICMP time exceeded” message including source host IP address, the content of the datagram and IP address of the router.
- 3. Source host increase TTL by 1 and send it again.



# Details of traceroute – man traceroute

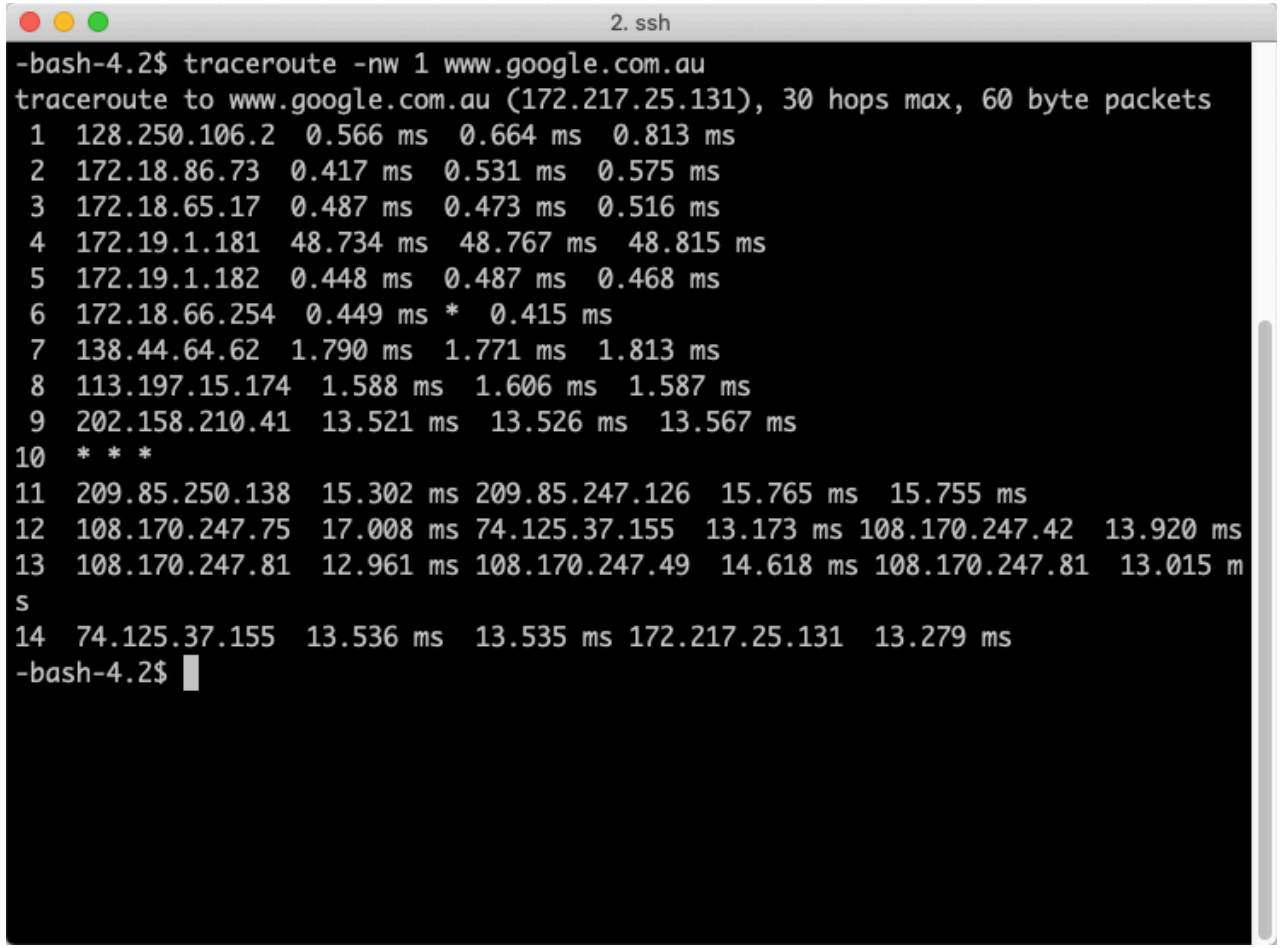
The help documentation for the ***traceroute*** utility can be accessed by running

- **man traceroute**
- **tracert /?**



# traceroute

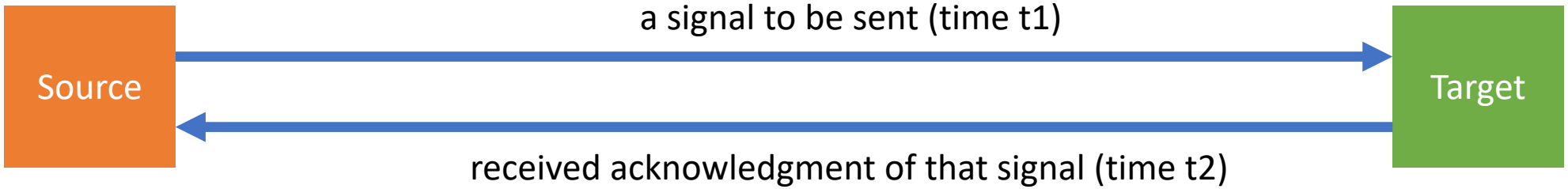
- Each record is one hop
- For each line, there are three time records.
- Traceroute –q 4 www.google.com
- “***” time out hops still count
  - Firewall blocks the ICMP messages
- Latency:
  - Block by some gateway
  - DNS – cannot resolve Host name and Domain name (-n)



- Connect to VPN
- AnyConnect
- remote.unimelb.edu.au/student

# Delay

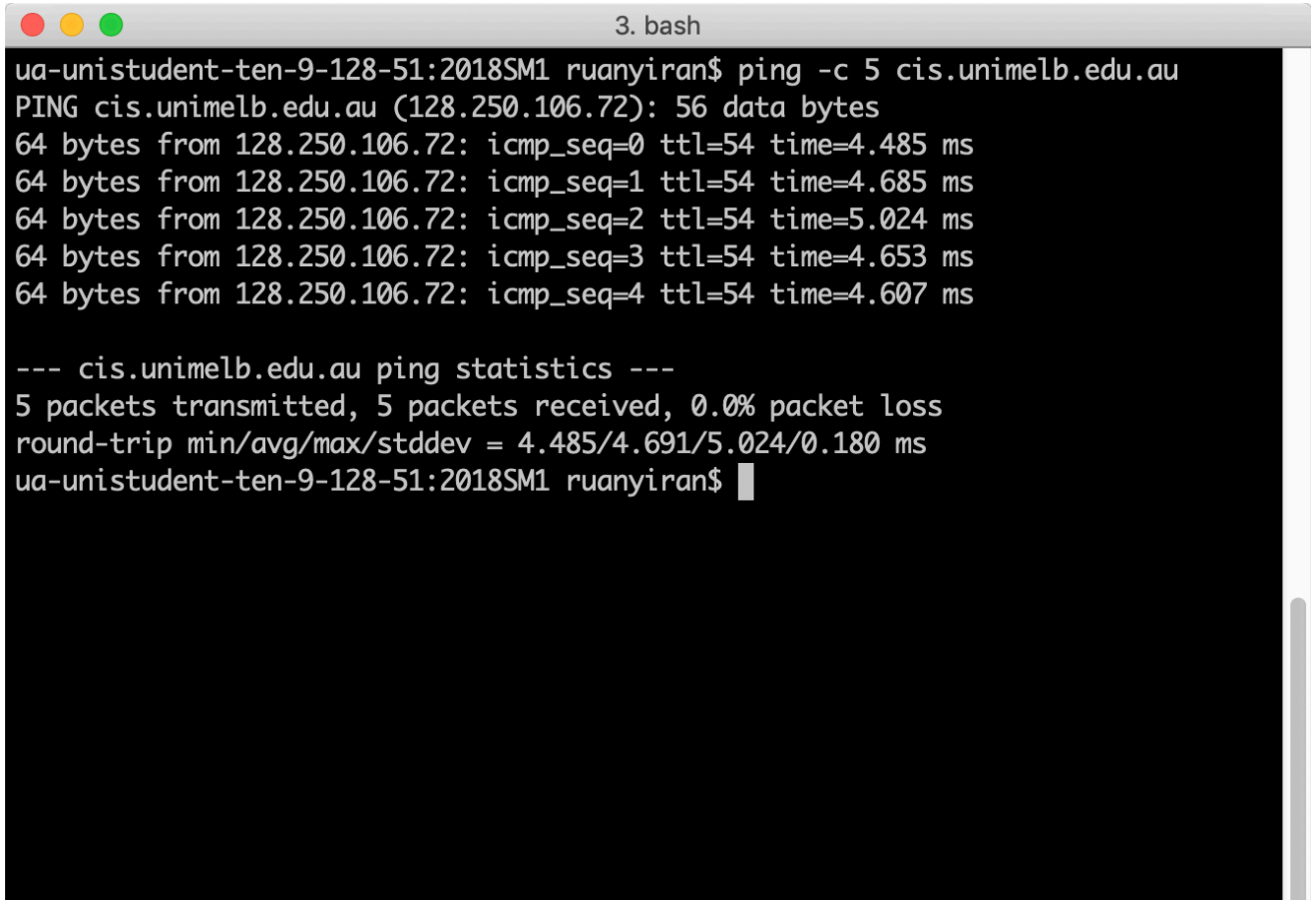
- Round-trip Time (RTT)
  - The total time of one source host to send a packet to the target and wait for its acknowledgement to be received.




$$RTT = t1 + t2$$

# Ping -> Delay

- We will use ***ping*** utility, to measure the round-trip delay of packets. The ping utility should be pre-installed on all major operating systems.
- Win: ping cis.unimelb.edu.au
- Mac: ping –c 5 cis.unimelb.edu.au
  - mac users need to set a specific number for testing packets



# ICMP – ECHO & ECHO REPLY

- Using ICMP
  - The ***ECHO*** and ***ECHO REPLY*** messages are sent by hosts to see if a given destination is reachable and currently alive. Upon receiving the ***ECHO*** message, the destination is expected to send back an ***ECHO REPLY*** message. These messages are used in the **ping** utility that checks if a host is up and on the Internet.

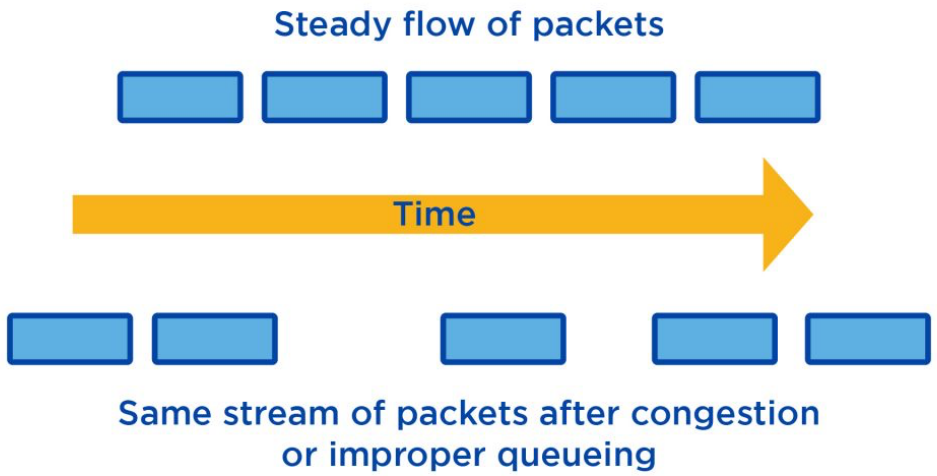
| Message type | Description |
|---|---|
| Destination unreachable | Packet could not be delivered |
| Time exceeded | Time to live field hit 0 |
| Parameter problem | Invalid header field |
| Source quench | Choke packet |
| Redirect | Teach a router about geography |
| Echo and echo reply | Check if a machine is alive |
| Timestamp request/reply | Same as Echo, but with timestamp |
| Router advertisement/solicitation | Find a nearby router |

**Figure 5-60.** The principal ICMP message types.

*Computer Network Page 48

# Jitter

- Jitter is defined as a variation in the delay of received packets.
- The standard deviation of the round-trip delay time will be taken as the value for jitter for this project.




(https://www.nextiva.com/blog/network-jitter.html)

# Jitter

$$\sigma = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2}$$

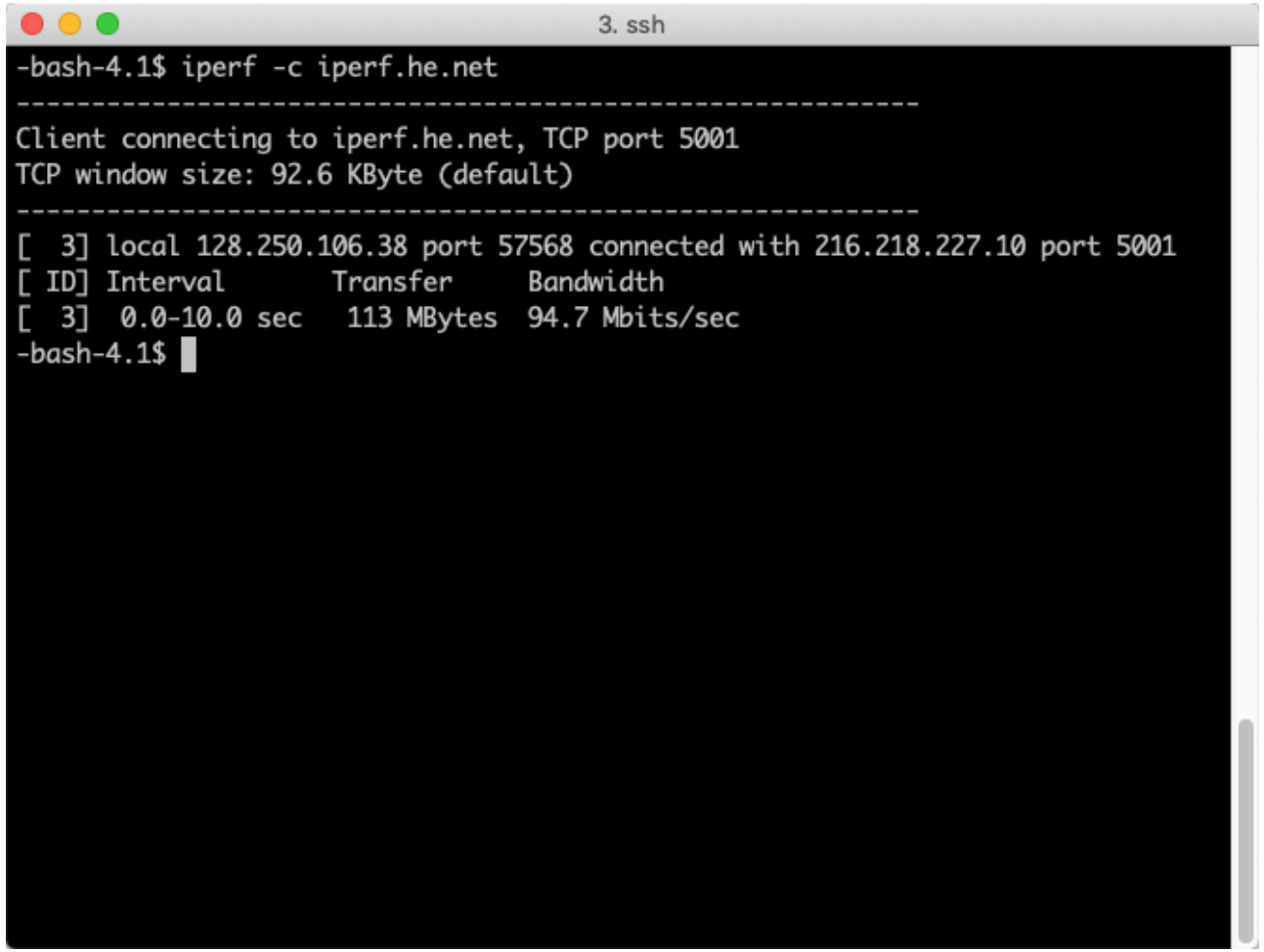
- where the $\bar{x}$ would be the mean of the set of data

# iperf -> Bandwidth

- iperf: perform bandwidth measurements
- Download: https://iperf.fr
- Two modes:
  - Server mode (iperf3 –s): host a server which will listen to incoming requests from a client.
  - Client mode (e.g. iperf3 -c iperf.eenet.ee): connect to the server, and packets will be exchanged and timed between the two hosts to calculate the bandwidth.
- In this project, we will be running ***iperf*** in client mode.

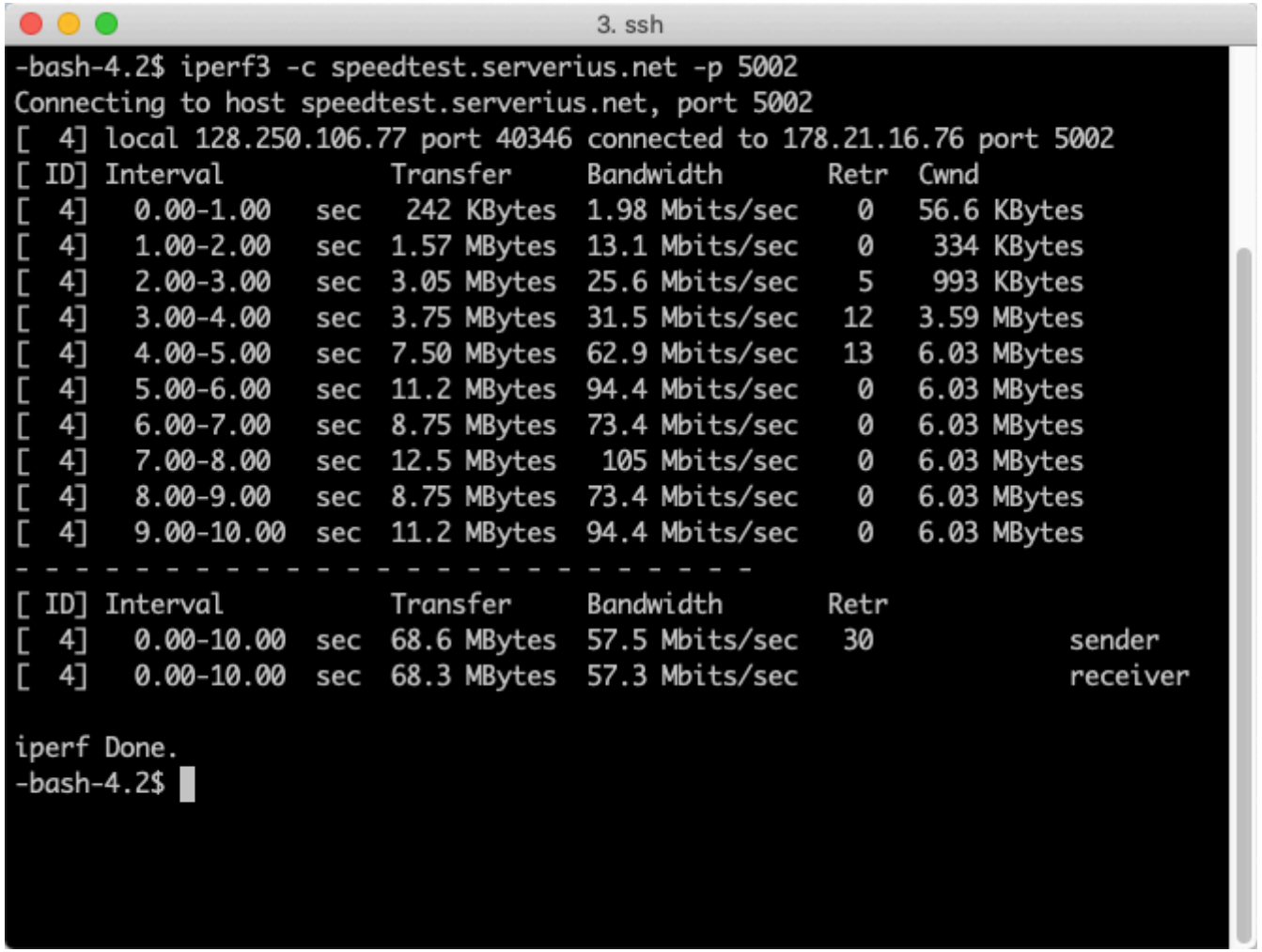
# iperf –c iperf.he.net

- Example



# iperf3 -c speedtest.serverius.net -p 5002

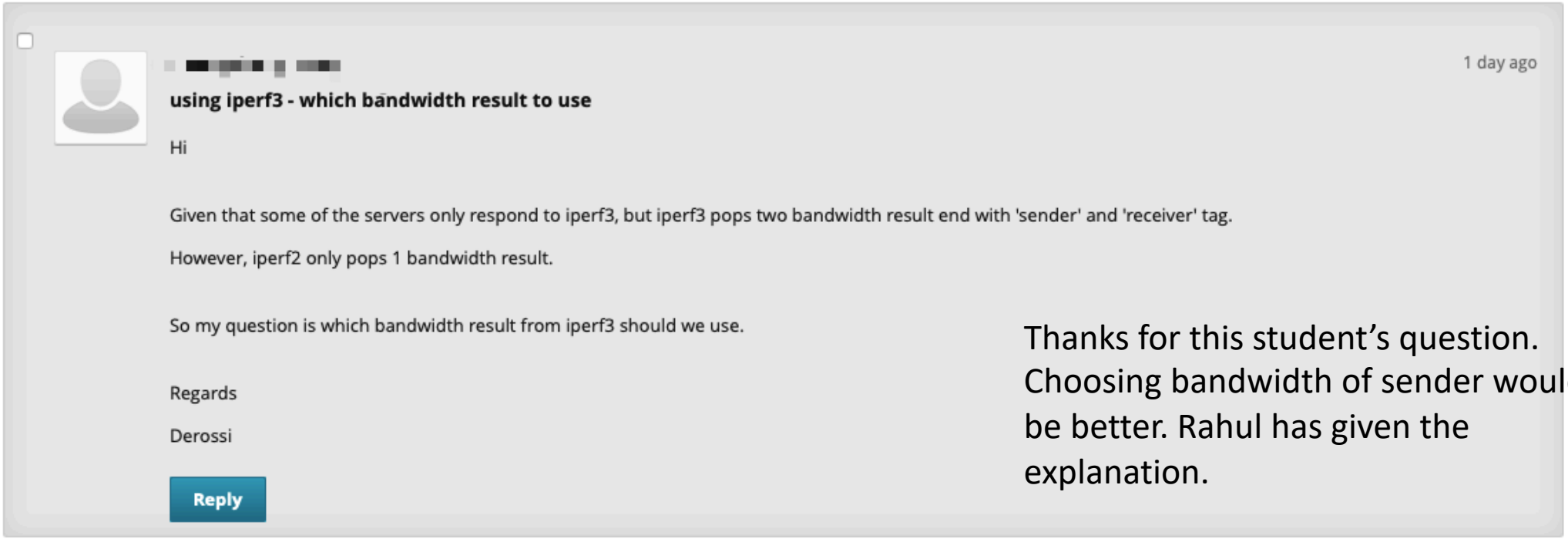
Note:
For speedtest.serverius.net in Table 1, we may need to use the port 5002.
Also, some iperf servers respond to iperf2, rest to iperf3 so you might want to use both iperf2 and iperf3 to verify if the server is responsive.



# iperf3

- sender - is iperf client, Upload speed from iperf client to iperf server is measured
  receiver - is iperf server, Download speed on iperf server from iperf client is measured

# Iperf3 – sender or receiver



[redacted]

1 day ago

**using iperf3 - which bandwidth result to use**

Hi

Given that some of the servers only respond to iperf3, but iperf3 pops two bandwidth result end with 'sender' and 'receiver' tag.

However, iperf2 only pops 1 bandwidth result.

So my question is which bandwidth result from iperf3 should we use.

Regards

Derossi

Reply

Thanks for this student's question. Choosing bandwidth of sender would be better. Rahul has given the explanation.



**Rahul Sharma**

12 hours ago

**RE: using iperf3 - which bandwidth result to use**

The sender one please, but it would be key to understand what the sender stat is trying to say in order to present a meaningful discussion.

Reply | Quote | Edit | Delete | Email Author

# Servers

- If you want to use server
- NOTICE:
  - ssh username@digitalis.eng.unimelb.edu.au -> iperf –c xxx
  - ssh username@digitalis2.eng.unimelb.edu.au -> iperf3 –c xxx