TA: Xifan Zheng
Email: zhengxifan0403@gmail.com

Welcome to CPSC 441!

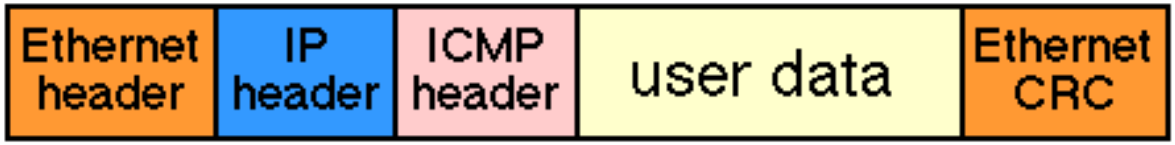
ICMP

- **I**nternet **C**ontrol **M**essage **P**rotocol
- ICMP messages are IP packets
- Used by network hosts to announce
  - Network errors
  - Network congestion
  - Network timeouts

- Not used directly by user except
  - ICMP Echo Request/Reply messages used in **Ping**
  - **Traceroute**

ICMP Header

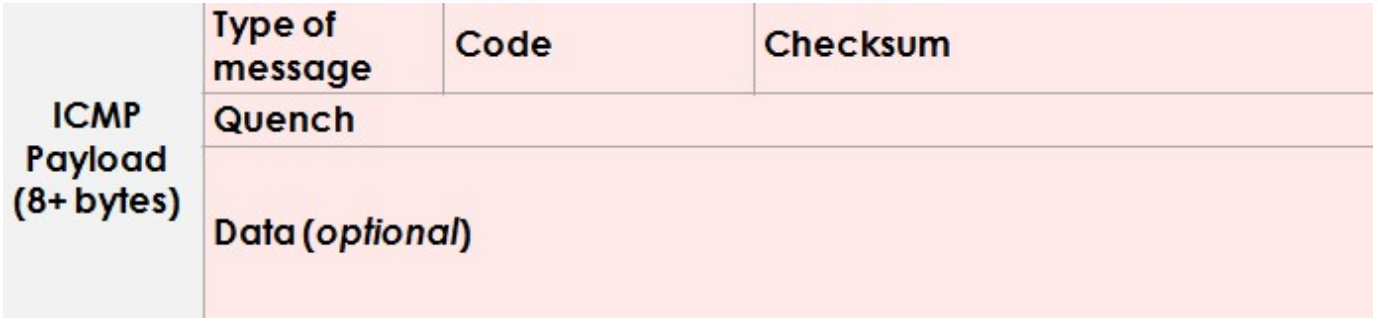
- ICMP Header starts after IP Header



ICMP packet				
	Bit 0 - 7	Bit 8 - 15	Bit 16 - 23	Bit 24 - 31
IP Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Payload (8+ bytes)	Type of message	Code	Checksum	
	Quench			
	Data (*optional*)			

From: http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

ICMP Header



- All ICMP packets will have an 8-byte header and variable-sized data section. The first 4 bytes of the header will be consistent.
  - **Type** – ICMP type. Include 43 types.
  - **Code** – Subtype to the given type.
  - **Checksum** – Error checking data. Calculated from the ICMP header+data, with value 0 for this field.
  - **Rest of Header** – Four byte field. Will vary based on the ICMP type and code.
  - **The ICMP 'Quench' (32 bits**) field, which in this case (ICMP echo request and replies), will be composed of identifier (16 bits) and sequence number (16 bits).

PING

- What ping is used for?
  - Checks if target host is alive
  - Troubleshoot network connectivity problems

- ICMP Echo Request (Type 8 code 0)
  - 64 byte packet
  - Host replies with ICMP Echo Reply (type 0 code 0)

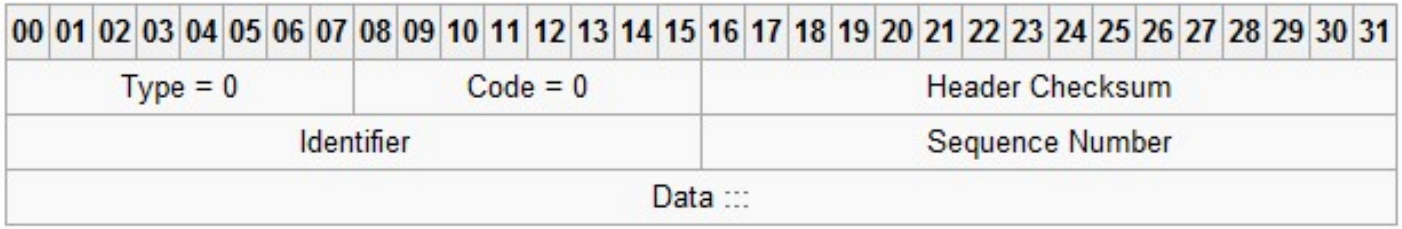
Echo request

- The *echo request* is an ICMP message whose data is expected to be received back in an *echo reply* ("ping").
- The host must respond to all echo requests with an echo reply containing the exact data received in the request message.
- The Identifier and Sequence Number can be used by the client to match the reply with the request that caused the reply.

0 0	0 1	0 2	0 3	0 4	0 5	0 6	0 7	0 8	0 9	1 0	1 1	1 2	1 3	1 4	1 5	1 6	1 7	1 8	1 9	2 0	2 1	2 2	2 3	2 4	2 5	2 6	2 7	2 8	2 9	3 0	3 1
Type = 8								Code = 0								Header Checksum															
Identifier																Sequence Number															
Data :::																															

- **Linux systems** use a unique identifier for every ping process, and sequence number is an increasing number within that process.
- **Windows** uses a fixed identifier, which varies between Windows versions, and a sequence number that is only reset at boot time.

Echo reply



- The ***echo reply*** is an ICMP message generated in response to an echo request
- The *identifier* and *sequence number* can be used by the client to determine which echo requests are associated with the echo replies.
- The data received in the echo request must be entirely included in the echo reply.
- Possible **reply messages** include !H, !N, or !P (host, network or protocol unreachable) !S (source route failed) !F (fragmentation needed)…

Ping Example

```
C:\Users\xifan zheng>ping www.google.ca -n 3

Pinging www.google.ca [74.125.141.94] with 32 bytes of data:
Reply from 74.125.141.94: bytes=32 time=24ms TTL=44
Reply from 74.125.141.94: bytes=32 time=24ms TTL=44
Reply from 74.125.141.94: bytes=32 time=29ms TTL=44

Ping statistics for 74.125.141.94:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 29ms, Average = 25ms
```

```
C:\Users\xifan zheng>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

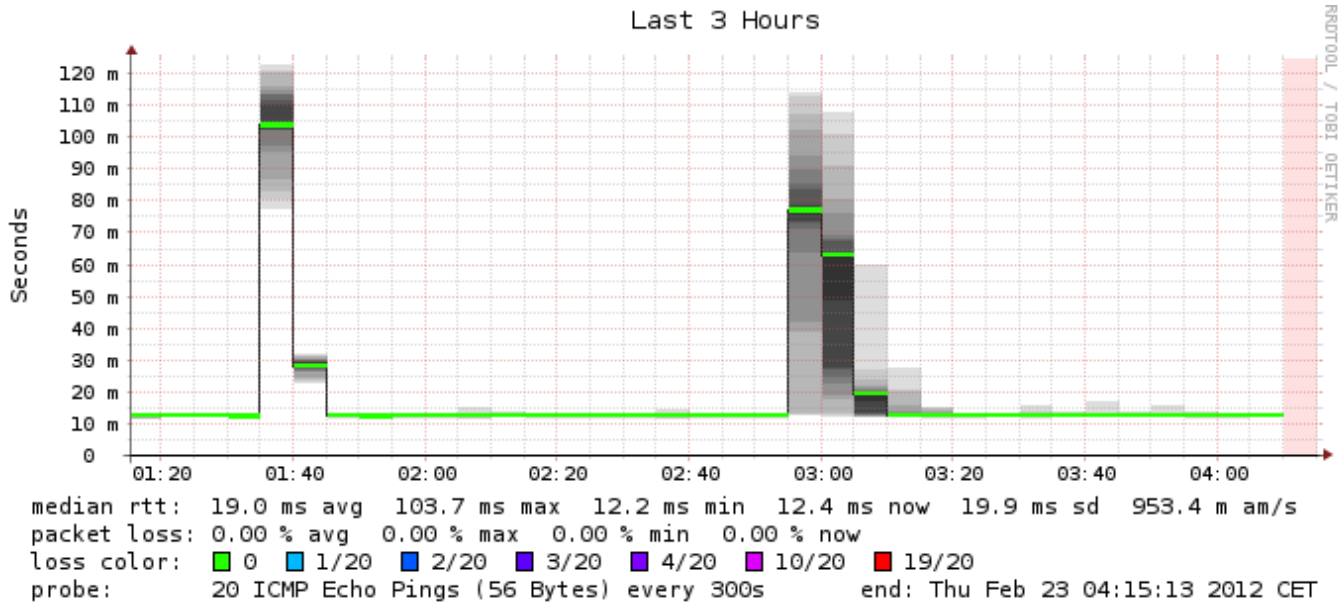
Two reasons for unreachable

- The host you ping is closed or doesn’t exist
- The host you ping has been configured to not to reply ping request (e.g. Firewall)

Different Ping utilities

- The ping page, a wealth of information regarding the Ping utility: http://www.ping127001.com/pingpage.htm
  - E.g., echoping, libping, netping (anti-smurf tool), webping, arping, fping, hping2, sping, xping, pingirva, pingx, Gping, Kping, IPing, Sing, etc.

- Example of a ping program that produces monitoring stats for hosts: Smokeping :keeps track of your network latency http://oss.oetiker.ch/smokeping/



Traceroute

- Finds the *route* that a packet would go across the network to reach a host.

- Command line tools:
  - $ traceroute host
  - $ tracepath host
  - > tracert host (Windows)

- Uses TTL (Time To Live, 8 bit field in IP header)
  - Specifies the time a packet is allowed to "live" in the network
  - At each hop, router or host decrements TTL value of packet by 1
  - When TTL = 1
    - Packet discarded
    - "ICMP Time Exceeded" error datagram sent back to source host

How does traceroute work?

- Sends out a batch of packets
  - First three packets have TTL = 1
  - Second three packets have TTL = 2
  - and so on….

- Each host along the way sees packet with TTL = 1
  - Sends ICMP warning message
  - Source host uses these messages to build list of all hosts in the route

Traceroute example

```
Tracing route to www.google.ca [74.125.129.94]
over a maximum of 30 hops:

  1     2 ms     2 ms     1 ms  h123-3.reznet.ucalgary.ca [136.159.123.3]
  2     2 ms     2 ms     1 ms  10.0.11.150
  3     2 ms     2 ms     1 ms  10.16.122.4
  4     2 ms     2 ms     2 ms  10.16.121.1
  5     7 ms     2 ms     4 ms  10.16.242.4
  6     3 ms     3 ms     6 ms  h66-244-233-17.bigpipeinc.com [66.244.233.17]
  7     6 ms     2 ms     2 ms  h208-118-103-166.bigpipeinc.com [208.118.103.166
]
  8     4 ms     2 ms     5 ms  clgr2rtr2.canarie.ca [199.212.24.66]
  9    40 ms    21 ms    22 ms  207.231.242.21
 10    21 ms    17 ms    16 ms  google-1-lo-std-707.sttlwa.pacificwave.net [207.
231.242.20]
 11    17 ms    19 ms    18 ms  209.85.249.34
 12    18 ms     *       20 ms  66.249.94.197
 13    25 ms    31 ms    25 ms  216.239.46.200
 14    24 ms    45 ms    24 ms  216.239.48.167
 15     *        *        *     Request timed out.
 16    26 ms    23 ms    26 ms  pd-in-f94.1e100.net [74.125.129.94]
```

resources

- Wikipedia entry on ping:
  http://en.wikipedia.org/wiki/Ping

- Wikipedia's entry on traceroute:
  http://en.wikipedia.org/wiki/Traceroute

- The ping page, a wealth of information regarding the Ping utility:
  http://www.ping127001.com/pingpage.htm

- Wikipedia's entry on ICMP:
  http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

Thanks for attending!