

# **Chapter 19: Internet Control Message Protocol**

Raj Jain

The Ohio State University

Columbus, OH 43210

Jain@CIS.Ohio-State.Edu

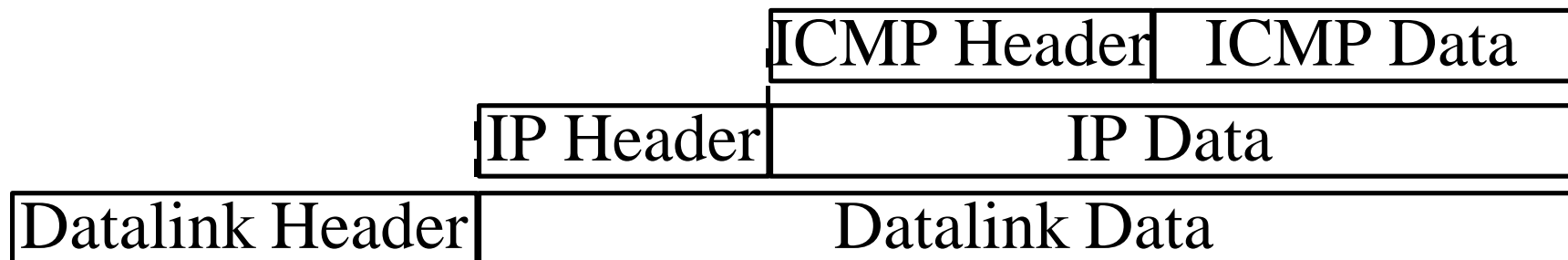
<http://www.cis.ohio-state.edu/~jain/>



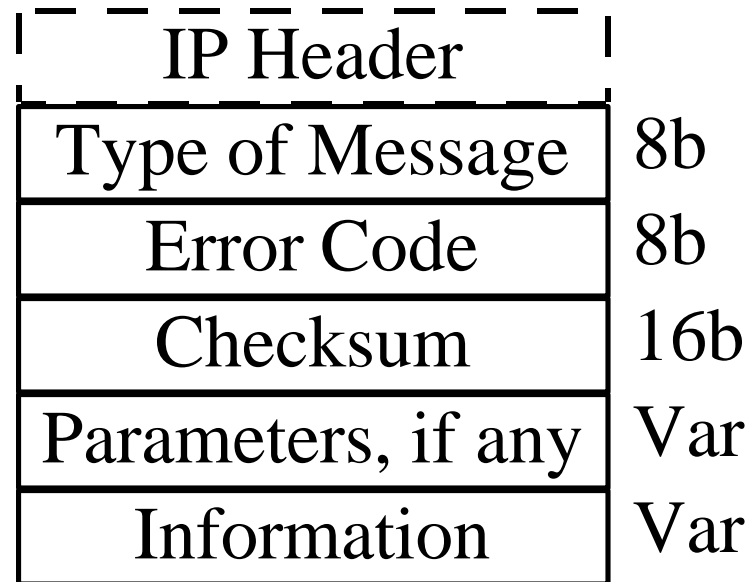
- ❑ What is ICMP?
- ❑ ICMP Messages
- ❑ ICMP applications: Ping, Traceroute, Path MTU discovery

# ICMP Features

- ❑ ICMP: Used by IP to send error and control messages
- ❑ ICMP uses IP to send its messages
- ❑ ICMP does not report errors on ICMP messages.
- ❑ ICMP message are not required on datagram checksum errors. (Some implementations still do)
- ❑ ICMP reports error only on the first fragment



# ICMP Message Format



# ICMP: Message Types

Type	Message
0	Echo reply
3	Destination unreachable
4	Source quench
5	Redirect
8	Echo request
11	Time exceeded
12	Parameter unintelligible
13	Time-stamp request
14	Time-stamp reply
15	Information request
16	Information reply
17	Address mask request
18	Address mask reply

# ICMP Messages

- ❑ Source Quench: Please slow down! I just dropped one of your datagrams.
- ❑ Time Exceeded: Time to live field in one of your packets became zero.” or “Reassembly timer expired at the destination.
- ❑ Fragmentation Required: Datagram was longer than MTU and “No Fragment bit” was set.
- ❑ Address Mask Request/Reply: What is the subnet mask on this net? Replied by “Address mask agent”

# Destination Unreachable

Code	Meaning
0	Network unreachable
1	Host unreachable
2	Protocol unreachable
3	Port unreachable
4	Fragmentation need and don't fragment bit set
5	Source route failed
6	Destination network unknown
7	Destination host unknown
8	Source host isolated
9	Communication with dest net administratively prohibited
10	Communication with dest host administratively prohibited
11	Network unreachable for type of service
12	Host unreachable for type of service

# Other ICMP Messages

- ❑ Redirect: Please send to router X instead of me.
  - 0 = Redirect datagrams for the network
  - 1 = Redirect datagrams for the host
  - 2 = Redirect datagrams for the type of service and net
  - 3 = Redirect datagrams for the type of service and host
- ❑ Time Stamp Request/Reply:

0	8	16	31
Type	Code	Checksum	
Identifier		Sequence Number	
Originate Timestamp			
Receive Timestamp			
Transmit Timestamp			

# Other ICMP Messages

- ❑ Information Request/Reply:  
Set source and destination addresses to 0 in the request and broadcast  
Server replies back with your IP address  
(Not used. Replaced by RARP and BOOTP)

# Ping

## ❑ Sample Output

Wed, 05 Feb 1997 15:21:37

Pinging snoopy.cis.ohio-state.edu [164.107.144.3] with 48 data bytes

Reply from 164.107.144.3: 48 bytes in 47 msec. TTL: 253

Reply from 164.107.144.3: 48 bytes in 46 msec. TTL: 253

Reply from 164.107.144.3: 48 bytes in 47 msec. TTL: 253

Reply from 164.107.144.3: 48 bytes in 46 msec. TTL: 253

Reply from 164.107.144.3: 48 bytes in 47 msec. TTL: 253

PING Statistics for snoopy.cis.ohio-state.edu

5 packets transmitted, 5 packets received, 0% packet loss

round-trip (ms) min/avg/max = 46/46/47

## ❑ Uses ICMP Echo request/reply messages

# Traceroute: Sample Output

164.107.61.200 164.107.61.1 164.107.120.1 164.107.144.3

Wed, 05 Feb 1997 14:57:33

Sending 48 data bytes to snoopy.cis.ohio-state.edu  
[164.107.144.3]

1:Received echo from ? [164.107.61.1] in 110 msec.

2:Received echo from avon-120.cis.ohio-state.edu  
[164.107.120.1] in 45 msec.

3:Received 48 bytes from snoopy.cis.ohio-state.edu  
[164.107.144.3] in 49 msec.

TraceRoute Statistics for snoopy.cis.ohio-state.edu

3 packets transmitted, 3 packets received, 0% packet loss

round-trip (ms) min/avg/max = 45/68/110

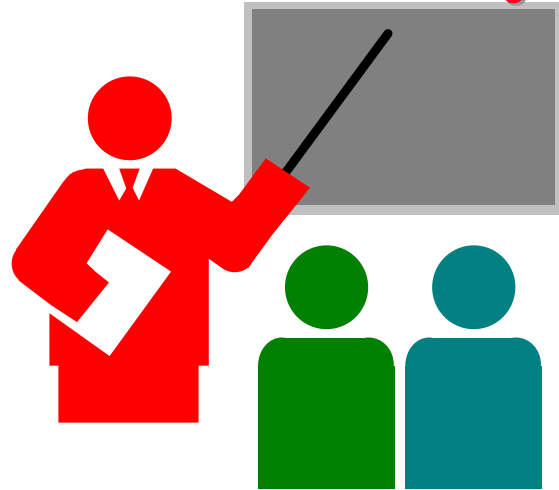
# Traceroute Mechanism

- ❑ Send the packet with time-to-live = 1 (hop)
- ❑ The first router discards the packet and sends an ICMP “time-to-live exceeded message”
- ❑ Send the packet with time-to-live = 2 (hops)
- ❑ The second router discards the packet and sends an ICMP “time-to-live exceeded message”
- ❑ This is repeated until the response is received from the destination.

# Path MTU Discovery

- ❑ Send a large IP datagram with “No fragment” bit set.
- ❑ Reduce size until success (No ICMP message received)

# Summary



- ❑ ICMP is the control sibling of IP
- ❑ ICMP is used by IP and uses IP as network layer protocol
- ❑ ICMP is used for ping, traceroute, and path MTU discovery.

# Homework

- Read chapter 19 and RFC792

# References

- ❑ [RFC0792] J. Postel, "Internet Control Message Protocol", 09/01/1981, 21 pages.
- ❑ [RFC1885] A. Conta, S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)", 01/04/1996, 20 pages.
- ❑ [RFC1788] W. Simpson, "ICMP Domain Name Messages", 04/14/1995, 7 pages.
- ❑ [RFC1473] F. Kastenholz, "The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol", 06/08/1993, 9 pages.

- ❑ [RFC1256] S. Deering, "ICMP Router Discovery Messages", 09/05/1991, 19 pages.
- ❑ [RFC1122] R. Braden, "Requirements for Internet hosts - communication layers", 10/01/1989, 116 pages.
- ❑ [RFC0844] C. Clements, "Who talks ICMP, too? - Survey of 18 February 1983", 02/18/1983, 5 pages.
- ❑ [RFC0789] E. Rosen, "Vulnerabilities of network control protocols: An example", 07/01/1981, 15 pages.