Lab # 4: ICMP Protocol

Internet Control Message Protocol

ICMP Protocol

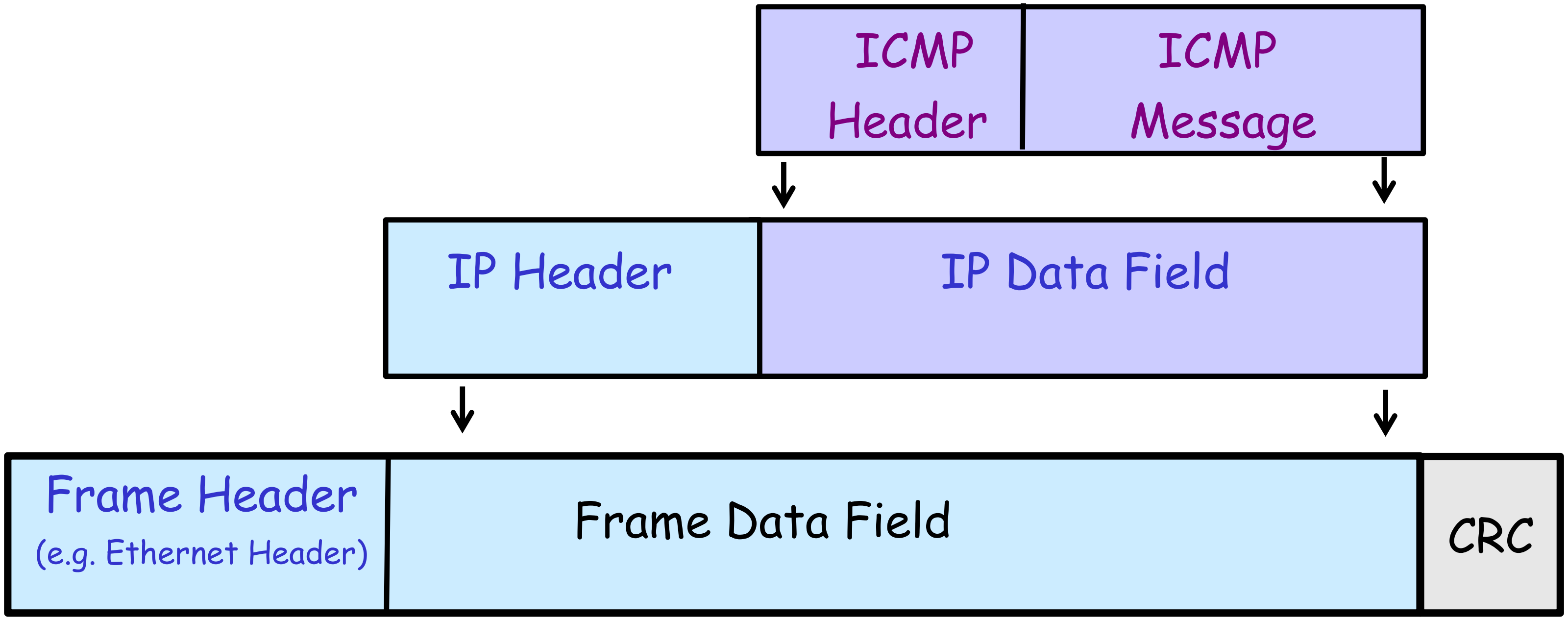
- On the Internet there are no hardware mechanisms available to check connectivity
- IP Protocol doesn’t provide tools for problems detection and troubleshooting
- A new module is introduced: ICMP * (Internet Control Message Protocol)
- This protocol allows hosts and routers to send control messages to other hosts and routers
- * RFC 792

ICMP Overview

- ICMP allows us to know, for example, why a datagram has not been delivered (there is no route, the destination does not respond, the time to life is exhausted, etc.)
- ONLY the sender of the datagram, that caused the error, is informed about the error
- ICMP doesn’t correct the problem (only inform!)

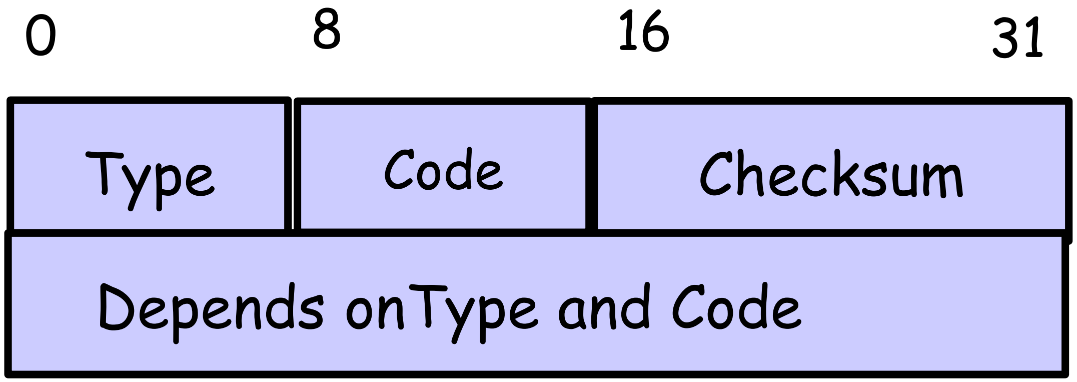
ICMP Message Encapsulation

- ICMP messages are encapsulated in IP datagrams
  - But ICMP is not considered a higher level protocol to IP



ICMP Message Format

- Each message has its own format, but all begin with the own fields:
  - Type (8 bits): Identifies the message type
  - Code (8 bits): More information about the message type
  - Checksum (16 bits): Use the same algorithm as IP



0	8	16	31
Type	Code	Checksum	
Depends onType and Code			

ICMP Messages Types

- The type of message determines its meaning and format.
  - There are 15 different types.
  - Among the main ones we have:

Type	ICMP Message	Request	Error
0	Echo reply	✓	
3	Unreachable Destination		✓
8	Echo request	✓	
11	Datagram Time exceeded		✓

  - The error messages contain the IP header + 8 first bytes of data from the original datagram

ICMP Error Messages

- Error messages are never generated in response to:
  - An ICMP error message
  - A datagram with a broadcast destination IP address
  - A fragment that is not the first fragment of the original datagram
  - A datagram whose source IP address does not define a single machine (that is, the source address can not be zero, the loopback address, broadcast addresses)
- All this to prevent broadcast storms

Echo Message (request/reply)

- The Echo reply message returns the same data that was received in the Echo request message
- They are used to build the *Ping* tool
- It is employed by administrators and users to detect problems on the network
- It allows hosts/routers to :
  - Check if a destination is active and if there is a route to it
  - Measure the time of "round trip"
  - Estimate the reliability of the route

Time Exceeded Message

- These types of messages can be sent by routers and hosts:
  - Routers: when they discard a datagram at the end of their time to life
  - Hosts: when a timeout occurs while waiting for all the fragments of a datagram
- The code field explains which of the two events has occurred

Unreachable Destination Messages

- They are sent by a router or host when it can not send or deliver an IP datagram
- They are sent to the sender of the original datagram
- The code field contains an integer with additional information.
- Some important ones are:

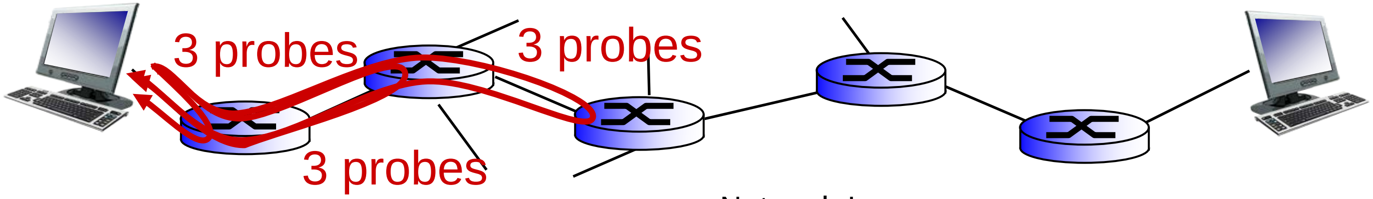
Cod.	Description
0	Unreachable Network
1	Unreachable Host
2	Unreachable Protocol
3	Unreachable Port
4	Fragmentation is required but DF flag enabled
6	Unknown Destination Network
7	Unknown Destination Host

Traceroute and ICMP

- source sends series of UDP segments to dest
  - first set has TTL =1
  - second set has TTL=2, etc.
  - unlikely port number
- when *n*th set of datagrams arrives to nth router:
  - router discards datagrams
  - and sends source ICMP messages (type 11, code 0)
  - ICMP messages includes name of router & IP address
- when ICMP messages arrives, source records RTTs

stopping criteria:

- UDP segment eventually arrives at destination host
- destination returns ICMP "port unreachable" message (type 3, code 3)
- source stops



ICMP Summary

- used by hosts & routers to communicate network-level information
  - error reporting: unreachable host, network, port, protocol
  - echo request/reply (used by ping)
- network-layer "above" IP:
  - ICMP msgs carried in IP datagrams
- ICMP message: type, code plus first 8 bytes of IP datagram causing error

Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header