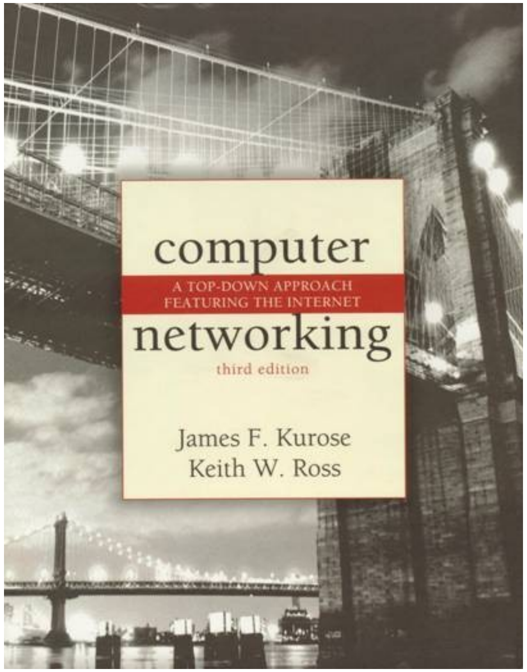
Chapter 4: Internet network protocols Revised by Quan Le-Trung, Dr.techn.

http://sites.google.com/site/quanletrung/



Computer Networking: A Top Down Approach Featuring the Internet, 3rd edition.
Jim Kurose, Keith Ross
Addison-Wesley, July 2004.

A note on the use of these ppt slides:

We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

❑ If you use these slides (e.g., in a class) in substantially unaltered form, that you mention their source (after all, we'd like people to use our book!)

❑ If you post any slides in substantially unaltered form on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

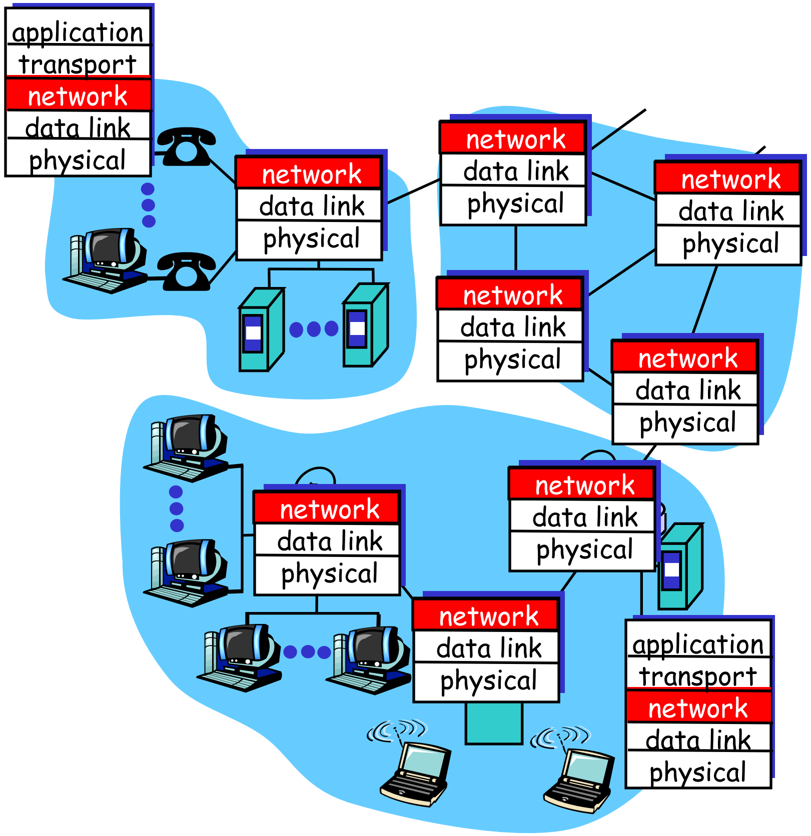
Thanks and enjoy! JFK/KWR

Internet network protocols

- Introduction & IP Datagram
- ICMP
- DHCP

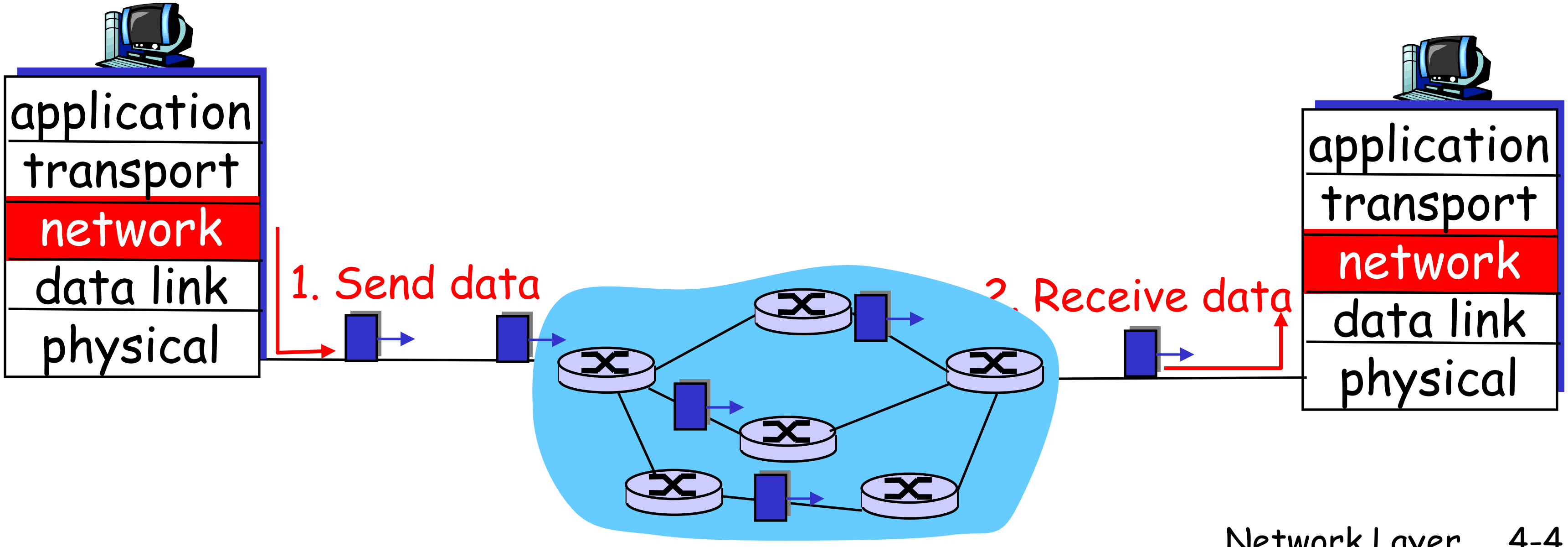
Network layer

- ❒ transport segment from sending to receiving host
- ❒ on sending side encapsulates segments into datagrams
- ❒ on rcving side, delivers segments to transport layer
- ❒ network layer protocols in *every* host, router
- ❒ Router examines header fields in all IP datagrams passing through it



Datagram networks

- no call setup at network layer
- routers: no state about end-to-end connections
  - no network-level concept of "connection"
- packets forwarded using destination host address
  - packets between same source-dest pair may take different paths



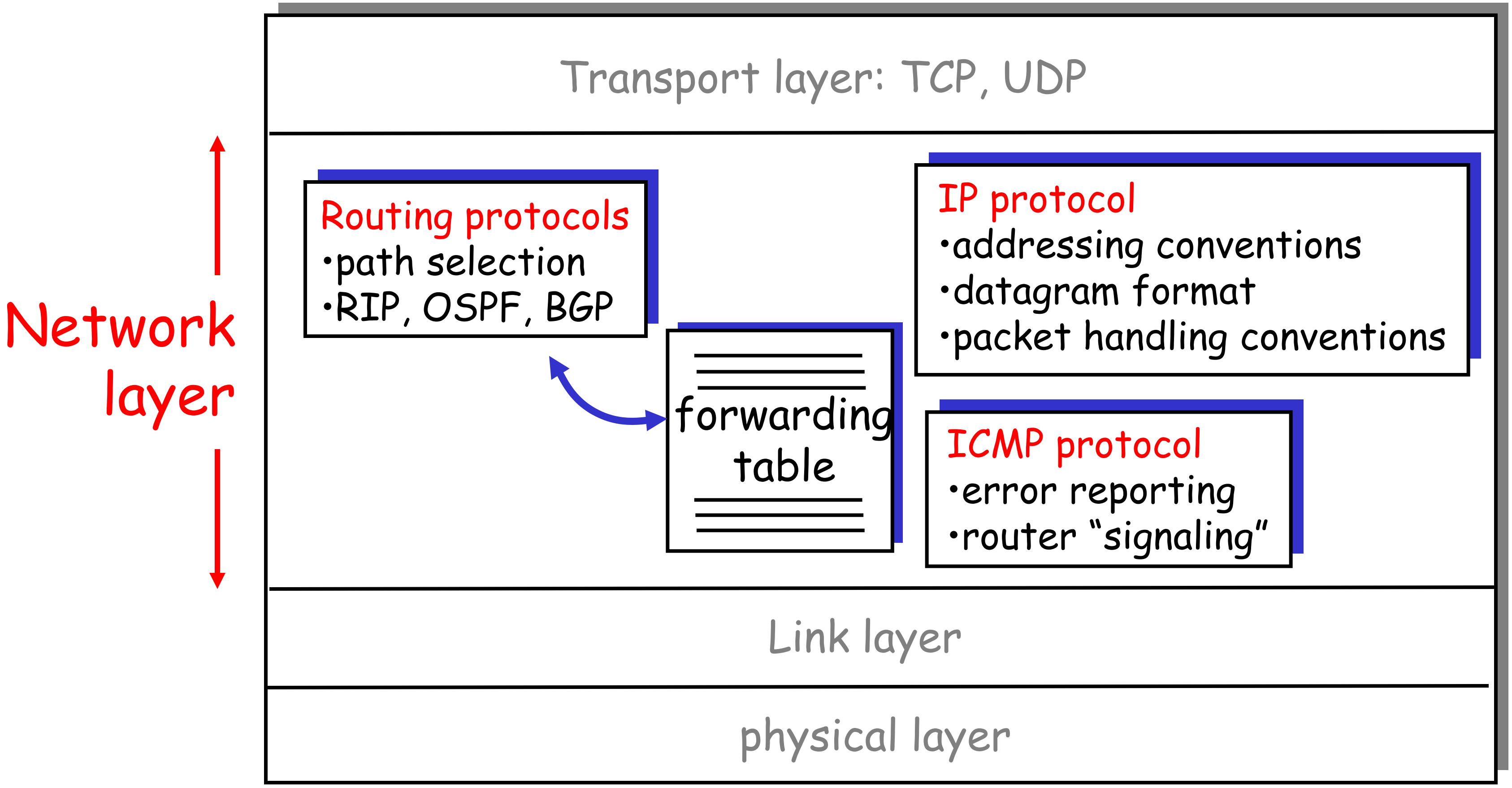
Datagram Networks: Internet

Internet

- data exchange among computers
  - “elastic” service, no strict timing req.
- “smart” end systems (computers)
  - can adapt, perform control, error recovery
  - simple inside network, complexity at “edge”
- many link types
  - different characteristics
  - uniform service difficult

The Internet Network layer

Host, router network layer functions:



Transport layer: TCP, UDP

Network layer

Routing protocols
- path selection
- RIP, OSPF, BGP

forwarding table

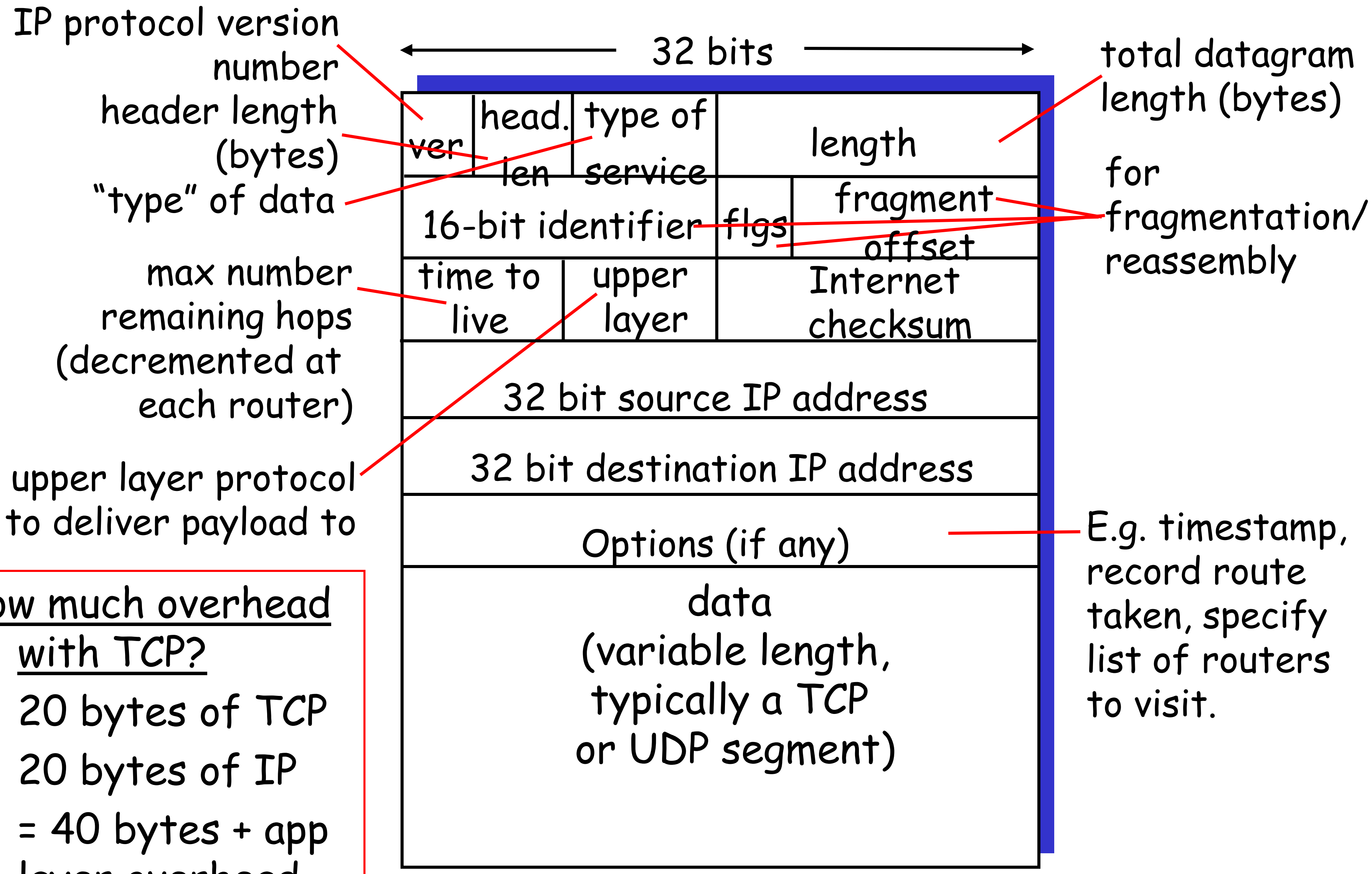
IP protocol
- addressing conventions
- datagram format
- packet handling conventions

ICMP protocol
- error reporting
- router "signaling"

Link layer

physical layer

IP datagram format



IP protocol version number

header length (bytes)

"type" of data

max number remaining hops (decremented at each router)

upper layer protocol to deliver payload to

total datagram length (bytes)

for fragmentation/ reassembly

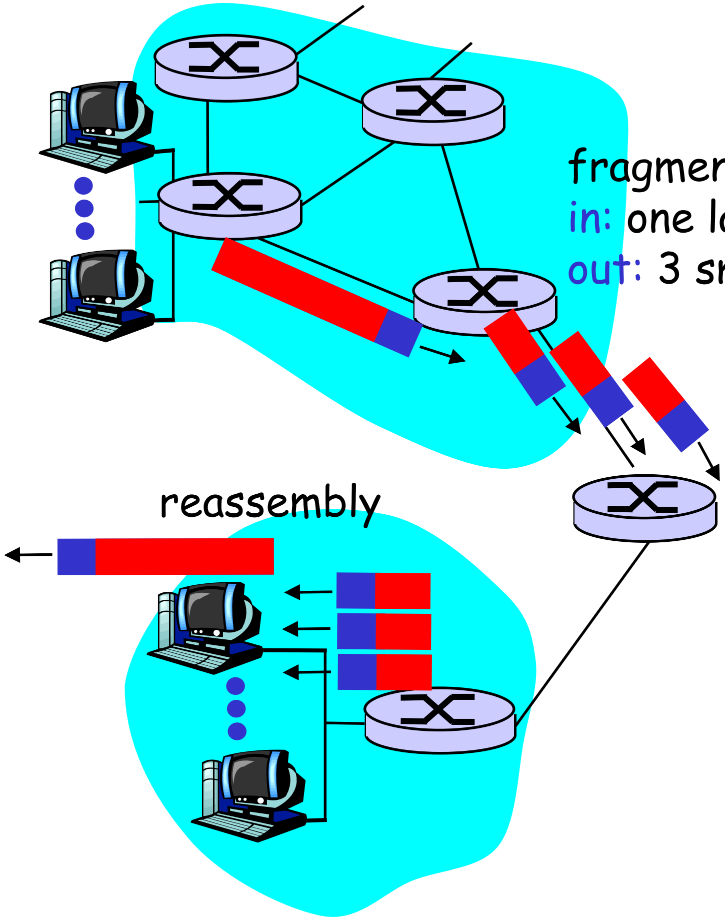
E.g. timestamp, record route taken, specify list of routers to visit.

how much overhead with TCP?

- 20 bytes of TCP
- 20 bytes of IP
- = 40 bytes + app layer overhead

IP Fragmentation & Reassembly

- network links have MTU (max.transfer size) - largest possible link-level frame.
  - different link types, different MTUs
- large IP datagram divided ("fragmented") within net
  - one datagram becomes several datagrams
  - "reassembled" only at final destination
  - IP header bits used to identify, order related fragments



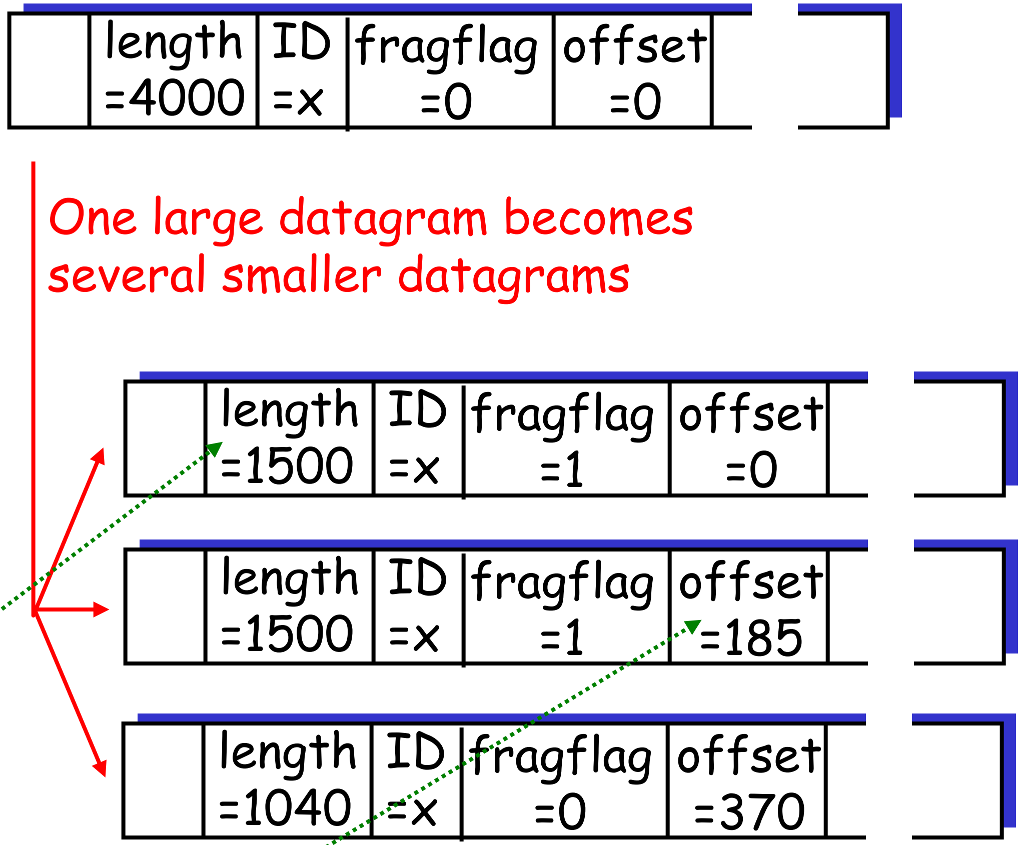
fragmentation:
in: one large datagram
out: 3 smaller datagrams

reassembly

IP Fragmentation and Reassembly

Example

- 4000 byte datagram
  - +40 header bytes (20 TCP, 20 IP)
- MTU = 1500 bytes
  - 20 bytes of header, e.g., IP
  - 1480 data bytes



length	ID	fragflag	offset
=4000	=x	=0	=0

One large datagram becomes several smaller datagrams

length	ID	fragflag	offset
=1500	=x	=1	=0
=1500	=x	=1	=185
=1040	=x	=0	=370

http://media.pearsoncmg.com/aw/aw_kurose_network_2/applets/ip/ipfragmentation.html

1480 bytes in data field

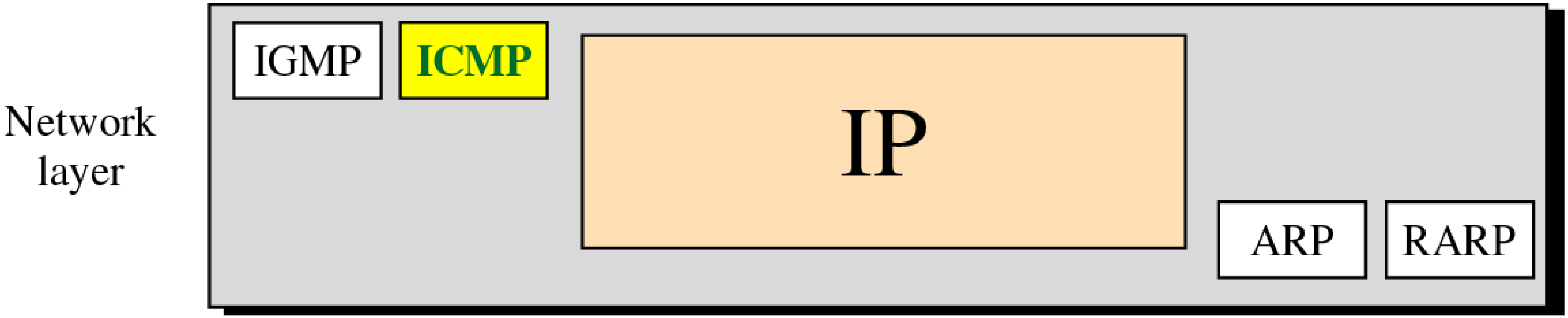
offset = 1480/8

CALCULATION

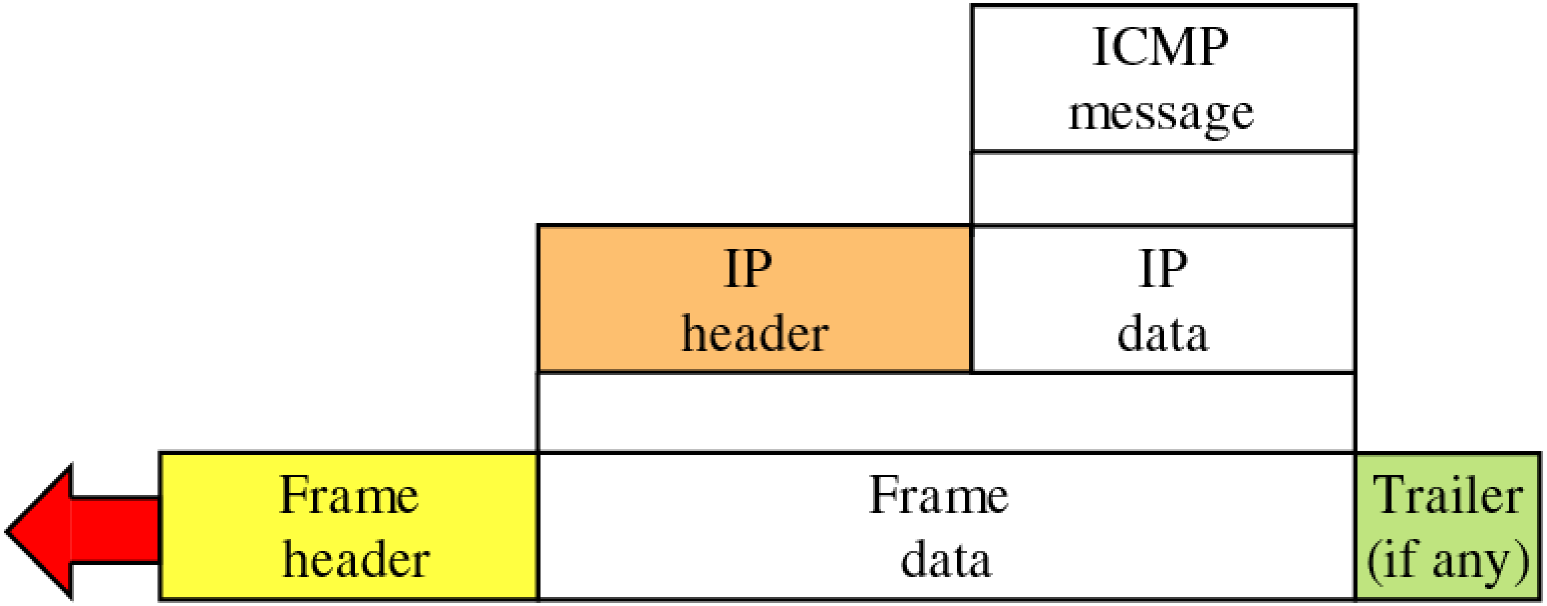
ICMP

- ICMP is a mechanism used by hosts and routers to send notification of datagram problems back to the sender
- As mentioned, IP is essentially an unreliable and connectionless protocol, ICMP allows IP to inform a sender if a datagram is undeliverable (router cannot route the packet)
- ICMP uses echo test/reply to test whether a destination is reachable and responding
- It also handles both control and error messages.
- Its sole function is to report problem, not correct it

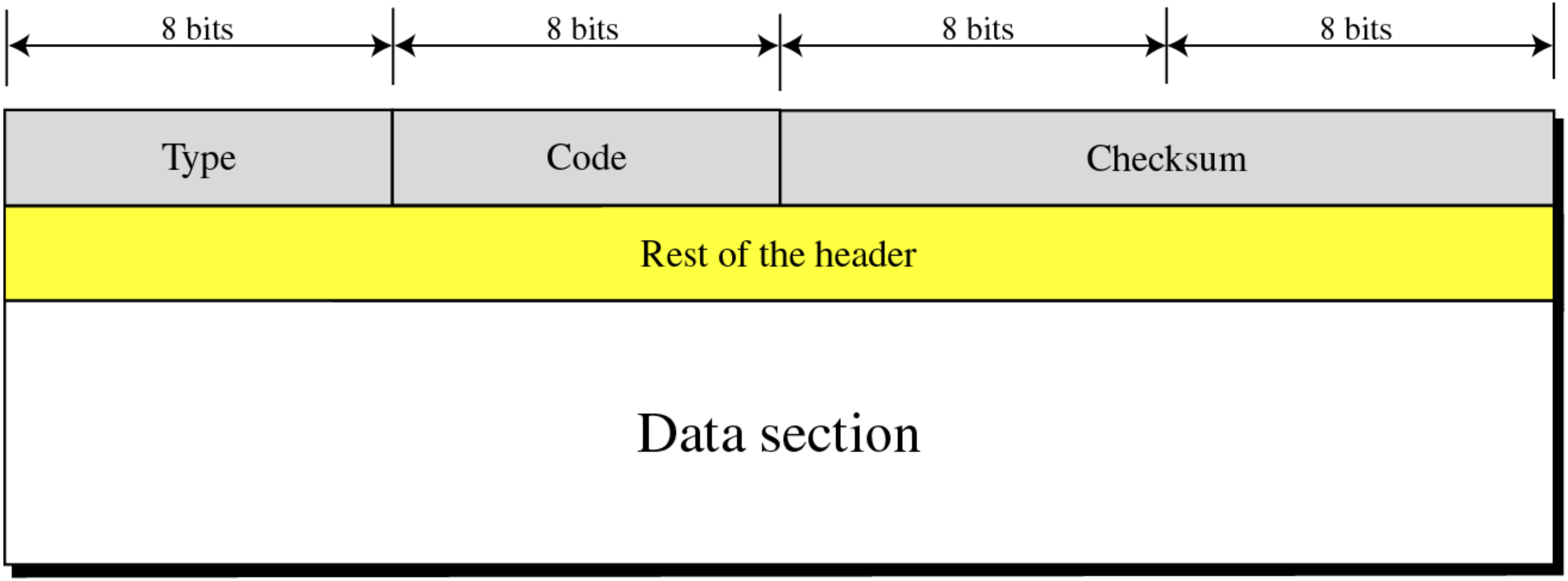
Position of ICMP in the network layer



Encapsulation of ICMP packet



General format of ICMP messages



8 bits

8 bits

8 bits

8 bits

Type

Code

Checksum

Rest of the header

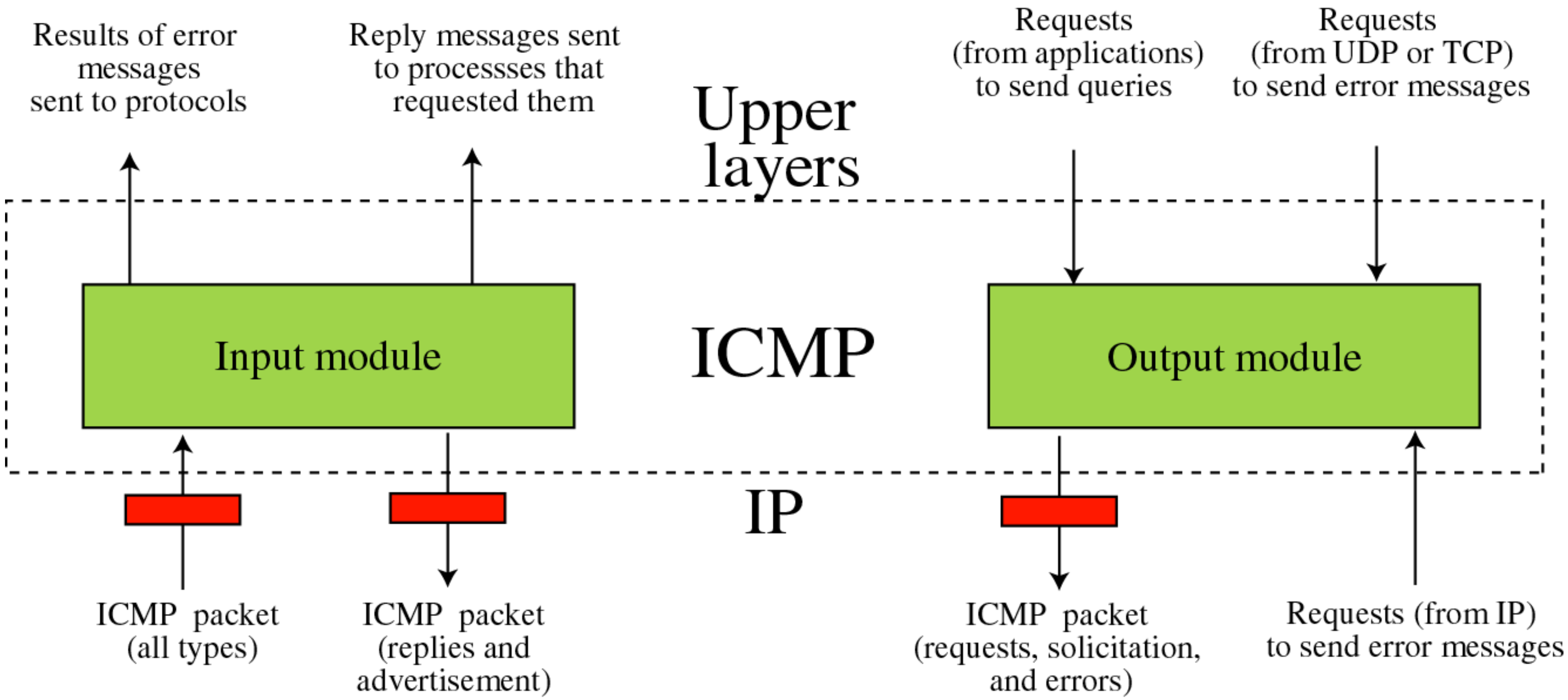
Data section

ICMP: Internet Control Message Protocol

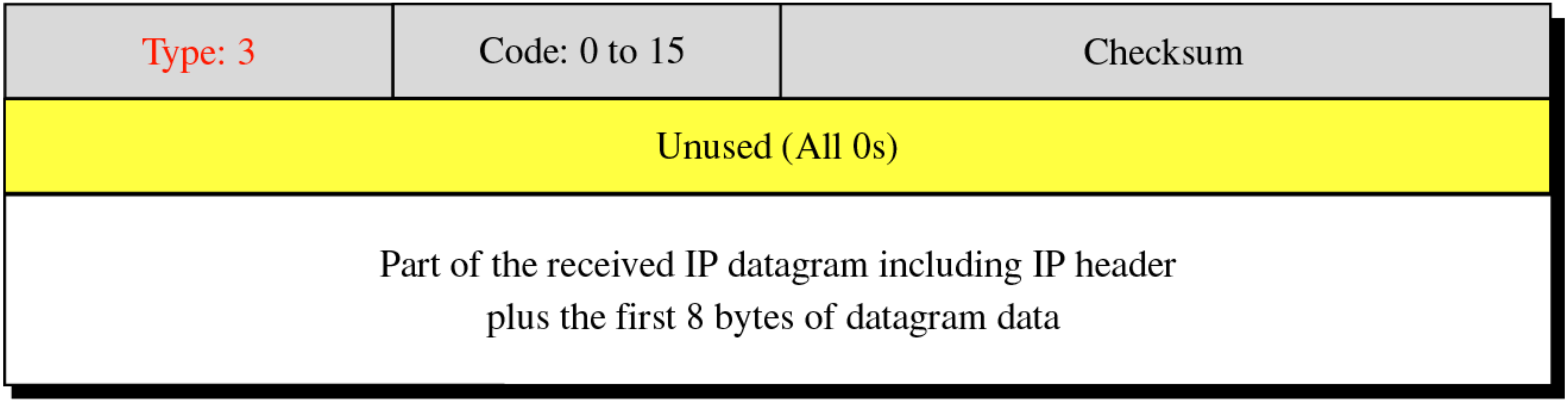
- used by hosts & routers to communicate network-level information
  - error reporting: unreachable host, network, port, protocol
  - echo request/reply (used by ping)
- network-layer "above" IP:
  - ICMP msgs carried in IP datagrams
- ICMP message: type, code plus first 8 bytes of IP datagram causing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

ICMP package


Results of error messages sent to protocols
Reply messages sent to processses that requested them
Upper layers
Requests (from applications) to send queries
Requests (from UDP or TCP) to send error messages
Input module
ICMP
Output module
IP
ICMP packet (all types)
ICMP packet (replies and advertisement)
ICMP packet (requests, solicitation, and errors)
Requests (from IP) to send error messages

Destination-unreachable format



Type: 3

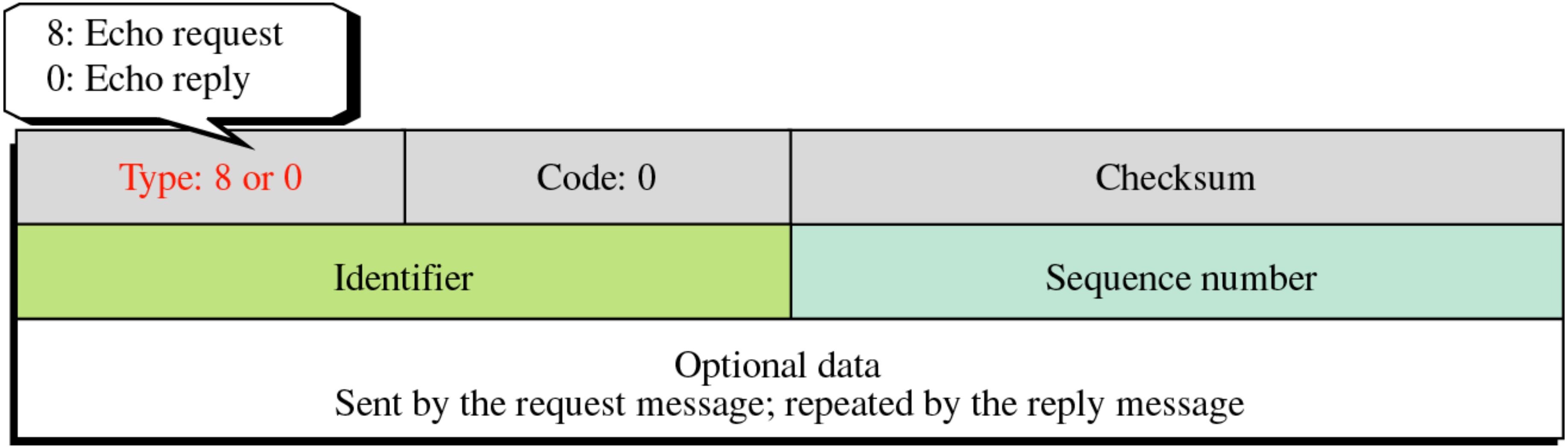
Code: 0 to 15

Checksum

Unused (All 0s)

Part of the received IP datagram including IP header
plus the first 8 bytes of datagram data

Echo-request and echo-reply message forma



8: Echo request
0: Echo reply

Type: 8 or 0

Code: 0

Checksum

Identifier

Sequence number

Optional data
Sent by the request message; repeated by the reply message

Ping command can use theses messages.

Traceroute and ICMP

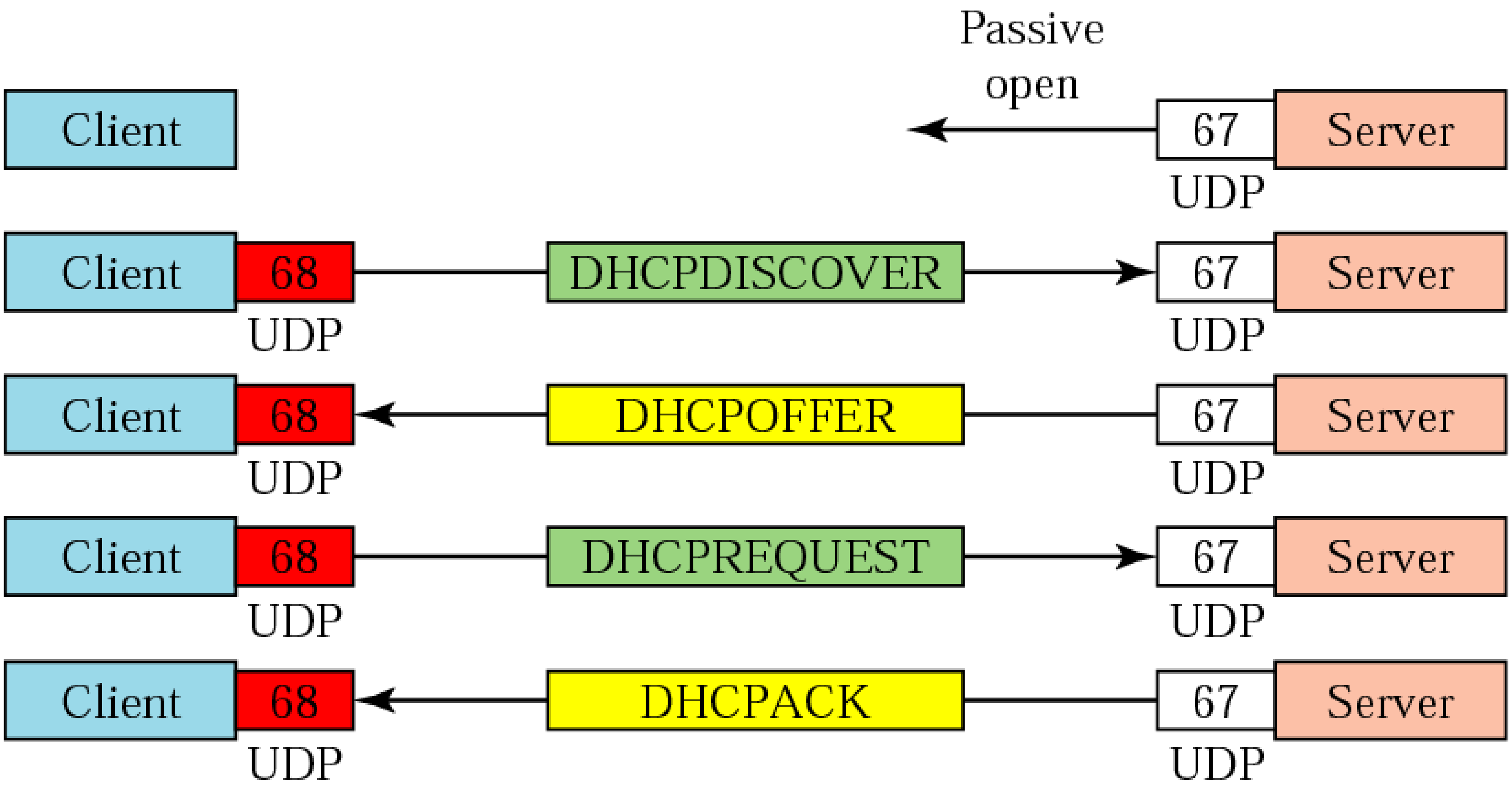
- Source sends series of UDP segments to dest
  - First has TTL =1
  - Second has TTL=2, etc.
  - Unlikely port number
- When nth datagram arrives to nth router:
  - Router discards datagram
  - And sends to source an ICMP message (type 11, code 0)
  - Message includes name of router& IP address
- When ICMP message arrives, source calculates RTT
- Traceroute does this 3 times

Stopping criterion

- UDP segment eventually arrives at destination host
- Destination returns ICMP "host unreachable" packet (type 3, code 3)
- When source gets this ICMP, stops.

See lecture02_icmp_diagrams.pdf for the sequence diagram! And DEMO via WIRESHARK

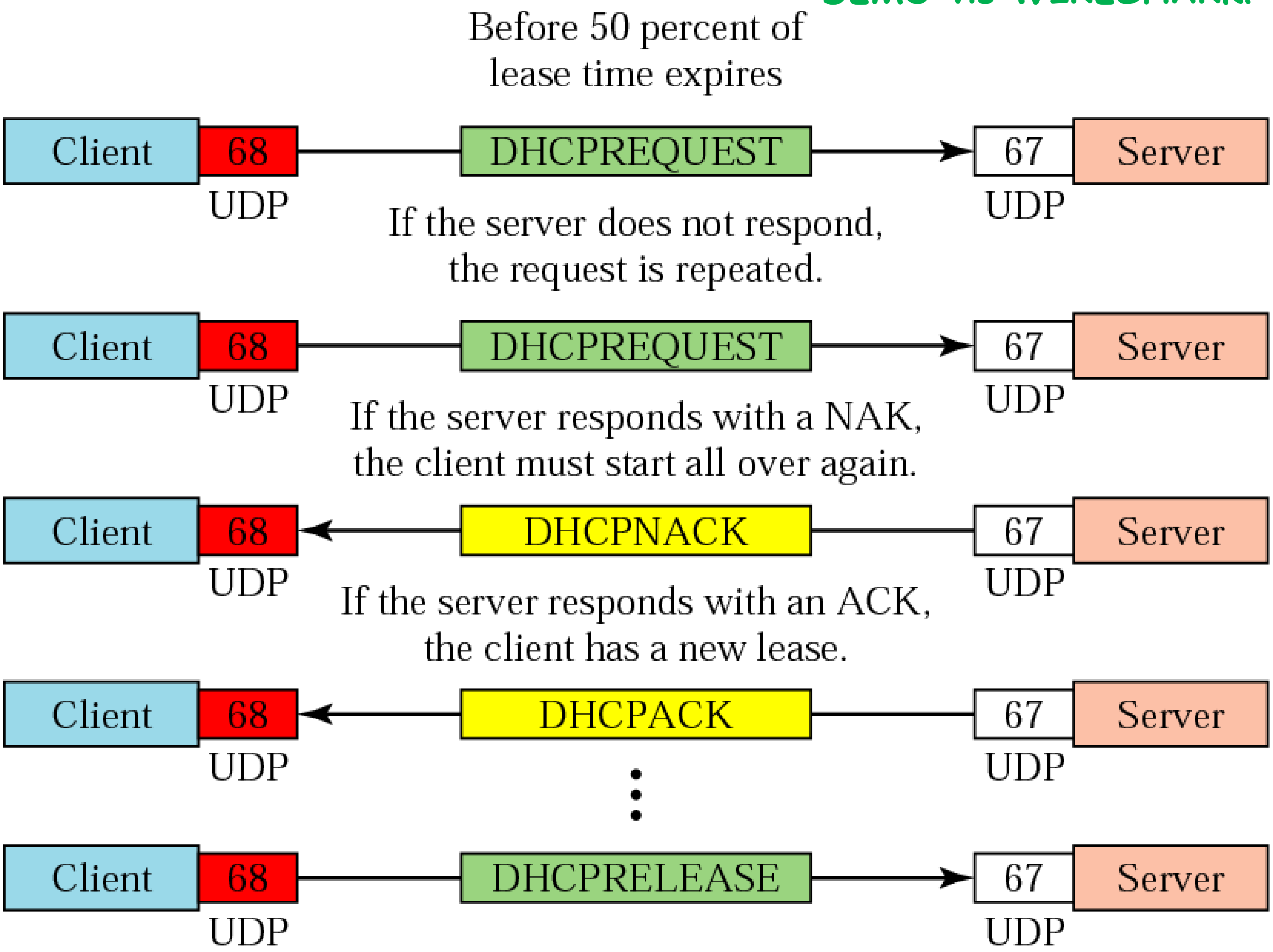
Exchanging messages



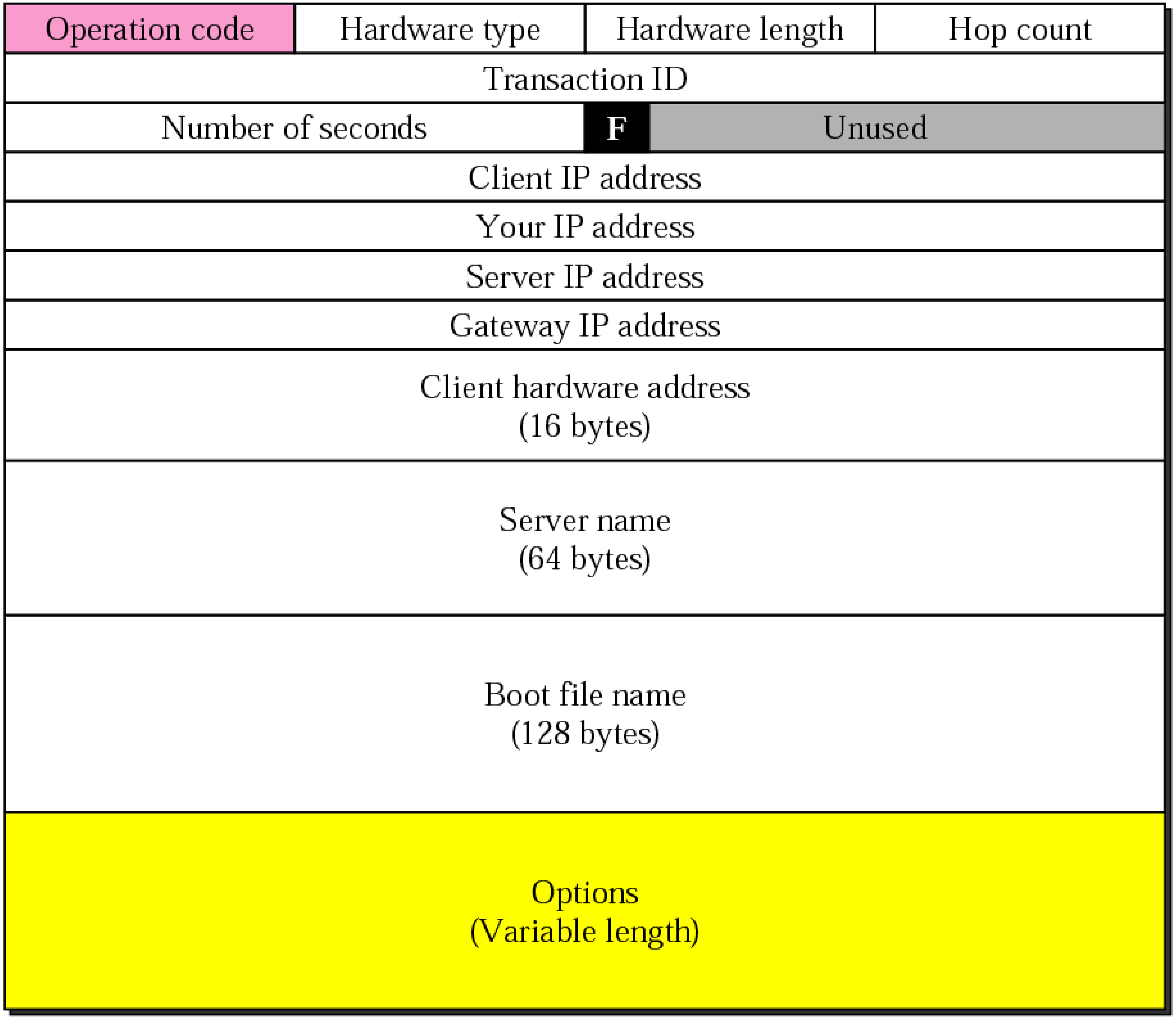
See lecture02_dhcp_diagrams.pdf for the sequence diagram! And DEMO vis WIRESHARK!

Exchanging messages

See lecture02_dhcp_diagrams.pdf for the sequence diagram! And DEMO vis WIRESHARK!


Before 50 percent of lease time expires
Client
68
UDP
DHCPREQUEST
67
UDP
Server
If the server does not respond, the request is repeated.
Client
68
UDP
DHCPREQUEST
67
UDP
Server
If the server responds with a NAK, the client must start all over again.
Client
68
UDP
DHCPNACK
67
UDP
Server
If the server responds with an ACK, the client has a new lease.
Client
68
UDP
DHCPACK
67
UDP
Server
Client
68
UDP
DHCPRELEASE
67
UDP
Server

DHCP packet



<table>
<tr><td>Operation code</td><td>Hardware type</td><td>Hardware length</td><td>Hop count</td></tr>
<tr><td colspan="4">Transaction ID</td></tr>
<tr><td colspan="2">Number of seconds</td><td>F</td><td>Unused</td></tr>
<tr><td colspan="4">Client IP address</td></tr>
<tr><td colspan="4">Your IP address</td></tr>
<tr><td colspan="4">Server IP address</td></tr>
<tr><td colspan="4">Gateway IP address</td></tr>
<tr><td colspan="4">Client hardware address
(16 bytes)</td></tr>
<tr><td colspan="4">Server name
(64 bytes)</td></tr>
<tr><td colspan="4">Boot file name
(128 bytes)</td></tr>
<tr><td colspan="4">Options
(Variable length)</td></tr>
</table>