#1 (Lec-12)

Chapter-7 (TCP/IP)

IPv4

28-June
Monday

Important frame/packet format → Wired LAN, IPv4, IPv6

Syllabus (7.1—7.5), 7.7, 7.8.

IP → connectionless protocol

Trying to move from datagram to virtual circuit switching.

- IGMP → Internet Group Management Protocol
- ICMP → Internet Control Message Protocol
- ARP → Address Resolution Protocol

IP encapsulation

→ All these are helper protocols and these packets are encapsulated by IP packet.

Ex- the physical address generated by ARP is encapsulated by IP

→ If a router receives an unfragmentable packet exceeding MTU (maximum transfer unit) then the packet is dropped and an error message is sent.

ICMP packets are used for error messages and the ICMP packet is encapsulated by IP.

IP provides encapsulation to other helper protocols.

Datagram (IP packet)

IP header (20—60 bytes)

* The protocol field in an IP packet determines receiving protocol.
* Time to live → maximum no. of hops (routers) visited by packet.
  - (The packet decrements by 1 in each hop).
  - Usually 2 times max no. of routers between 2 hosts
  - When ttl = 0, then packet is dropped.

→ 3-bit-flag

X	D	M
Reserved	Do not fragment	More fragment

More fragment – [more fragments are com…]
- → 1 (not last fragment)
- → 0 (last fragment)

a) Version

→ Valid 4/6 [0100 or 0110]

b) Header Length

No. of bytes of packet [4 bits]

→ Multiplying by 4 we get header length

If the packet is

$\underbrace{0100}_{Ip4}\,\underbrace{1110}_{14}$

↳ (14×3) = 42 bytes

Header len field can have (5 to 15) values.

c) ~~Frame offset~~

(*) Identification number is counted in the same session.
The fragmented packets have same identification no.

#2 (lec-13)

Chapter-7 (TCP/IP)
IPv4 (continued)

30-June
Wednesday

Service Type

			4 bit	X

8 bit

[For priority] → 3 bit for precedence

~~Select~~ TOS (type of service)

	D	T	R	C	
					0000 (Normal)
· Delay					1000 Minimise Delay
· Throughput					0100 Maximise throughput
· Reliability					0010 Maximize Realiability
· Cost					0001 Minimise cost

Newer version of service type

6 bits	X	X

$2^6 = 64$ code-points

Differential Service Interpretation

Category		
1	0	Internet
2	11	Local
3	01	Temporary

0, 2, 4, 6, ...

3, 7, 11, ...

1, 5, 9, ...

→ This kind of assignment is done for backwards compatibility

[(*) Only data portion of the packet can be fragmented, The header is just copied.]

Offset → the starting value of the whole data frame divide by 8

Data

0 — 1399   offset value → $0/8 = 0$

Data

1400 — 2799   offset value → $1400/8 = 175$

By multiplying offset value by 8, we get actual value.

Option Format (TLV)

Type	Length	Value
8 bit	8 bit	Variable

Type: 1 - 2 - 5

Copy Class Number

- Option
  - → Single Byte
    - → No Operation
    - → End of Operation
  - → Multiple Byte
    - → Record Route
    - → Source Route
      - → Strict,
      - → Loose
    - → Timestamp

- Strict → All the addresses must be visited but no other addresses can be visited
- Loose → All addresses must be visited, more addresses can be visited if required.

In case of source routing,
destination IP address changes.

Record Route

Type	Length	~~Value~~ Pointer	Value
7	(No. of bytes for recording) Single IP address is ~~8~~ 4 bytes (32 bits)	~~AHH~~ Pointing to the next empty space	

If length is 15 then it can store ~~0~~3 IP addresses

→ The IP addresses are stored in value for Record route when a new router is visited

→ For source route, at first all IP addresses are stored and only those are visited (for strict)

For timestamp, the router puts their time-stamp in the value field. Overflow determines the no. of routers who couldn't put timestamp value ~~in~~ because value ~~ful~~

→ Timestamp can be done with strict routing.

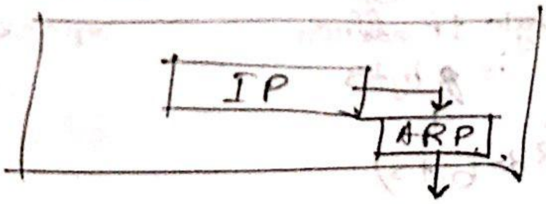
IP Package → The modules responsible for packaging the IP address.

→ Read the ~~????~~ pseudocode.

#3
Lec-14

ARP
TCP/IP, Chapter-8

(*) ARP → maps the logical address to a physical address and sends/relays frame to data link layer.



ARP has a request and reply packet
request → broadcast
reply → unicast

Static Mapping disadvantages

→ Some devices change MAC addresses after rebooting.
→ Changing Network Interface card (NIC) changes P.A.

IP → connectionless, unreliable
But using ARP, and physical address, we solve this problem.

ARP Packet → Query Packet [Broadcast]
→ Response Packet [Unicast]

(*) ARP requests to find target ~~IP~~ IP address's physical address.

(*) In the ethernet frame used for ARP query or request packet, the physical address is broadcast address.

APP Packet

Handware Type		Protocol Type
H.W Len	Protocol Len	Packet type (Req or response)
Sender MAC Address		
Sender IP Address		
Target Receiver ~~IP~~ MAC Address (0 for request)		
Target Receiver IP Address		

Variable Length

[The answer to ARP Request]

Proxy ARP

→ For subnetting (to restrict broadcast domain effect)

(*) A proxy ARP router replies to any ARP request, for those particular destinations, with its own physical address.

(a set of hosts)

I.e. reply packet has ARP proxy router's physical address in sender MAC address portion.

When the router receives the actual ~~MA~~ IP packet, it forwards to the actual sender.

ARP Package

→ Components of ARP and their relationships

Cache is used to store repeating MAC address requests. The cache table stores such addresses for limited time.

State →
- Free
- Pending
- Resolved

ICMP

→ For error reporting messages
(shortcoming of IP for unreliability)

→ query messages

[Encapsulated in an IP packet]
(Goes to upper layer)

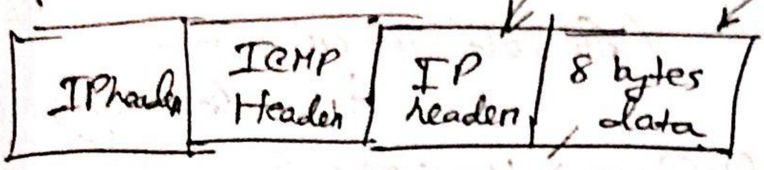
#4
Lec-15

ICMP
Chapter-9

ICMP Packet

Old dropped packet IP header

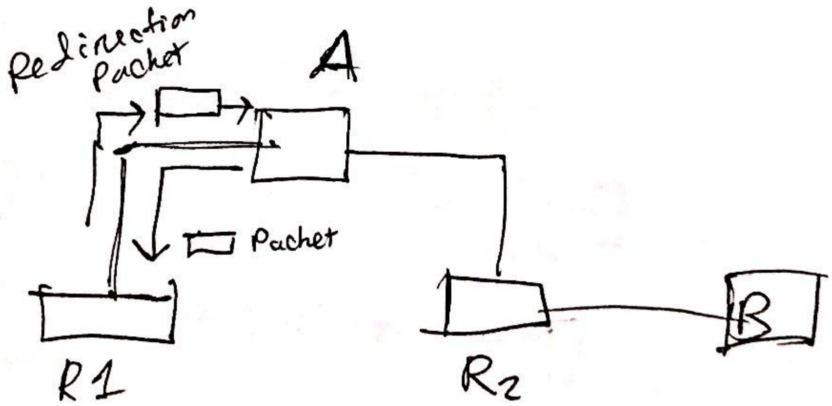
First 8 bytes of data from dropped packet.



ICMP packet encapsulated in an IP packet.

Redirection Concept

→ A host machine has no routing capability and sends it to wrong router, The wrong router redirects the message to host and tells it to send to appropriate router.



Cases where ICMP is not generated

→ In response to datagram carrying ICMP error.

→ A fragmented datagram not the first fragment.

→

→ For special addresses 127.0.0.0 or 0.0.0.0

127.0.0.0 → $\boxed{\text{Loopback address}}$

(for self-referencing and troubleshooting)

0.0.0.0. → unspecified address

→ used during packet generation, assigned by a device after it boots up,