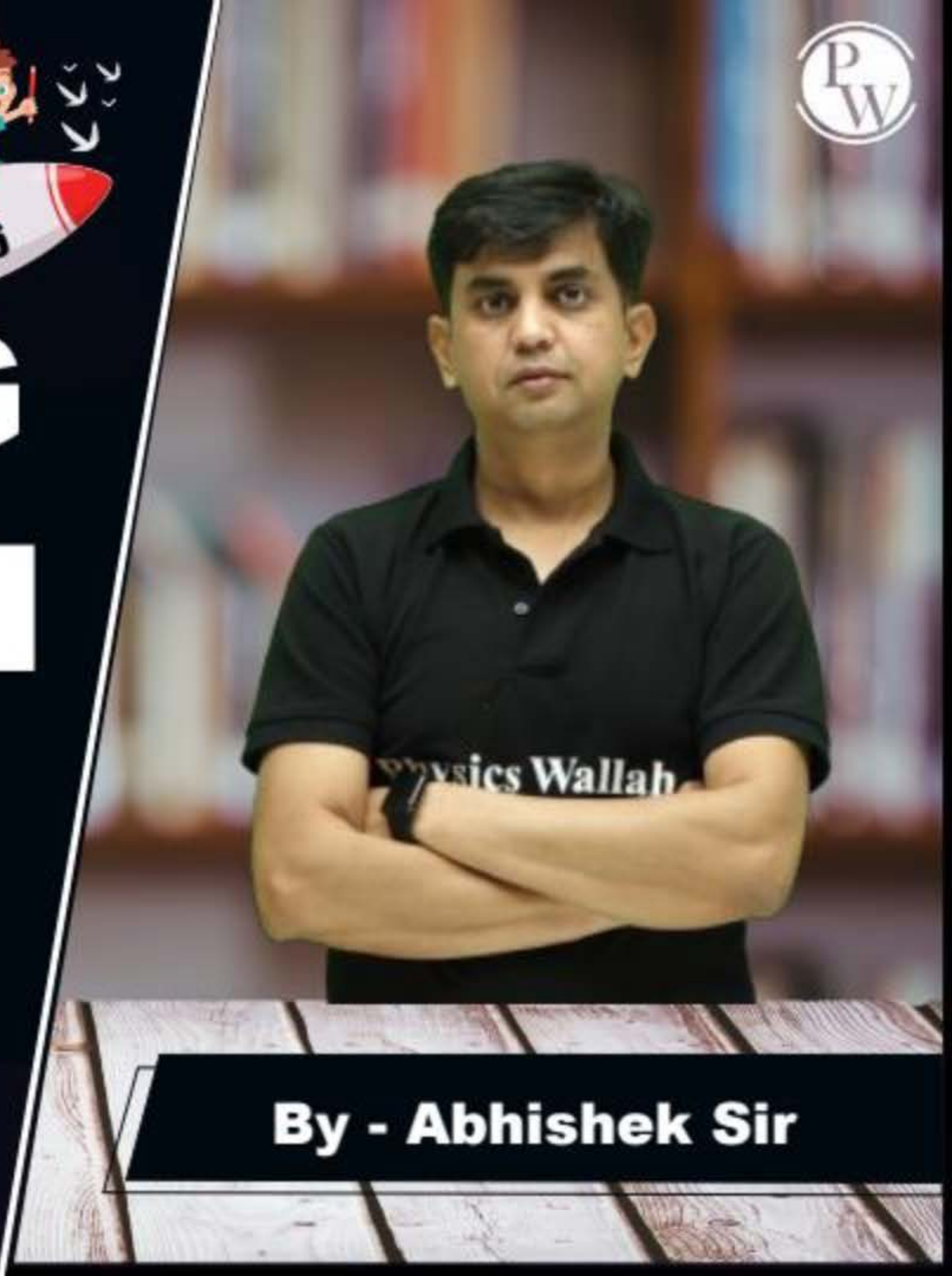
CS & IT ENGINEERING

Computer Network 1

IPv4 Header

Lecture No. - 05



By - Abhishek Sir

Recap of Previous Lecture

Topic Fragmentation and Reassembly

Topics to be Covered

Topic — DF Flag

Topic — Time-to-Live

Topic — Protocol Type

Topic — Header Checksum

ABOUT ME

Hello, I'm Abhishek

- GATE CS AIR - 96
- M.Tech (CS) - IIT Kharagpur
- 12 years of GATE CS teaching experience

Telegram Link : https://t.me/abhisheksirCS_PW

@ABHISHEKSIRCS_PW

[NAT] [GATE-2018][2 Mark]

#Q. Consider an IP packet with a length of 4,500 bytes that includes a 20-byte IPv4 header and a 40-byte TCP header. The packet is forwarded to an IPv4 router that supports a Maximum Transmission Unit (MTU) of 600 bytes. Assume that the length of the IP header in all the outgoing fragments of this packet is 20 bytes. Assume that the fragmentation offset value stored in the first fragment is 0. The fragmentation offset value stored in the third fragment is ________ .

$\boxed{\text{Ans} = 144}$

Total Length = [4500 bytes]
Header Size = [20 bytes]

Old Payload Size = [Total Length - Header Size] bytes
= [4500 − 20] bytes

MTU = [600 bytes]

New Payload Size = [MTU - Header Size] bytes
= 600 byte − 20 byte
= 580 byte [when M bit is zero]
if M bit is one, max^m payload size = 576 bytes

$$\text{Offset value of the } 3^{rd} \text{ IP fragment} = \text{Old offset value} + \left[\frac{2 * \text{New Payload Size}}{8}\right]$$

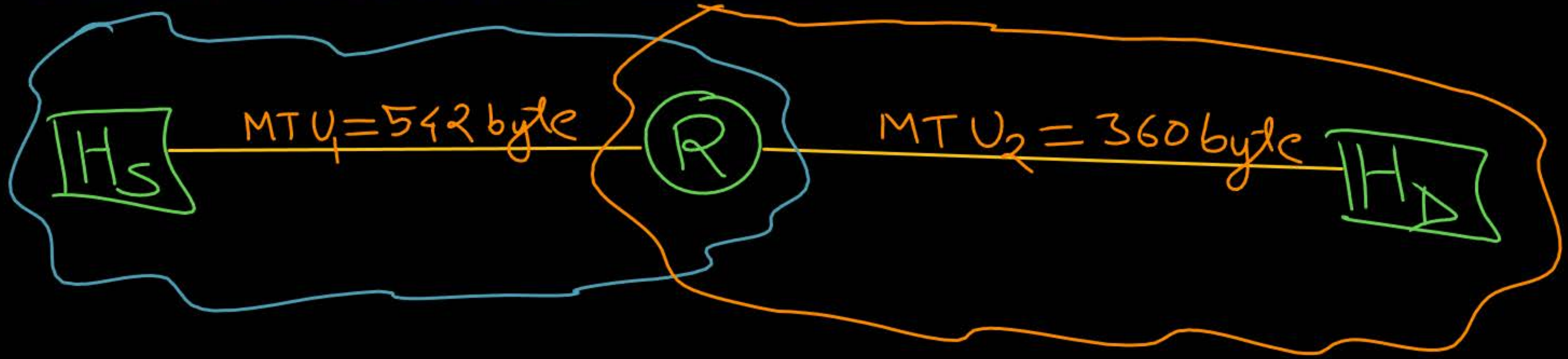
$$= 0 + \left[\frac{2 * 576 \text{ byte}}{8}\right]$$

$$= 0 + \left[\frac{1152 \text{ byte\_no}}{8}\right]$$

$$= 144 \text{ word\_no}$$

[NAT] [GATE-2024][2 Mark]

#Q. Consider sending an IP datagram of size 1420 bytes (including 20 bytes of IP header) from a sender to a receiver over a path of two links with a router between them. The first link (sender to router) has an MTU (Maximum Transmission Unit) size of 542 bytes, while the second link (router to receiver) has an MTU size of 360 bytes. The number of fragments that would be delivered at the receiver is ______.



$\boxed{\text{Ans} = 6}$

Total Length = 1420 bytes
Header Size = 20 bytes

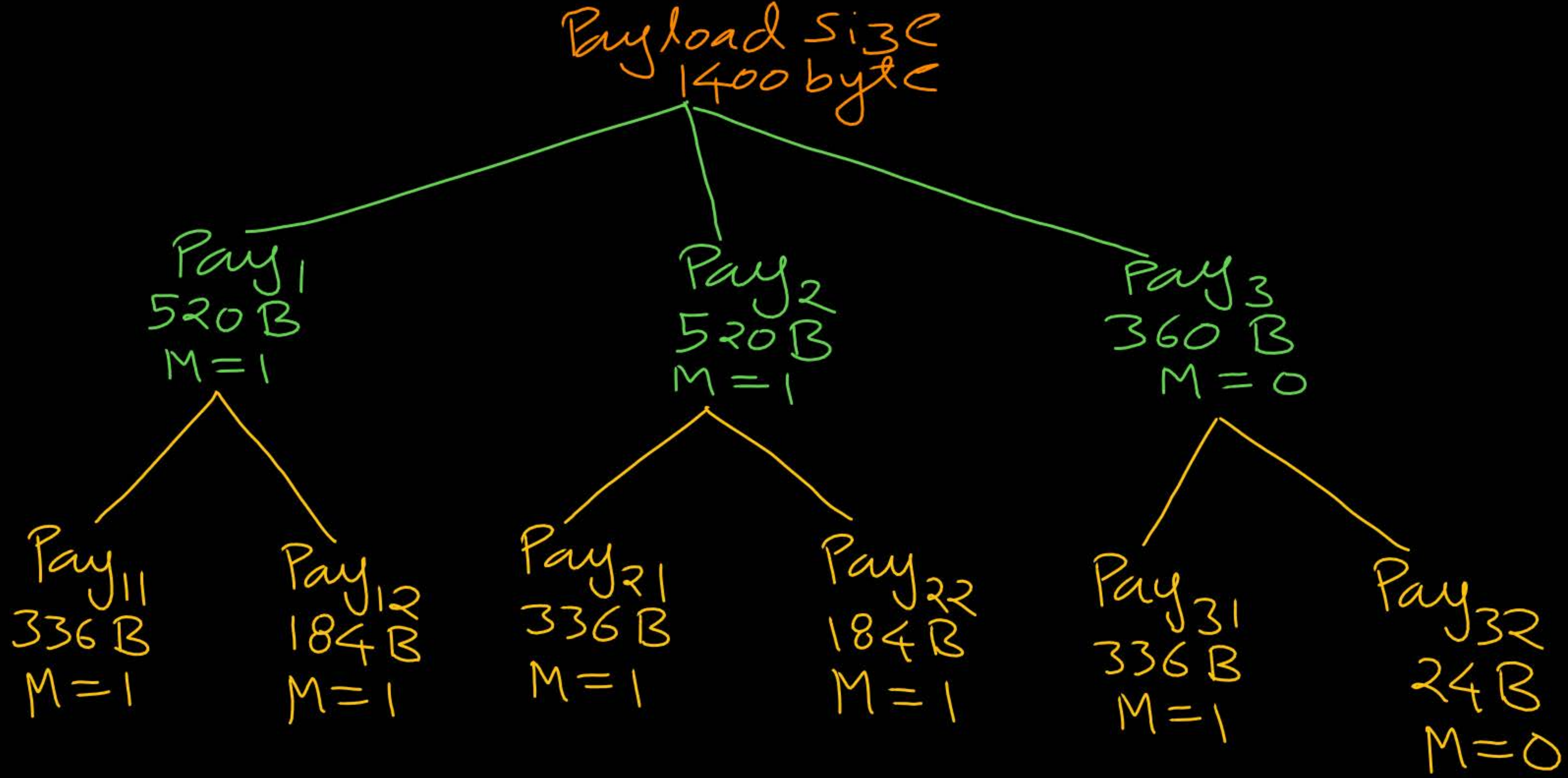
Old Payload Size = [Total Length – Header Size] bytes
= 1400 byte

MTU_1 = 542 bytes

New Payload $Size_1$ = [MTU_1 – Header Size] bytes
= 522 byte [520 byte]

MTU_2 = 360 bytes

New Payload $Size_2$ = [MTU_2 – Header Size] bytes
= 340 byte [336 byte]


Payload size
1400 byte
Pay1
520 B
M=1
Pay2
520 B
M=1
Pay3
360 B
M=0
Pay11
336 B
M=1
Pay12
184 B
M=1
Pay21
336 B
M=1
Pay22
184 B
M=1
Pay31
336 B
M=1
Pay32
24 B
M=0

[MSQ] [GATE-2024][1 Mark]

#Q. Which of the following statements about IPv4 fragmentation is/are $\boxed{\text{TRUE?}}$

(A) The fragmentation of an IP datagram is performed $\boxed{\text{only}}$ at the source of the datagram FALSE

(B) The fragmentation of an IP datagram is performed at any IP router which finds that the size of the datagram to be transmitted exceeds the MTU TRUE

(C) The reassembly of fragments is performed $\boxed{\text{only}}$ at the destination of the datagram TRUE

(D) The reassembly of fragments is performed at all intermediate routers along the path from the source to the destination FALSE

$\boxed{\text{Ans: B\&C}}$

[MSQ] [GATE-2021][2 Mark]

#Q. Consider two hosts P and Q connected through a router R. The maximum transfer unit (MTU) value of the link between P and R is 1500 bytes, and between R and Q is 820 bytes.

A TCP segment of size 1400 bytes was transferred from P to Q through R, with IP identification value as 0x1234. Assume that the IP header size is 20 bytes. Further, the packet is allowed to be fragmented, i.e., Don't Fragment (DF) flag in the IP header is not set by P.

Which of the following statements is/are correct?

Ans = A & C

(A) Two fragments are created at R and the IP datagram size carrying the second fragment is 620 bytes.

(B) If the second fragment is lost, R will resend the fragment with the IP identification value 0×1234. FALSE

(C) If the second fragment is lost, P is required to resend the whole TCP segment.

(D) TCP destination port can be determined by analysing only the second fragment.

[TCP segment 1400 byte]

(20+) Payload 1400 byte [off = 0, M = 0]

Pay1
(20+) 800 byte
off = 0
M = 1

Pay2
20+600 byte
off = 100
M = 0

TCP Segment Size = [1400 bytes]

IPv4 Header Size = [20 bytes]

MTU_1 = 1500 bytes

New Payload $Size_1$ = [MTU_1 – Header Size] bytes

= 1480 bytes

MTU_2 = 820 bytes

New Payload $Size_2$ = [MTU_2 – Header Size] bytes

= 800 byte

Topic : DF Flag

DF : Do not fragment

→ Source host can restrict further fragmentation (division) of datagram at any intermediate router

→ In such cases, source host set DF bit [DF = 1]

→ e.g "Remote Booting"

→ Default value of DF flag is "Zero"

→ Set / reset by source host only.

Topic : DF Flag

At intermediate Router :- [For arrived IP Packet]

if [Total Length > next network MTU]

if [DF_bit == 1]

→ Router discard the IP packet

→ generate ICMP Error Message for source host "Fragmentation Needed and Don't Fragment was Set"

Topic : IPv4 Packet Header

<table>
<tr><td>0</td><td></td><td></td><td colspan="3">16</td><td>31</td></tr>
<tr><td>VER</td><td>HLEN</td><td>Type of Services</td><td colspan="4">Total Length (16 - bits)</td></tr>
<tr><td colspan="3">Identification Number</td><td>0</td><td>DF</td><td>MF</td><td>Fragmentation Offset</td></tr>
<tr><td colspan="2">Time-to-Live</td><td>Protocol Type</td><td colspan="4">Header Checksum</td></tr>
<tr><td colspan="7">Source IPv4 Address (32 - bits)</td></tr>
<tr><td colspan="7">Destination IPv4 Address (32 - bits)</td></tr>
<tr><td colspan="7">Optional Header (Options)</td></tr>
<tr><td colspan="7">Payload</td></tr>
</table>

Topic : Time-to-Live

Range → 0 to 255

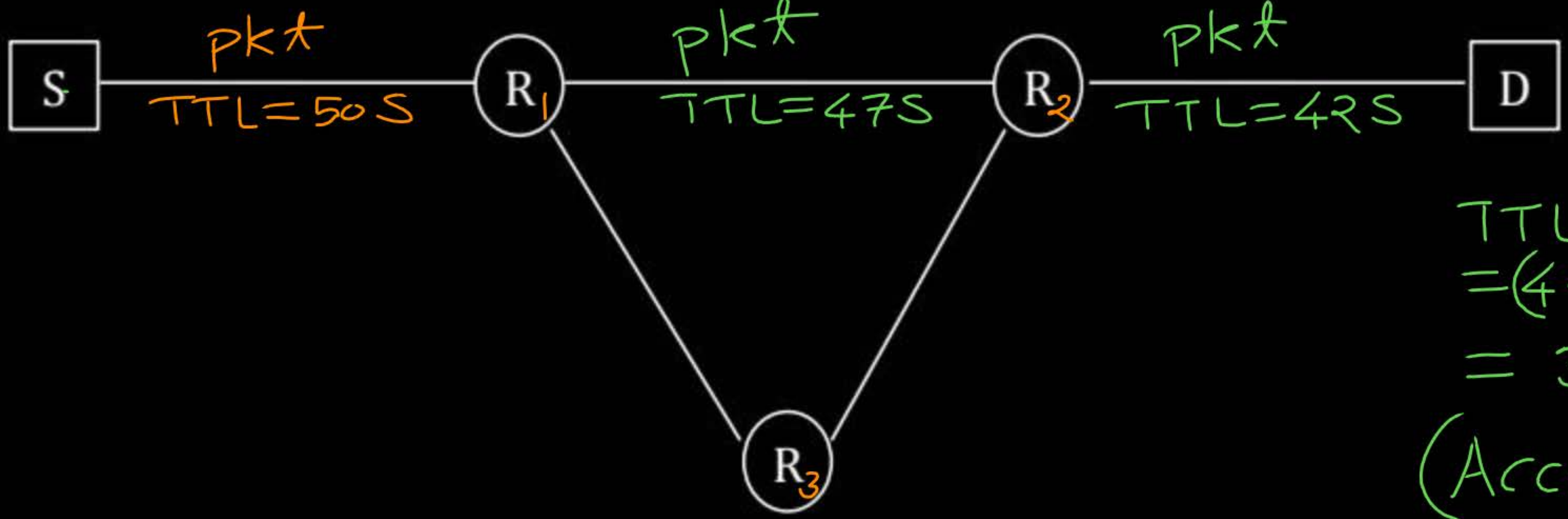
→ Time-to-live (TTL) is 8-bit field

→ Life time of an IP datagram *

→ Prevent indefinite traversing of an IP datagram in the network
[Router's may form circuit / loop]

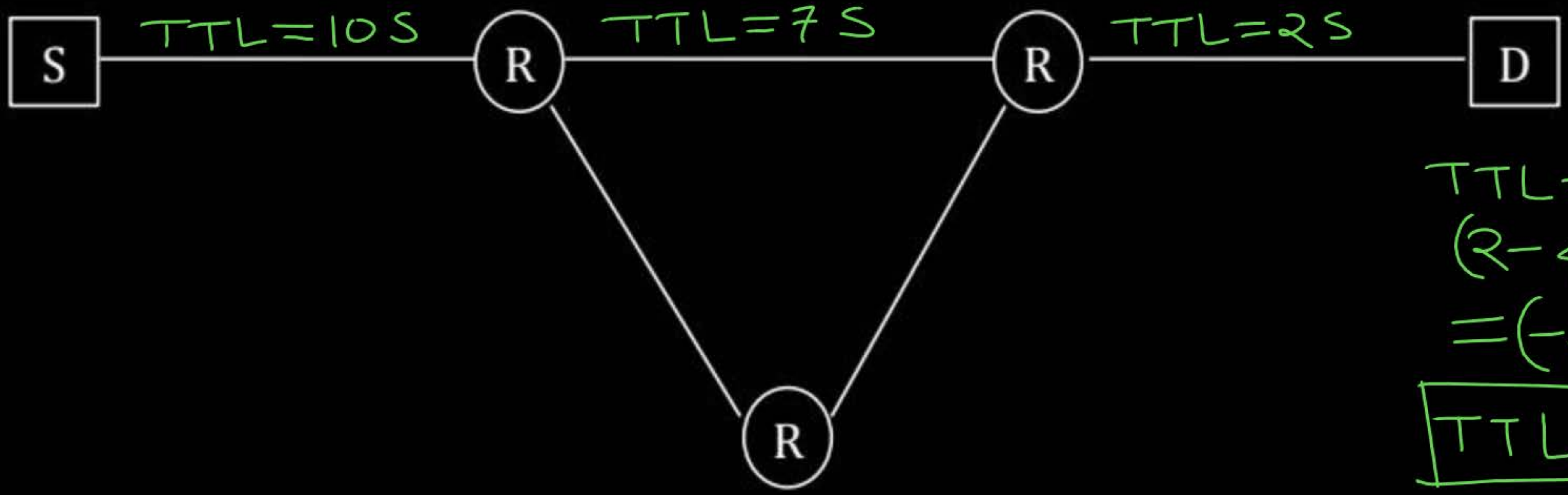
Topic : Time-to-Live

TTL → sec or ms



TTL
$=(42-4)$
$=38$ sec
(Accept)

Topic : Time-to-Live



TTL = $(2-4)$

$= (-2sec)$

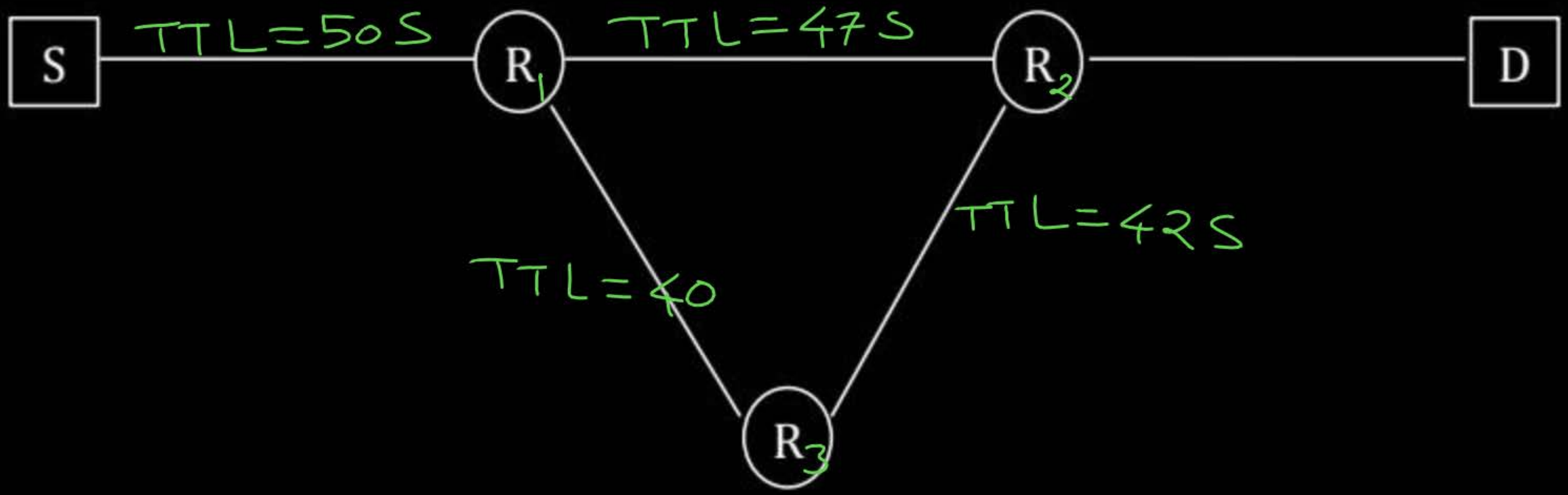
$\boxed{TTL < 0}$

Discard

(ICMP Error)

Topic : Time-to-Live

if (TTL <= 0) AT Router
* Discard
* ICMP Error



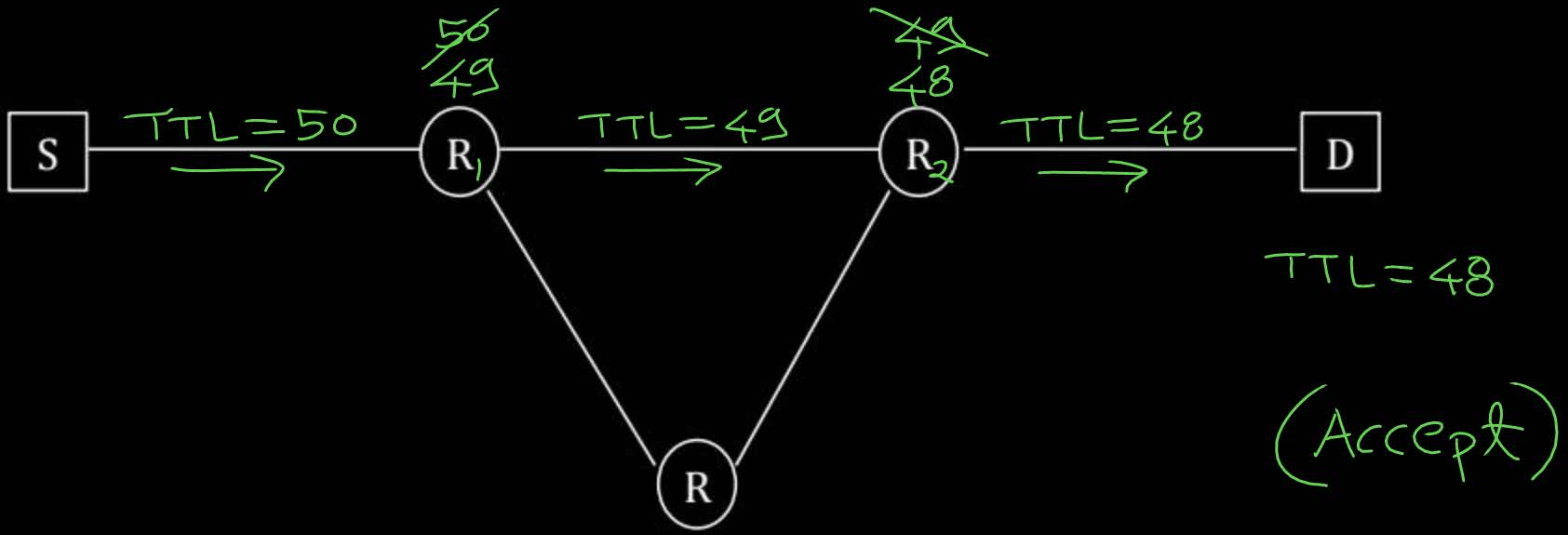
Topic : Time-to-Live

** **

→ Each intermediate router decrement TTL value by one // TTL--;

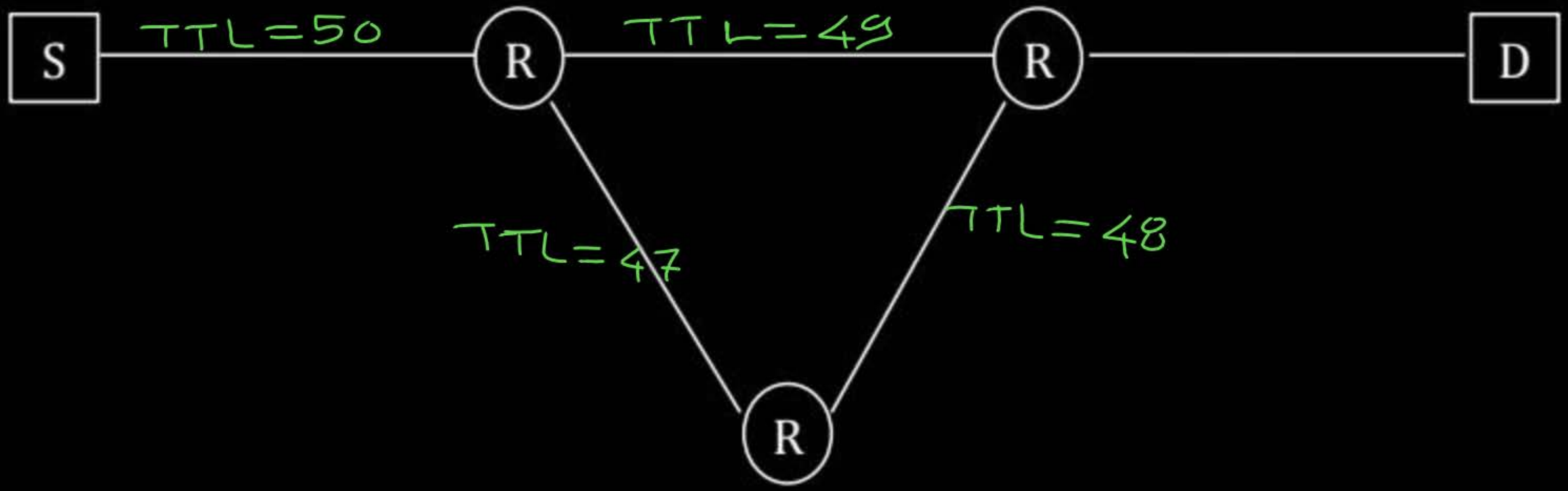
→ if TTL value decremented to zero // [TTL ≤ 0]
then router discard the datagram
and send ICMP error message "Time Exceeded" to source host

Topic : Time-to-Live

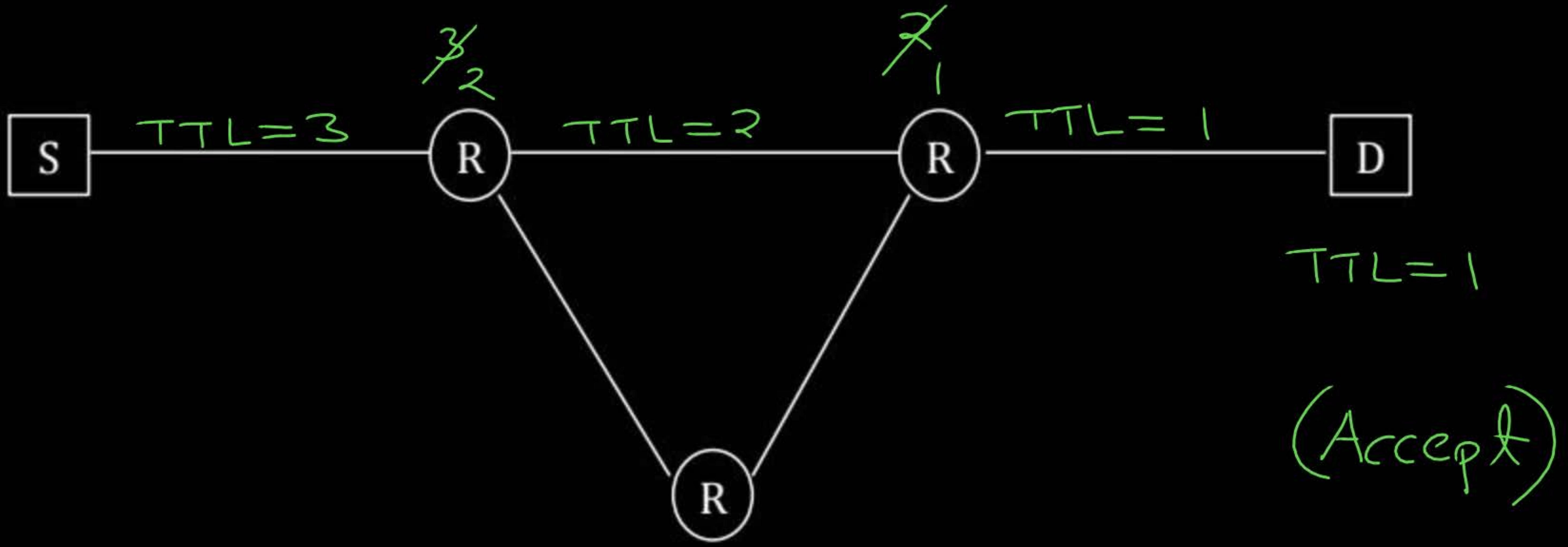


Topic : Time-to-Live

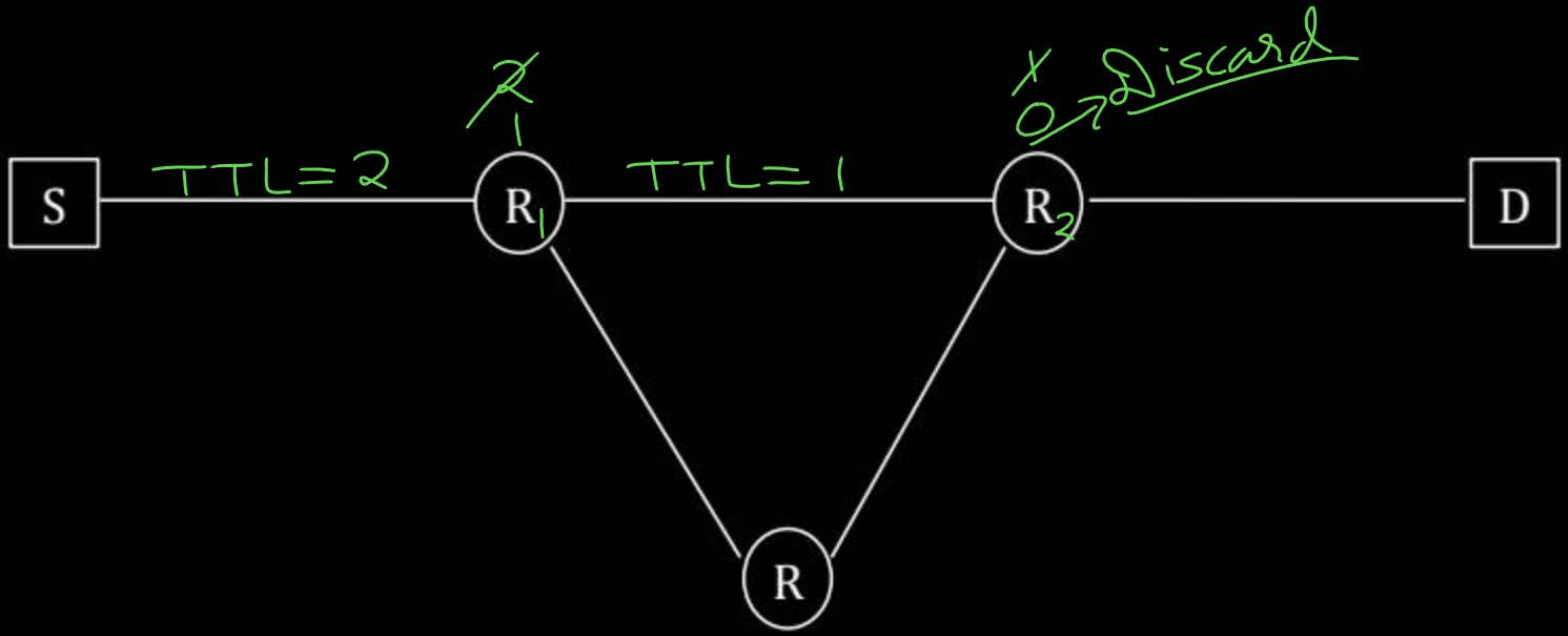
AT Router
TTL--;
if(TTL==0)
*Discard, ICMP;



Topic : Time-to-Live



Topic : Time-to-Live



[MCQ] IIT-KGP, H.W. [GATE-CS-2006] [1 Mark]

#Q. For which one of the following reasons does Internet Protocol (IP) use the time-to-live (TTL) field in the IP datagram header ?

(A) ~~Ensure packets reach destination within that time~~

(B) ~~Discard packets that reach later than that time~~

(C) Prevent packets from looping indefinitely

(D) ~~Limit the time for which a packet gets queued in intermediate routers.~~

$\boxed{\text{Ans: C}}$

[MCQ] IIT-G, [GATE-2010] [1 Mark]

#Q. One of the header fields in an IP datagram is the Time to Live (TTL) field. Which of the following statements best explains the need for this field ?

A. It can be used to prioritize packets ToS

B. It can be used to reduce delays ToS

C. It can be used to optimize throughput ToS

D. It can be used to prevent packet looping

$\boxed{\text{Ans: D}}$

Topic : Time-to-Live

→ Destination Host may decrement TTL value by one // TTL--;

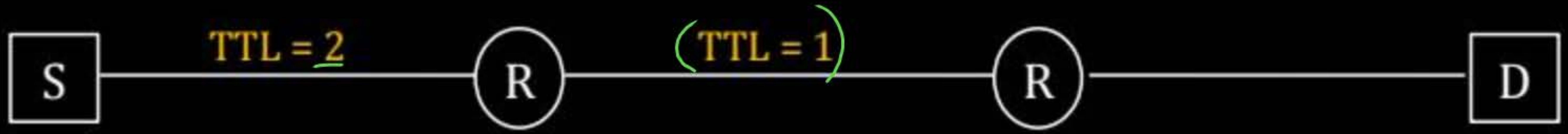
→ if TTL value decremented to less then zero // [TTL < 0]
then destination host discard the datagram
and send ICMP error message "Time Exceeded" to source host

CASE I :

TTL = 1

TTL = ~~1~~ 0
[Discard,
Send ICMP Error]

CASE II :

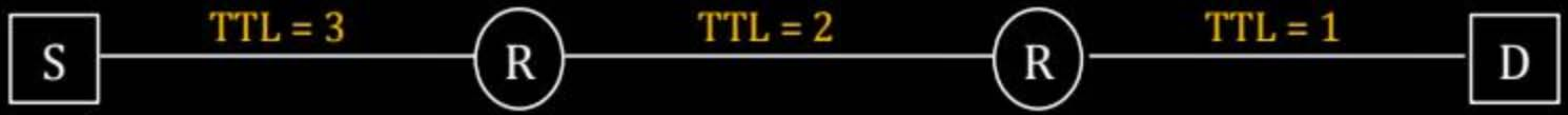


TTL = 2

TTL = ~~2~~ 1

TTL = ~~1~~ 0
[Discard,
Send ICMP Error]

CASE III :



TTL = 3

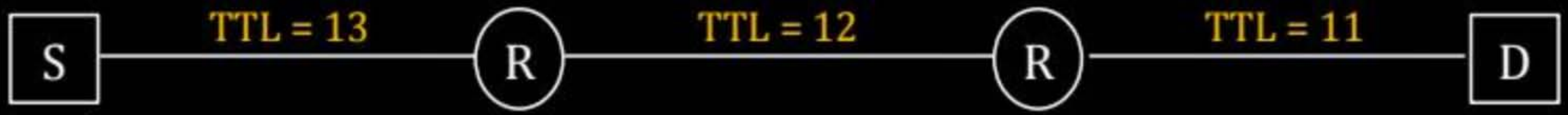
TTL = ~~3~~ 2

TTL = ~~2~~ 1

$\boxed{\text{TTL} = \cancel{1}\ 0}$ option

[Forward to higher layer]

CASE IV :



TTL = 13

TTL = ~~13~~ 12

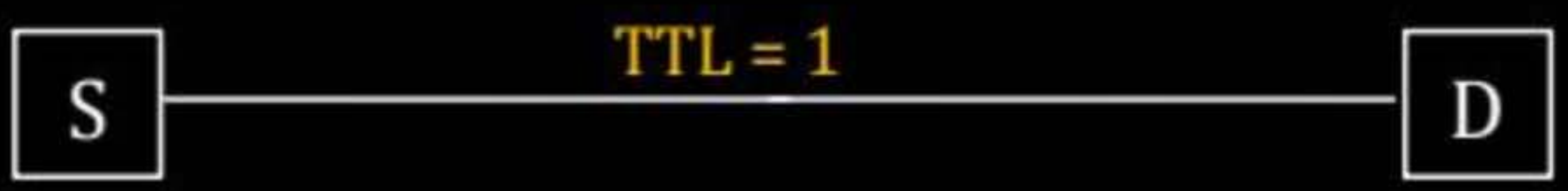
TTL = ~~12~~ 11

optional

TTL = ~~11~~ 10

[Forward
to higher layer]

CASE V :



TTL = 1

TTL = ~~1~~ 0 optional

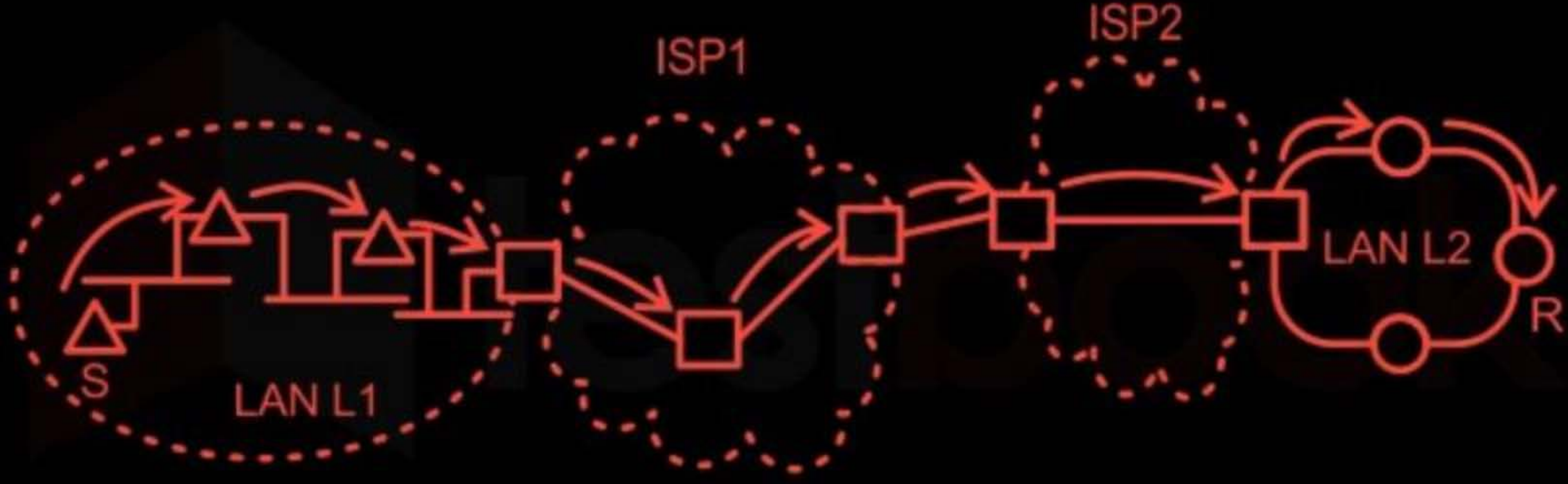
[Forward
to higher layer]

(Accept)

Note : TTL = 1, can use when source and destination host are directly connected.

[NAT] IIT-KGP, H.W. [GATE-2014][1 Mark]

#Q. In the diagram shown below L1 is an Ethernet LAN and L2 is a Token-Ring LAN. An IP packet originates from sender S and traverses to R, as shown. The link within each ISP, and across two ISPs, are all point to point optical links. The initial value of TTL is 32. The maximum possible value of TTL field when R receives the datagram is _____ .



Topic : Time-to-Live

→ Hop Limit 8-bit field in IPv6 Header

→ Same as Time-to-live (TTL) field of IPv4 Header

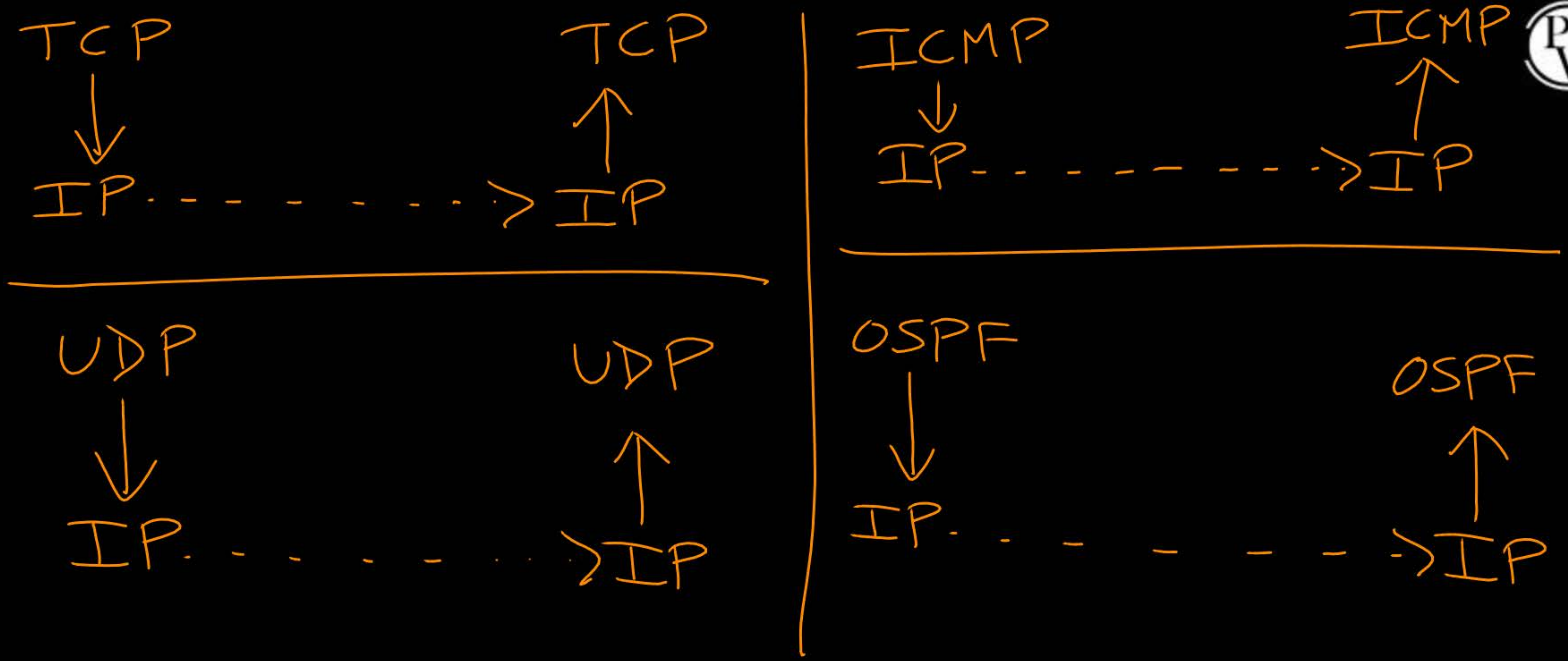
Topic : Protocol Type

→ Protocol Type is 8-bit field in IPv4 Header

→ Indicates higher-level protocol

→ Indicates the type of protocol encapsulated in the payload

→ Demultiplexing of protocol at receiver


TCP
IP
TCP
IP
UDP
IP
UDP
IP
ICMP
IP
ICMP
IP
OSPF
IP
OSPF
IP

Topic : Protocol Type

Number	Protocol
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

[MCQ] [GATE-2025] [1 Mark]

#Q. A machine receives an IPv4 datagram. The protocol field of the IPv4 header has the protocol number of a protocol X. Which ONE of the following is NOT a possible candidate for X?

(A) Internet Control Message Protocol (ICMP) $\rightarrow$ IP

(B) Internet Group Management Protocol (IGMP) $\rightarrow$ IP

(C) Open Shortest Path First (OSPF) $\rightarrow$ IP

(D) Routing Information Protocol (RIP) $\rightarrow$ UDP $\rightarrow$ IP

$\boxed{\text{Ans: D}}$

Topic : Header Checksum

→ Header Checksum is 16-bit field in IPv4 Header

→ Internet Checksum

→ Ensures the integrity of the IPv4 header during routing

Topic : Header Checksum

→ Calculated over the IPv4 header only [including optional header]

→ Block Size is 16-bits

→ 16 bit one's complement of the one's complement sum of all 16 bit words in the IPv4 header.

Topic : Header Checksum

Block Size = 16 bits

While computing the checksum, the value of the checksum field should be initialized with zero.

IPv4 Header

VER	HLEN	Type of Service
Total Length		
Identification Number		
Flag	Fragmentation Offset	
Time-to-Live	Protocol Type	
Checksum [0 0 0 0 . . . . 0 0 0 0]		
Source IP Address (16-bits)		
Source IP Address (16-bits)		
Destination IP Address (16-bits)		
Destination IP Address (16-bits)		

Topic : Header Checksum

→ Checksum verification is performed at every intermediate router and destination host

→ if error is detected in IPv4 header (computed checksum is nonzero) then discards the datagram → No Error Message
→ ICMP Error Message

→ After processing the IPv4 datagram, New Checksum is generated by every intermediate router, before forwarding it.

Topic : IPv4 Header

→ At intermediate Router : (for every received IPv4 datagram)

1. Verify Header Checksum,
   if error detected, discard the datagram
   and send ICMP error to source host

2. TTL = TTL – 1; [Decrement TTL by one]
   if TTL <= 0, then discard the datagram
   and send ICMP error to source host

3. Process the datagram,
   to determine next forwarding interface

4. Update Checksum field with new generated checksum
   and forward the datagram

Topic : IPv4 Header

→ At destination host : (for every received IPv4 datagram)

1. Verify Header Checksum,
   if error detected, discard the datagram
   and send ICMP error to source host

⟹ Comulsary

2. TTL = TTL – 1; [Decrement TTL by one]
   if TTL < 0, then discard the datagram
   and send ICMP error to source host

⟹ optional

3. Process the datagram,
   to determine higher level protocol

4. Forward the payload to higher level protocol

Topic : Source IP Address

→ Source IP Address is 32-bit field in IPv4 Header

→ Fourth word of IPv4 Header [Word size = 4 byte]

→ Assigned by source host only

→ Does not change during routing

→ May update in case of NAT device

Topic : Destination IP Address

→ Destination IP Address is 32-bit field in IPv4 Header

→ Fifth word of IPv4 Header [Word size = 4 byte]

→ Assigned by source host only

→ Does not change during routing

→ May update in case of NAT device

[MSQ] IISC, H.W. [GATE-2024][1 Mark]

#Q. Which of the following fields of an IP header is/are always modified by any router before it forwards the IP packet?

(A) Source IP Address

(B) Protocol

(C) Time to Live (TTL)

(D) Header Checksum

[MCQ]

IIT-K, H.W. [GATE-2015][1 Mark]

#Q. Which one of the following fields of an IP header is NOT modified by a typical IP router ?

A) Checksum

B) Source address

C) Time to Live (TTL)

D) Length

[MCQ] IIT-KGP, H.W. [GATE-2014][1 Mark]

#Q. Host A (on TCP/IPv4 network A) sends an IP datagram D to host B (also on TCP/IPv4 network B). Assume that no error occurred during the transmission of D. When D reaches B, which of the following IP header field(s) may be different from that of the original datagram D ?

(i) TTL (ii) Checksum (iii) Fragment

A (i) only

B (i) and (ii) only

C (ii) and (iii) only

D (i), (ii) and (iii)

[MCQ] IIT-D, H.W. [GATE-IT-2004] [2 Mark]

#Q. In the TCP/IP protocol suite, which one of the following is NOT part of the IP header ?

(A) Fragment Offset

(B) Source IP address

(C) Destination IP address

(D) Destination port number

2 mins Summary

Topic DF Flag

Topic Time-to-Live

Topic Protocol Type

Topic Header Checksum

THANK - YOU

@ABHISHEKSIRCS_PW