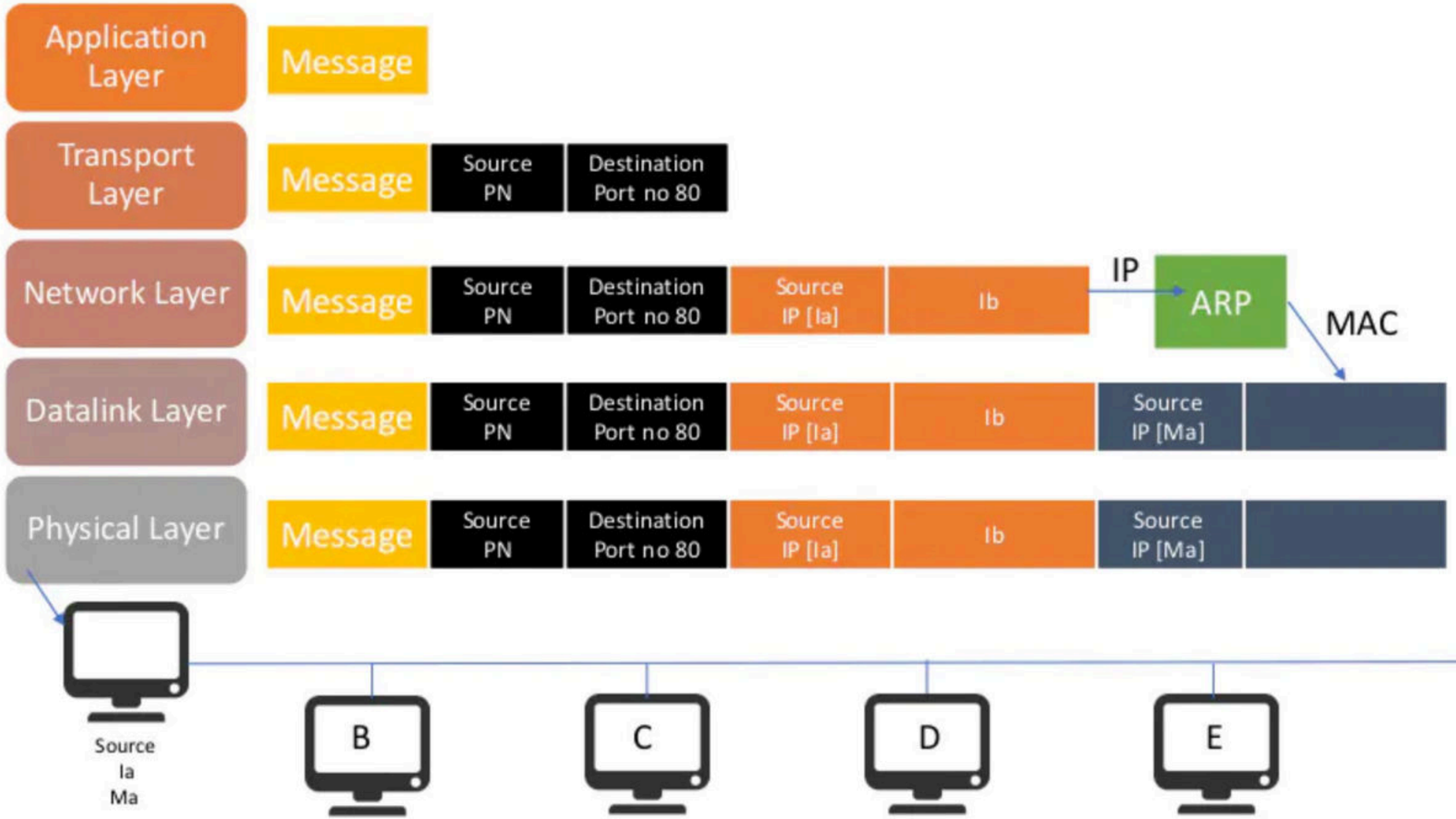
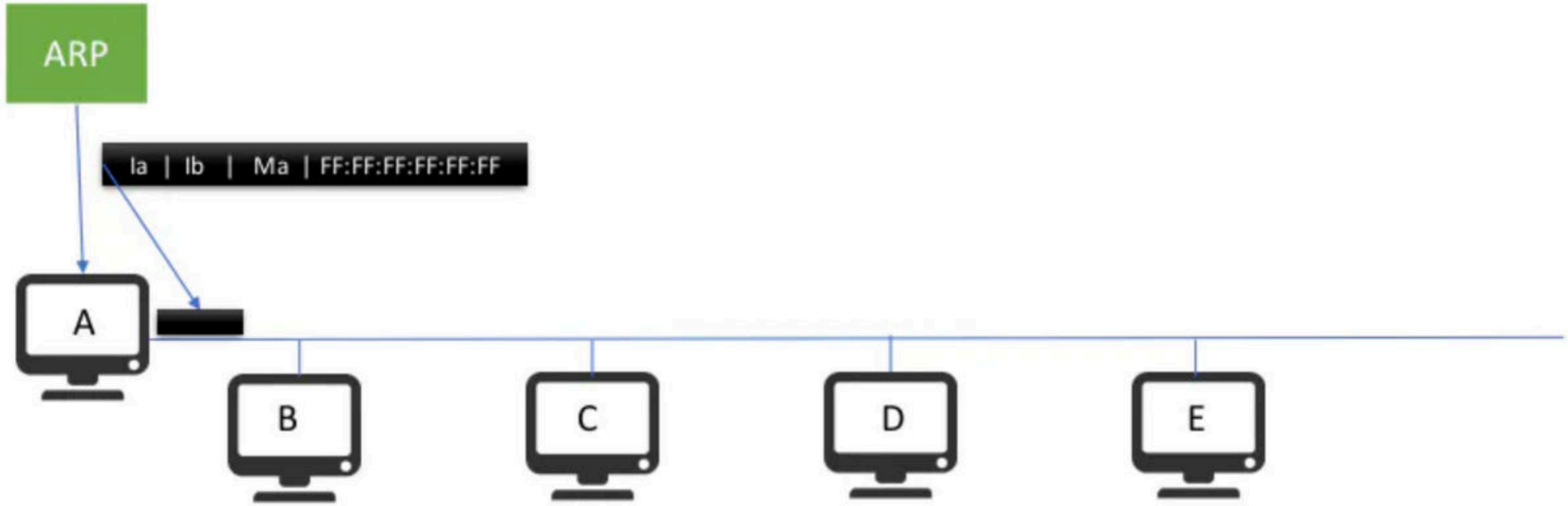
Computer Networks

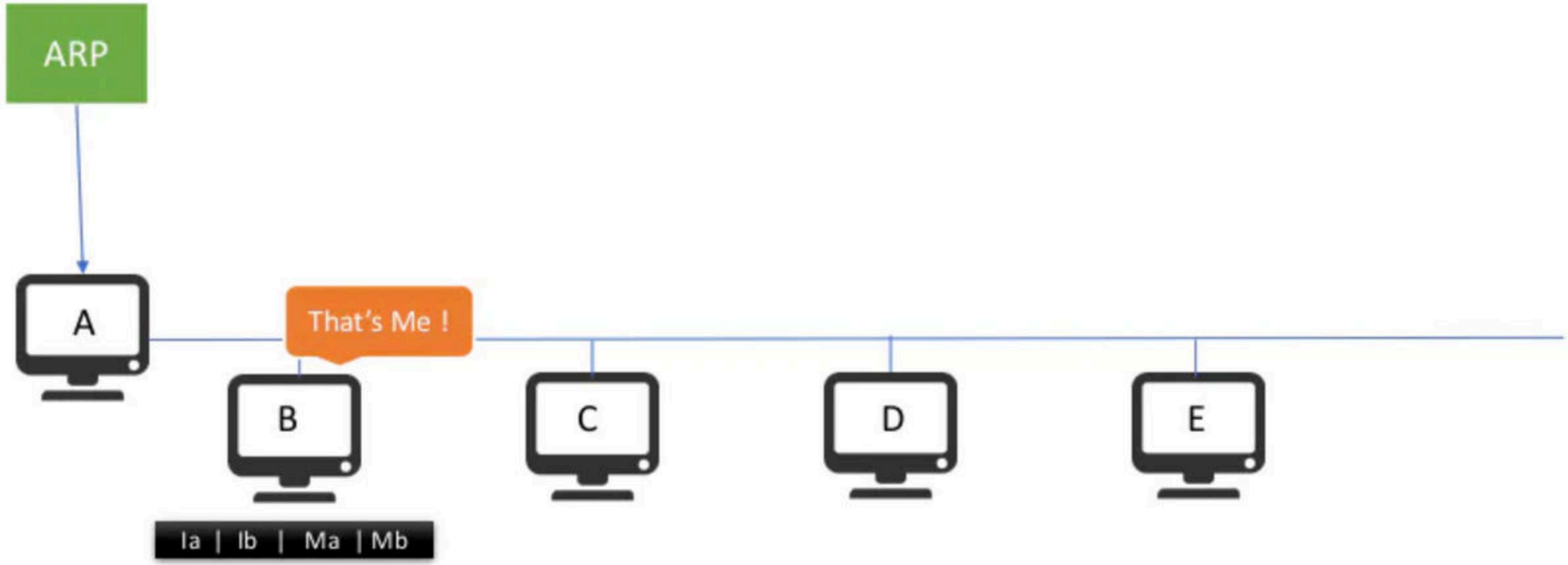
ARP

ADDRESS RESOLUTION PROTOCOL [ARP]

IP → ARP → MAC

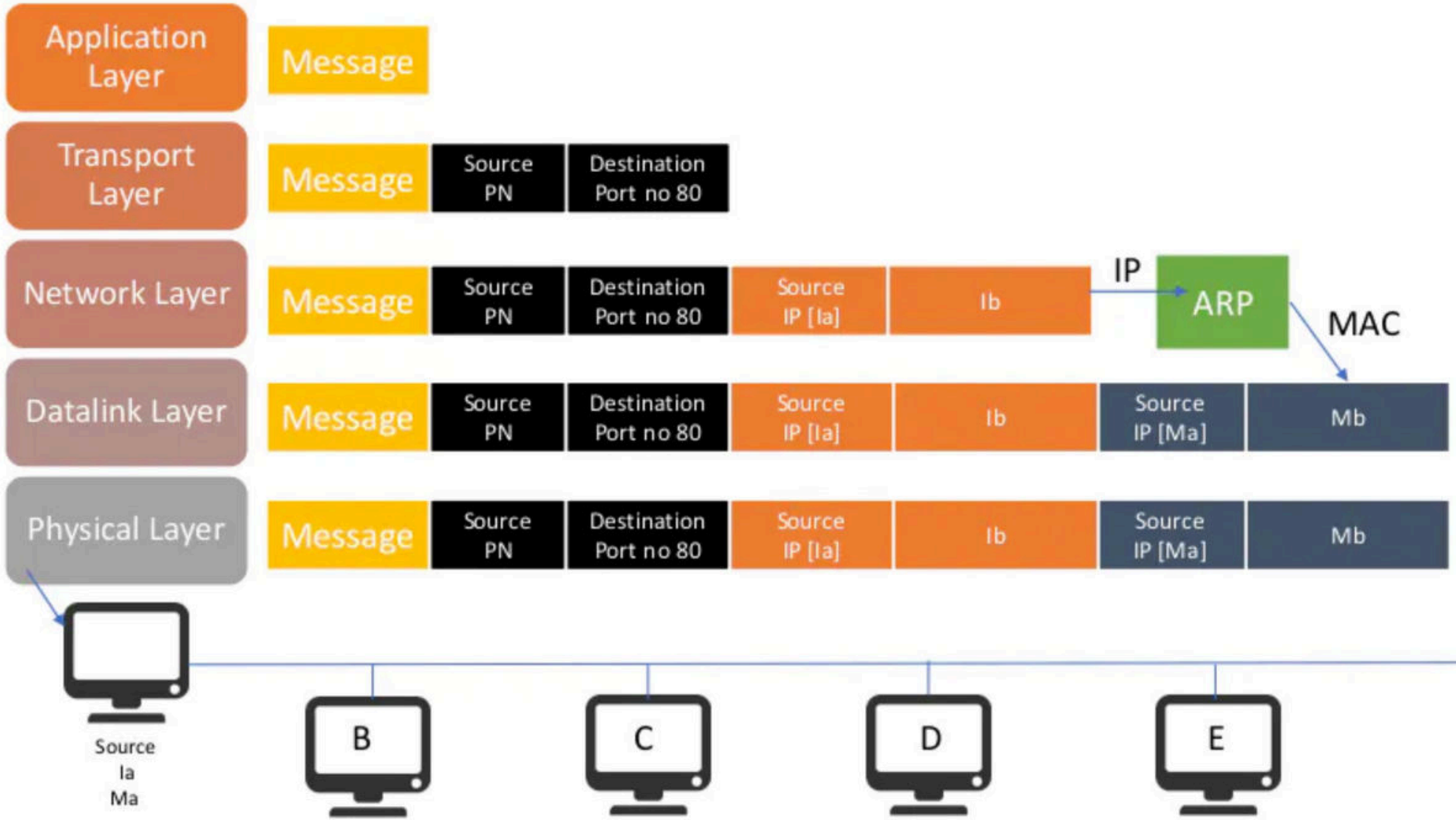



ARP
Ia | Ib | Ma | FF:FF:FF:FF:FF:FF
A
B
C
D
E


ARP
A
That's Me !
B
C
D
E
Ia | Ib | Ma | Mb

ADDRESS RESOLUTION PROTOCOL [ARP]

IP → ARP → MAC



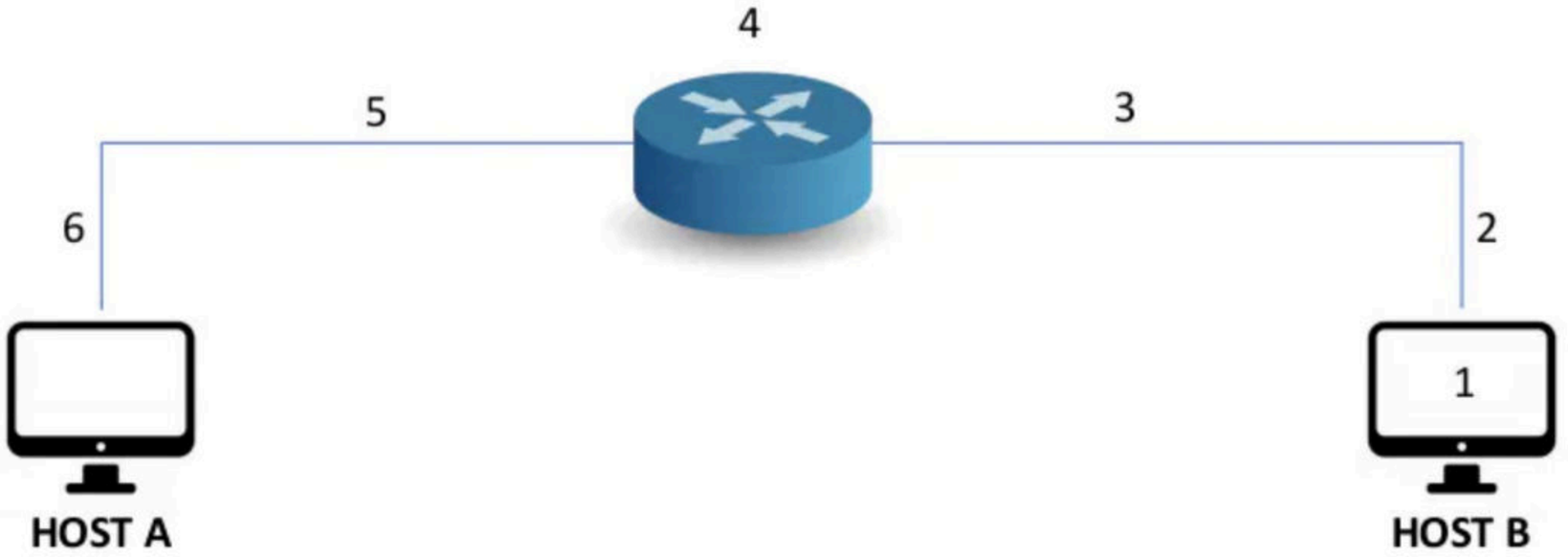
KEY POINTS ABOUT ARP

- ARP Request is Broadcast
- ARP reply is Unicast
- Finding the MAC Address of Another host
- Finding the MAC Address of a Router
- Router wants to find MAC address of Another Router
- Router can find MAC address of a Host

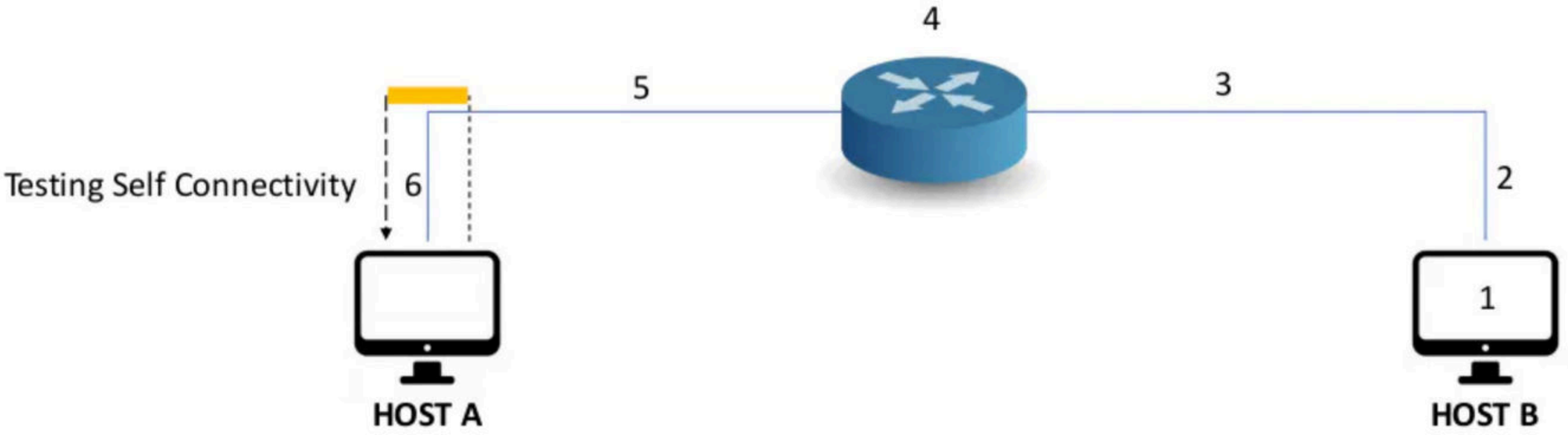
Computer Networks

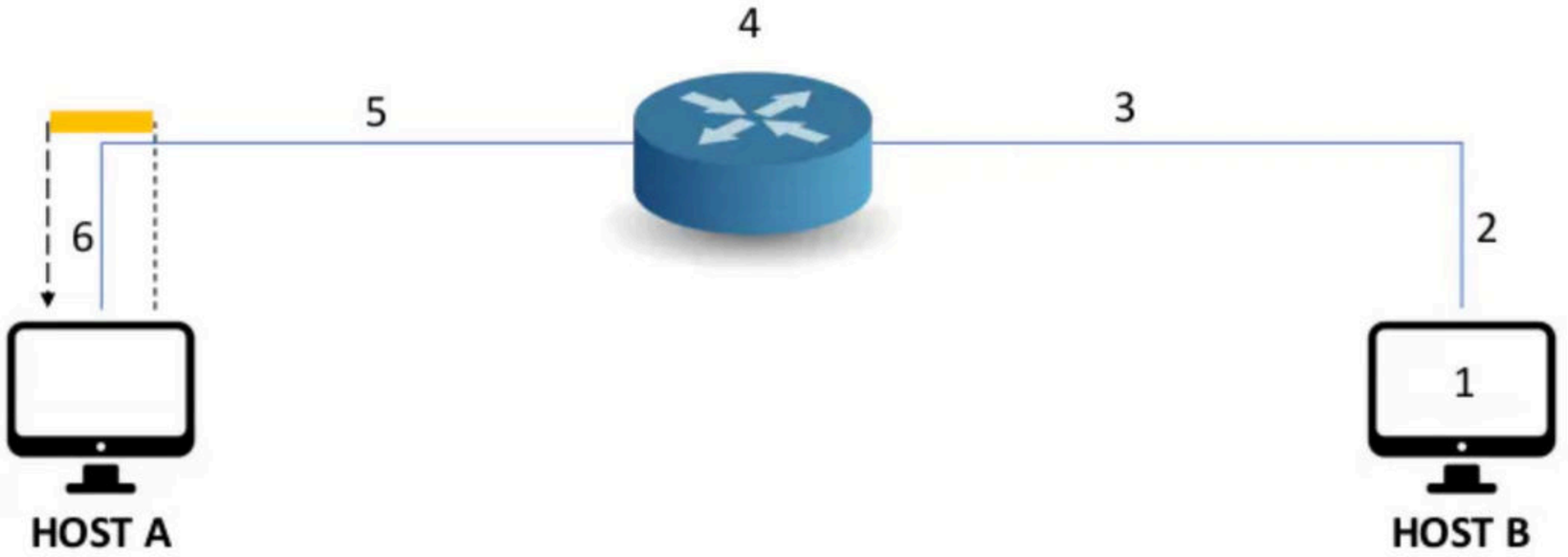
Special Address 127

Suppose A has sent some data to B but B has not responded
What could be the possibilities?
1,2,3,4,5,6 are the possibilities of failure.

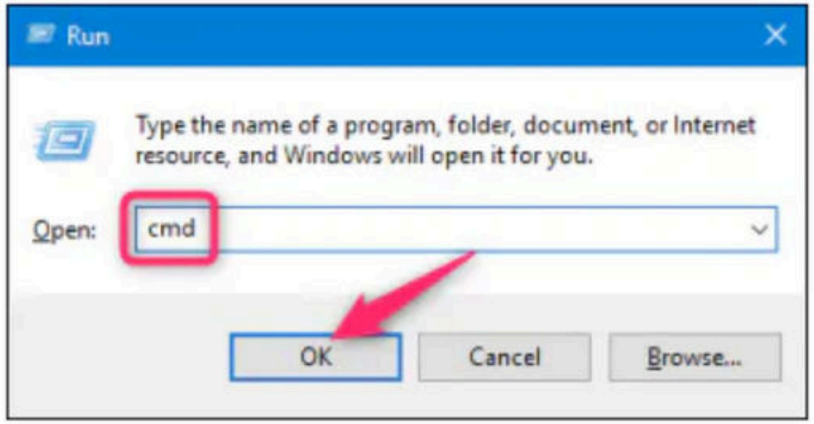


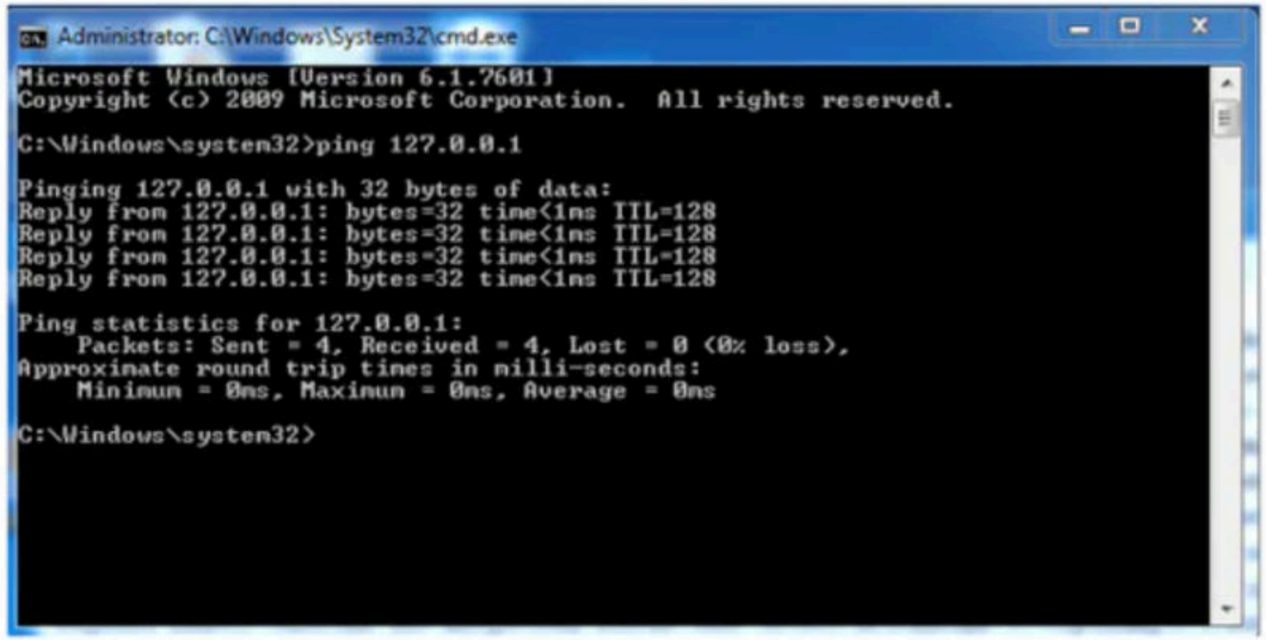
Point 6 deals with NIC card of A
So, How we can check if the NIC is working or not?
A can send a packet to itself.





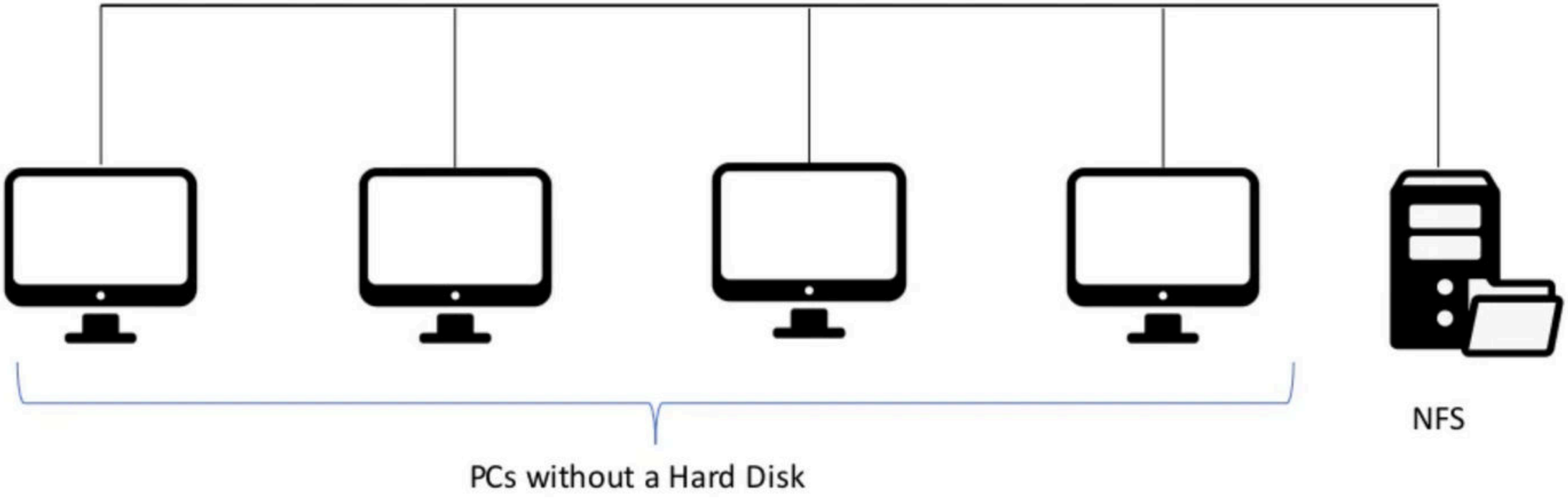
For Testing Self Connectivity
IP address 127 is used
Loop back Address


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
cmd
OK
Cancel
Browse...

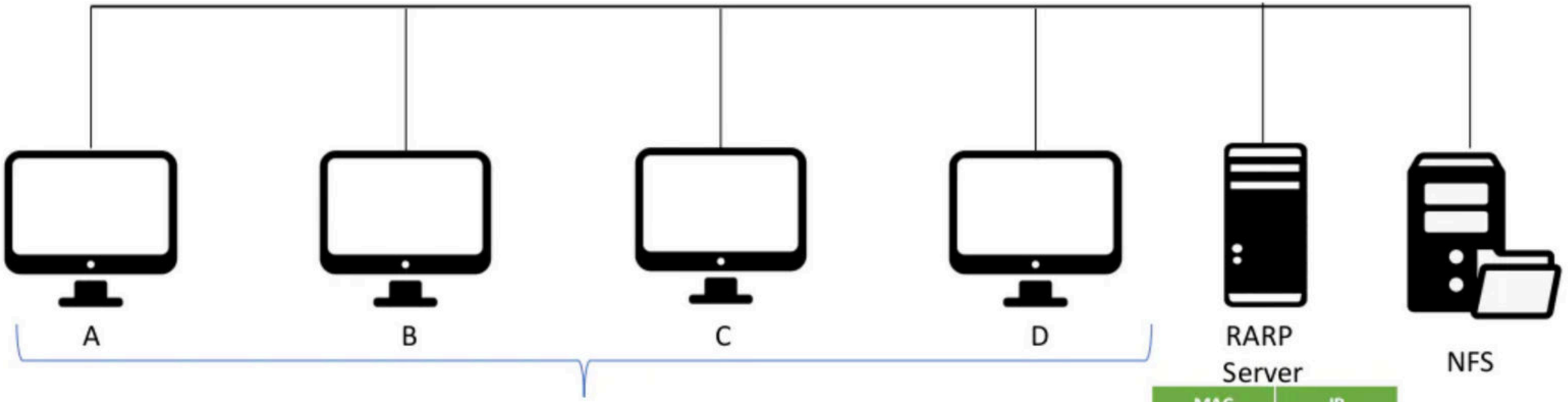

Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Windows\system32>

Computer Networks

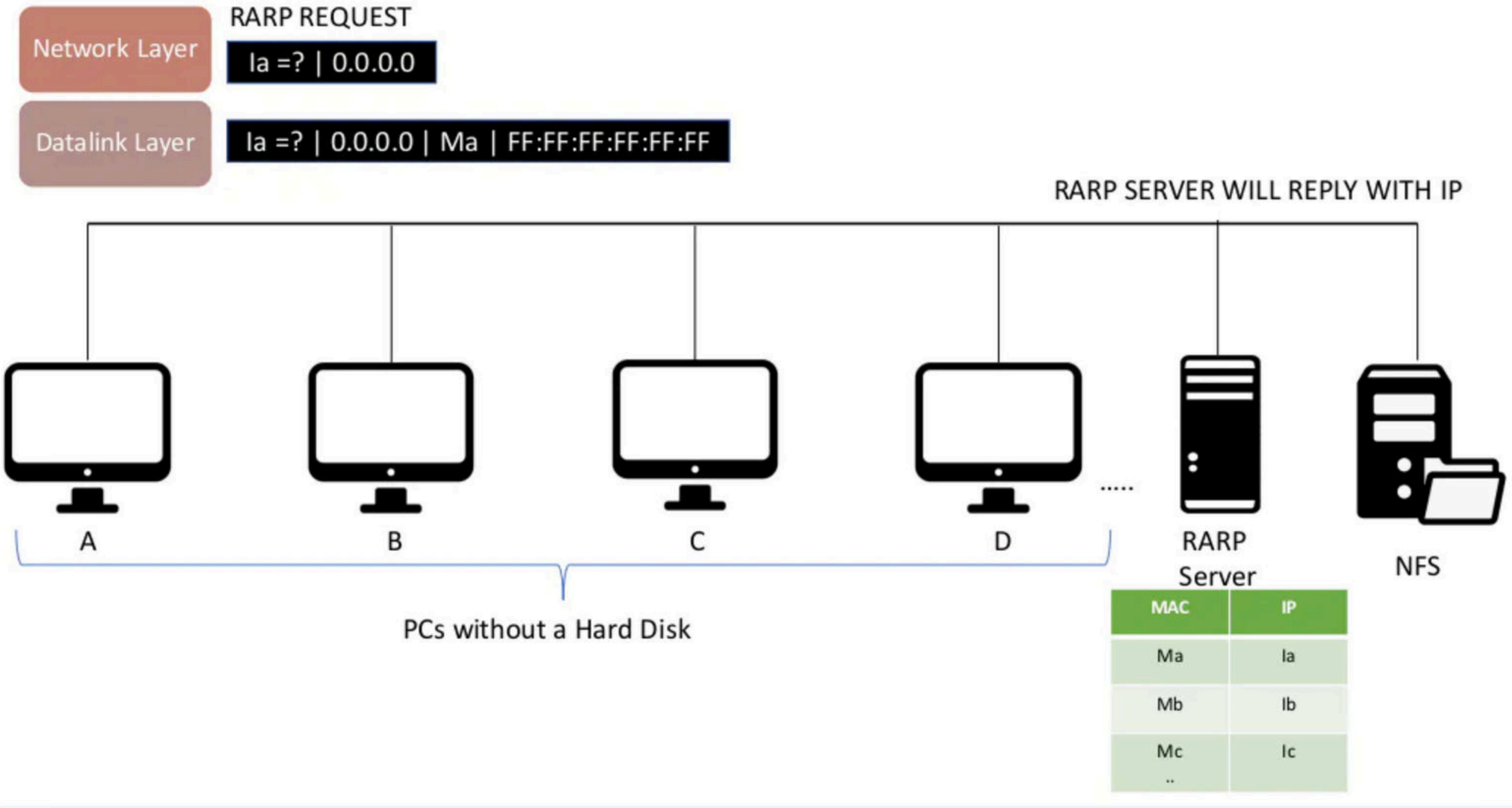
RARP



MAC- ROM
IP - RAM



MAC	IP
Ma	Ia
Mb	Ib
Mc ..	Ic

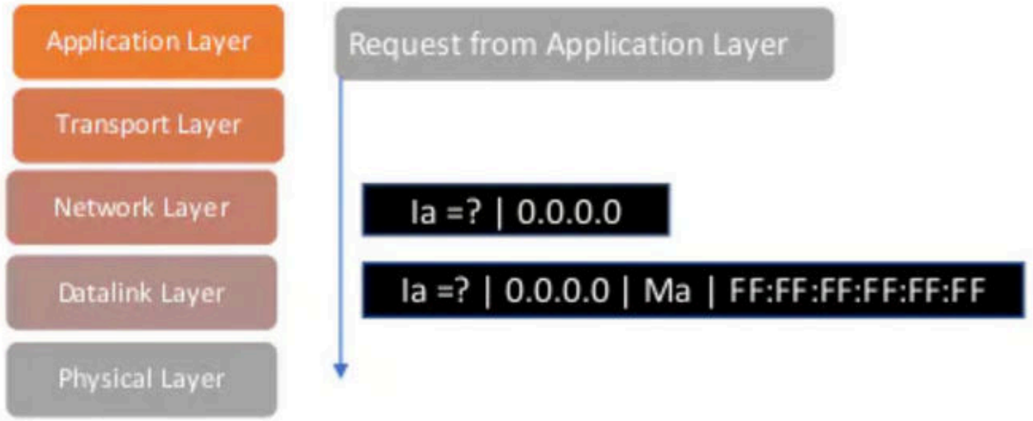

Network Layer
RARP REQUEST
Ia =? | 0.0.0.0
Datalink Layer
Ia =? | 0.0.0.0 | Ma | FF:FF:FF:FF:FF:FF
RARP SERVER WILL REPLY WITH IP
A
B
C
D
.....
RARP Server
NFS
PCs without a Hard Disk
MAC
IP
Ma
Ia
Mb
Ib
Mc
Ic
..

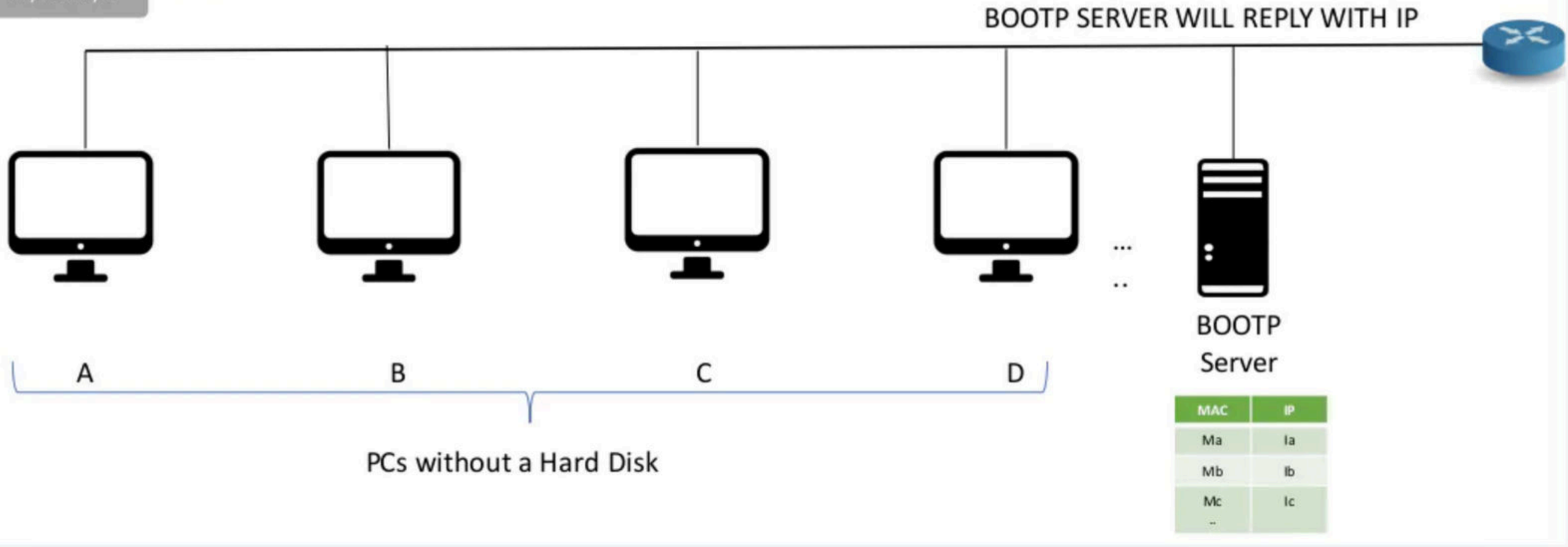
Computer Networks

BOOTP AND DHCP

BOOTP stands for Bootstrap Protocol.

BOOTP is similar to RARP except that BOOTP works at Application Layer





Advantage: Only one BOOTP sever is required
Disadvantage: Mapping Table is Static

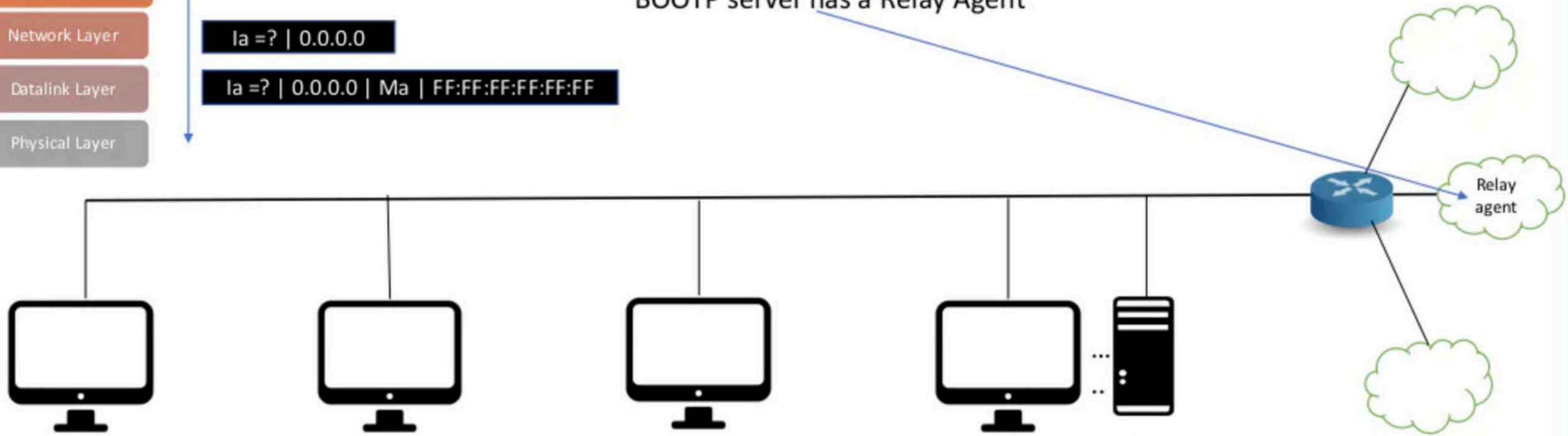
Application Layer
Transport Layer
Network Layer
Datalink Layer
Physical Layer

Request from Application Layer

Ia =? | 0.0.0.0

Ia =? | 0.0.0.0 | Ma | FF:FF:FF:FF:FF:FF

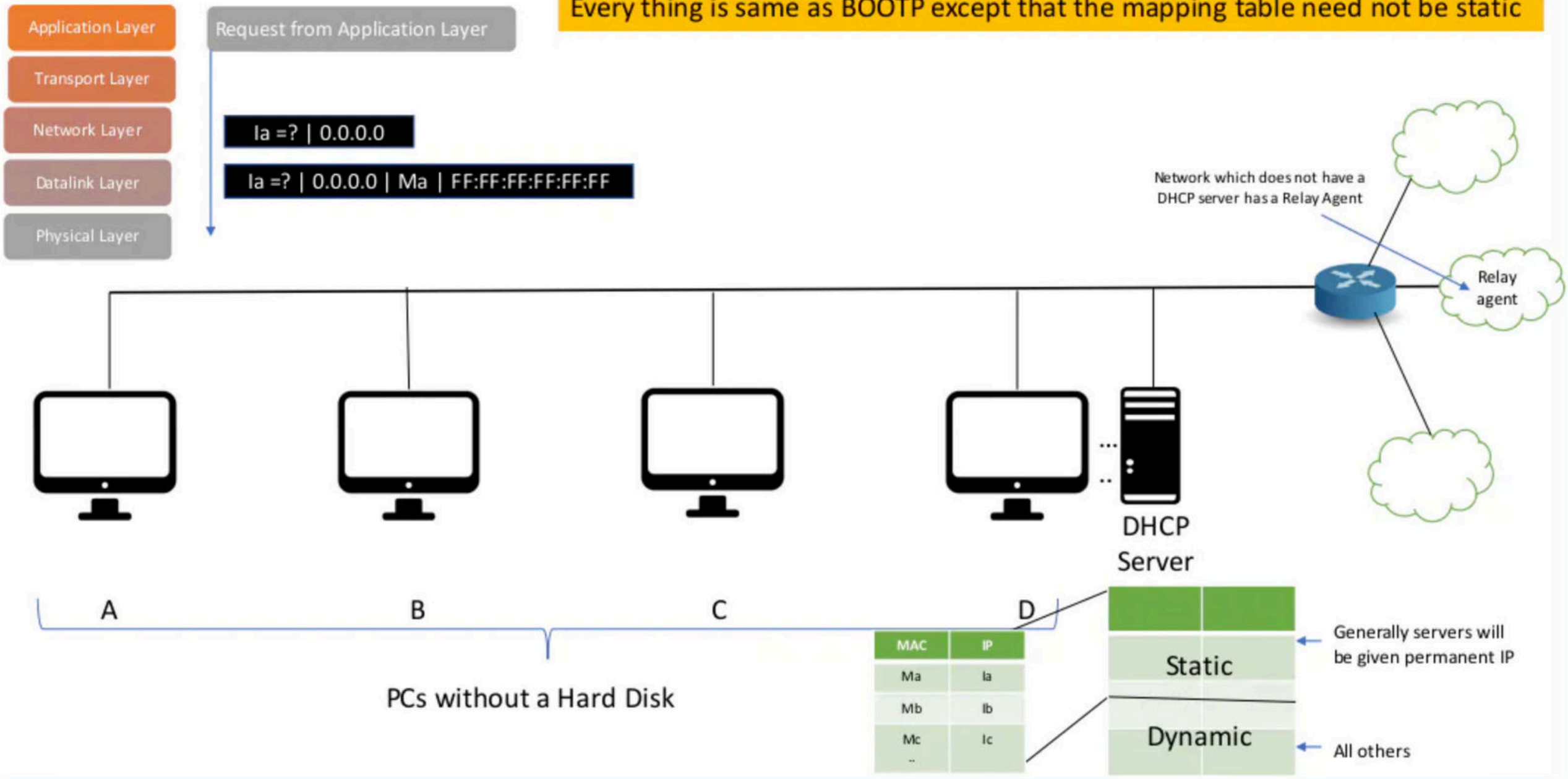
Network which does not have a BOOTP server has a Relay Agent



PCs without a Hard Disk

DHCP – Dynamic Host Configuration Protocol

Every thing is same as BOOTP except that the mapping table need not be static



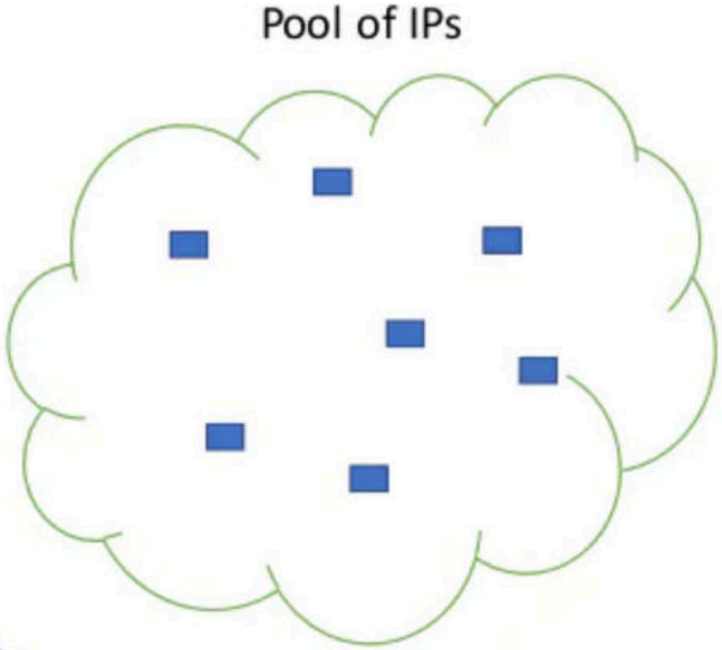
DHCP MAPPING TABLE

Static

MAC	IP
Ma	Ia
Mb	Ib
Mc	Ic
Md	Id
....	...

Dynamic

MAC	IP	Least Time
Ms	Is	10 mins



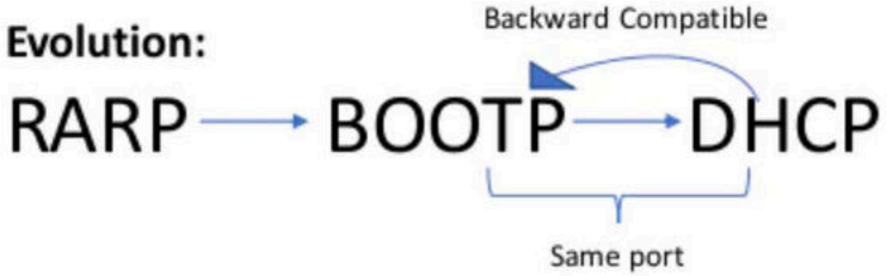
Picking from the pool of IPs

Note : If renew requests is not sent the IP is pulled and added back to the pool

Advantage and points to remember:

- Only One DHCP server is enough.
- Dynamic Table

Evolution:

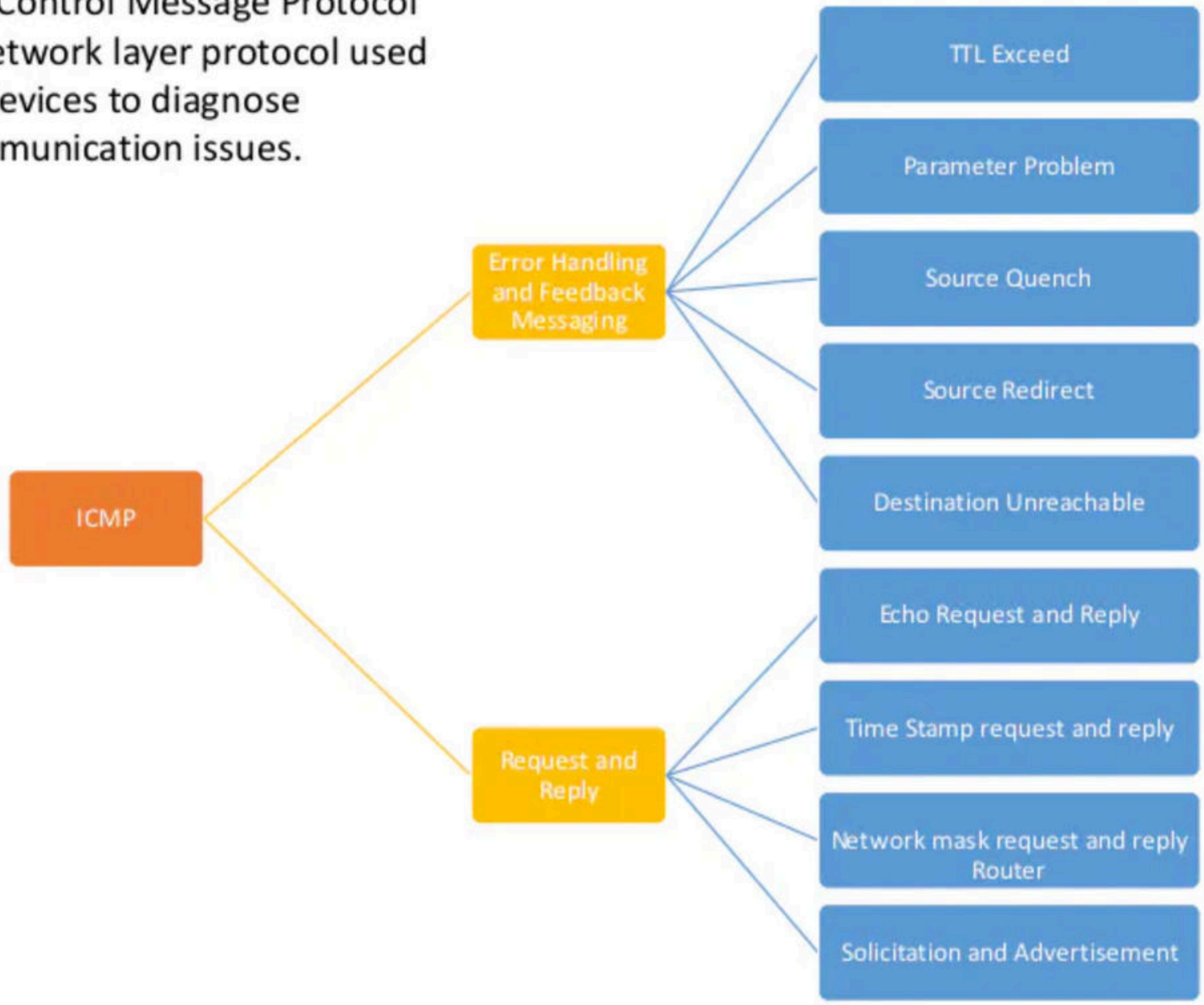


Computer Networks

ICMP

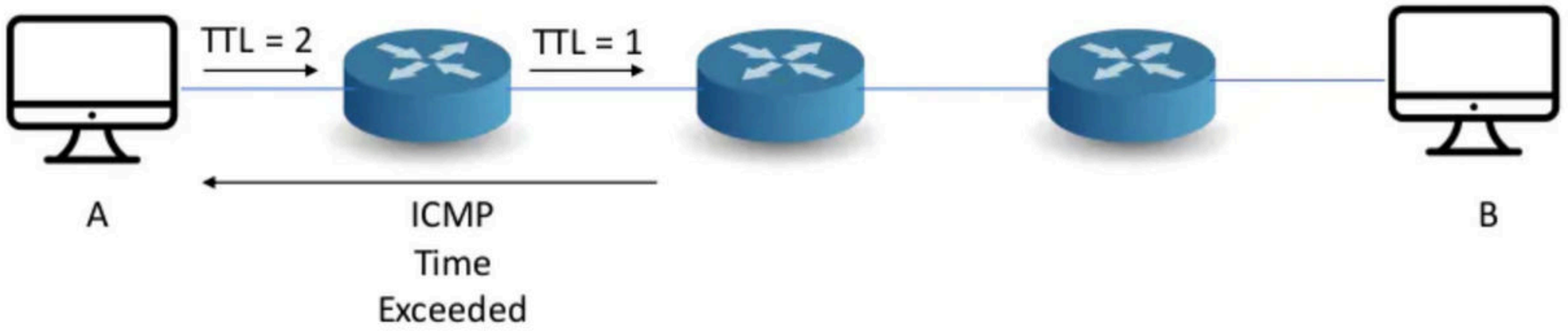
Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues.

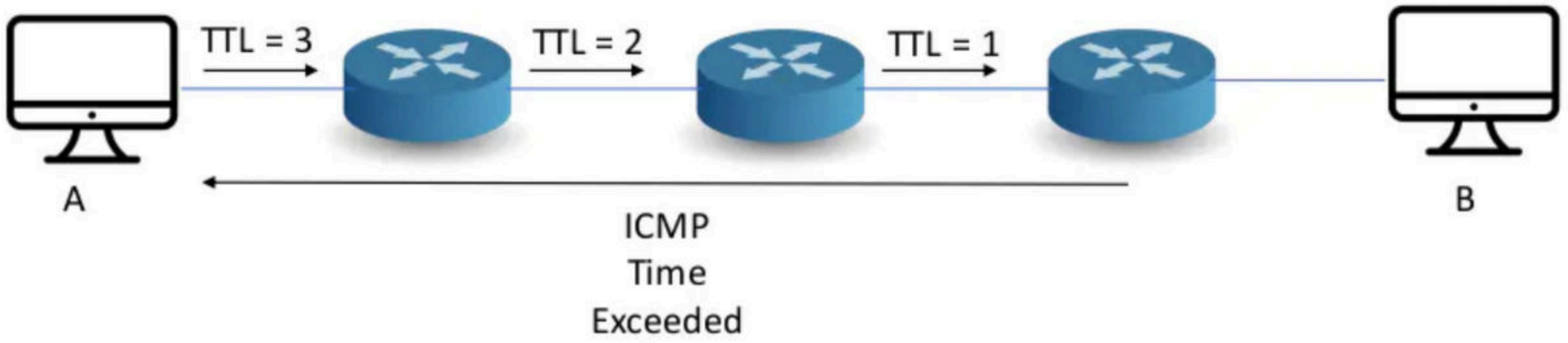


TTL Exceed

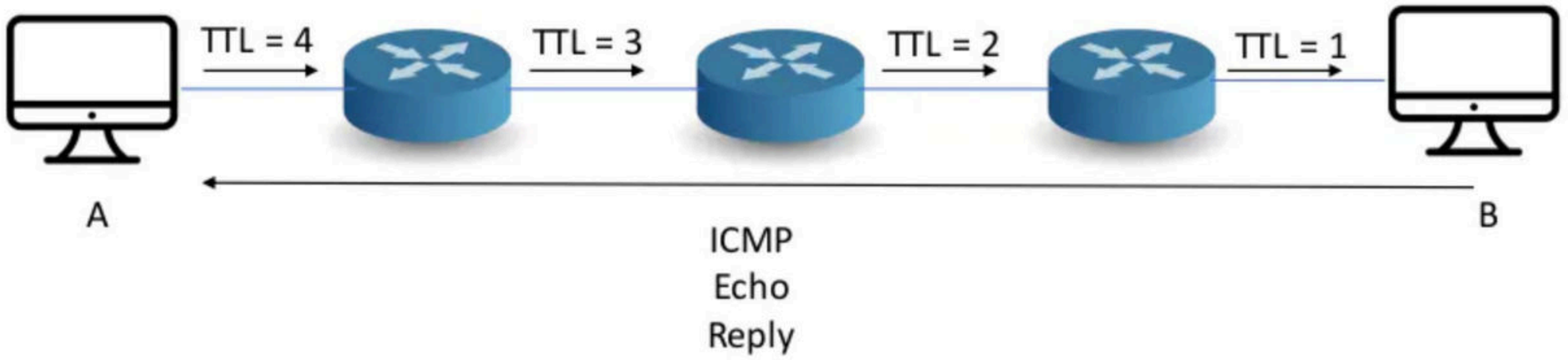
TTL Exceed



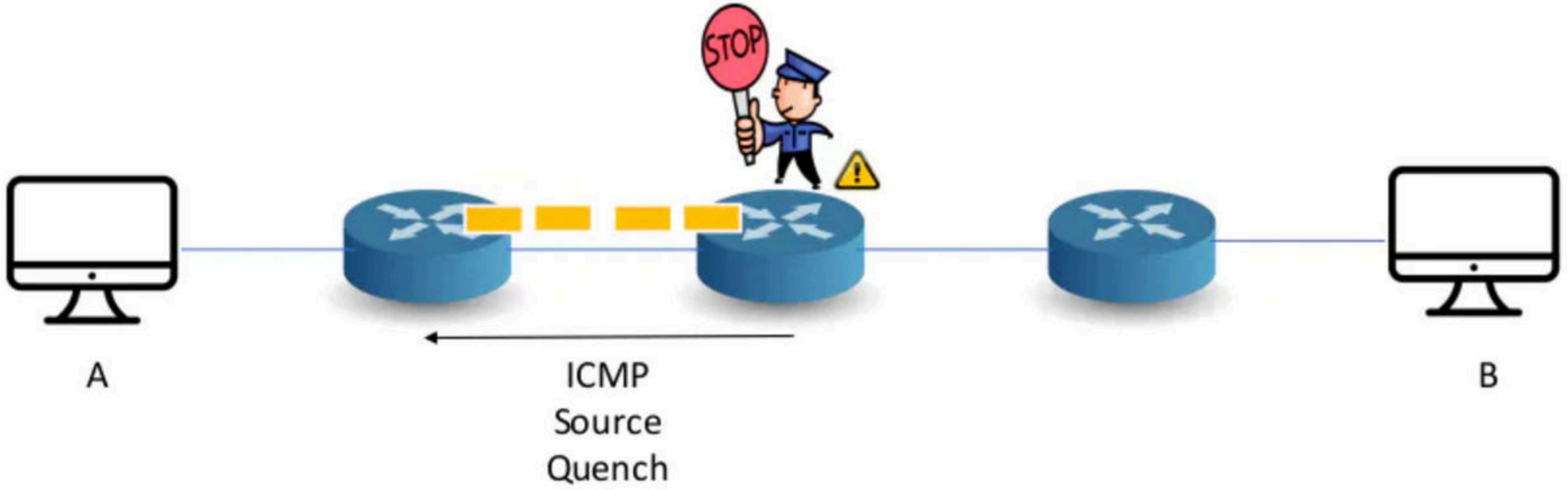
TTL Exceed



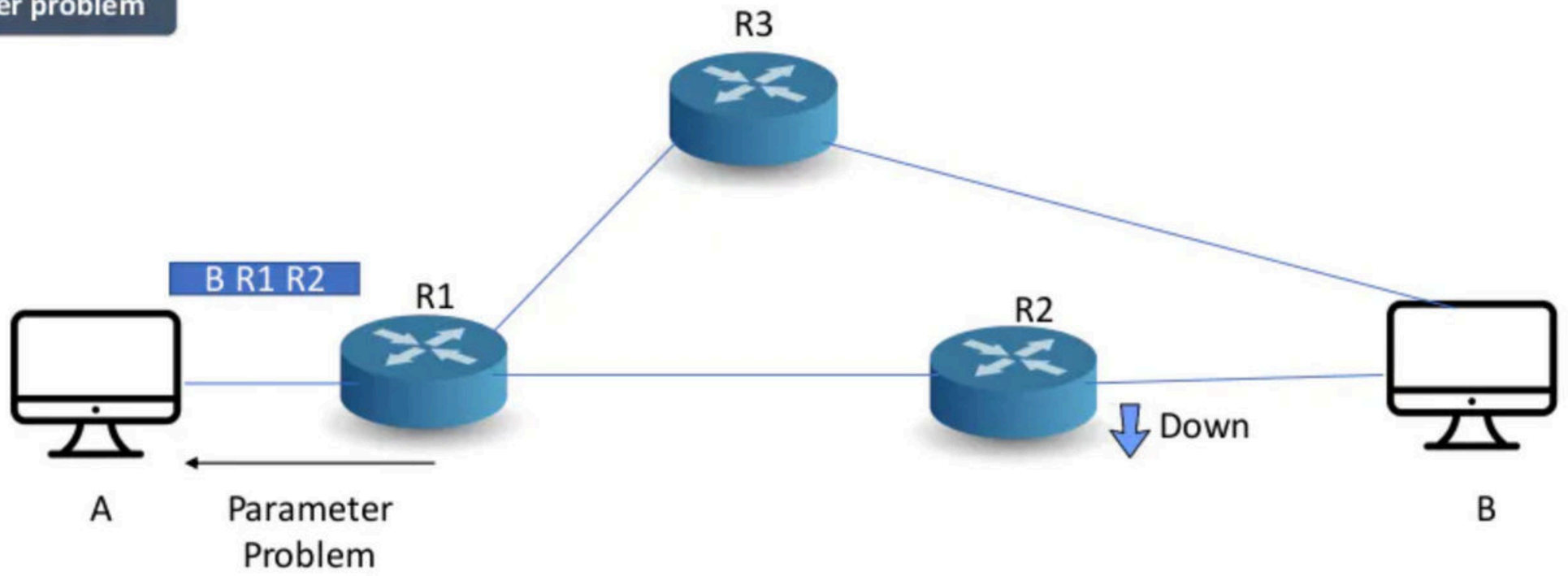
TTL Exceed



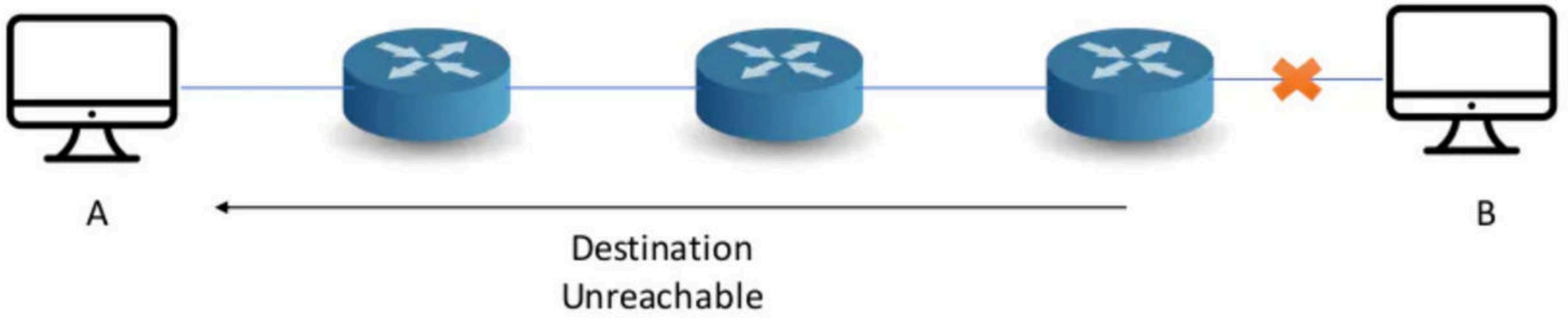
Source quench



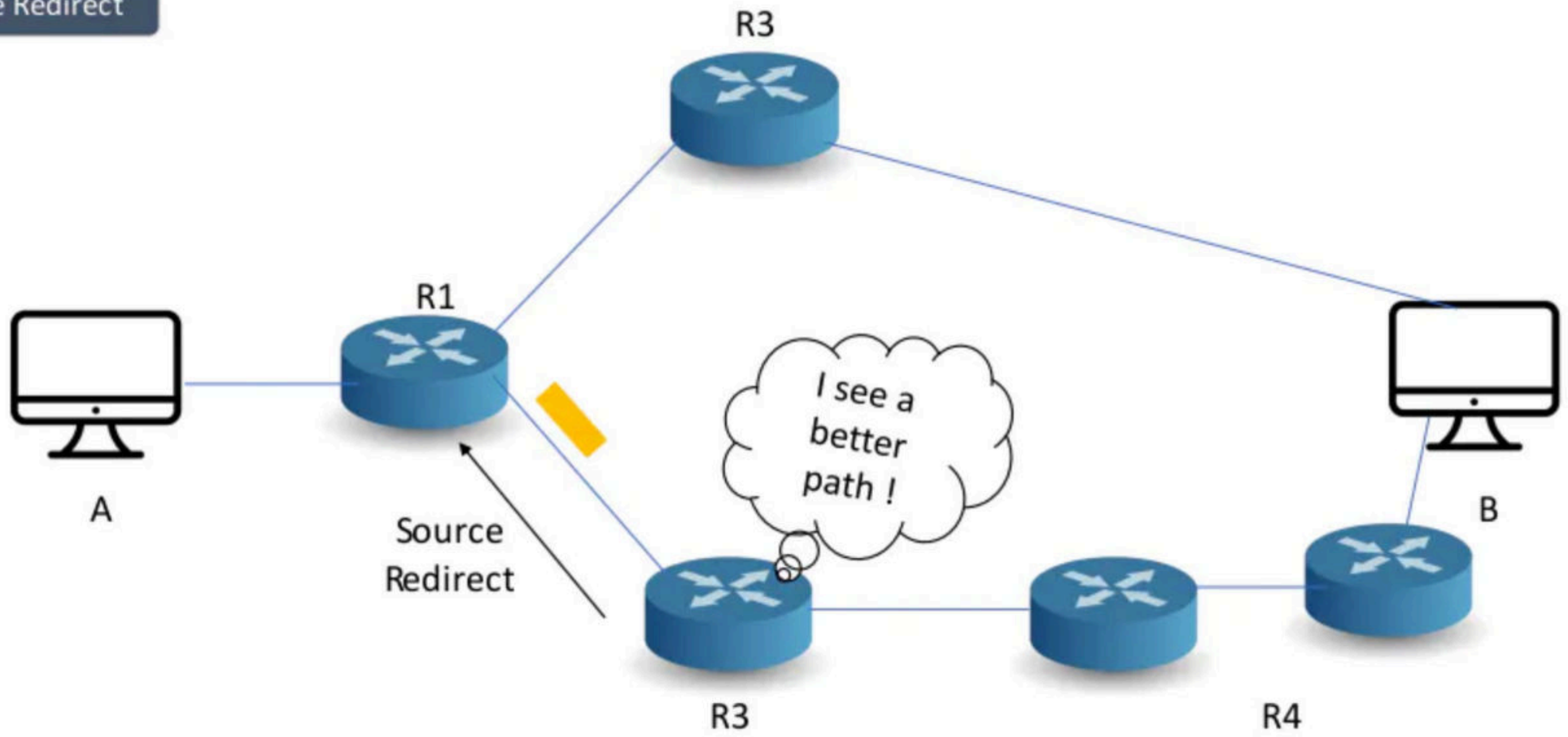
Parameter problem



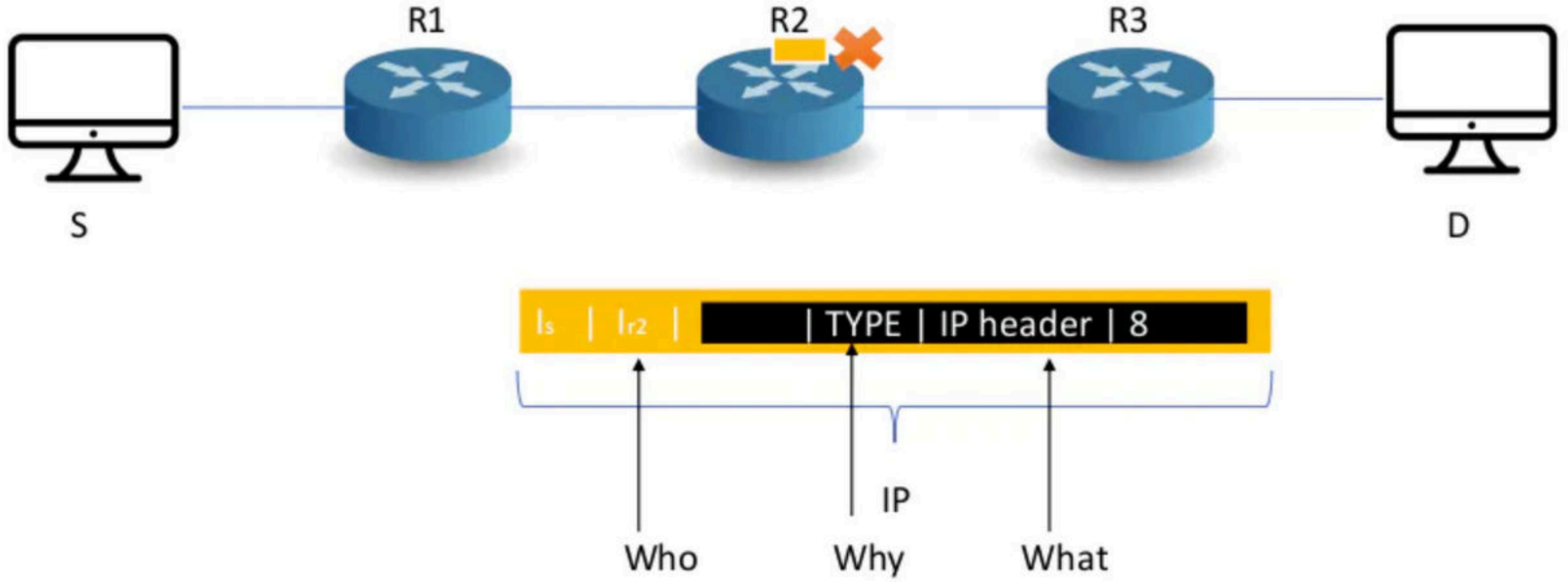
Destination unreachable



Source Redirect



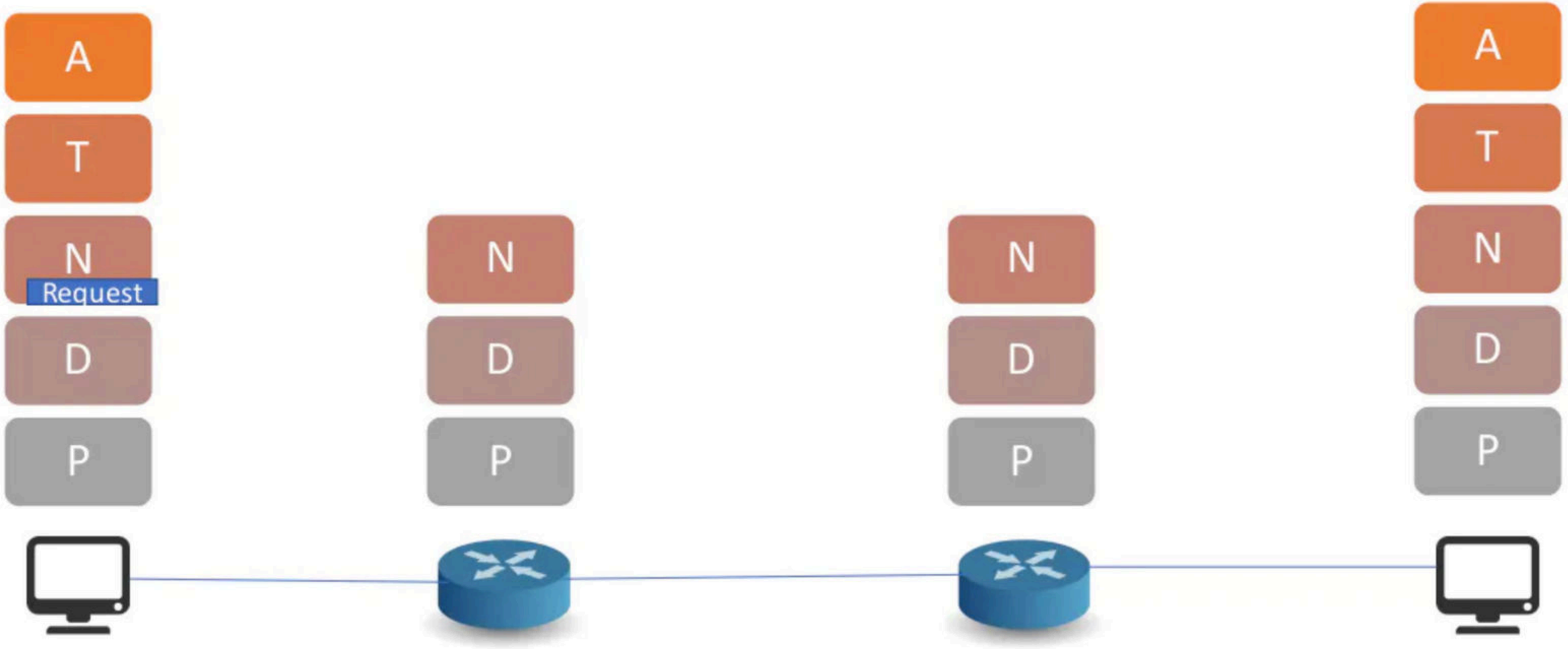
These are things that sender should know:
Who discarded ?
Why it got discarded ?
What packet did you discard?



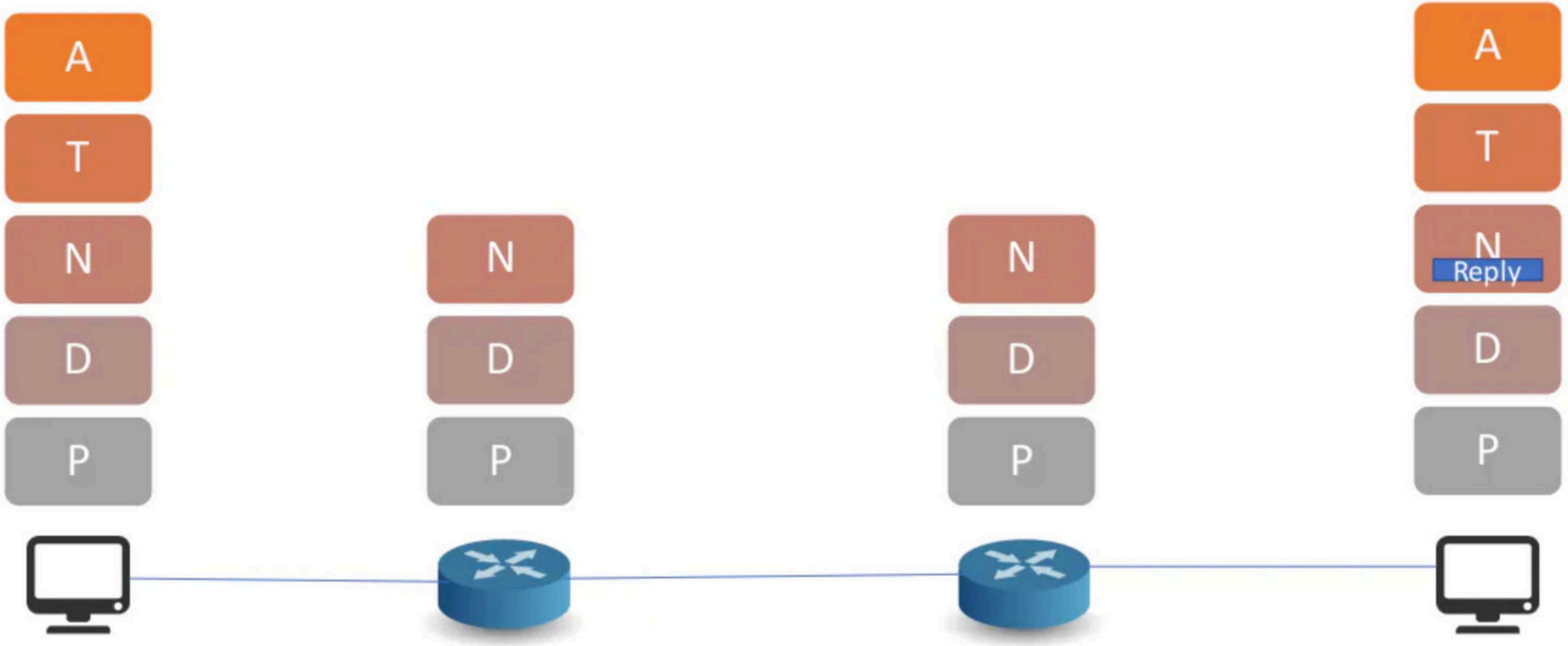
Computer Networks

ICMP Part 2

Echo Request and Reply



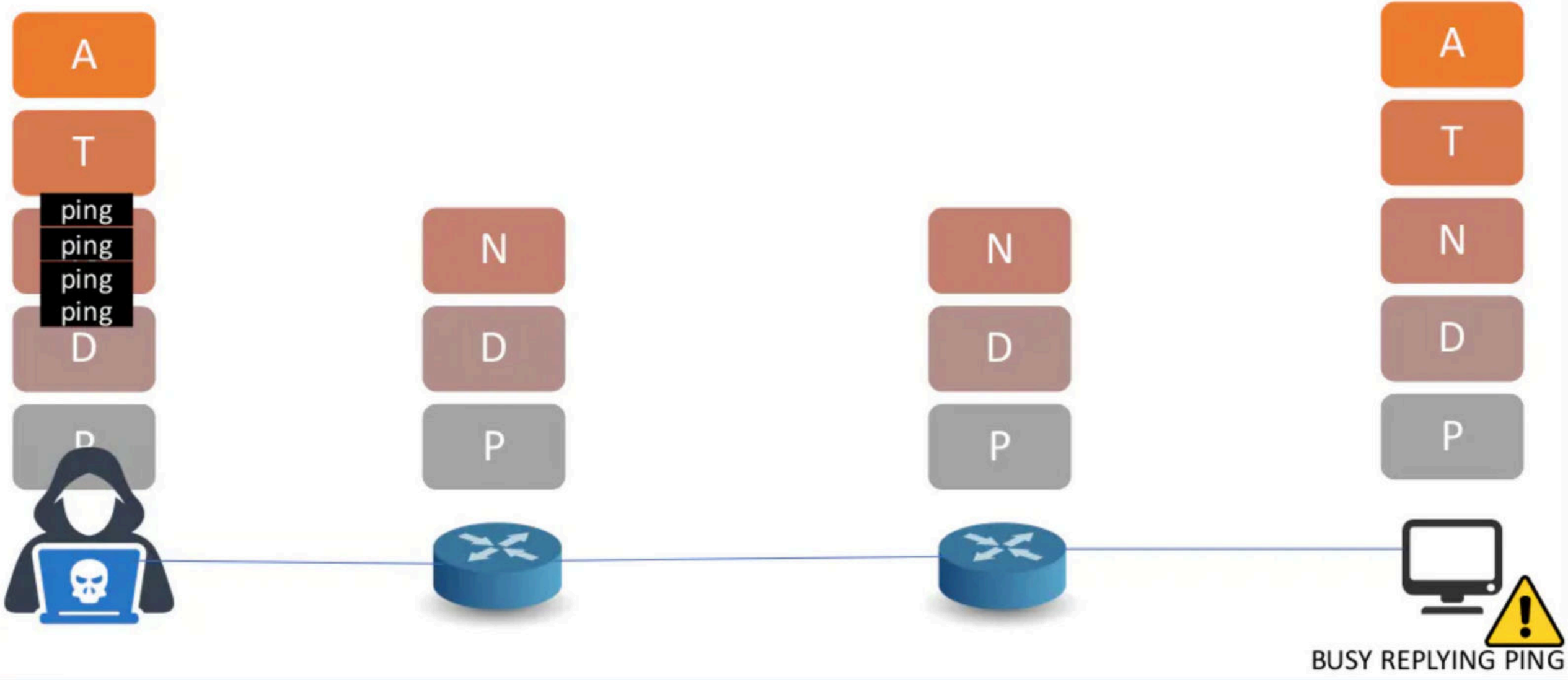
Echo Request and Reply



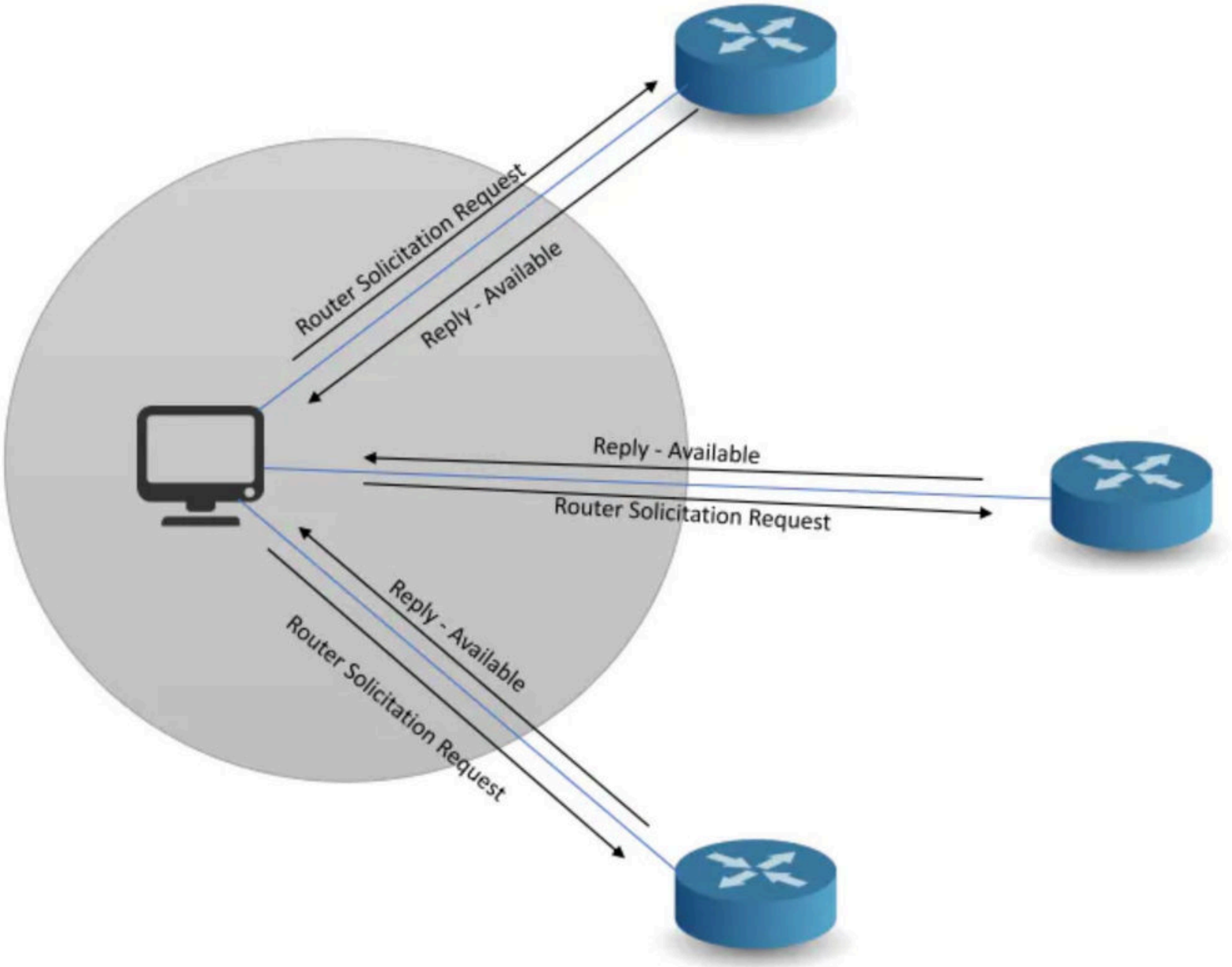
Echo Request and Reply

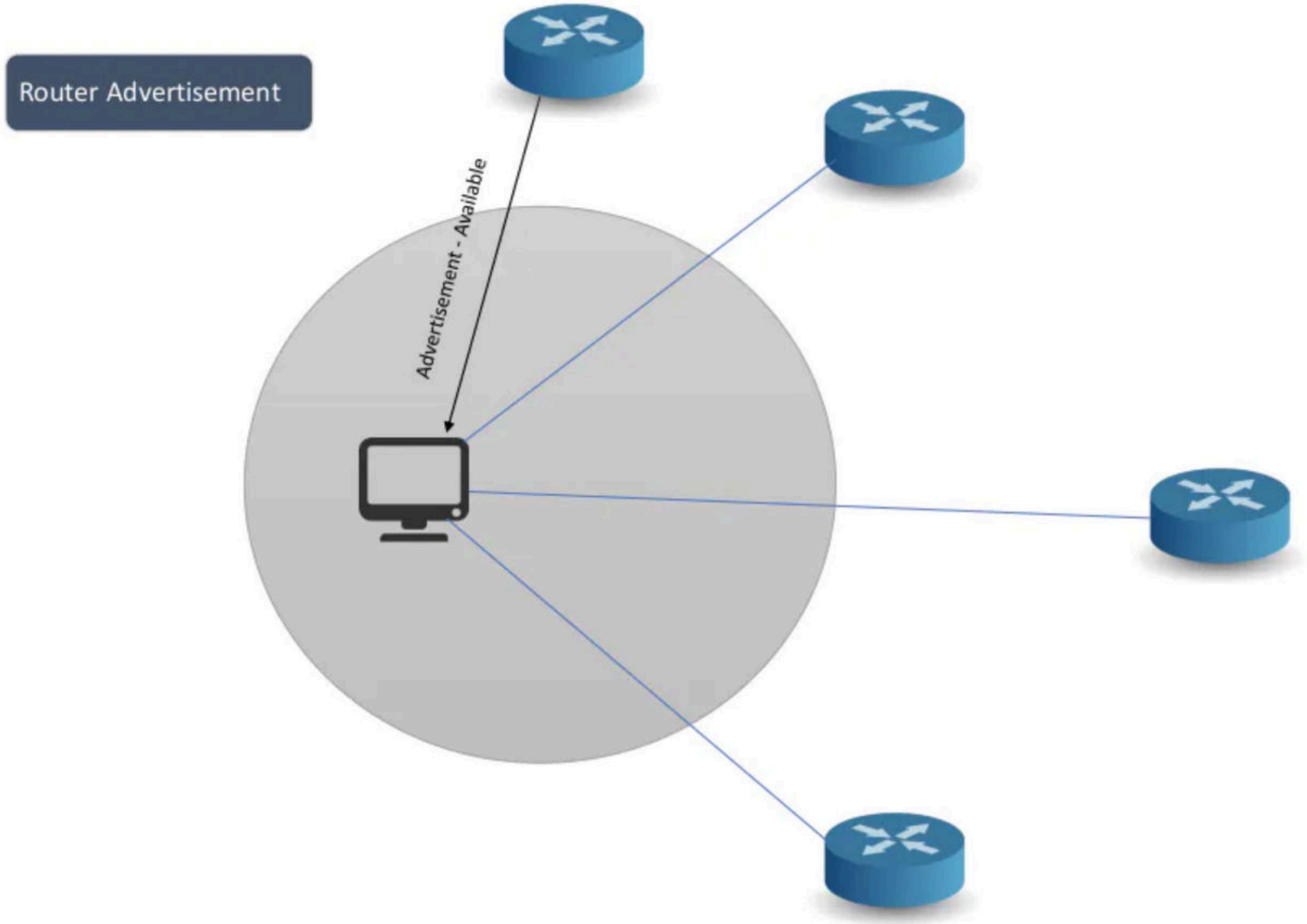
Attack possible
DENIAL OF SERVICE

PING is the Packet InterNet Grope

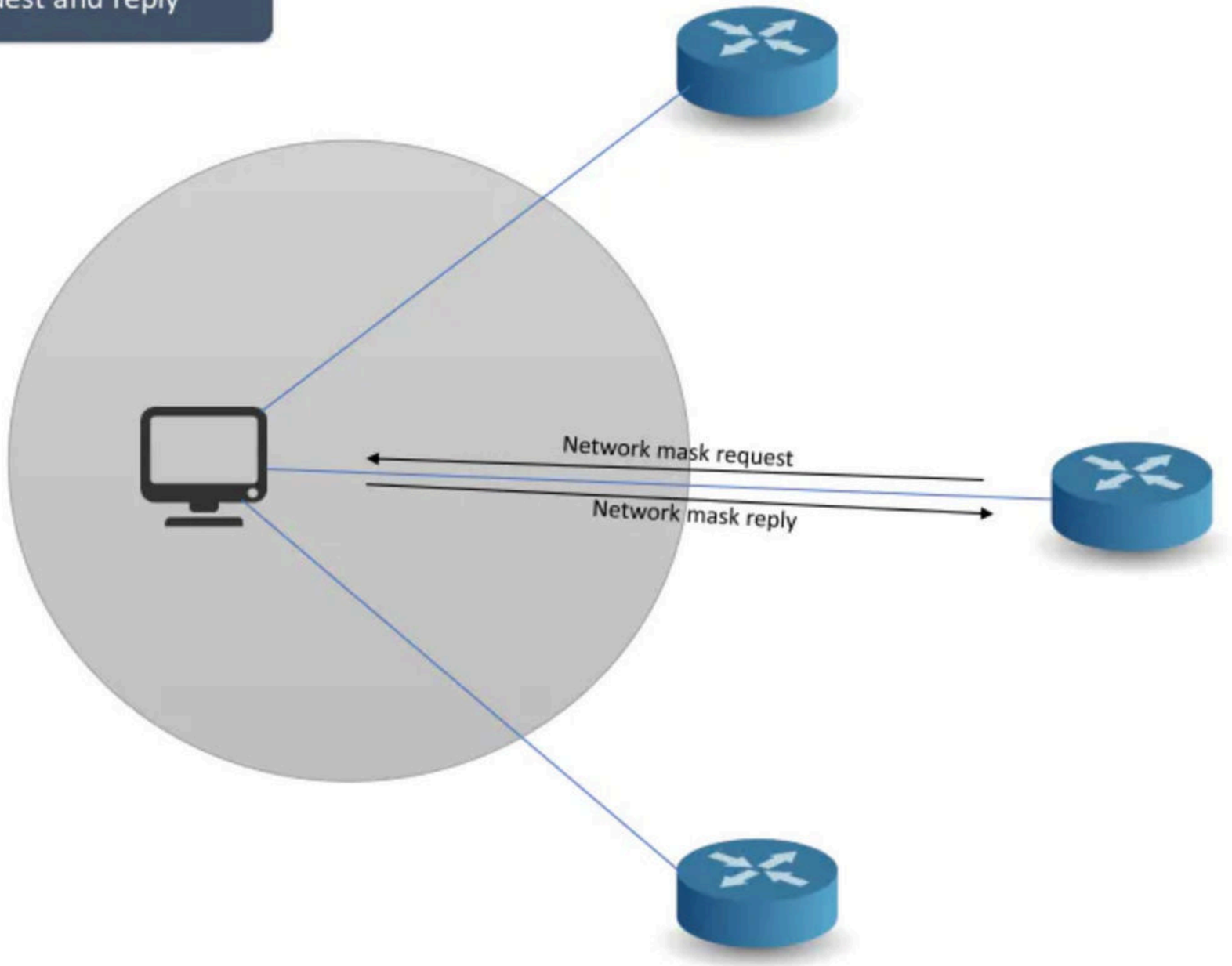


Router Solicitation




Router Advertisement
Advertisement - Available

Network mask request and reply



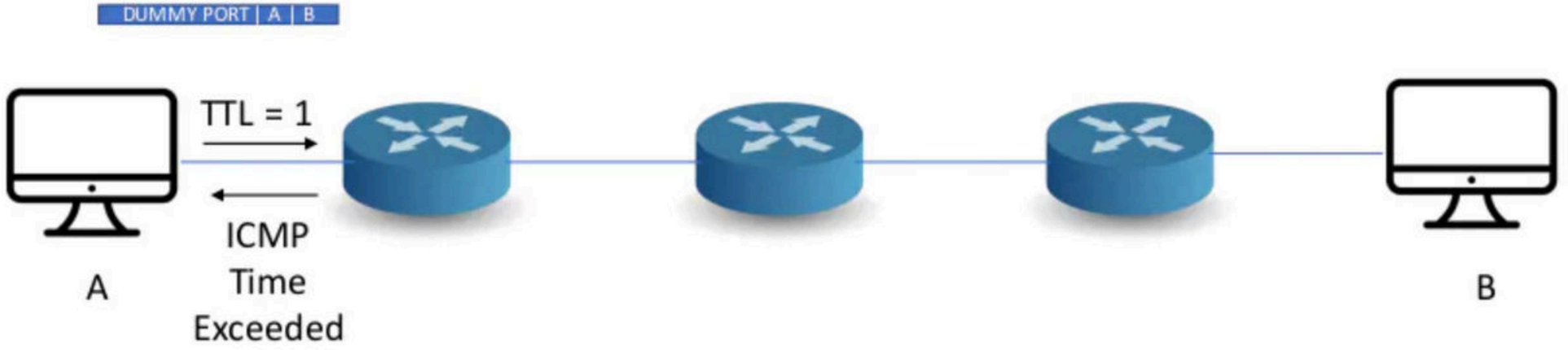
Timestamp request and reply

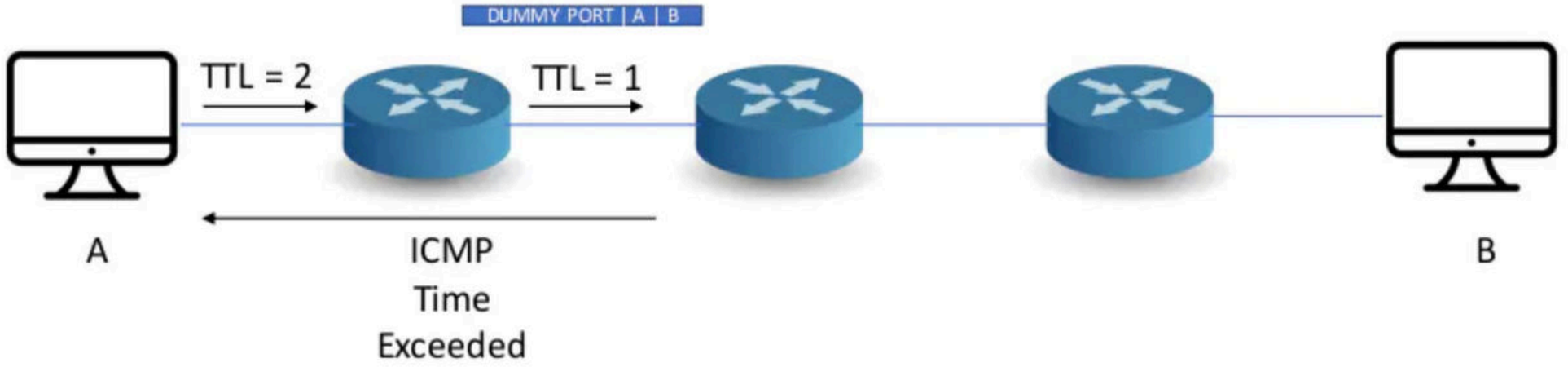
- ICMP Timestamp Request and Timestamp Reply messages are used by network routers to synchronize their system clocks for time and date.
- When a router needs to synchronize its system time, it sends an ICMP Timestamp Request message to the other router.
- Once the ICMP Timestamp Request message is received by the other router, it will respond back with an ICMP Timestamp Reply message.
- Timestamp Reply message contains other router's date and time.
- ICMP Timestamp Request and Timestamp Reply messages are not used much these days, because there an entire protocol itself is dedicated for network device time synchronization.

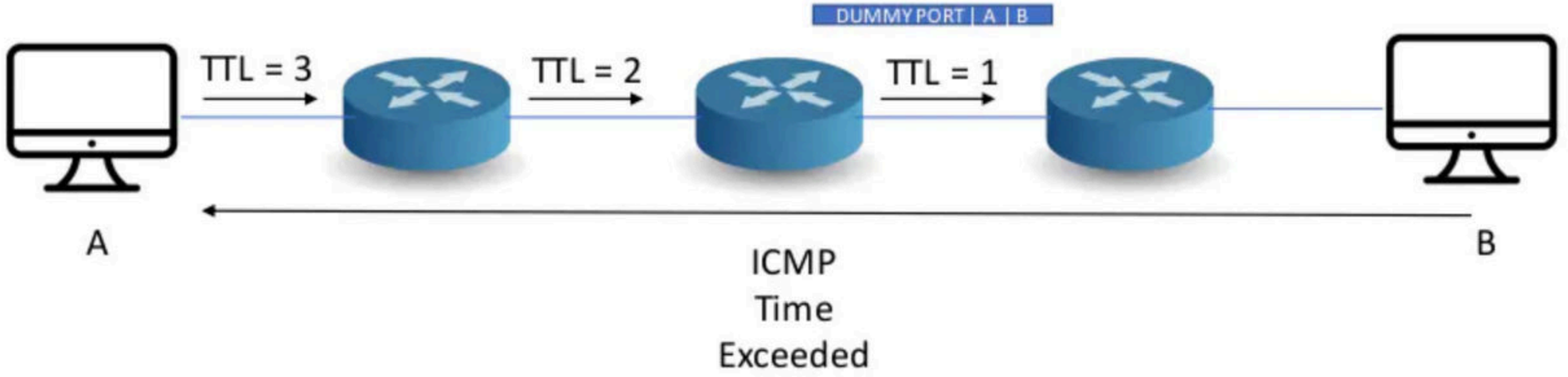
Computer Network

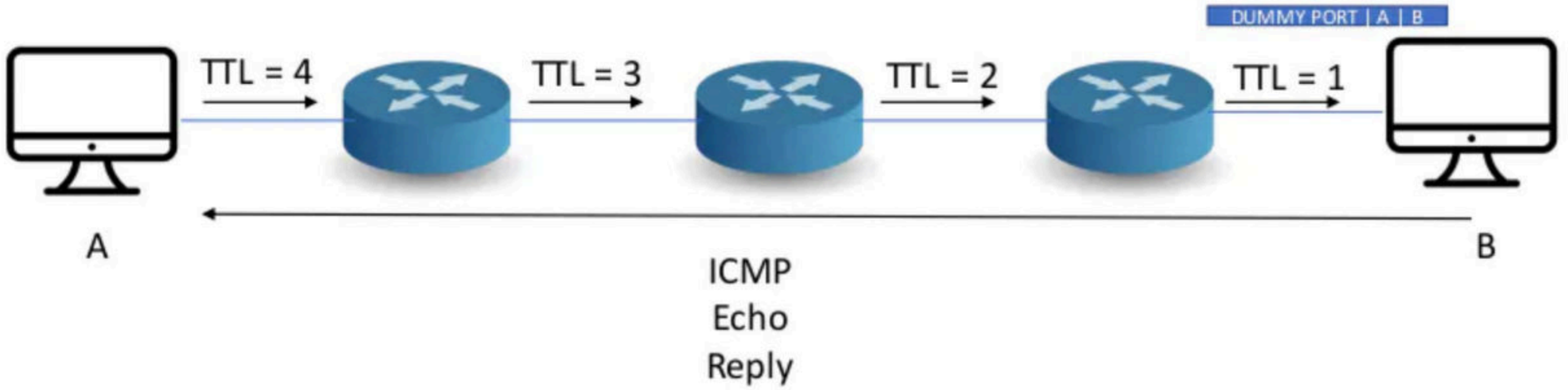
Trace route

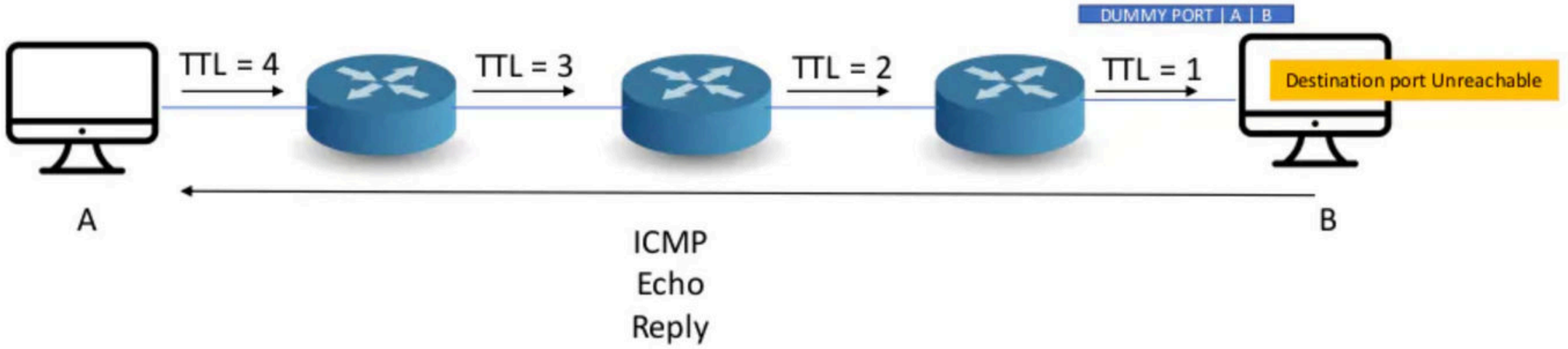
Trace route Command on Linux **traceroute** domain

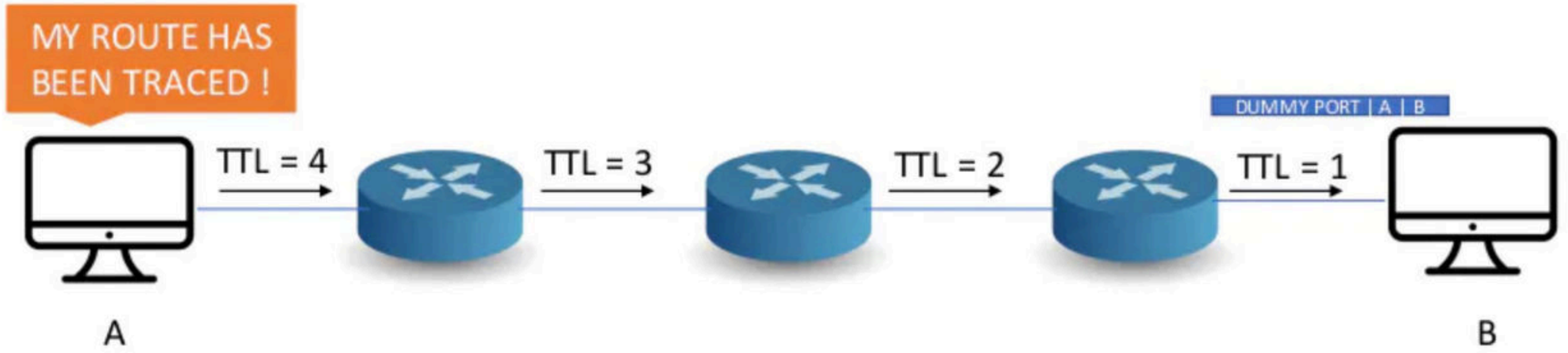



DUMMY PORT | A | B
TTL = 2
TTL = 1
A
ICMP
Time
Exceeded
B


DUMMY PORT | A | B
TTL = 3
TTL = 2
TTL = 1
A
B
ICMP
Time
Exceeded

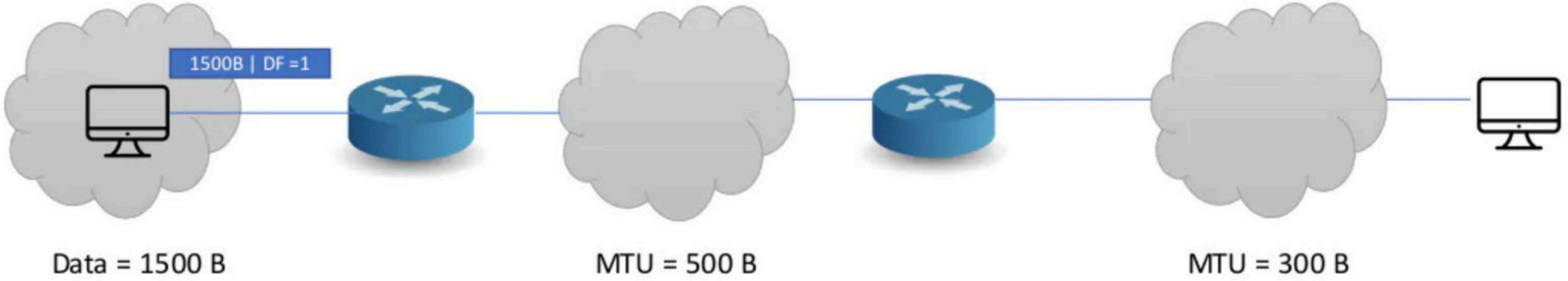

DUMMY PORT | A | B
TTL = 4
TTL = 3
TTL = 2
TTL = 1
A
B
ICMP
Echo
Reply

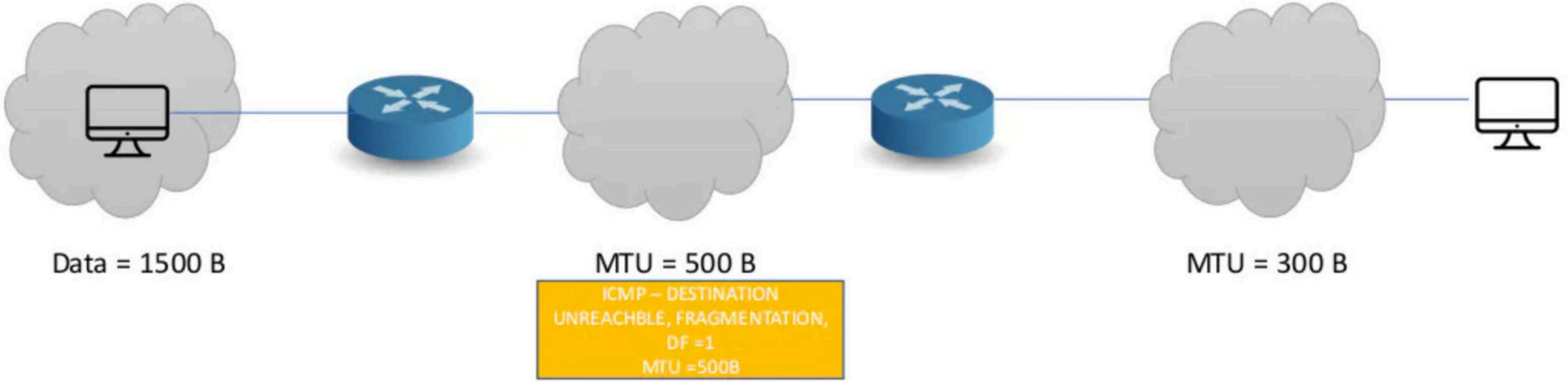

DUMMY PORT | A | B
TTL = 4
TTL = 3
TTL = 2
TTL = 1
Destination port Unreachable
A
B
ICMP
Echo
Reply

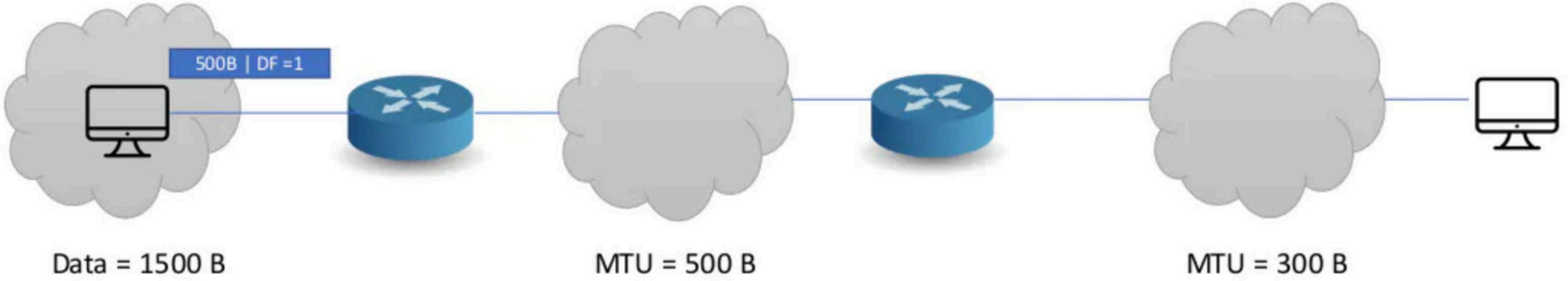

MY ROUTE HAS BEEN TRACED !
TTL = 4
TTL = 3
TTL = 2
TTL = 1
DUMMY PORT | A | B
A
B

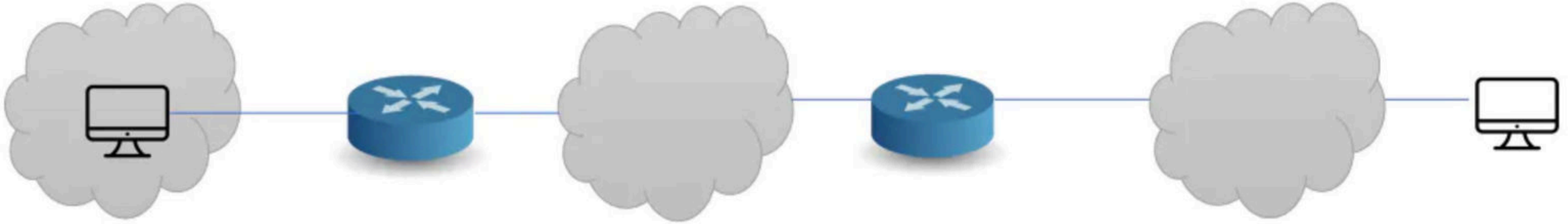
Computer Networks

Path MTU Discovery


1500B | DF =1
Data = 1500 B
MTU = 500 B
MTU = 300 B


Data = 1500 B
MTU = 500 B
ICMP – DESTINATION UNREACHBLE, FRAGMENTATION, DF =1 MTU =500B
MTU = 300 B


500B | DF =1
Data = 1500 B
MTU = 500 B
MTU = 300 B

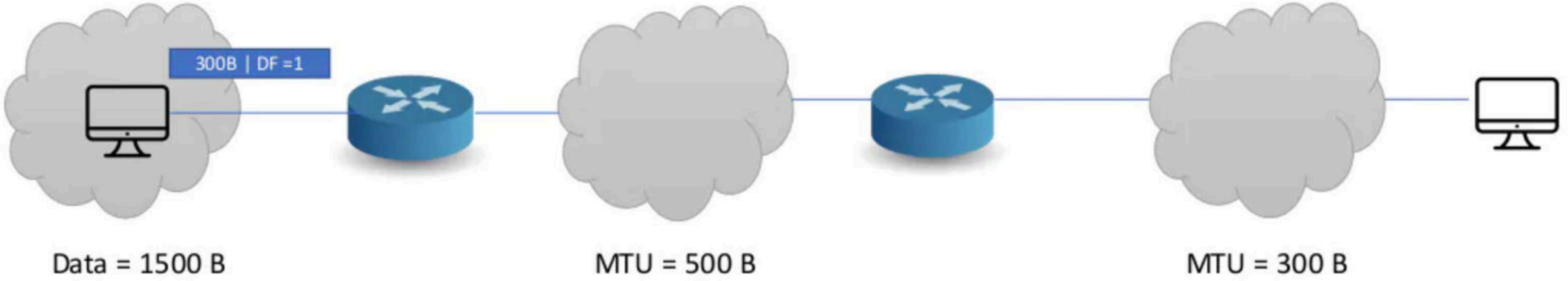


Data = 1500 B

MTU = 500 B

MTU = 300 B

ICMP – DESTINATION UNREACHBLE, FRAGMENTATION, DF =1
MTU =300B


300B | DF =1
Data = 1500 B
MTU = 500 B
MTU = 300 B