# Hardware and various devices used in networking

● **Cables, Repeaters and Hubs —**

→ networks of computer called computer network.

**Hardware:**

● **Cables** :

AL       various kinds of ~~watewires~~    only one can sent data at a time.

TL

NL     range ← (100m)

DLL     10 Base T (10Mbps, No multiplexing,

PL      10 Base 2 (10Mbps, No mul, 200m)

[A]     10 Base 5 (10mbps, No mul, 500 meter)

host

(computer)    100 Base T

→ 1) all work at physical layer (PL)

2) all have the problem Authentica
        -tion.

3) collisions possible.
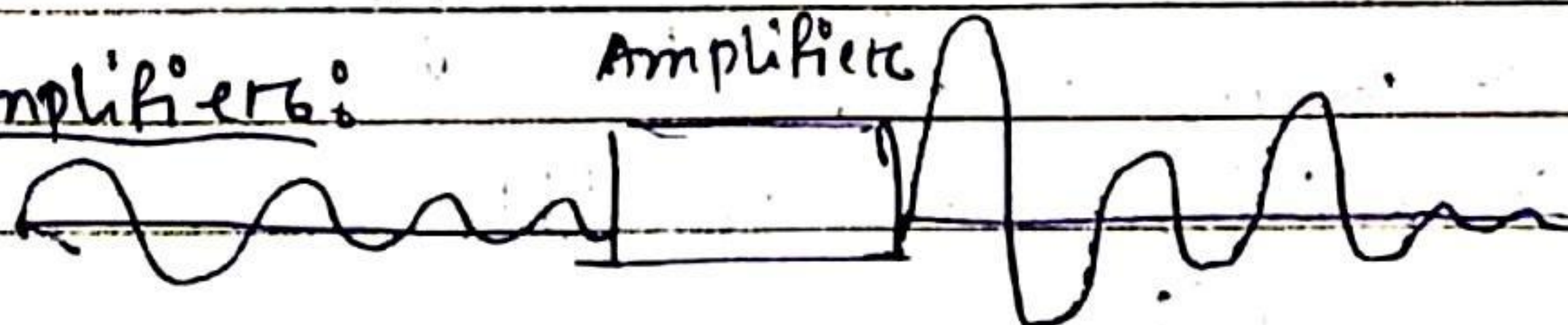    (Collision Domain is n)

4)

● **Repeater :**    R

   10base5     repeater    10base5
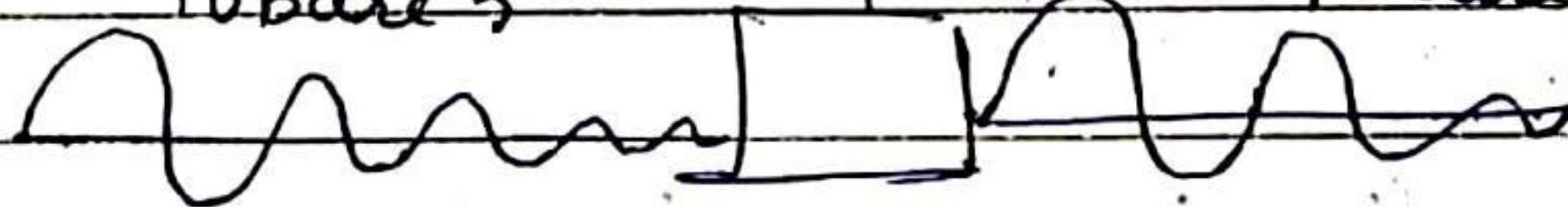


● **Amplifier:**    Amplifier

LAN : less than 10KM.

MAN : (10KM – 100KM)

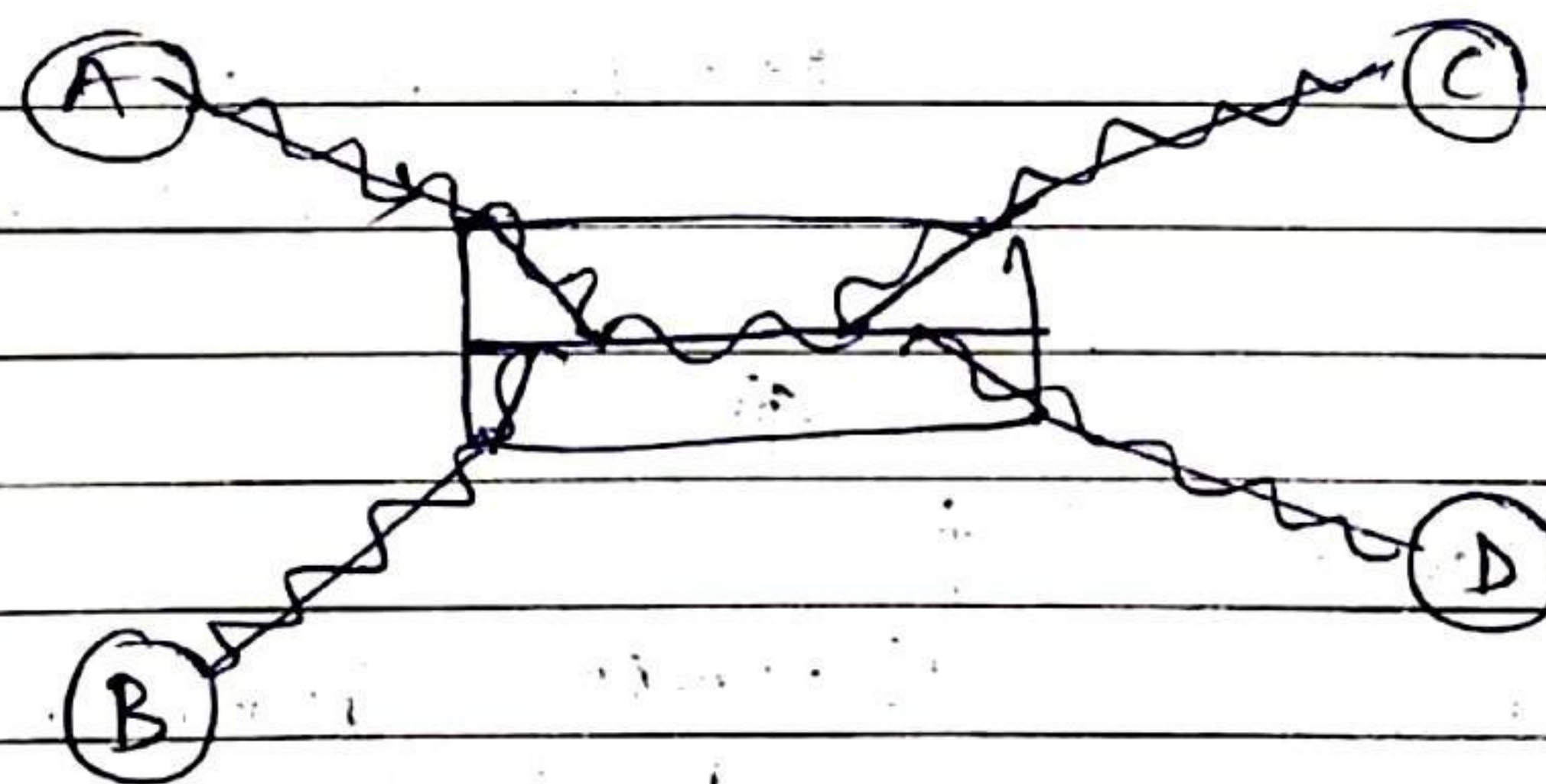WAN : More than 100KM.

- Reapeater -
  → Reapeater used to connect two lan segment.
    → work at DL
    → Collision are possible.
      (Collision domain – n)
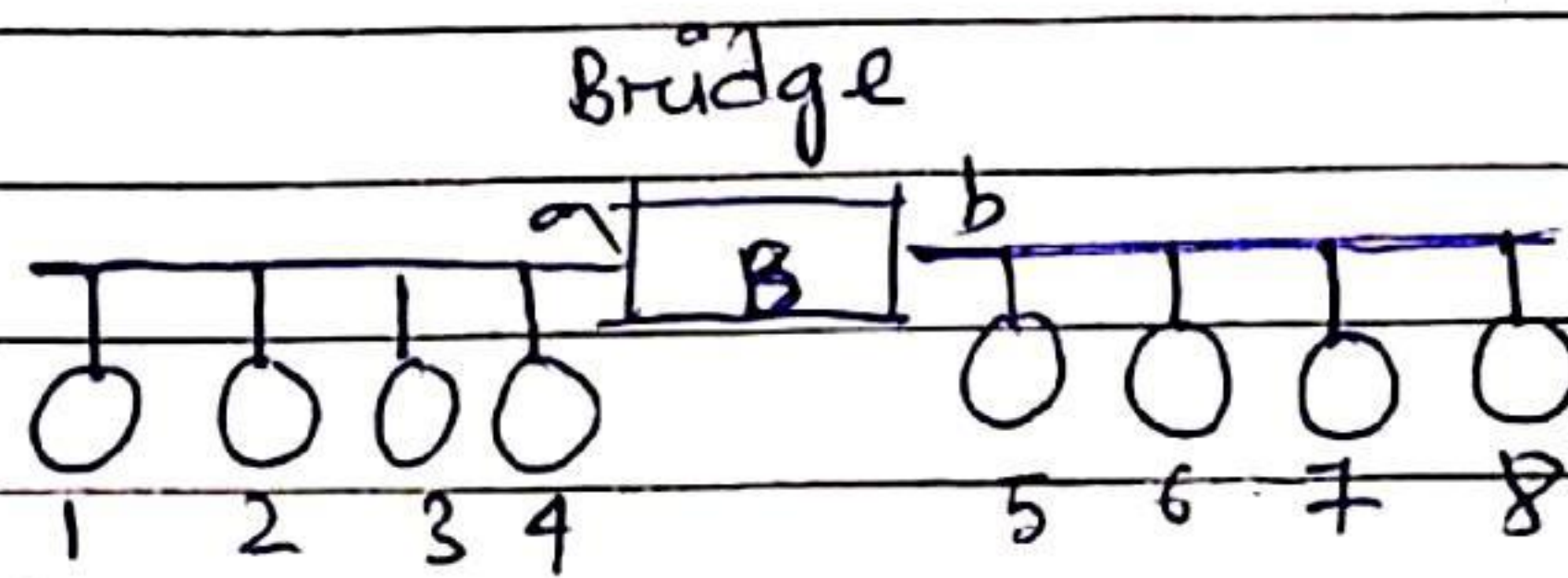    → Range of the lan is Increased.

- Hub -

  → Multiport reapeater.

    4-port repeater.



  → Traffic is very high.
  → Work at pL.
  → collision are possible.
       (CD-n)
  → Cost is less.
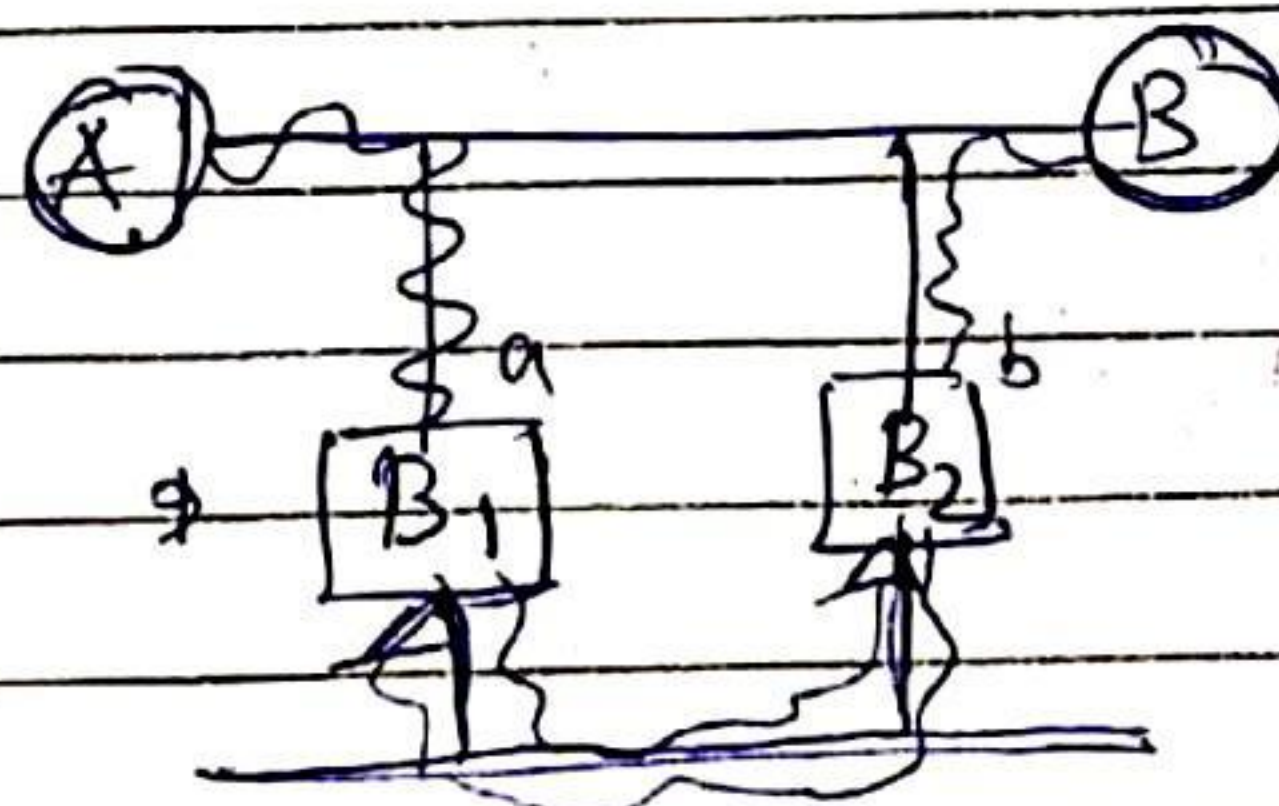
- **Bridges** —

Bridge



① ⑨ bridge works at both PL & DLL.

| MAC | port | Type of Bridges |
|-----|------|-----------------|
| 1 | a | i. Static bridges. |
| 2 | a | ii. Dynamic bridges |
| 3 | a | or |
| 4 | a | learning , |
| 5 | b | or |
| 6 | b | Transparent " |
| 7 | b | |
| 8 | b | |

④ → bridges cupable to filtering.
⑤ → Do forwarding. & Flooding.
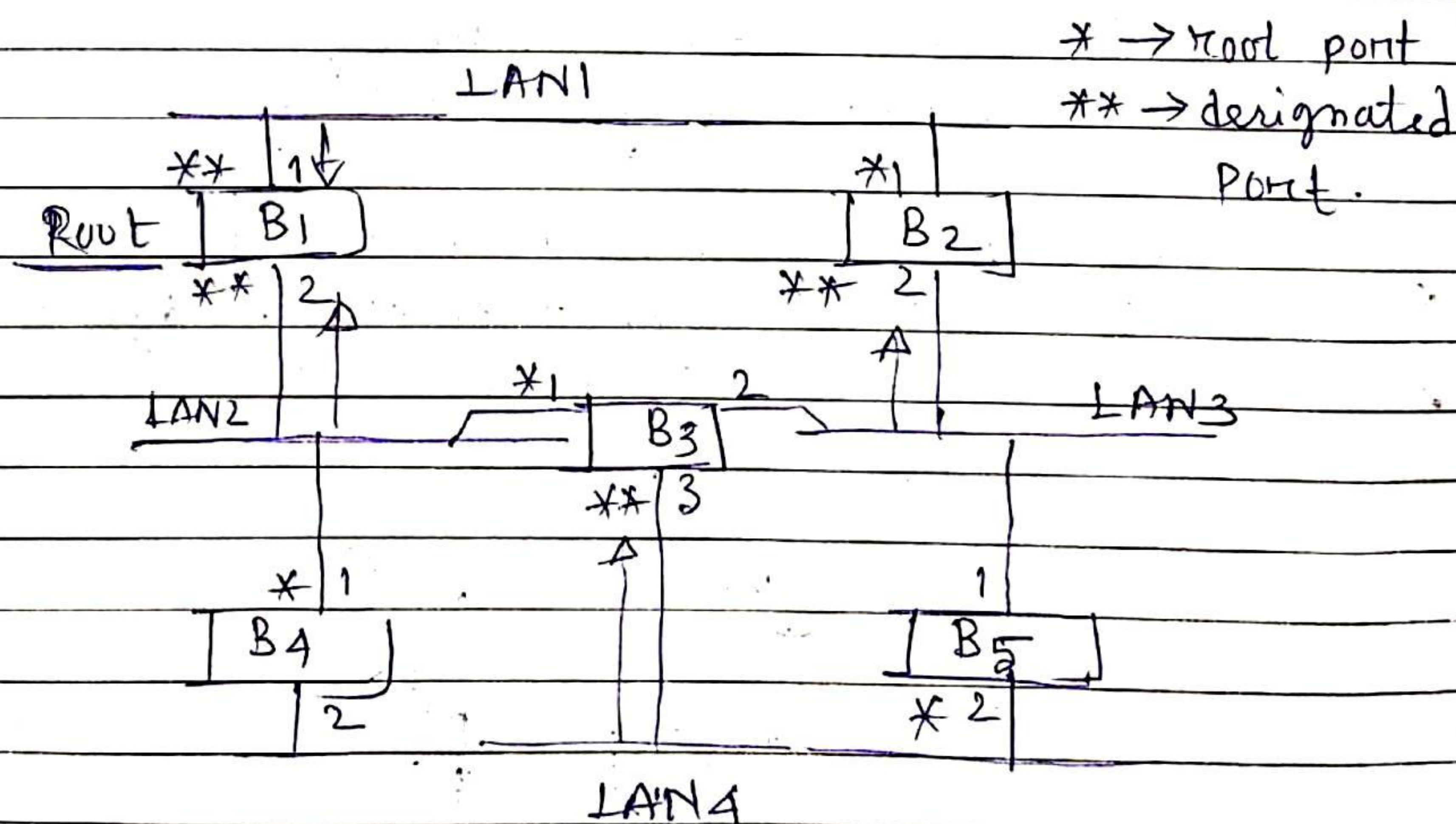
② store and forward a packet.
⑧ {→ No collicions inside the a bridge.
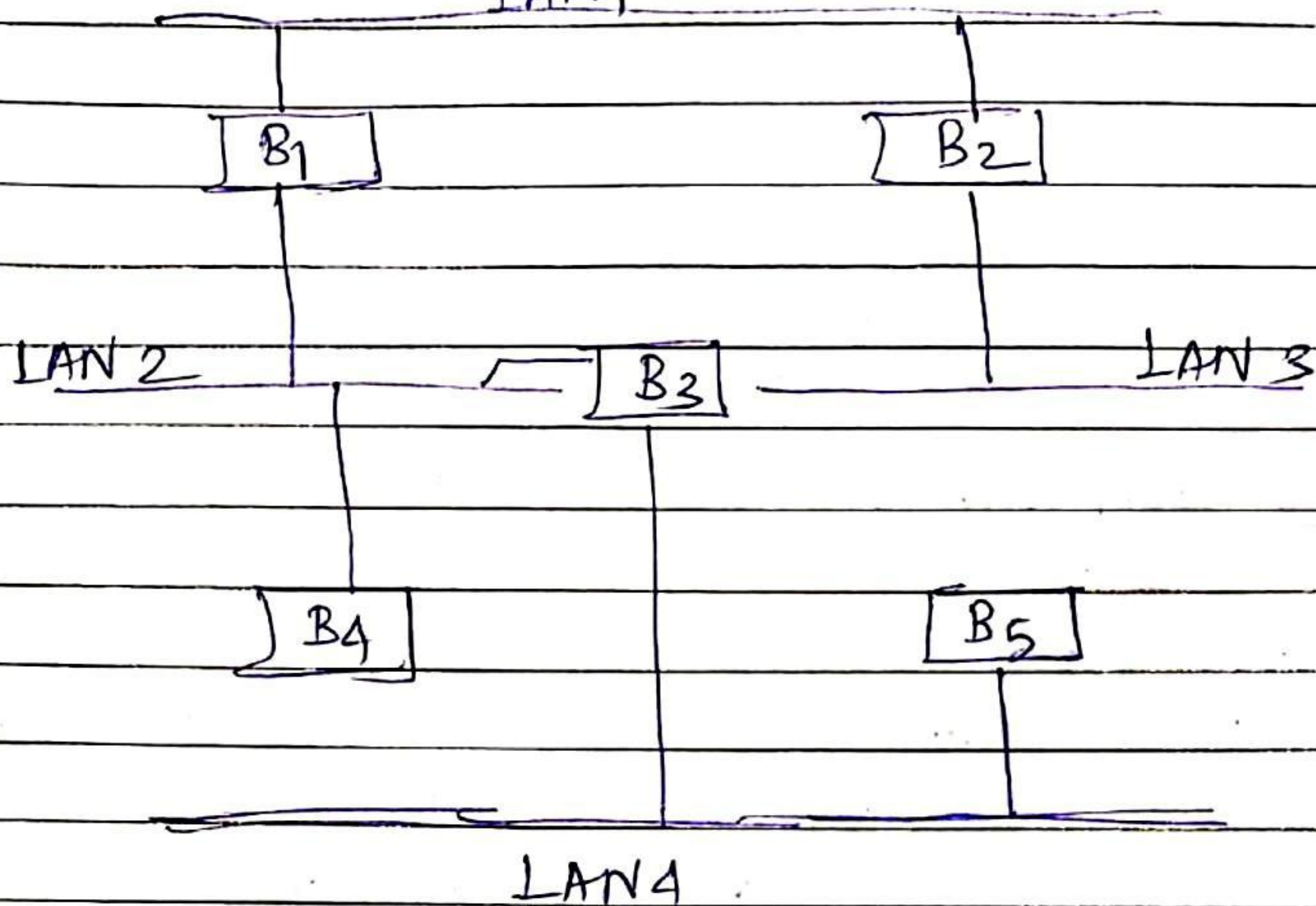      Collision Domain is reduced

- Spanning tree Algorithm in Bridges :—
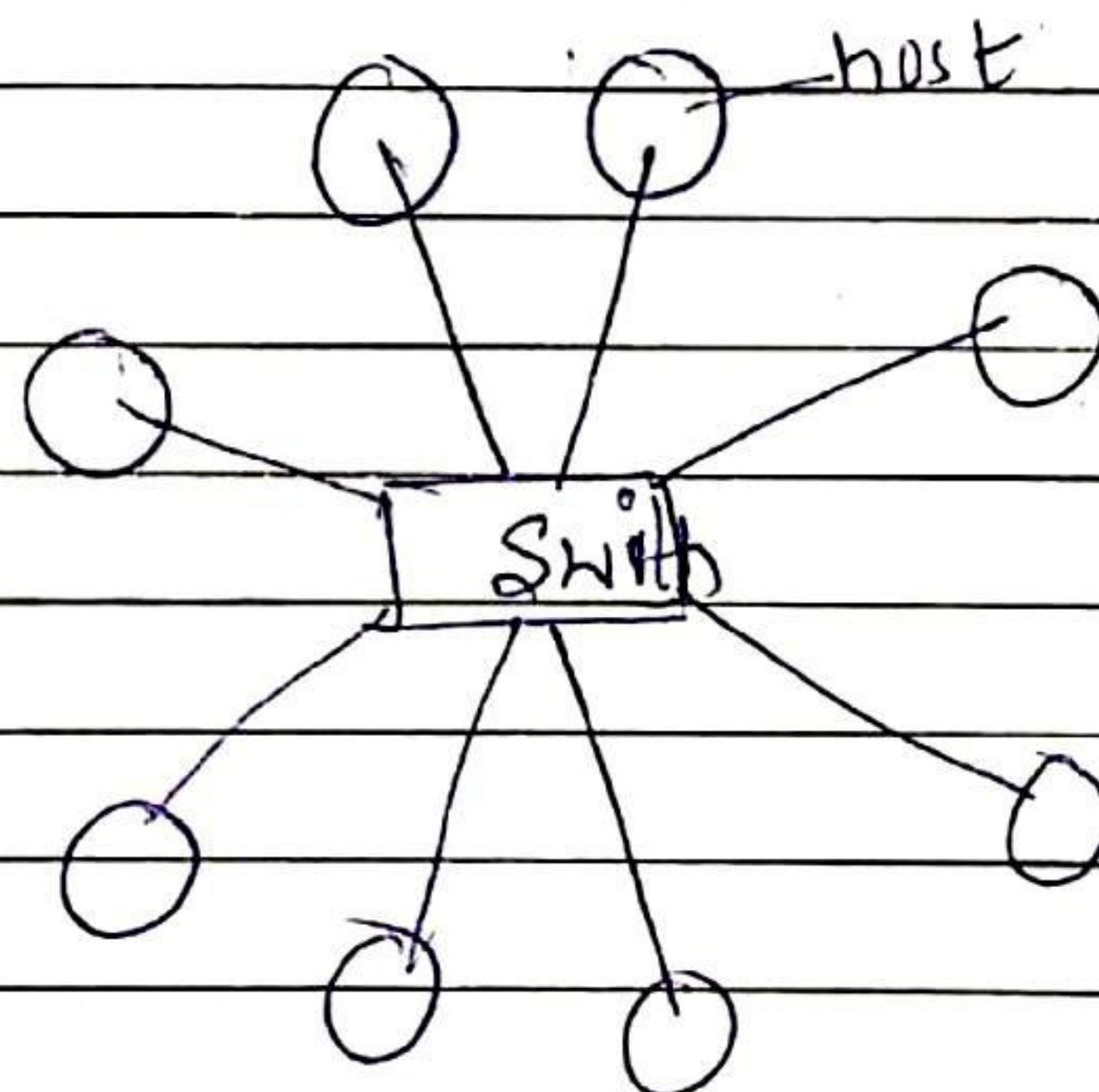  (to avoid infinite loop problem)

  Spanning three algorithm :

  1) Every bridge has a built-in ID. The one with smallest ID is taken as root bridge.

  2) mark one port of each bridge which is closest to root bridge as root port. (*)

  3) Every LAN chooses a bridge closest to its as a designated bridge for that LAN make the corresponding port as designated port.

  4) mark the root port and designated port as forwarding ports and black remaining.
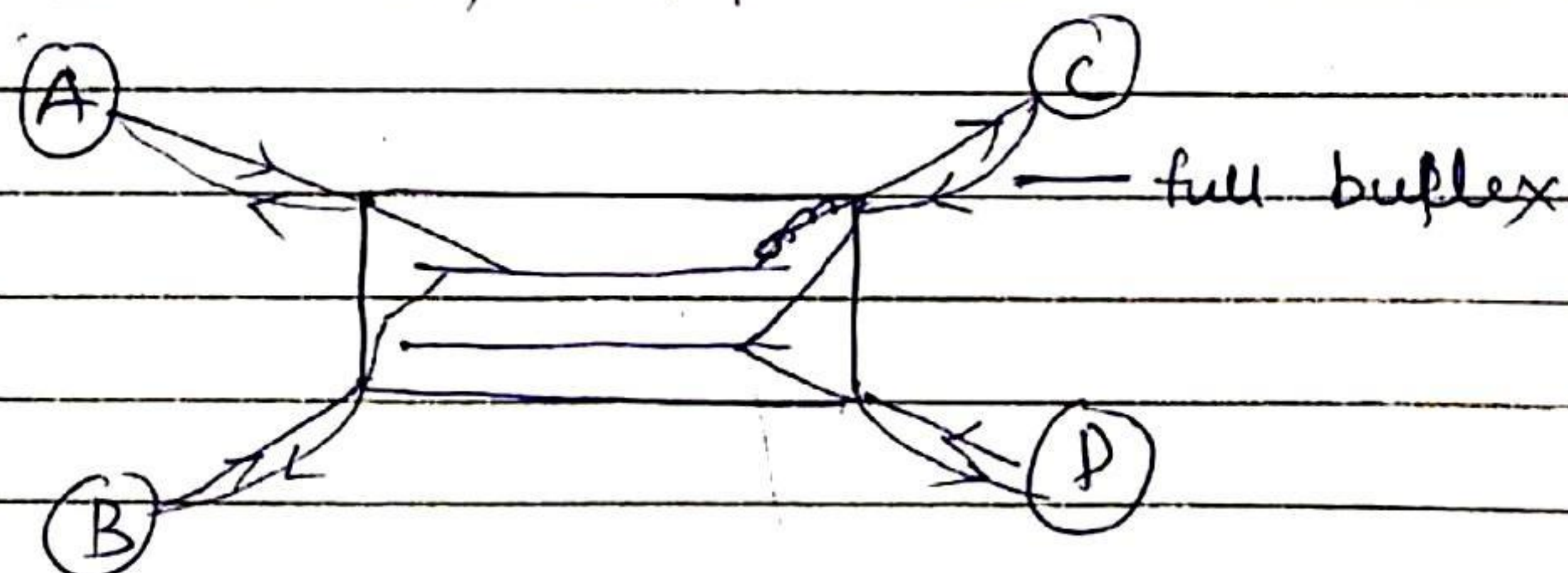


* → root port
** → designated port.

→ remove the connection where no $\neq$.

LAN 1

| B1 |          | B2 |

LAN 2          | B3 |          LAN 3

| B4 |          | B5 |

LAN 4

- SWITCH



host

Switch

8-port switch
16    "    "
32
64    "    "
128   "    "

① It can contain both PL & DLL.

(A)          (C) — full buplex

(B)          (D)

② No collision in switch.
   Collision Domain reduce to "0".

③ Mack address can be seen by switch.

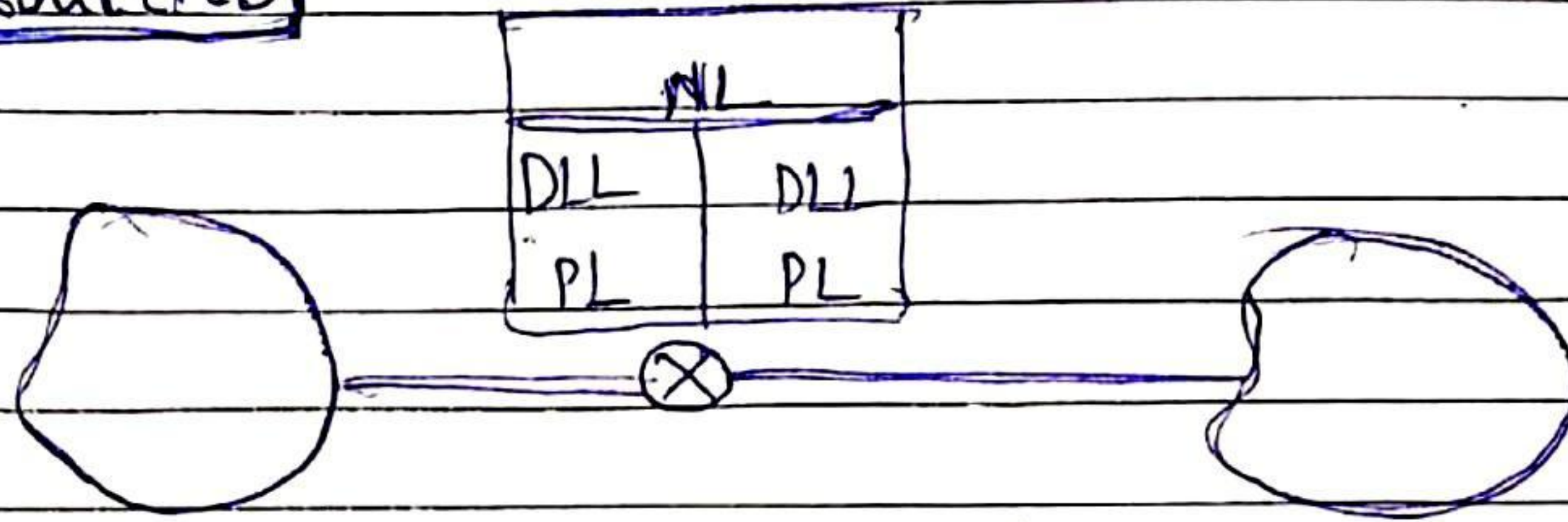④ Traffic is very very less. compare to h

dis adv:

→ Costly.

• Collision domain and broadcast domain of all devices —

( Wire + Hub + Repeater + Bridges + switches )
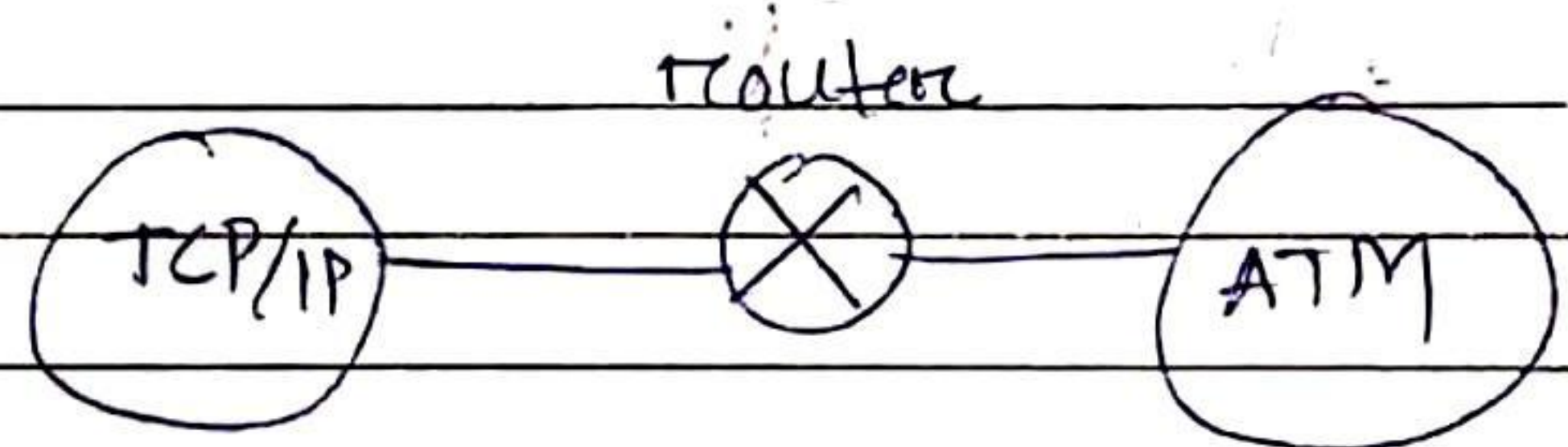
↳ called LAN component.

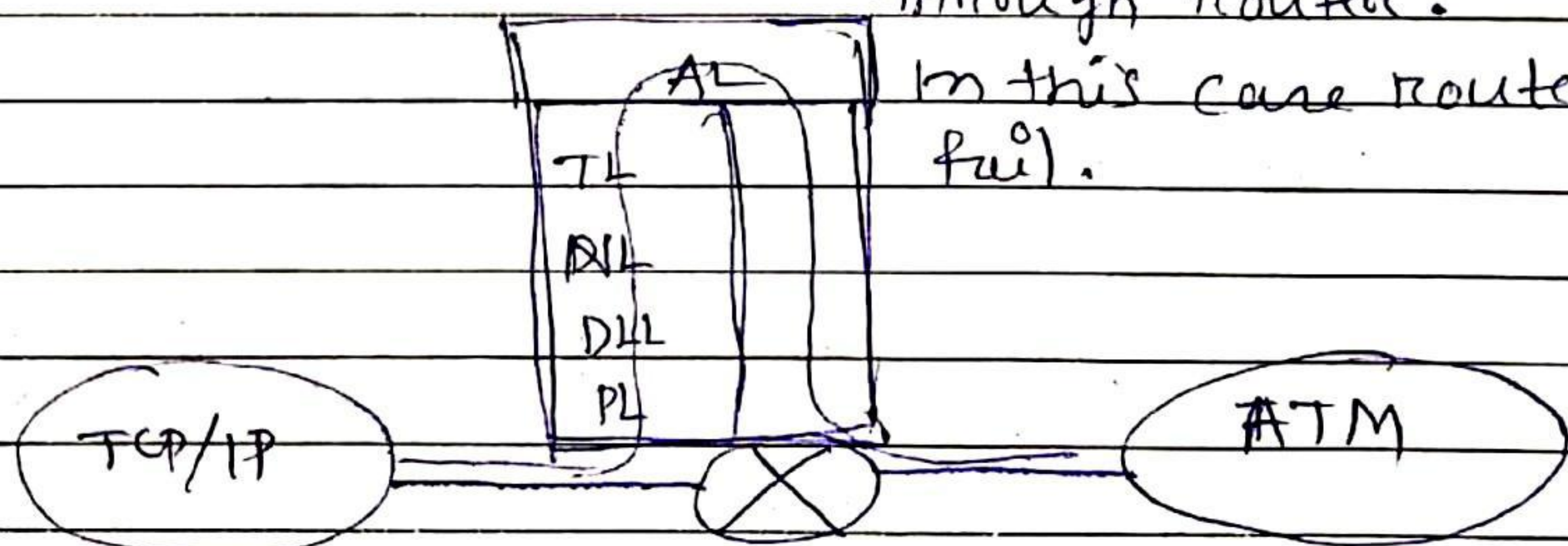| | Broadcast Domain | collision Domain |
|---|---|---|
| Repeater | Same | Same |
| Hub | same | same |
| Bridge | same | Reduces |
| Switch | same | Reduces (0) |
| Routers | reduces | Reduces |
| Getways | reduces | Reduces. |

- **Routers**



① It ε able to do filtering.
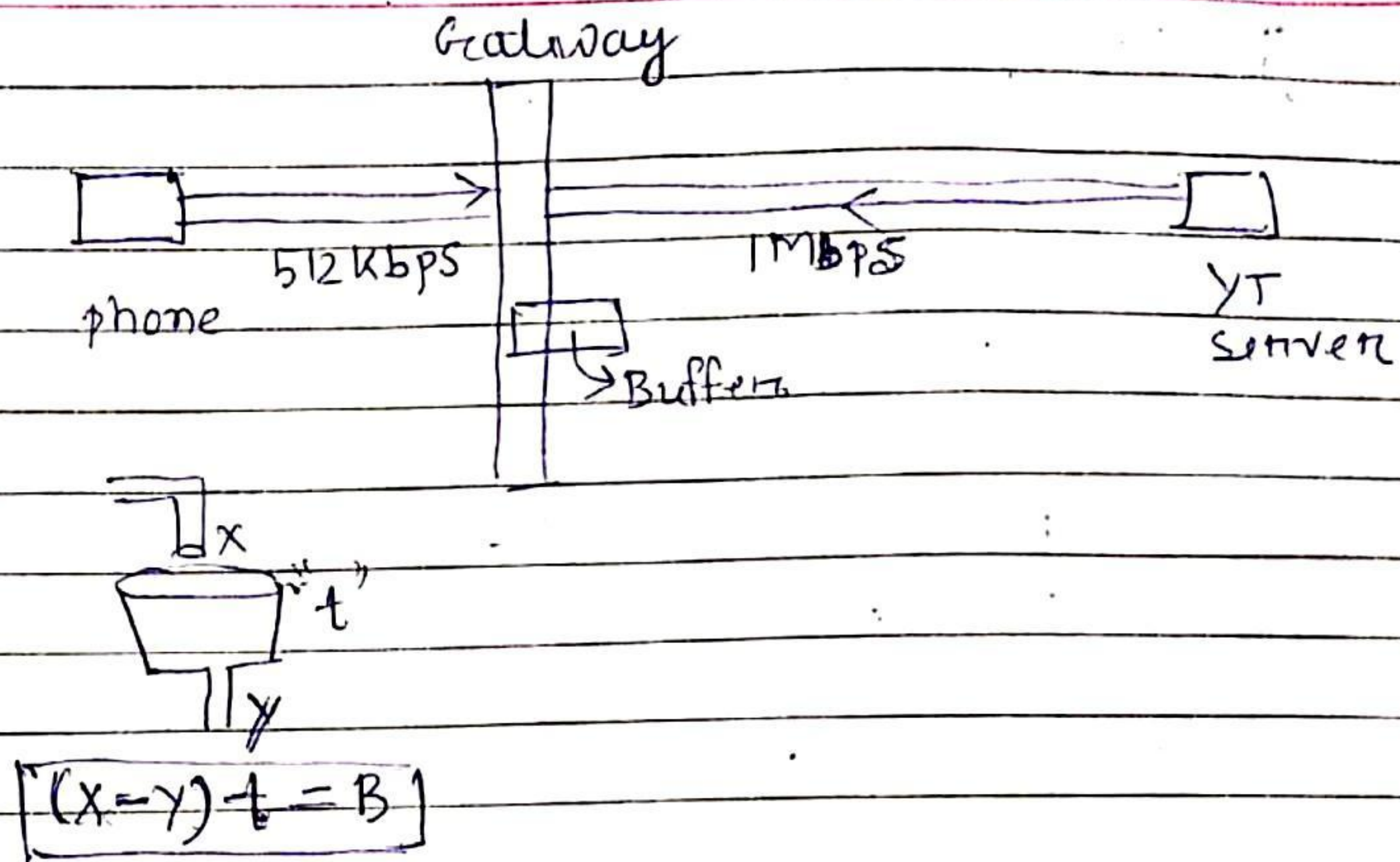② Forwarding.
③ Flloading
④ No collision.

- **Gateway**



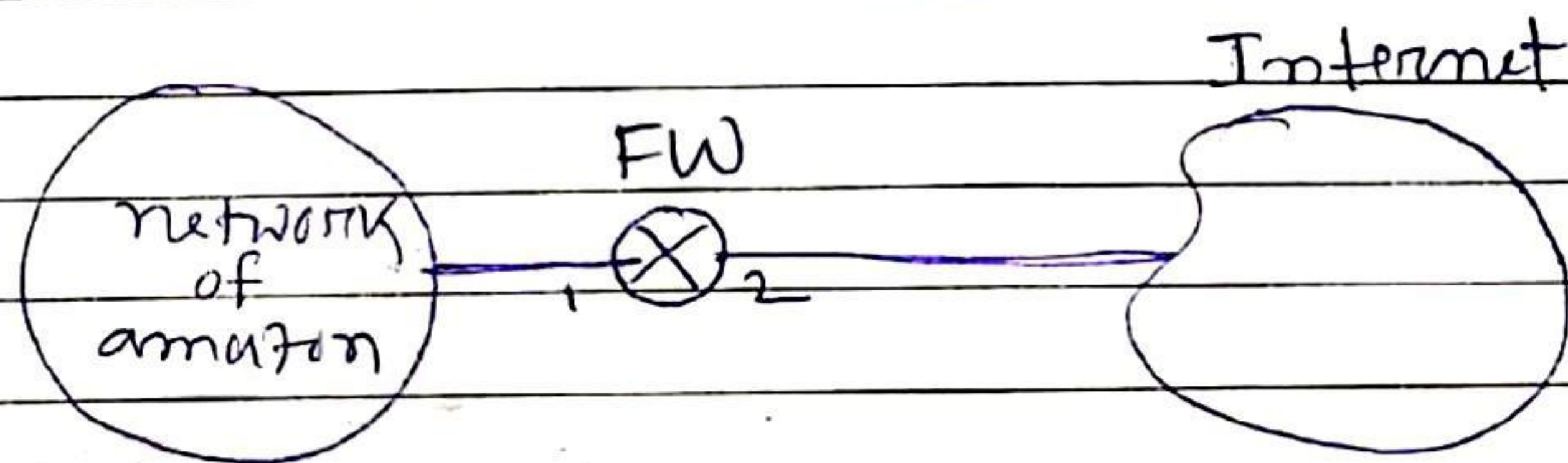→ two diff protocal connected through router.
In this case router fail.



applications of gateway - Gateway

① protocol converter.
② used for Proxy.   (as)
③ used as NAT server.
④ used as firewall.
⑤ ~~DPP (Deep packet~~
⑤ DPI (Deep packet inspection).

Gateway

phone    512Kbps        1Mbps      YT Server

→Buffer

x

"t"

y

$$(x-y)t = B$$

• **Firewalls** :

Internet

FW

network
of
amazon        ⊗
         1      2

Types of Firewall —

① Layer 3 FW or packet filtering FW.

② Layer 4 FW.

③ Layer 5 FW or proxy FW.

1. **Layer 3 FW:** (PL, DLL, NL)

   (1) SIP, DIP. (Block hosts)
   (2) protocol. (TCP, UDP, ICMP, IGMP)
                  (Block a protocol)
   (3) Block can block protocol from a particular host.

2. **Layer 4 FW:** (PL, DLL, NL, TL)

   (1) IP (Block host)

   (2) protocol (can Block a protocol)

   (3) Port (Block a service)
           (HTTP, SMTP, FTP)
   (4) Can Block a particular service on a particular host.

3. **Layer 5 FW:** (PL, DLL, NL, TL, AL)

   (1) IP (can block host)
   (2) ports (block services)
   (3) can block service on a host.
   (4) AL (username, password)
           (can block an user)