LAN Devices

Network Interface Card

- Also called Network Adapter
- Connects a host to a network medium
- Provides the physical interface between computer and cabling.
- It prepares data, sends data, and controls the flow of data. It can also receive and translate data into bytes for the CPU to understand.
- Contain unique MAC Address to control data communication
- Transceiver may be used to connect to mismatched media type

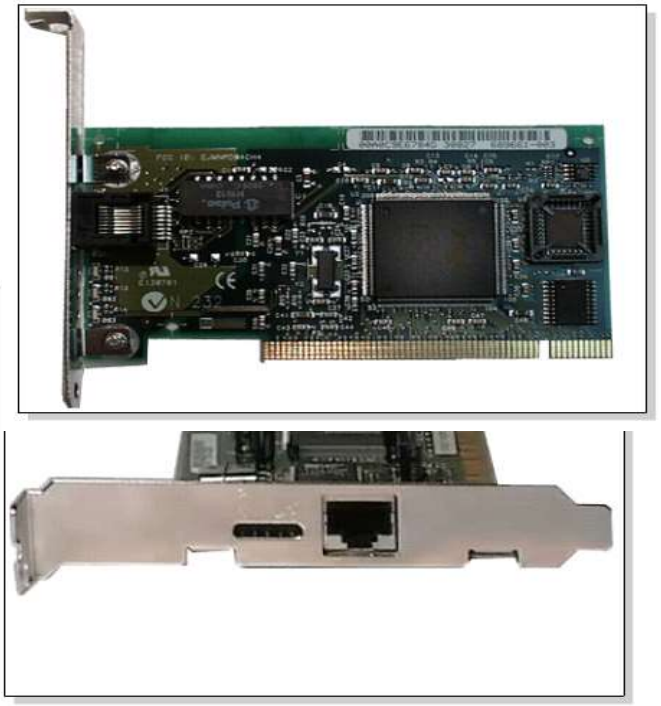
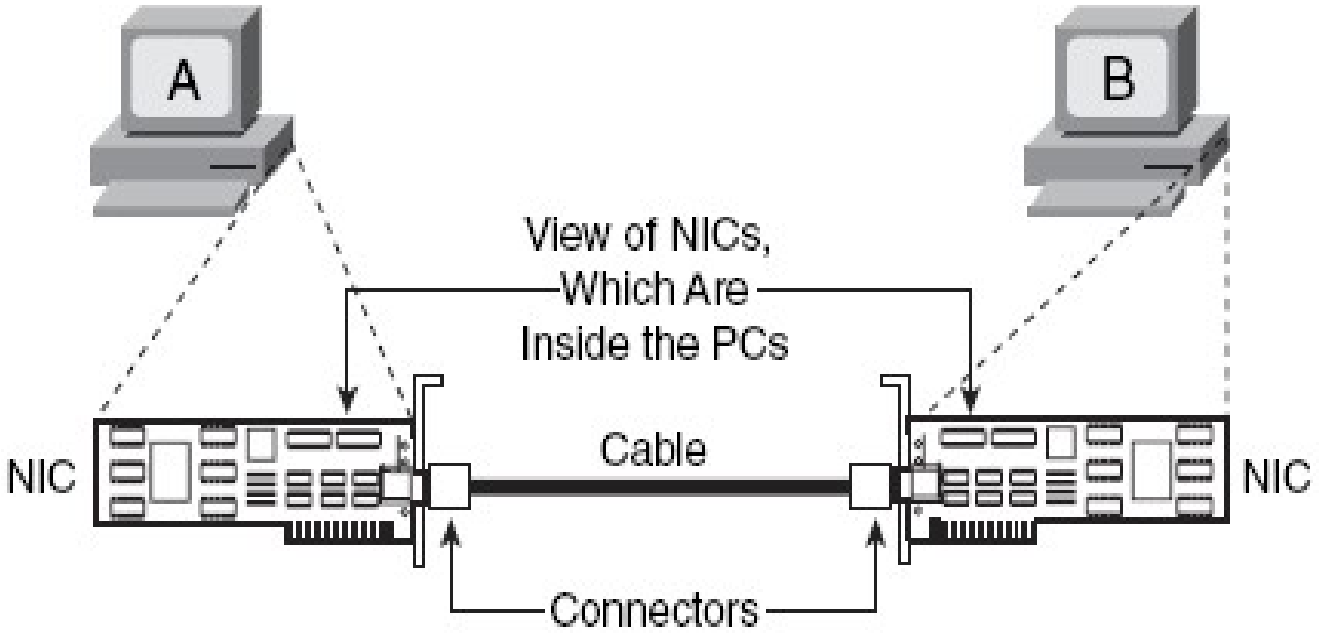
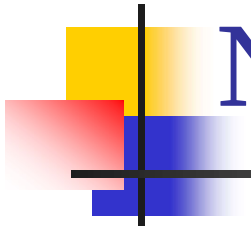


Figure ' Connecting the Copper Conductors in a Cable to the NICs





Network Devices

IEEE committee identified the following possible internetworking scenarios.

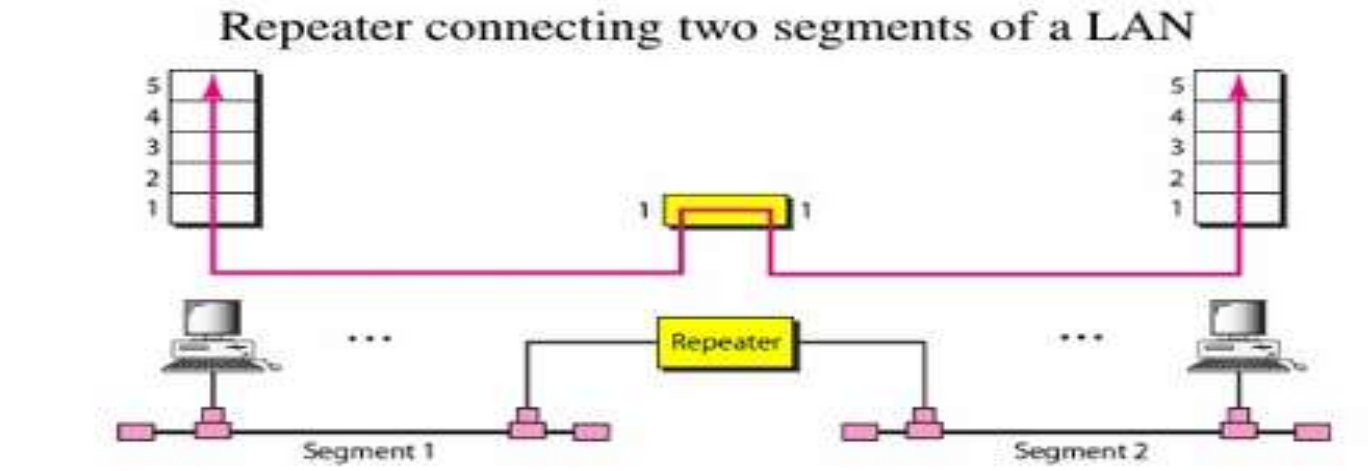
- A single LAN
- Two LANs connected together (LAN-LAN)
- A LAN connected to a WAN (LAN-WAN)
- Two LANs connected through a WAN (LAN-WAN-LAN)

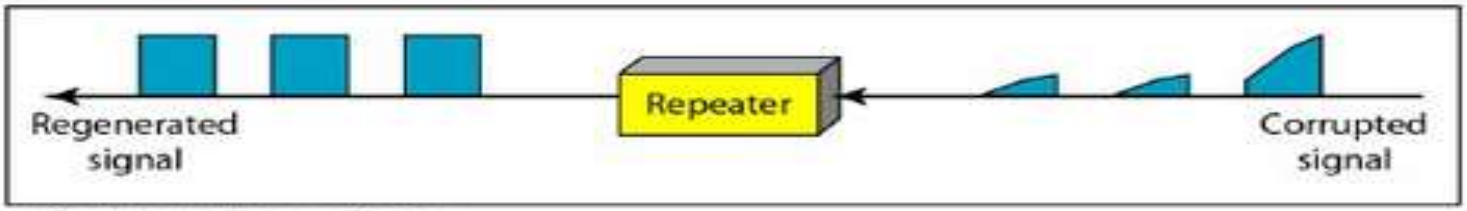
Various internetworking devices such as repeaters, hubs, bridges, switches, routers and gateways are required to link them together.

Repeaters

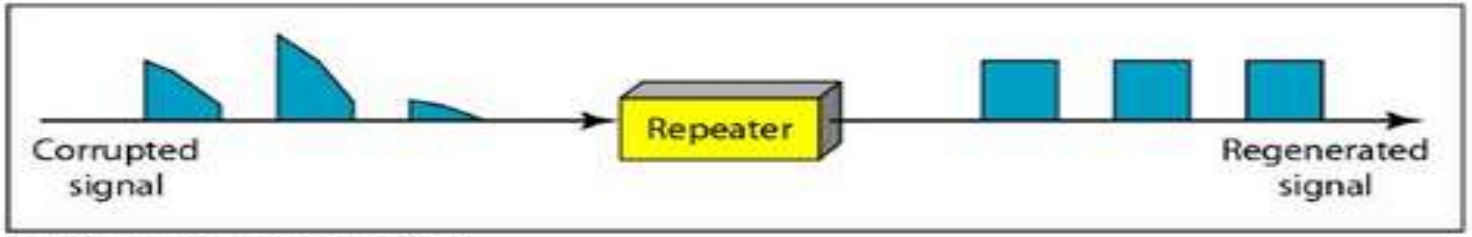
- Repeater is a powerful network device which is used to increase the length of the network by eliminating the effect of attenuation on the signal.
- A single Ethernet segment can have a maximum length of 500 meters with a maximum of 100 stations. To extend the length of the network, a repeater may be used
- The purpose of the Ethernet repeater is to carry signal from one Ethernet cable and take it to the other cable without attenuation or loss of signal strength.
- A repeater exists as the first layer of the OSI layer that is physical layer.
- Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay.

Repeaters





a. Right-to-left transmission.

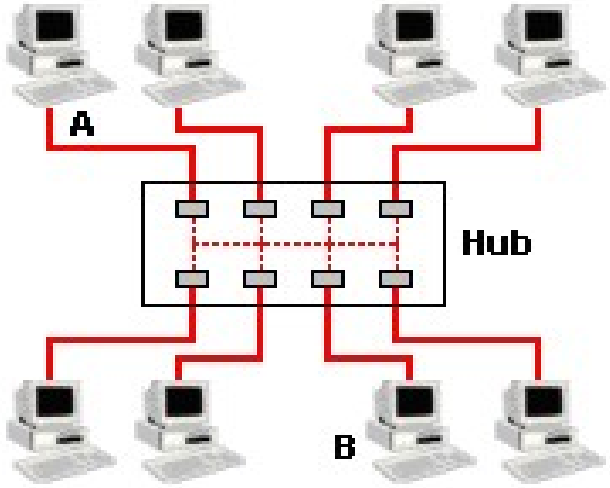


b. Left-to-right transmission.

Function of a repeater

Hub

- Multi-port repeaters with 4 to 24 ports (typical repeater usually has 2 ports)
- It repeats what it receives on one port to all other ports, including the port on which the signal was received, so that the transmitting device may monitor and recover from collisions.
- Converts the network to Star topology
- Commonly used in 10Base-T and 100Base-T networks



Hub Types

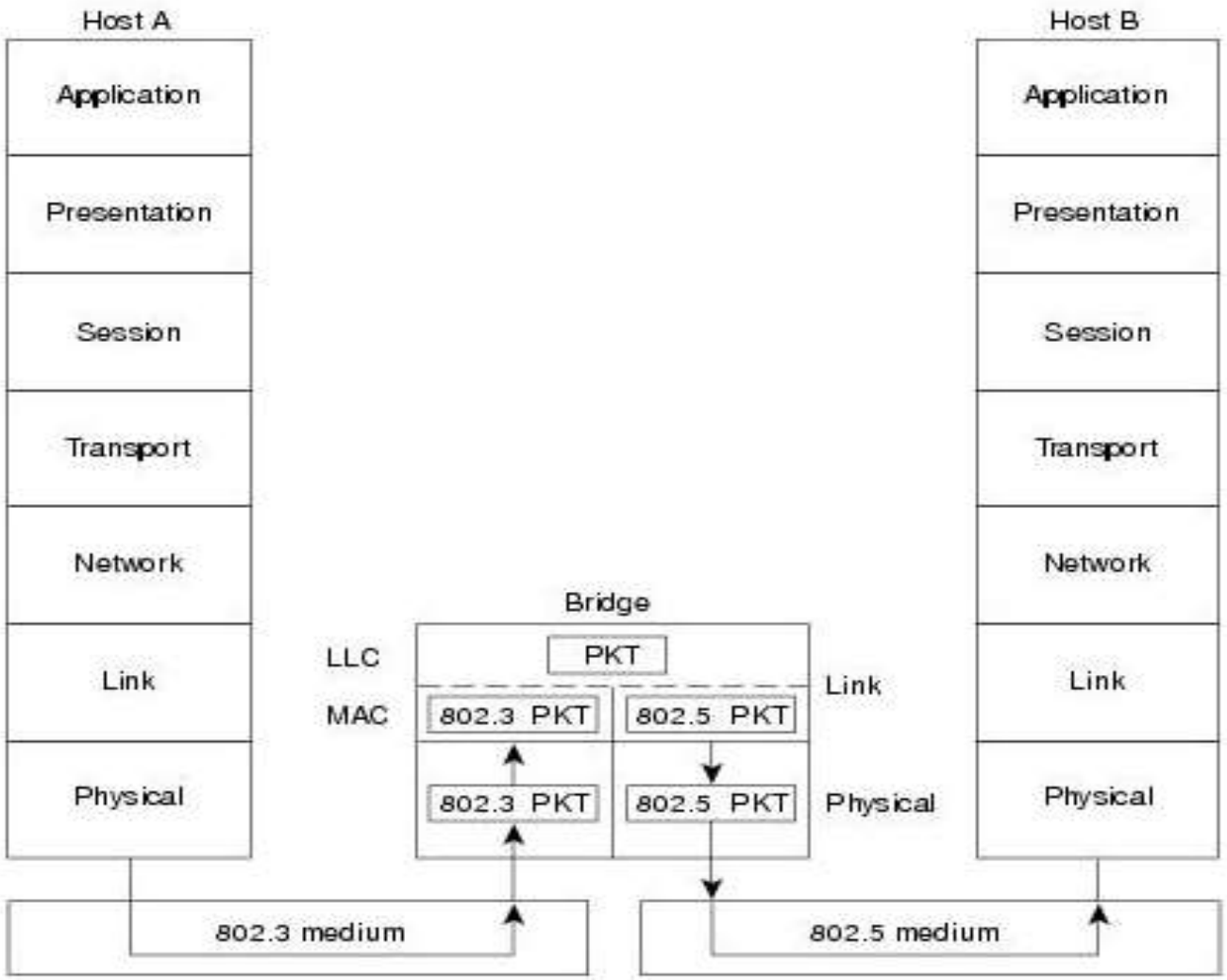
- Passive
  - Serves as a physical connection point only
  - Does not manipulate or view the traffic
  - Does not boost or clean the signal.
  - Used only to share the physical media
  - Does not need electrical power
- Active
  - Needs electrical power to amplify signal
- Intelligent Hub /Smart Hub
  - Contain Microprocessor chips and diagnostic capabilities
  - Enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.
  - Expensive

Bridges

- The device that can be used to interconnect two separate LANs is known as a bridge.
- It is commonly used to connect two similar or dissimilar LANs.
- Operates in both the PHYSICAL and the data link layer.
- As a PHYSICAL layer device, it regenerates the signal it receives.
- As a data link layer device, the bridge can check the PHYSICAL/MAC addresses (source and destination) contained in the frame.

Translational Bridges

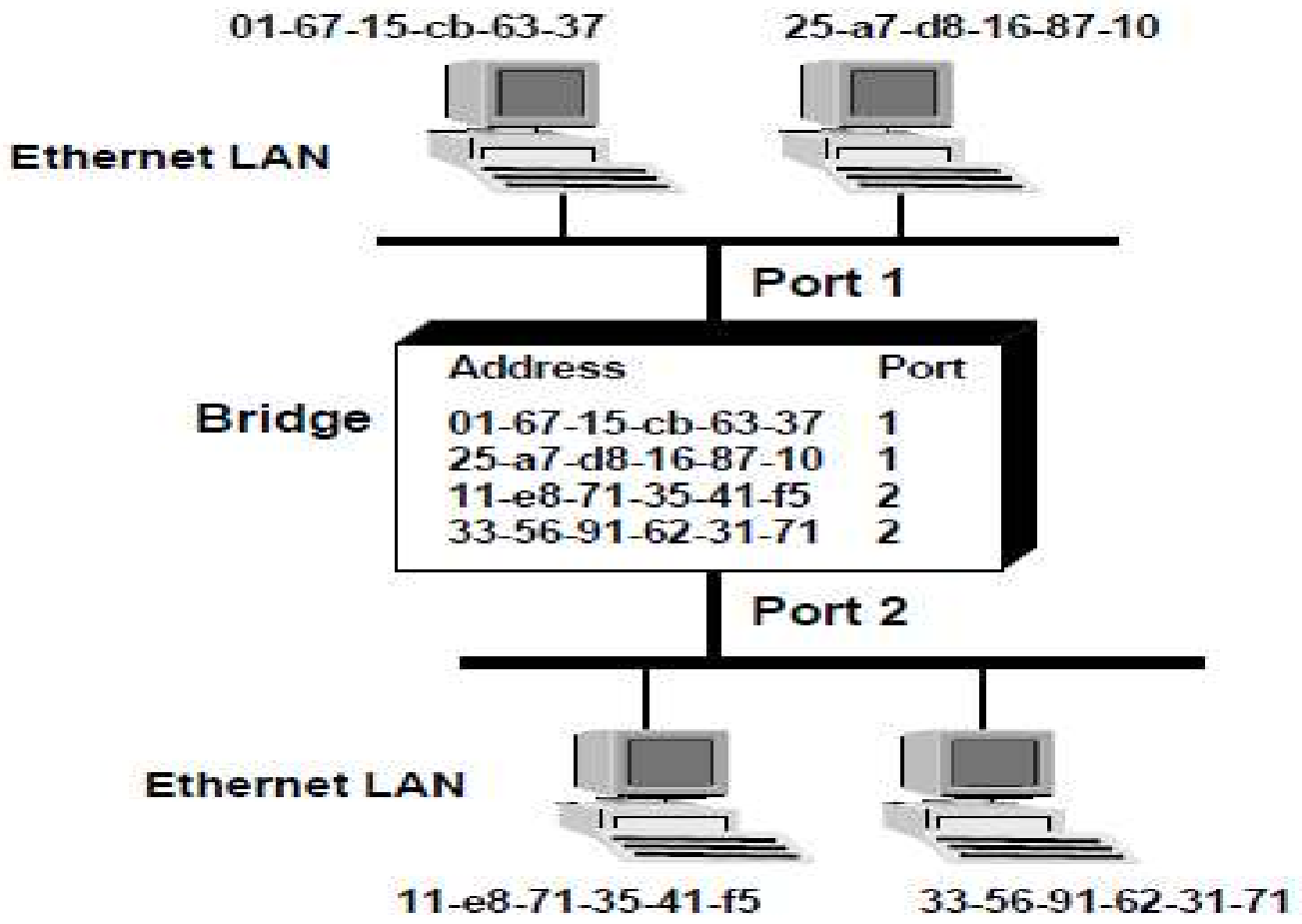
Figure: A MAC-Layer Bridge Connects the IEEE 802.3 and IEEE 802.5 Networks



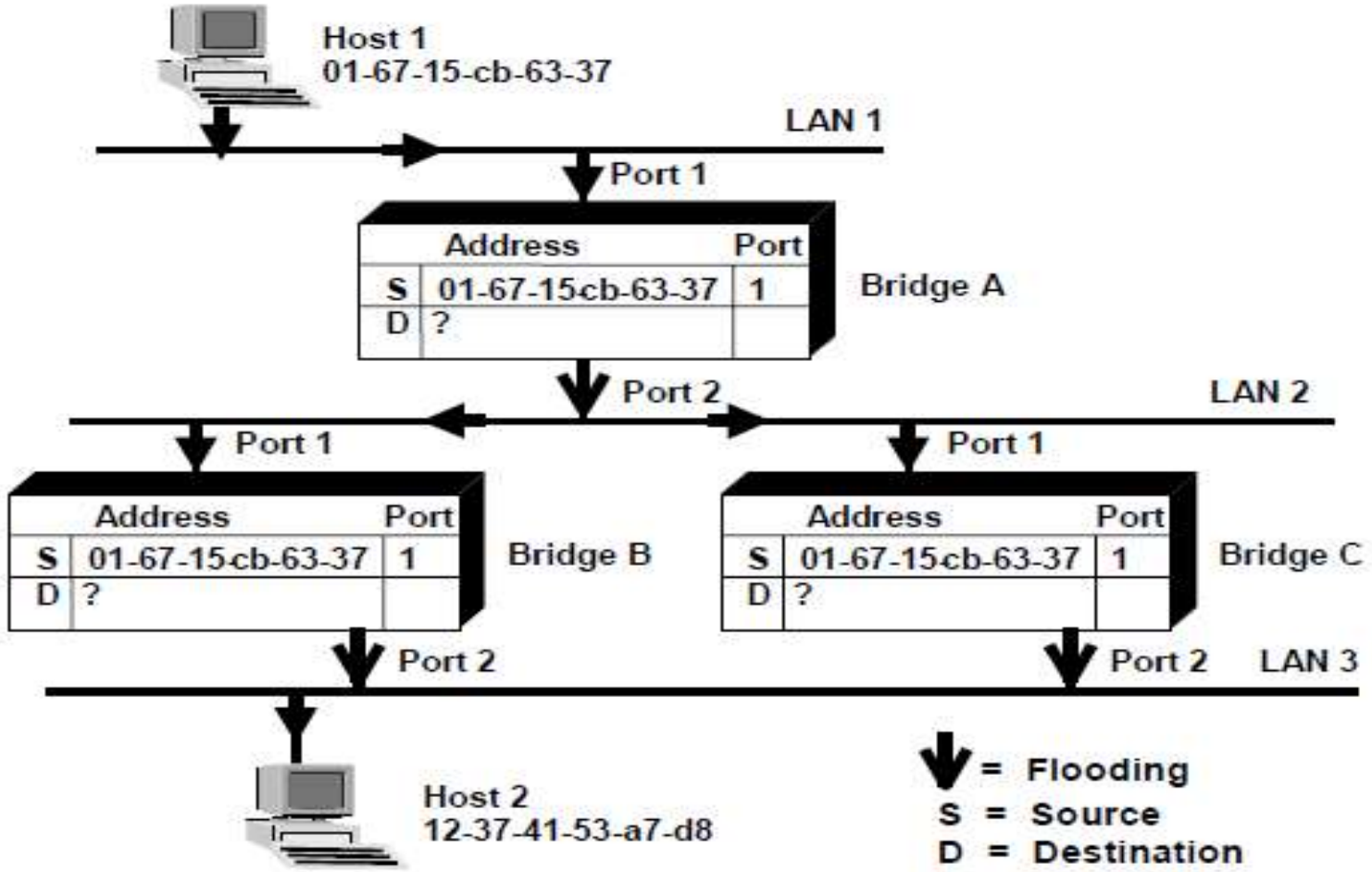
How Bridges Work?

- A bridge has a table used in filtering decisions.
- It can check the destination address of a frame and decide if the frame should be forwarded or dropped.
- If the frame is to be forwarded, the decision must specify the port.
- A bridge has a table that maps address to ports.
- Bridges have three basic functions:
  - Forwarding a frame from one segment to another across the bridge.
  - Filtering a frame that does not need to cross the bridge to reach its destination.
  - Flooding a frame to all ports when the location of the destination address is unknown.
- Increases network performance

Transparent Learning Bridges Build Forwarding Tables

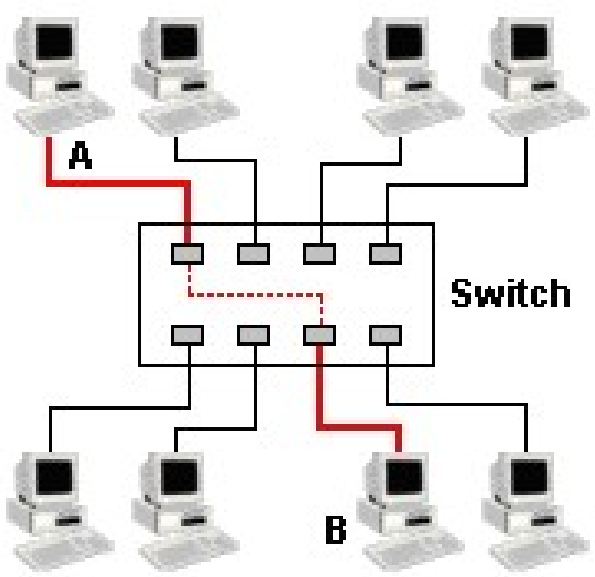


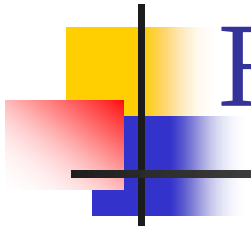
The Frame is Flooded Across the Network



Switches

- Sometimes called multi-port bridge
- A switch is essentially a fast bridge having additional sophistication that allows faster processing of frames.
- Improves congestion and reduce traffic





Functions of Switch

- Some of important functionalities are:
  - Ports are provided with buffer
  - Switch maintains a directory: #address - port#
  - Each frame is forwarded after examining the #address and forwarded to the proper port#
  - Three possible forwarding approaches: Cut-through, Collision-free and Fully-buffered.

Functions of Switch

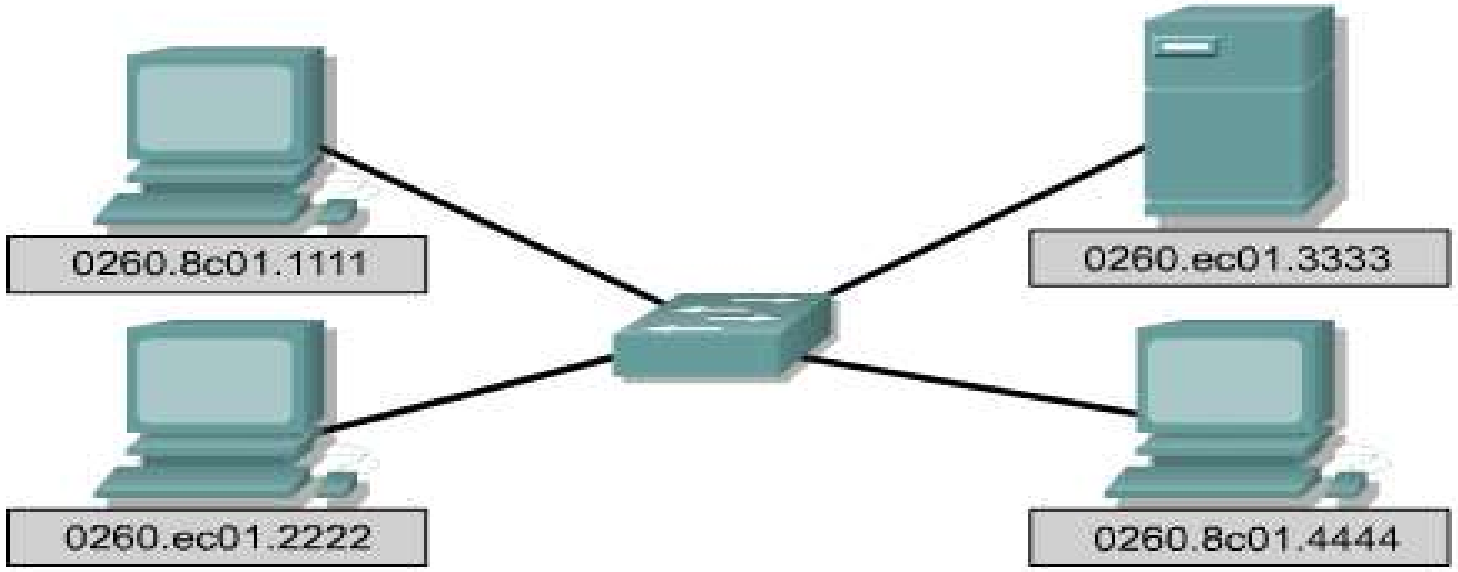
- **Cut-through:** A switch forwards a frame immediately after receiving the destination address. As a consequence, the switch forwards the frame without collision and error detection.

- **Collision-free:** In this case, the switch forwards the frame after receiving 64 bytes, which allows detection of collision. However, error detection is not possible because switch is yet to receive the entire frame.

- **Fully buffered:** In this case, the switch forwards the frame only after receiving the entire frame. So, the switch can detect both collision and error free frames are forwarded.

Switching Table

Interface	MAC Address
E0	0260.8c01.1111
E1	0260.ec01.2222
E2	0260.ec01.3333
E3	0260.8c01.4444

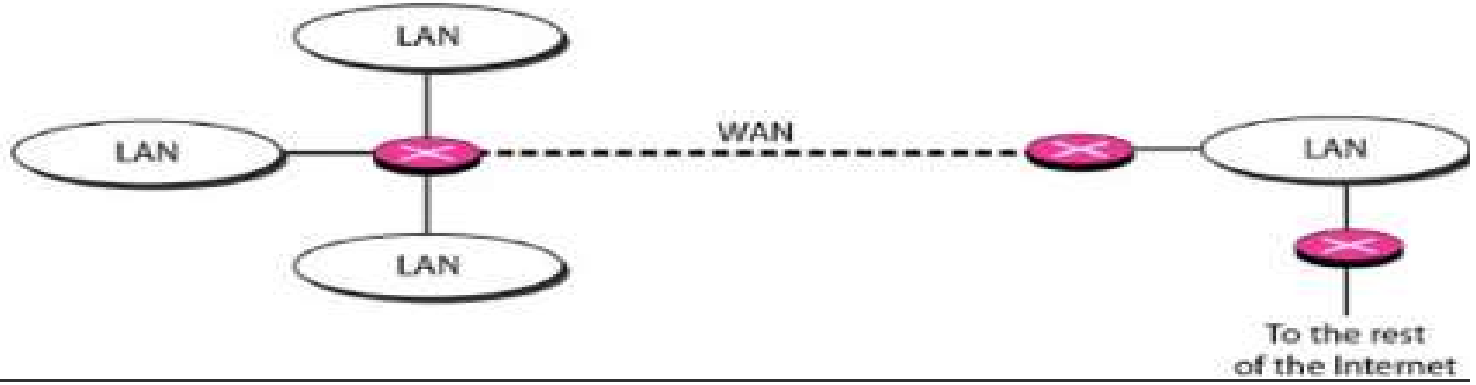


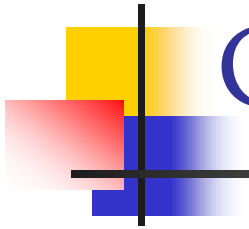
Advantages of Switch

- Switches operate at much higher speeds than bridges
- Can support new functionality, such as Virtual LANs.
- Allows multiple users to communicate at the same time through Virtual circuits and dedicated network segments
- Crates Virtually Collision free environment
- Improves network speed, bandwidth and performance
- Very cost effective since the hardware and cables in place can be reused

Router

- Also called 3-layer switches
- Routes packets based on their logical addresses (host-to-host addressing) .
- A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decision about the route.
- The routing tables are normally dynamic and are updated using routing protocols.





Components of Router

- A router has four basic components:
  - **Input port** performs physical and data-link layer functions of the router. Ports are also provided with buffer to hold the packet before forwarding to the switching fabric.
  - **Output ports** perform the same functions as the input ports, but in the reverse order.
  - **The routing processor** performs the function of the network layer. The process involves table lookup.
  - **The switching fabric** moves the packet from the input queue to the output queue by using specialized mechanisms. The switching fabric is realized with the help of multistage interconnection networks.

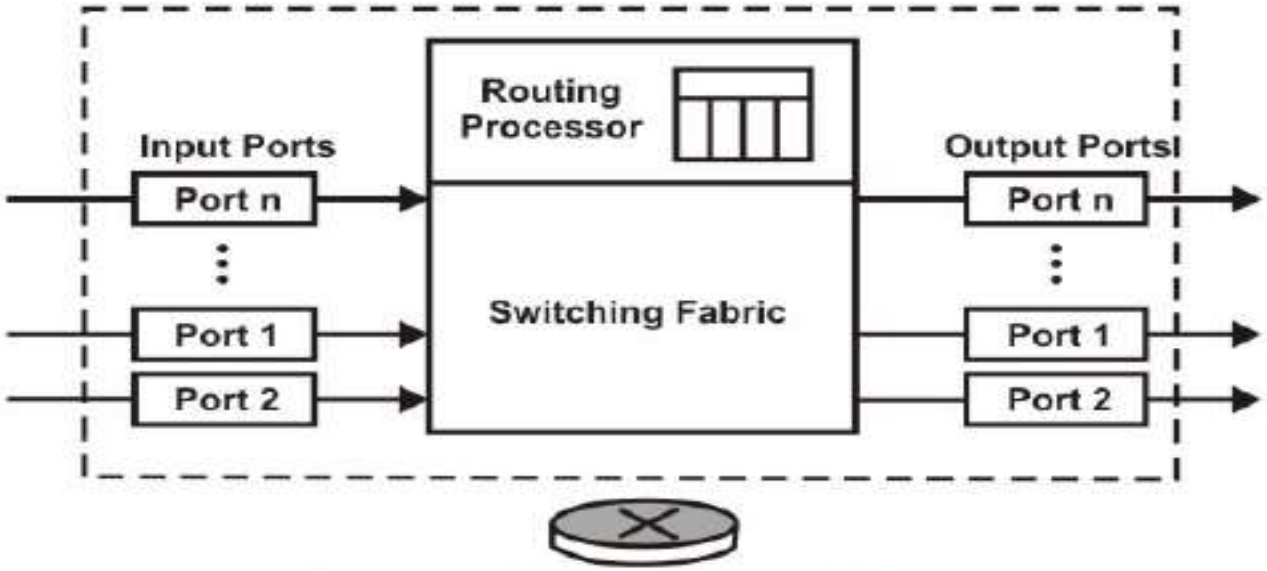
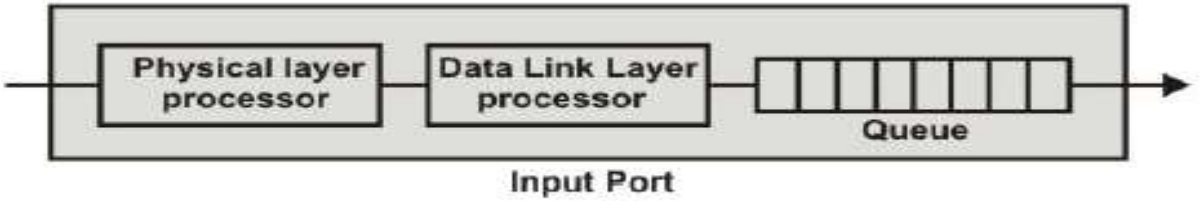
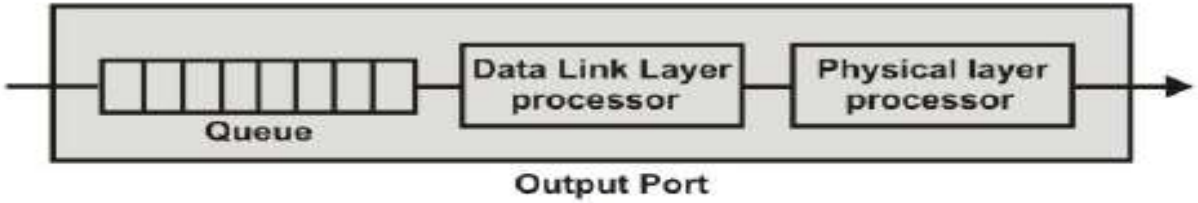


Figure Schematic diagram of a router



(a)



(b)

Figure Schematic diagram of a router

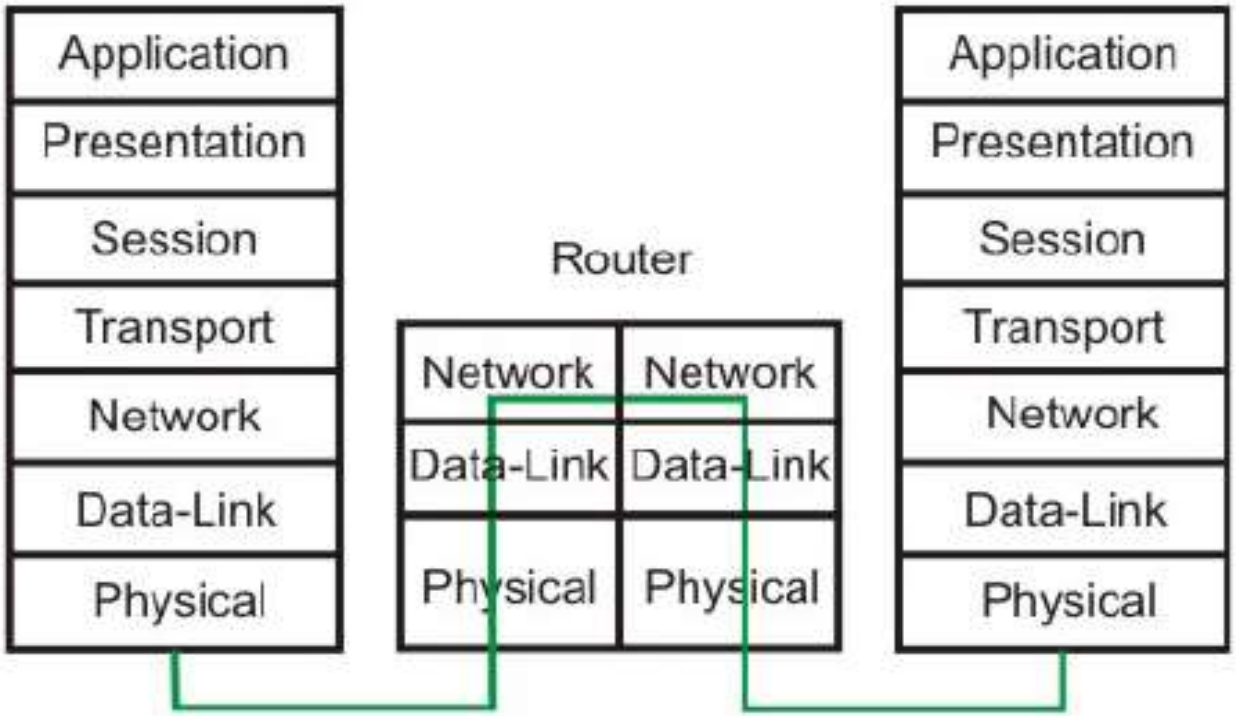


Figure Communication through a router

Gateway

- A gateway is a hardware device that acts as a "gate" between two networks.
- It may be a router, firewall, server, or other device that enables traffic to flow in and out of the network.
- A router is a common type of gateway used in home networks. It allows computers within the local network to send and receive data over the Internet.
- A firewall is a more advanced type of gateway, which filters inbound and outbound traffic, disallowing incoming data from suspicious or unauthorized sources.
- A proxy server is another type of gateway that uses a combination of hardware and software to filter traffic between two networks. For example, a proxy server may only allow local computers to access a list of authorized websites.
- Gateways can operate at all layers of the OSI model

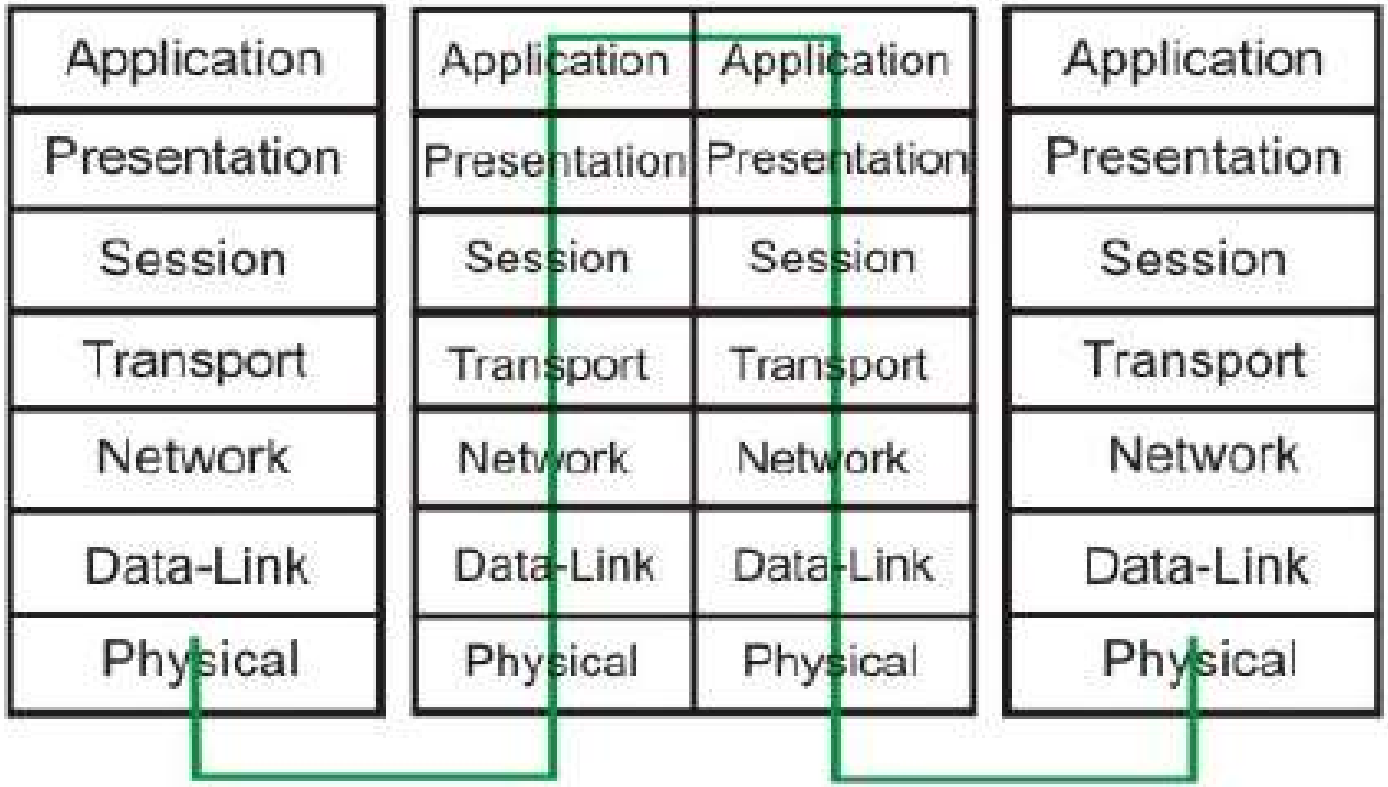
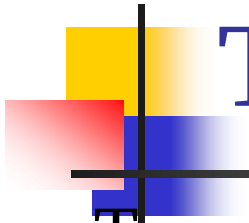


Figure Communication through a gateway

Ping

- A ping is perhaps the most commonly used tool when troubleshooting a network.
- Ping (Packet Internet Groper) tool is included with most operating systems. It is invoked using a ping command.
- Ping command uses ICMP (Internet Control Message Protocol).
- Ping works by sending an ICMP echo request message to the specified IP address.
- If the computer with the destination IP address is reachable, it responds with an ICMP echo reply message.



Traceroute

- Traceroute is a CLI (Command-line interface)-based tool used to identify the path used by a packet to reach its target.
- This tool also uses ICMP messages, but unlike ping, identifies every router in a path.
- Traceroute is useful when troubleshooting network problems because it can help identify where exactly the problem is.
- The traceroute command on Windows is named *tracert*.

IP Address and Host Name

IP Address (Internet Protocol address):

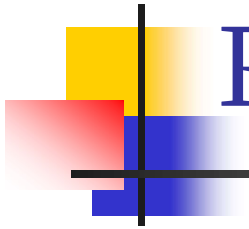
- Also know as Logical Address, is the network address of the system across the network.
- To identify each device in the world-wide web, Internet Assigned Numbers Authority (IANA) assigns IPV4 (Version 4) address as unique identifier for each device on the Internet.
- Length of the IP address is : 32-bits. (Hence we have 2^{32} ip addresses available.)
- Commands: C:\>ipconfig

Host Name:

- Each device in the network is associated with a unique device name known as Hostname.
- Commands: C:\Windows\System32>hostname

MAC Address

- **MAC Address (Media Access Control address):**
- Also known as physical address, is the unique identifier of each host and is associated with the NIC (Network Interface Card).
- MAC address is assigned to the NIC at the time of manufacturing. Length of the MAC address is : 12-digit/ 6 bytes/ 48 bits.
- **ARP (Address Resolution Protocol)** is used to convert the IP address to its corresponding MAC Address.
- ARP is used by the Data Link Layer to identify the MAC address of the Receiver's machine.
- C:\>arp –a is used to discover what machines are directly connected to the host.



Port

- Port can be referred as logical channel through which data can be sent/received to an application.
- Any host may have multiple applications running, and each of this application is identified using the port number on which they are running on.
- Port number is a 16-bit integer; hence we have 2^{16} ports available which are categorized as shown below:

PORT TYPES	RANGE
Well known Ports	0 – 1023
Registered Ports	1024 – 49151
Ephemeral (Temporary) Ports	49152 – 65535

- Command to see active port C:\>netstat –a
- The unique combination of IP address and Port number together are termed as Socket

DNS Server

- DNS (**Domain Name system**) is basically a server which translate web addresses or URL (ex: www.google.com) into their corresponding IP addresses.
- The command '**nslookup**' gives the IP address of the domain you are looking for. This also provides the information of our DNS Server.
- Command: C:\Windows\System32>nslookup www.google.com