NETWORK COMPONENTS

Network Adapters

- Also called network interface cards (NICs)
- Connectivity devices enabling a workstation, server, printer, or other node to receive and transmit data over the network media
- In most modern network devices, network adapters contain the data transceiver

Types of Network Adapters

- For a desktop or Power PC, network adapter is likely to be a type of **expansion board**
  - Expansion boards connect to the system board through **expansion slots**
- The circuit used by the system board to transmit data to the computer's components is the computer's **bus**

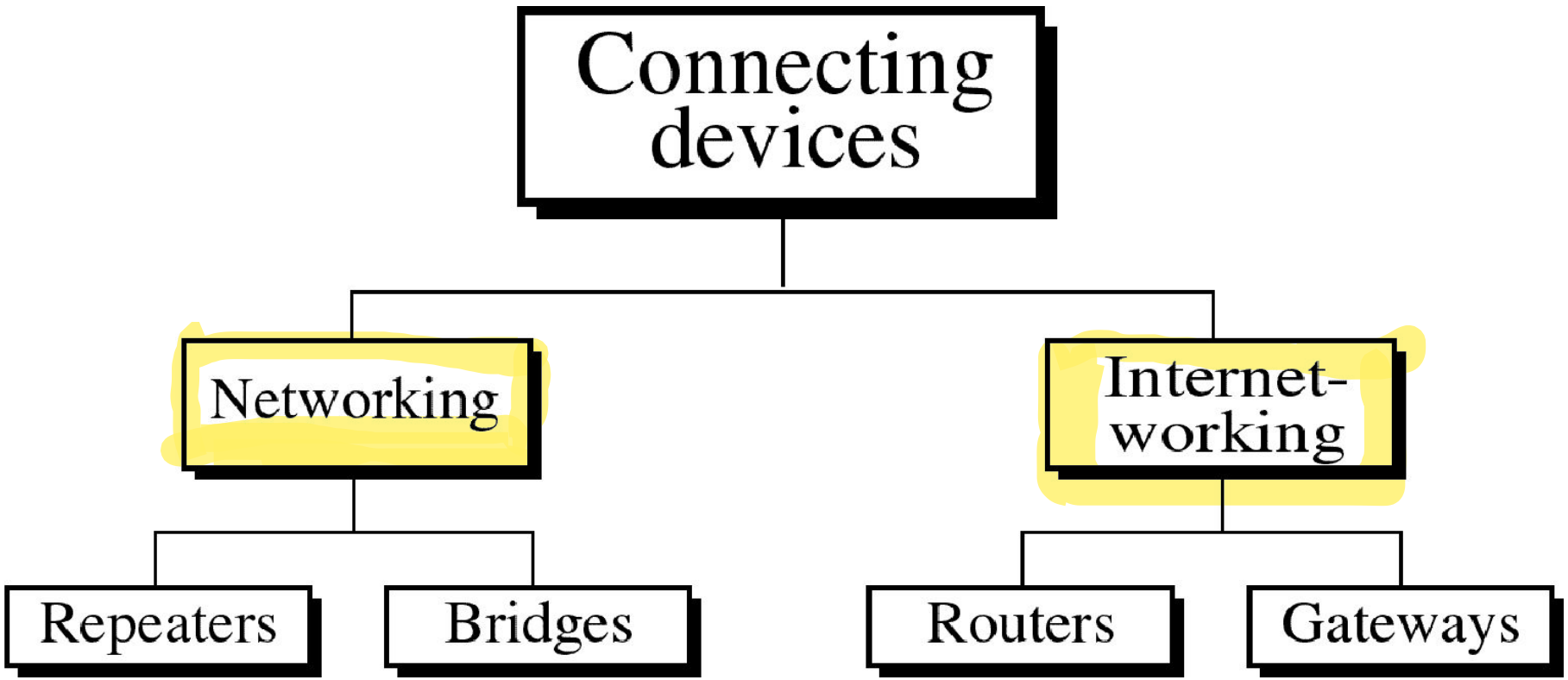
Types of Network Adapters

- PCMIA (Personal Computer Memory Card International Association)
  - Developed in early 1990s to provide standard interface for connecting any type of device to a portable computer
  - More commonly known as **PC Cards**
- USB (Universal Serial Bus) port
  - Standard external bus that can be used to connect multiple types of peripherals
- A parallel port network adapter
- Wireless network adapters
- A variety of Ethernet network adapters

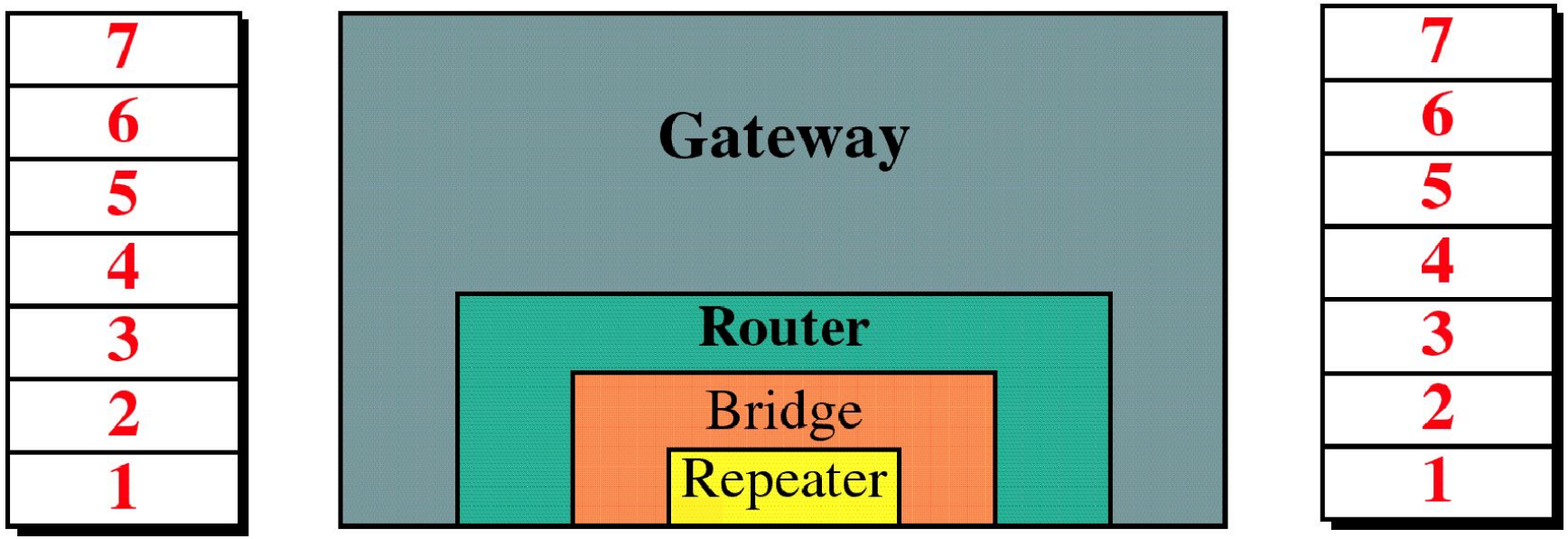
Modem : A modem is a computer peripherals that allows you to connects and communicate with other computers via telephone lines.

Modem comes in two varieties:

1. Internal Modem: The modem which is fixed inside the computer.
2. External Modem: This modem is connected externally to a computer.


Connecting devices
Networking
Internet-working
Repeaters
Bridges
Routers
Gateways

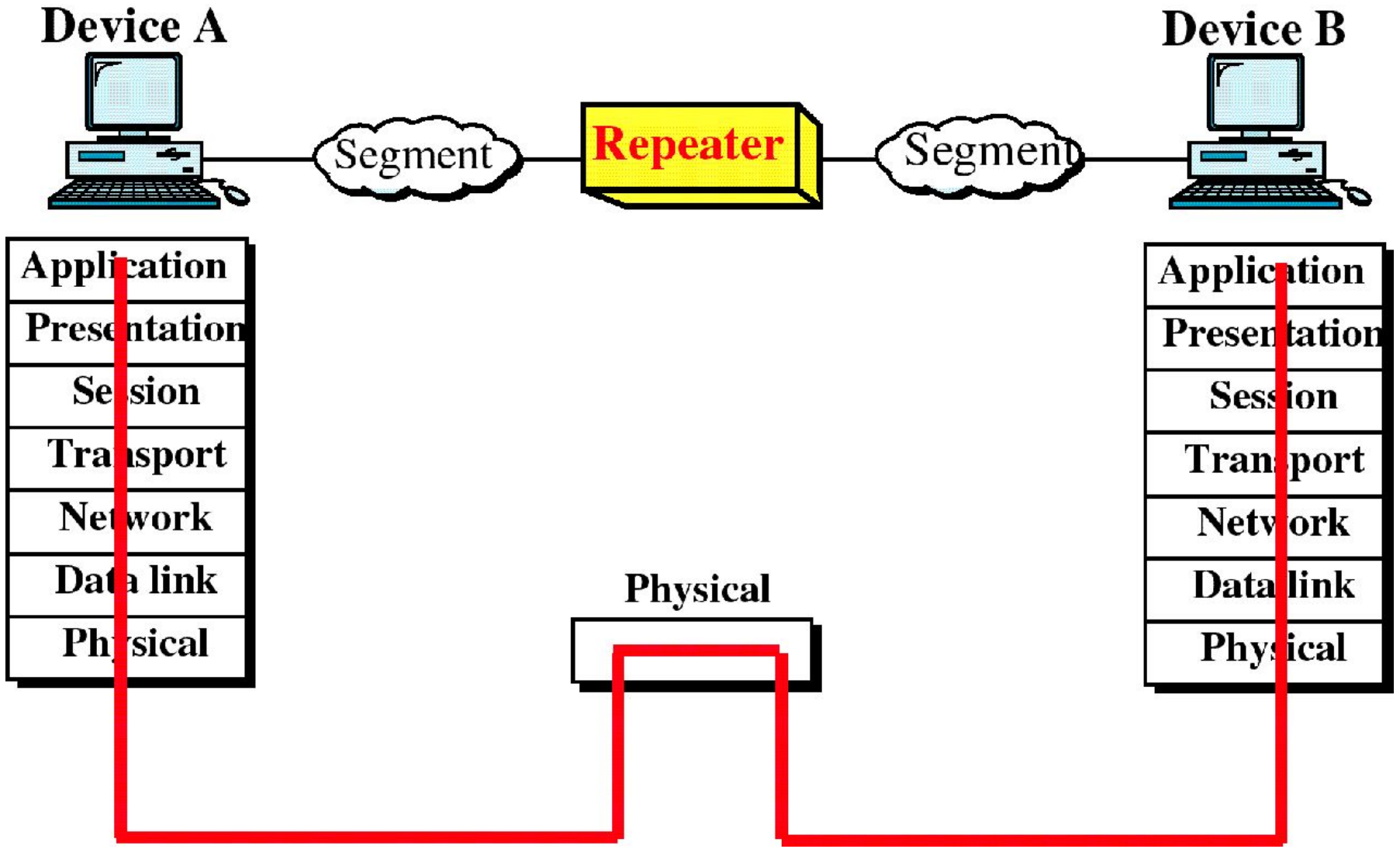
Connecting Devices and the OSI Model



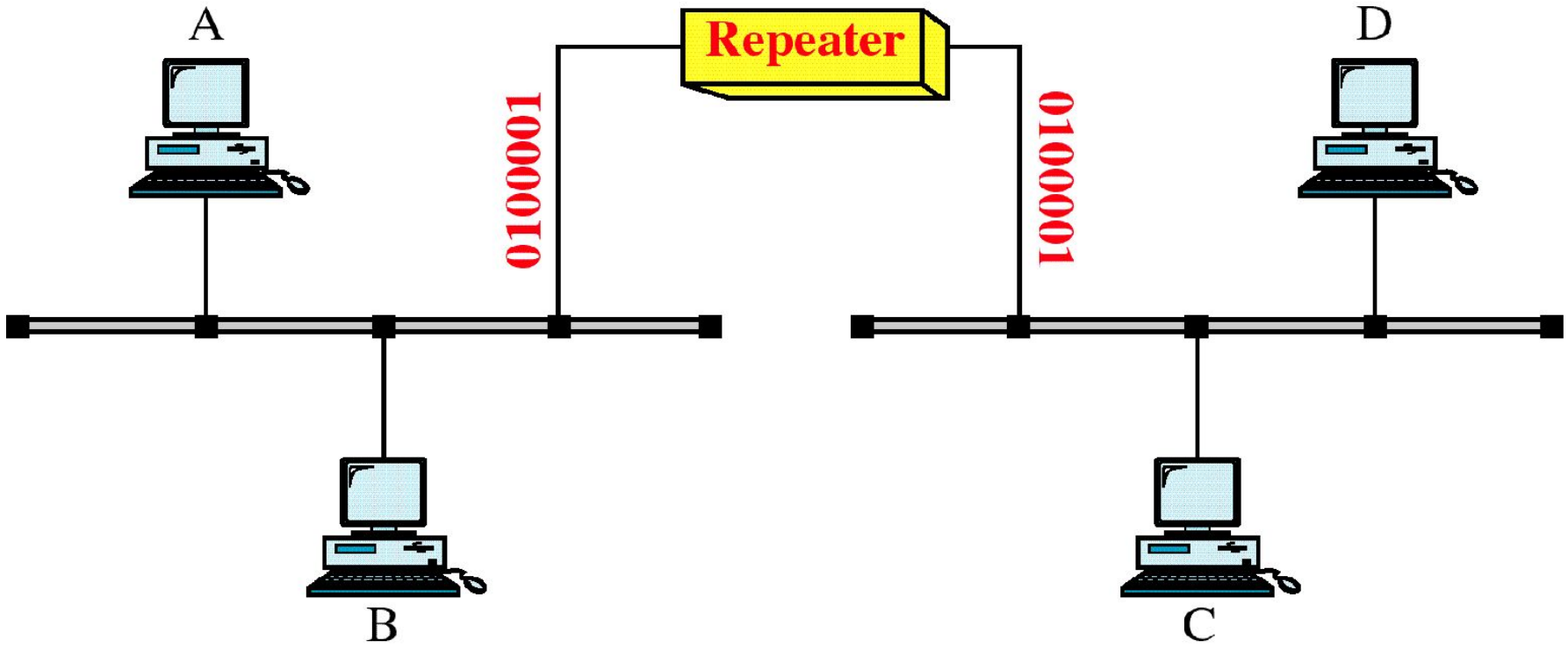
Repeaters

- Connectivity devices that regenerate and amplify an analog or digital signal

Repeater and OSI Model



A Repeater



Function of a Repeater

(a) Right-to-left transmission.

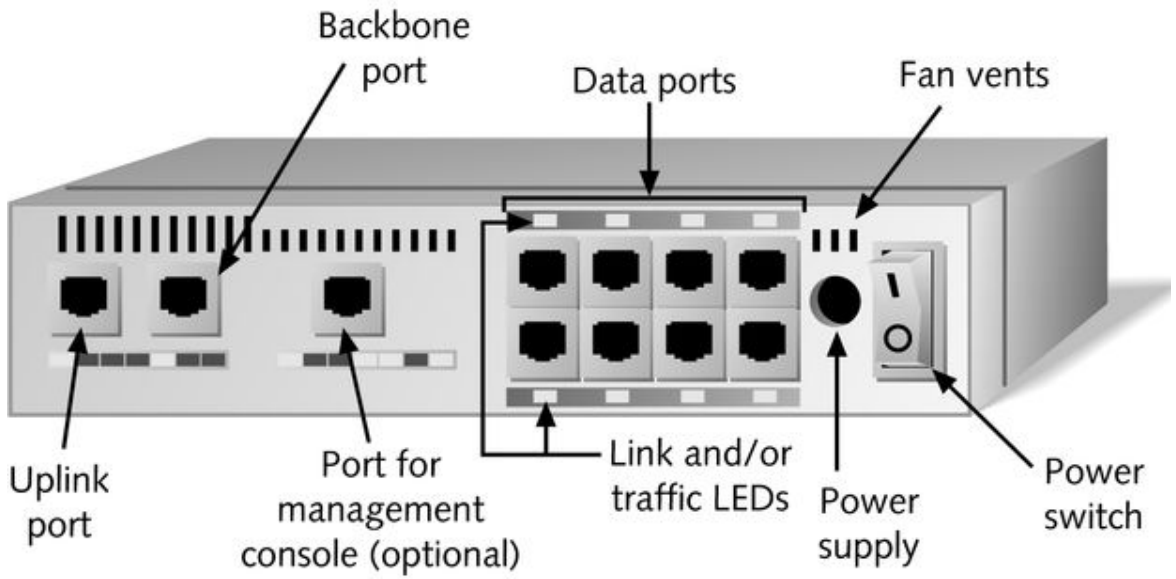
(b) Left-to-right transmission.

Repeaters

- Traditionally, any discussion of networking components would include repeaters, but today repeaters are a little outdated.
- Repeaters were once used to increase the usable length of the cable, and they were most commonly associated with coaxial network configurations.
- Because coaxial networks have now fallen out of favor, and because the functionality of repeaters has been built in to other devices, such as hubs and switches, repeaters are rarely used.

Hubs

- Multiport repeater containing multiple ports to interconnect multiple devices



- *Hubs* are simple network devices, and their simplicity is reflected in their low cost
- Computers connect to a hub via a length of twisted-pair cabling.
- In addition to ports for connecting computers, even an inexpensive hub generally has a port designated as an uplink port that enables the hub to be connected to another hub to create larger networks.

Most hubs are referred to as either active or passive.

- *Active* regenerate a signal before forwarding it to all the ports on the device and requires a power supply. Small workgroup hubs normally use an external power adapter, but on larger units the power supply is built in.
- *Passive* hubs, which today are seen only on older networks, do not need power and they don't regenerate the data signal.

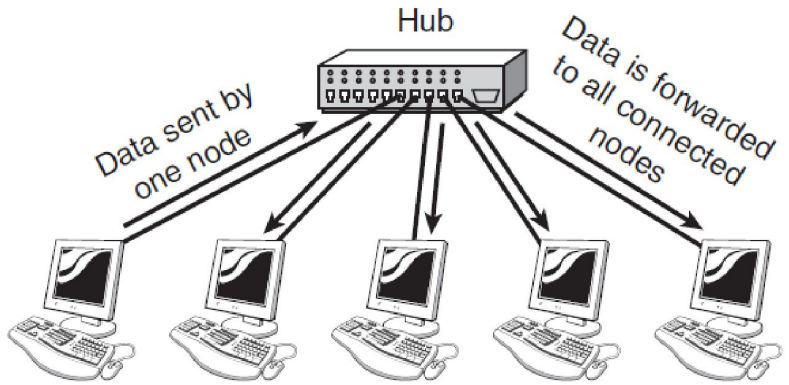
Hubs

- Intelligent hubs
  - Possesses processing capabilities
- Standalone Hubs
  - Hubs that serve a group of computers that are isolated from the rest of the network
    - Best suited to small, independent departments, home offices, or test lab environments
  - Disadvantage to using a single hub for many connection ports is that it introduces a **single point of failure** on the network
- Stackable Hubs
  - Physically designed to be linked with other hubs in a single telecommunications closet

The basic function of a hub is to take data from one of the connected devices and forward it to all the other ports on the hub.

This method of operation is inefficient because, in most cases, the data is intended for only one of the connected devices.

Due to the inefficiencies of the hub system and the constantly increasing demand for more bandwidth, hubs are slowly but surely being replaced with switches.



Switches

- Subdivide a network into smaller logical pieces

- A switch forwards data only to the port on which the destination system is connected.
- It looks at the Media Access Control (MAC) addresses of the devices connected to it to determine the correct port. A *MAC address* is a unique number that is stamped into every NIC.
- By forwarding data only to the system to which the data is addressed, the switch decreases the amount of traffic on each network link dramatically.

Three methods to deal with data as it arrives:

Cut-through

- In a cut-through configuration, the switch begins to forward the packet as soon as it is received. i.e. switch reads a frame's header and decides where to forward the data before it receives the entire packet.

- No error checking is performed on the packet, so the packet is moved through quickly. The downside of cut-through is that because the integrity of the packet is not checked, the switch can propagate errors.

- Store and forward mode
  - In a store-and-forward configuration, the switch waits to receive the entire packet before beginning to forward it. It also performs basic error checking. i.e. switch reads the entire data frame into its memory and checks it for accuracy before transmitting the information
- Fragment-free—Building on the speed advantages of cut-through switching, fragment- free switching works by reading only the part of the packet that enables it to identify fragments of a transmission.

Full Duplex Switches

- A full duplex switch allows for simultaneous transmission and reception of data to and from a workstation.
- This full duplex connection helps to eliminate collisions.
- To support a full duplex connection to a switch, two sets of wires are necessary - one for the receive operation and one for the transmit operation.

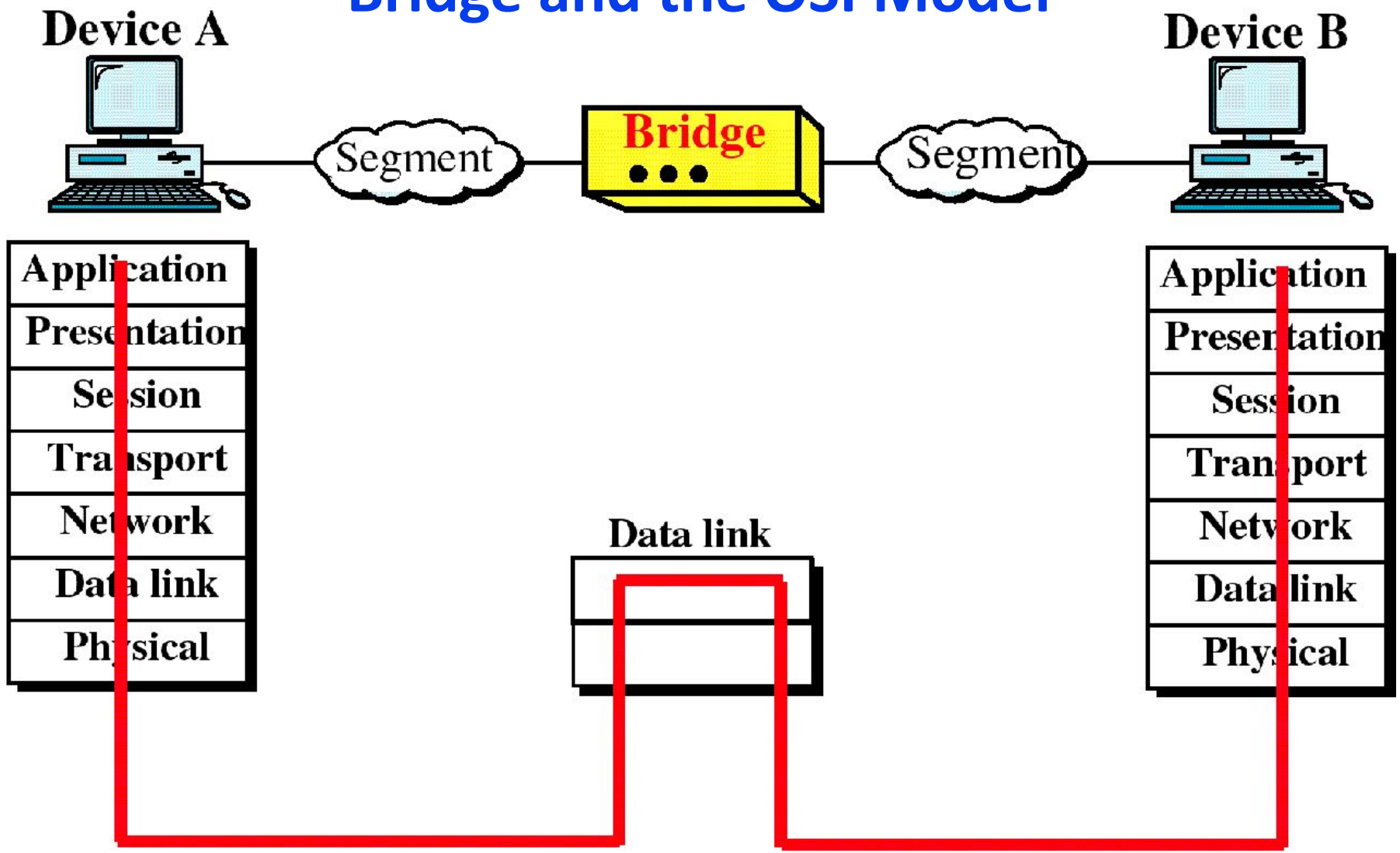
Bridges

- Like a repeater, a bridge has a single input and single output port
- Unlike a repeater, it can interpret the data it retransmits

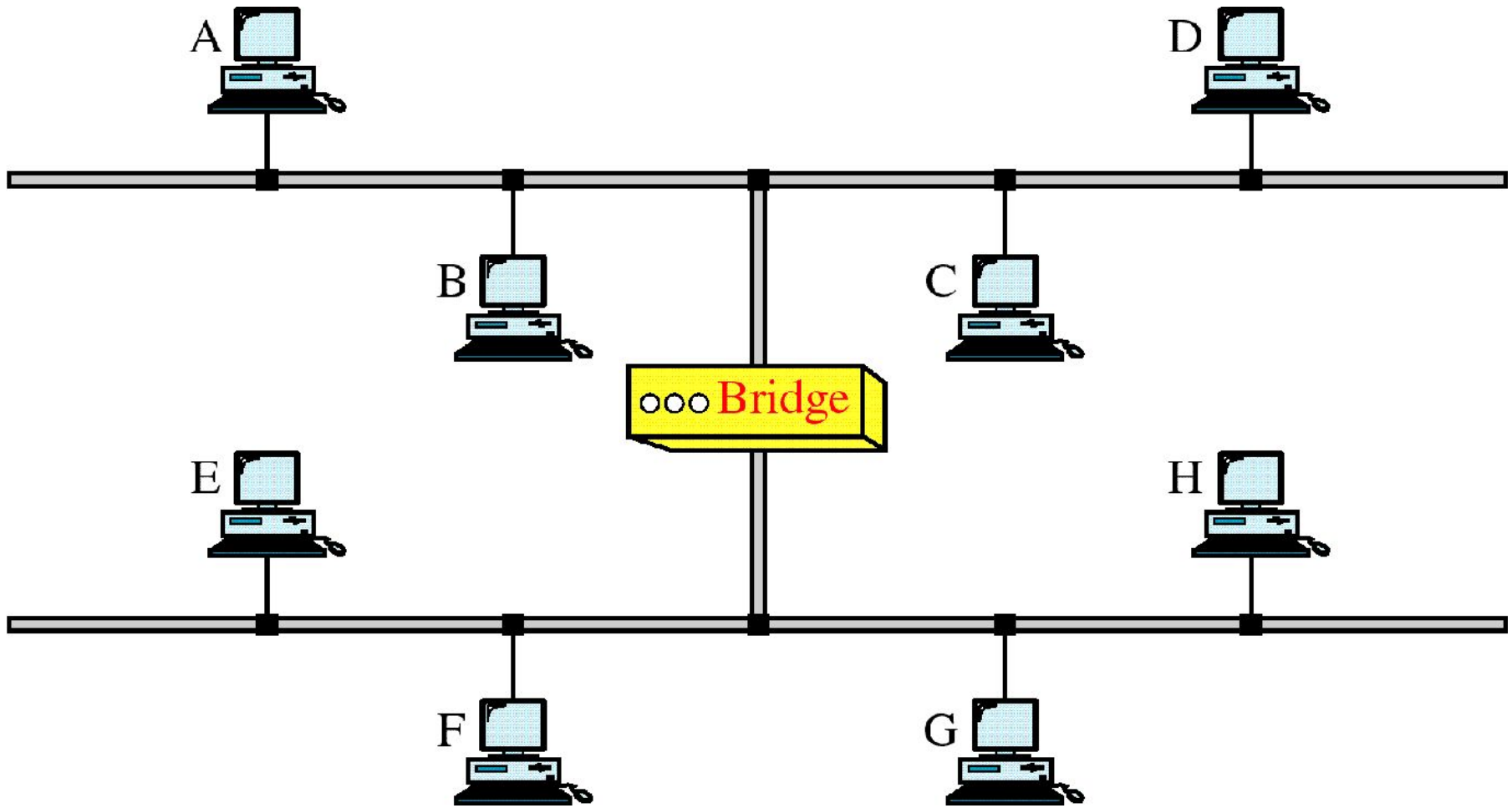
Bridges

- A bridge (or bridge-like device) can be used to connect two similar LANs, such as two CSMA/CD LANs.
- A bridge can also be used to connect two closely similar LANs, such as a CSMA/CD LAN and a token ring LAN.
- The bridge examines the destination address in a frame and either forwards this frame onto the next LAN or does not.
- The bridge examines the source address in a frame and places this address in a routing table, to be used for future routing decisions.

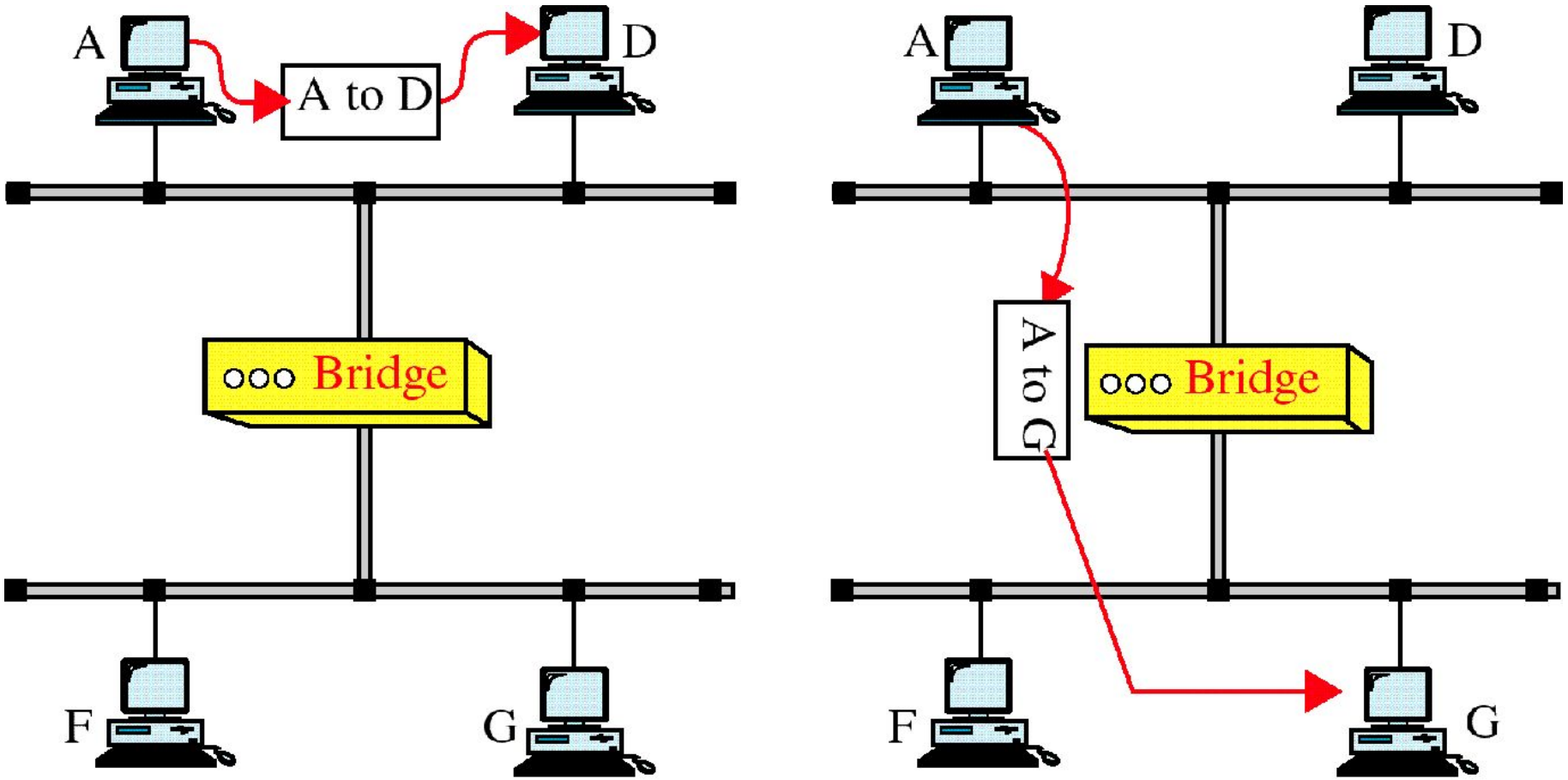
Bridge and the OSI Model



A Bridge



Function of a Bridge



a. A packet from A to D

b. A packet from A to G

Types of Bridges

- Transparent
  - Basic Bridge
  - Learning Bridge
  - Spanning Tree Bridge
- Translational bridge
- Source-routing Bridge
- Remote Bridge

Transparent Basic Bridge

- A transparent bridge does not need programming but observes all traffic and builds routing tables from this observation called backward learning.
- Each bridge has two connections (ports) and there is a routing table associated with each port.
- A bridge observes each frame that arrives at a port, extracts the source address from the frame, and places that address in the port's routing table.
- A transparent bridge is found with CSMA/CD LANs.

The Transparent Learning Bridge

- The whole operation of this bridge is operated by the bridge processor which is responsible for routing traffic across its ports.
- The processor decides the destination ports of associated MAC addresses by accessing a routing database.
- When a frame arrives the processor will check the output port in the database on which the frame will be relayed.
- If the destination address is not in the database then the processor will broadcast that frame onto all ports except the port from which the frame was arrived.
- The bridge processor also stores the source address in the frame because this source address may be the destination address for another incoming frame.

The Transparent Spanning Tree Bridge

- These bridges use a subnet of the full topology to create a loop free operation.
- The received frame is checked by the bridge in following manner.
  - The destination address of arrived frame is checked with routing table in the database.
  - Here more information is required for bridge so the bridge port is also stored in the database. This information is known as port state information and it helps in deciding that, a port can be used for this destination address or not.
  - The port can be in a block state to fulfill the requirements of spanning tree operations or in a forwarding state. If the port is in forwarding state the frame is routed across the port.
  - The port can have different status such as; it may be in “disabled” state for the maintenance reason or may also be unavailable temporarily if databases are being changed in the bridge because of result of the change in the routed network.

Translational bridge

- Translational bridge—A translational bridge can convert from one networking system to another. It translates the data it receives.
- Translational bridges are useful for connecting two different networks, such as Ethernet and Token Ring networks.
- Depending on the direction of travel, a translational bridge can add or remove information and fields from the frame as needed.

Source-routing Bridge

- A source-routing bridge is found with token ring networks do not learn from routing tables.
- The source-route bridge derives its name from the fact that the entire route of the frame is embedded within the frame. This allows the bridge to make specific decisions about how the frame should be forwarded through the network.
- When a workstation wants to send a frame, it must know the exact path of network / bridge / network / bridge / network …
- If a workstation does not know the exact path, it sends out a discovery frame and records the path

Remote Bridge

- A remote bridge is capable of passing a data frame from one local area network to another when the two LANs are separated by a long distance and there is a wide area network connecting the two LANs.
- A remote bridge takes the frame before it leaves the first LAN and encapsulates the WAN headers and trailers.
- When the packet arrives at the destination remote bridge, that bridge removes the WAN headers and trailers leaving the original frame.

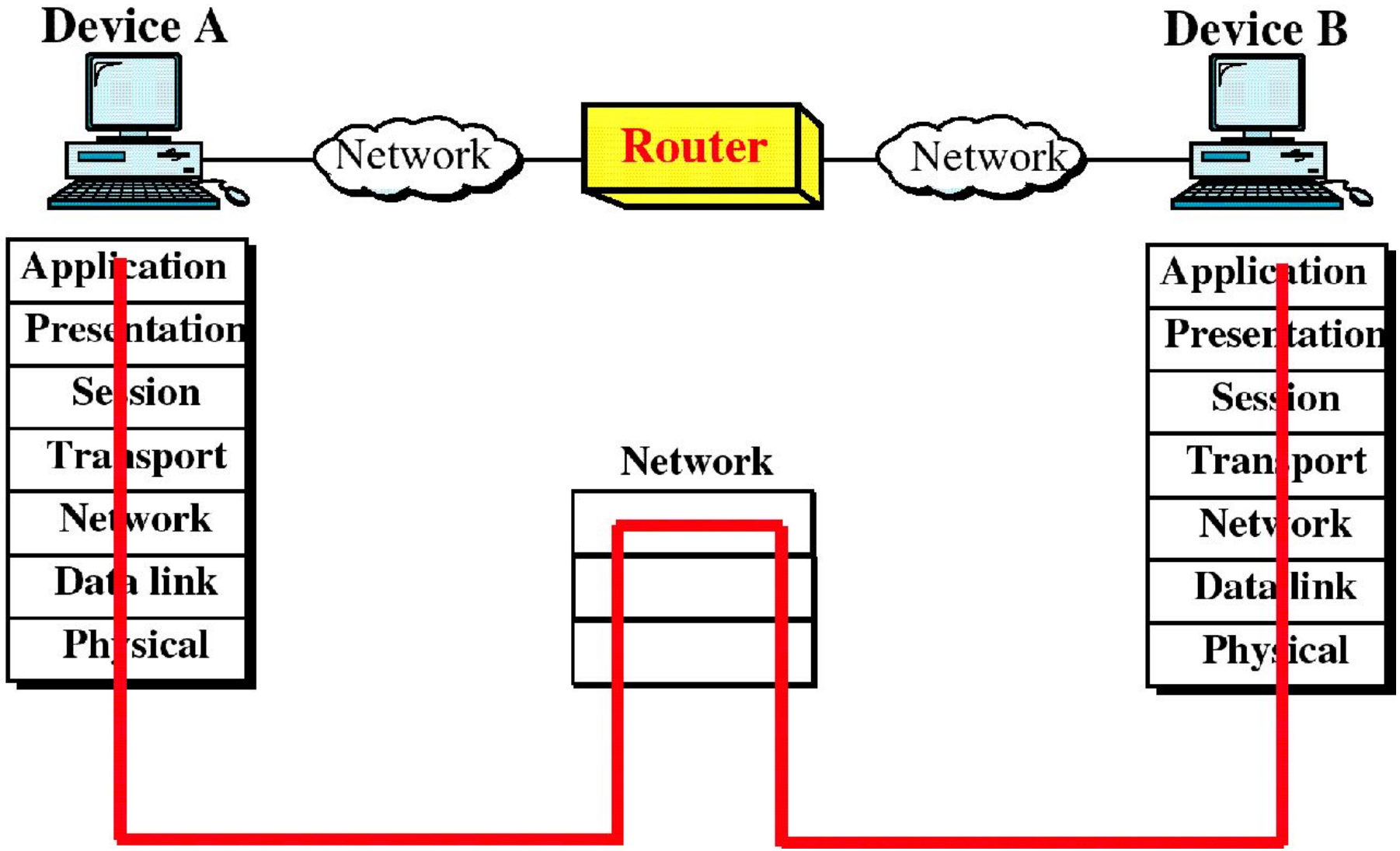
Routers

- Multiport connectivity device
- Can integrate LANs and WANs running at different transmission speeds and using a variety of protocols
- Routers operate at the Network layer (Layer 3) of the OSI Model
- A router accepts an outgoing packet, removes any LAN headers and trailers, and encapsulates the necessary WAN headers and trailers
- Because a router has to make wide area network routing decisions, the router has to dig down into the network layer of the packet to retrieve the network destination address

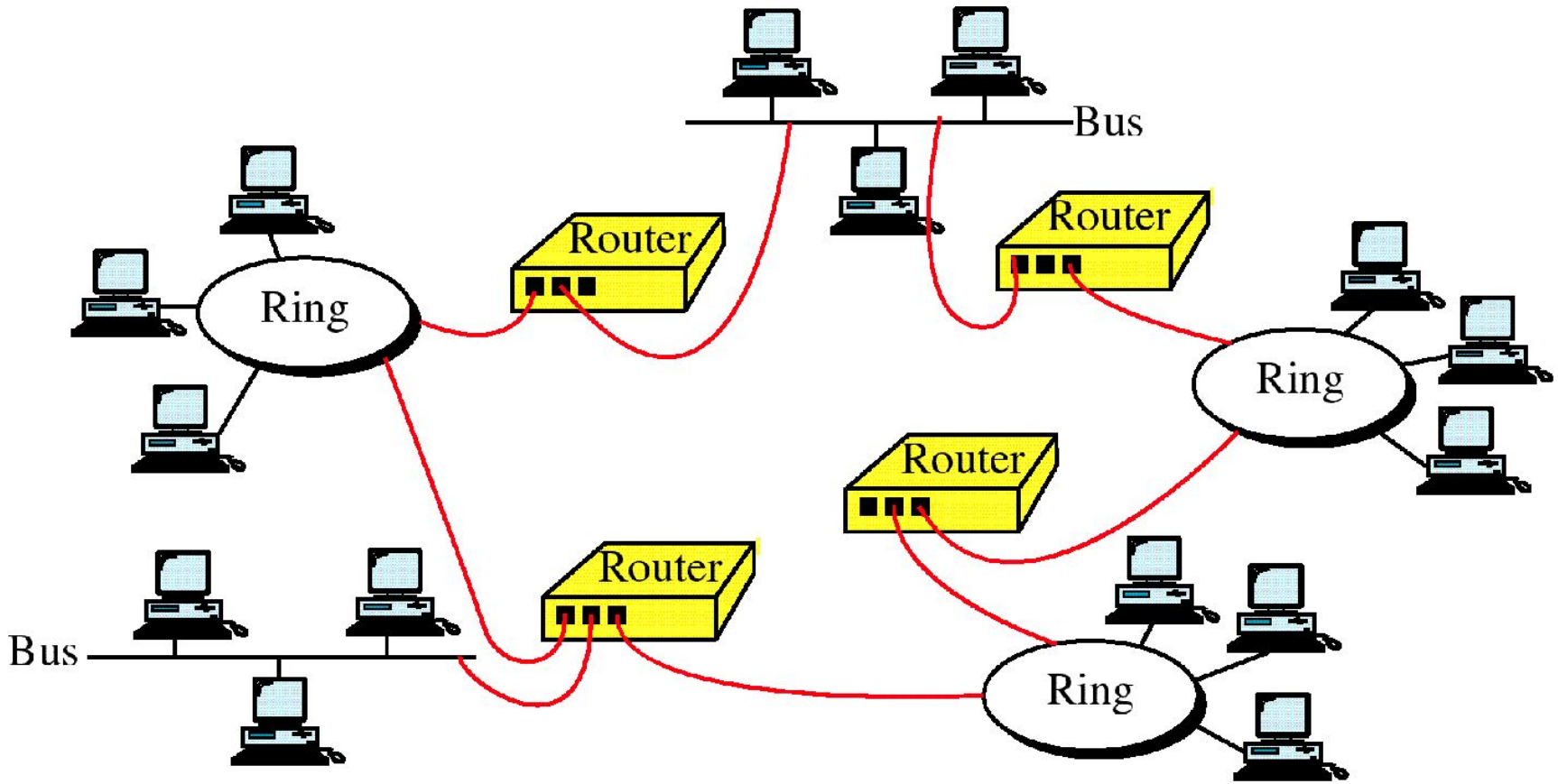
Router Features and Functions

- Filter out broadcast transmission to alleviate network congestion
- Prevent certain types of traffic from getting to a network
- Support simultaneous local and remote activity
- Provide high network fault tolerance through redundant components
- Monitor network traffic and report statistics to a Management Information Base (MIB)
- Diagnose internal or other connectivity problems and trigger alarms
- Routers often incorporate firewall functions

Router and the OSI Model



Routers in an Internet



Brouters and Routing Switches

- Bridge router
  - Also called a **brouter**
  - Industry term used to describe routers that take on some characteristics of bridges
- Routing switch
  - Router hybrid that combines a router and a switch

Gateways

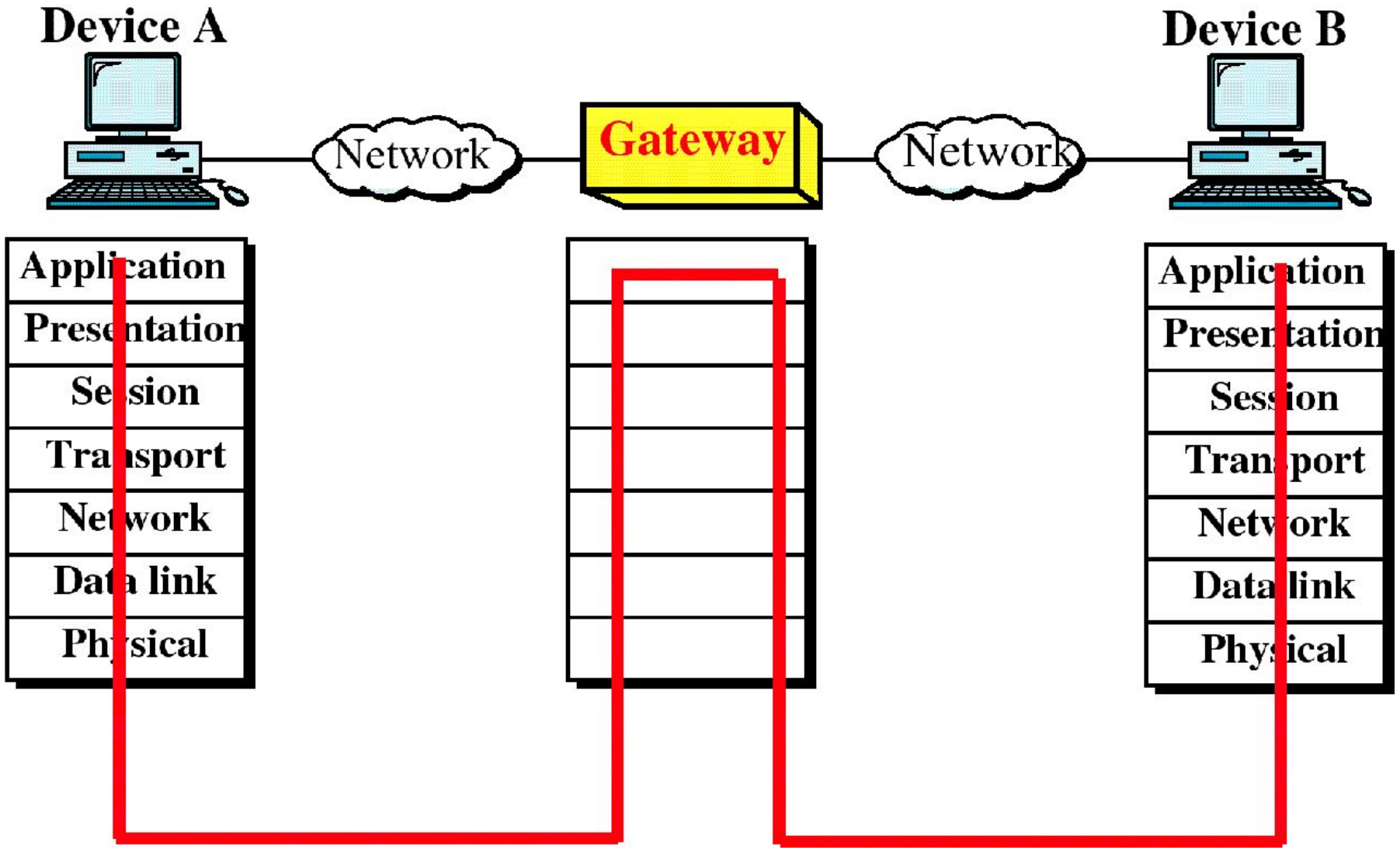
Combination of networking hardware and software that connects two dissimilar kinds of networks

A **gateway** is a piece of networking hardware used in telecommunications for telecommunications networks that allows data to flow from one discrete network to another.

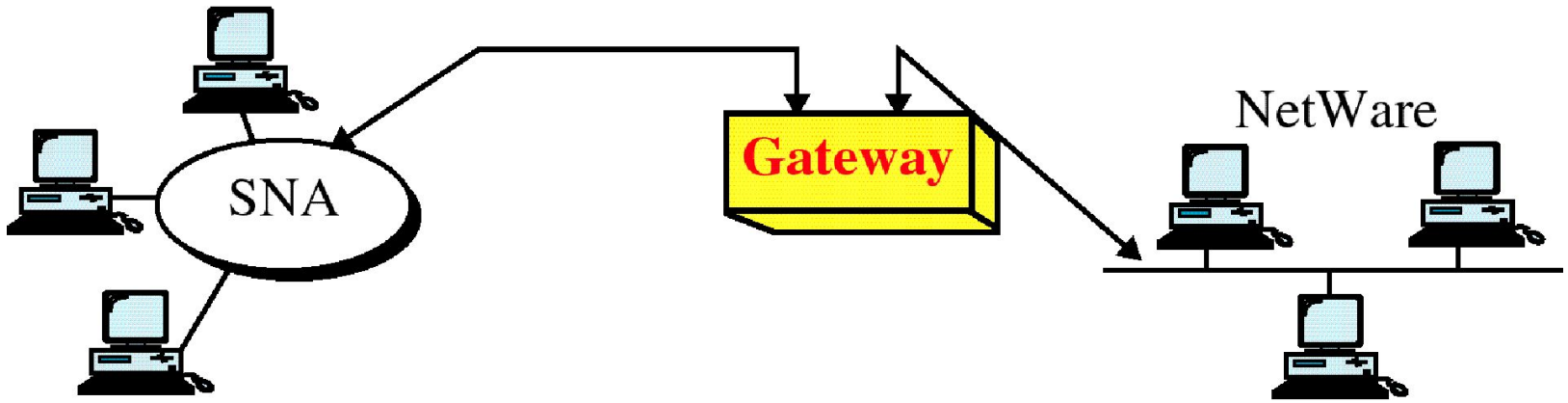
- Popular types of gateways include:
  - E-mail gateways
  - IBM host gateways
  - Internet gateways
  - LAN gateways

- A gateway is often characterized as being the combination of a router and a modem.
- Gateways are basically protocol converters, facilitating compatibility between two protocols and operating on any layer of the open systems interconnection (OSI) model.

Gateway and the OSI Model



A Gateway



Types of gateways

Gateways can take several forms and perform a variety of tasks. Examples of this include:

- Web application firewalls- This type filters traffic to and from a web server and looks at application-layer data.
- Cloud storage gateways- This type translates storage requests with various cloud storage service API calls. It allows organizations to integrate storage from a private cloud into applications without migrating into a public cloud.
- API, SOA or XML gateways – This type manages traffic flowing into and out of a service, microservices-oriented architecture or XML-based web service.

- IoT gateways-This type aggregates sensor data from devices in an IoT environment, translates between sensor protocols and processes sensor data before sending it onward.
- Media gateways- This type converts data from the format required for one type of network to the format required for another.
- Email security gateways- This type prevents the transmission of emails that break company policy or will transfer information with malicious intent.
- VoIP trunk gateways- This type facilitates the use of plain old telephone service equipment, such as landline phones and fax machines, with a voice over IP (VoIP) network.

Gateways and routers

- Gateways are distinct from routers or switches in that they communicate using more than one protocol and can operate at any of the seven layers of the open systems interconnection model (OSI)
- Gateways and routers are similar in that they both can be used to regulate traffic between two or more separate networks.
- However, a router is used to join two similar types of networks and a gateway is used to join two dissimilar networks.
- Dissimilar could be used to describe networks that use different primary protocols.

Wireless Networks

- The key hardware components of a wireless computer network include adapters, routers and access points, antennas, and repeaters.
- Wireless network adapters (also known as wireless NICs or wireless network cards) are required for each device on a wireless network. All laptop computers, tablets, and smartphones incorporate wireless capability as a built-in feature.

Wireless Routers and Access Points

- Wireless routers are the heart of a wireless network. These routers function comparable to routers for wired Ethernet networks. The wireless router usually connects directly to the modem supplied by the high-speed internet service provider by wire. Everything else in the home connects wirelessly to the router.
- AP (Access Point)
- A device that allows wireless devices to connect to a wired network using Wi-Fi or related standards Client Device : The device with a wifi radio that you use to connect to a wireless access point, e.g. a computer, cell phone or tablet device.

Wireless Antennas

- Access points and routers can use a Wi-Fi wireless antenna to increase the communication range of the wireless radio signal.
- Converts electrical signals to radio waves. It is normally connected to a radio transmitter or radio receiver, and is the interface between the electrical signals in the radio, and the movement of the signals through the air.
- These antennas are built in to most routers but are optional and removable on some older equipment.

Wireless Repeaters

- A wireless repeater connects to a router or access point to extend the reach of the network.
- Often called a signal booster or range expander, a repeater serves as a two-way relay station for wireless radio signals.
- Repeaters allow equipment that is otherwise unable to receive a network's wireless signal to join.