Computer Network (CN)

What is CN

- A CN is set of nodes connected by communication links.
  - Node is a device capable of sending and receiving data.
    - End node: starting/end point in the communication, may generate the data
    - Intermediary Node: Do not generate the data, just forward the data, switch, router etc.
  - Communication links carries the information.
    - Wired (Guided): Twisted pair, coaxial cable, optical fiber
    - Wireless (Unguided): Infrared Waves, Radio Waves, Microwaves, Satellite
- A CN is mainly used for resource sharing and saves lot of infrastructure cost.

Desirable Characteristics of CN

- Fault tolerance: Continue working despite of failure, ensure no loss of service. e. g. path from college to home
- Scalability: Ability to grow based on the needs and have good performance after growth e. g. internet
- Quality of service: Ability to set priorities and manage data traffic to reduce data loss, delay etc. e. g. email and voIP data
- Security: Ability to prevent unauthorized access, misuse, forgery by ensuring confidentiality, integrity and availability.

Data Communication

- Data communication are the exchange of data between two nodes via some form of communication link.
- All communication scheme will have the following things in common
  - Sender/Source Node
  - Receiver/Destination Node
  - Medium
  - Protocol

Protocol

- Protocol is a set of rules that govern communication. Elements of protocol are
  - Message encoding: based on wired/ wireless communication link, data must be encoded in the suitable form.
  - Message formatting: To identify the sender and receiver, their information is added with the data.
  - Message timing: Flow control and response timeout
  - Message size: Break the big message in smaller one based on the capacity of transmission medium.
  - Message delivery option: unicast, multicast, broadcast

Transmission Mode

- Transmission mode refers to the direction of information flow between two devices
  - Simplex: Communication is unidirectional as on a one-way street. Only one of the two station on a link can transmit, other can only receive. e. g. keyboard, mouse, traditional monitors
  - Half duplex: Each station can both transmit and receive but not at the same time. e. g. walkie-talkie
  - Full duplex: Both station can transmit and receive simultaneously e. g. mobile

Line Configuration

- Line Configuration defines the attachment of communication devices to a link. Its of two types:
  - Point to Point
    - Dedicated link between two devices
    - E. g. connection between TV and its remote
  - Multipoint
    - More than two specific devices share a single link
    - Link is shared in two ways:
      - Spatially: Several devices can use the link simultaneously
      - Time shared: Link is shared based on turn

Node Relationship

- Relationship between the nodes in a network is of two types:
  - Peer to peer
    - No body superior, no body inferior
    - All nodes have equal rights
    - No centralized administration
    - Not scalable
  - Client server
    - Server nodes are generally more powerful than the client nodes
    - Server nodes have more rights
    - Centralized administration
    - Scalable

Topology

- Topology defines the physical or logical arrangements of links in a network.
  - Mesh: Every device has a dedicated point to point link to every other device.
  - Ring: Each device has a dedicated point-to-point link configuration only with the two devices on either side of it.
  - Star: Each device has a point-to-point link only to a central controller (hub). Devices are not directly linked to each other.
  - Tree: A tree topology is a variation of star topology where most of the nodes are connected to secondary/passive hub and these passive hub are connected to central/active hub.
  - Bus: It's a multipoint topology where one long cable acts as a backbone to link all the devices in the network.

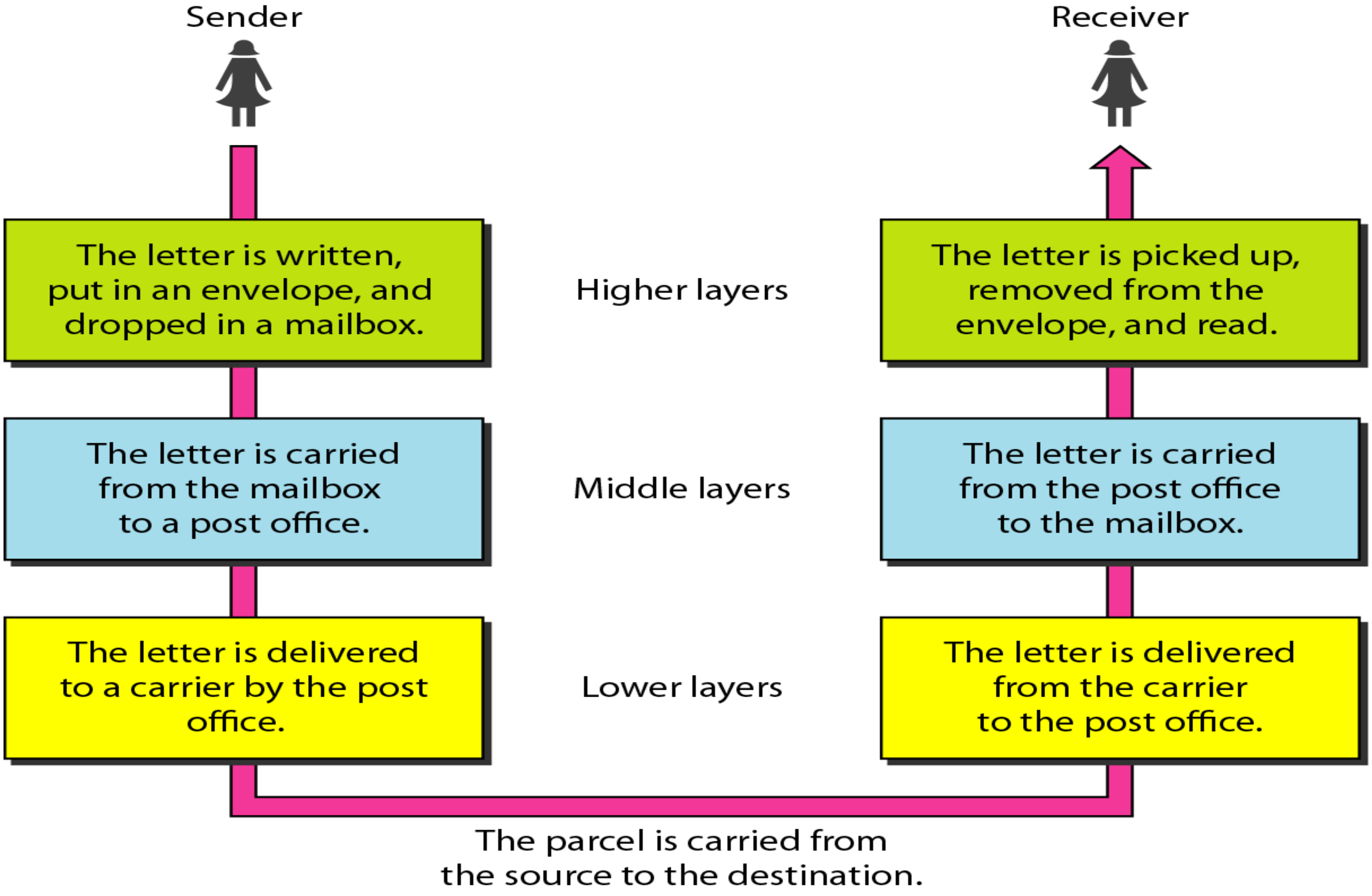
Network Types

- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)

OSI Model

- Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards.
- An ISO standard that covers all aspects of network communication is Open System Interconnection (OSI) model. It was first introduced in the late 1970s.

OSI Model



Sender

Receiver

The letter is written, put in an envelope, and dropped in a mailbox.

Higher layers

The letter is picked up, removed from the envelope, and read.

The letter is carried from the mailbox to a post office.

Middle layers

The letter is carried from the post office to the mailbox.

The letter is delivered to a carrier by the post office.

Lower layers

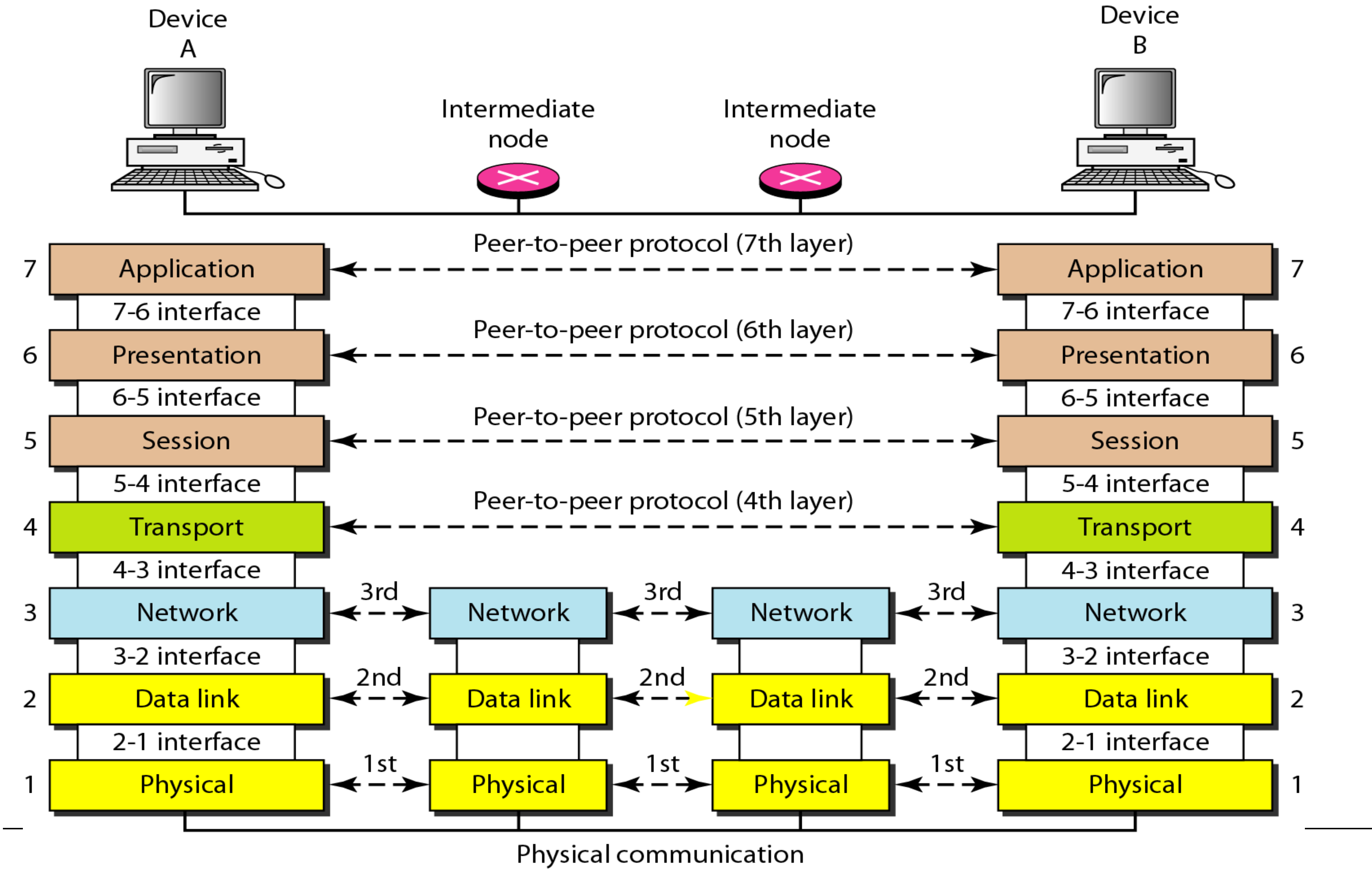
The letter is delivered from the carrier to the post office.

The parcel is carried from the source to the destination.

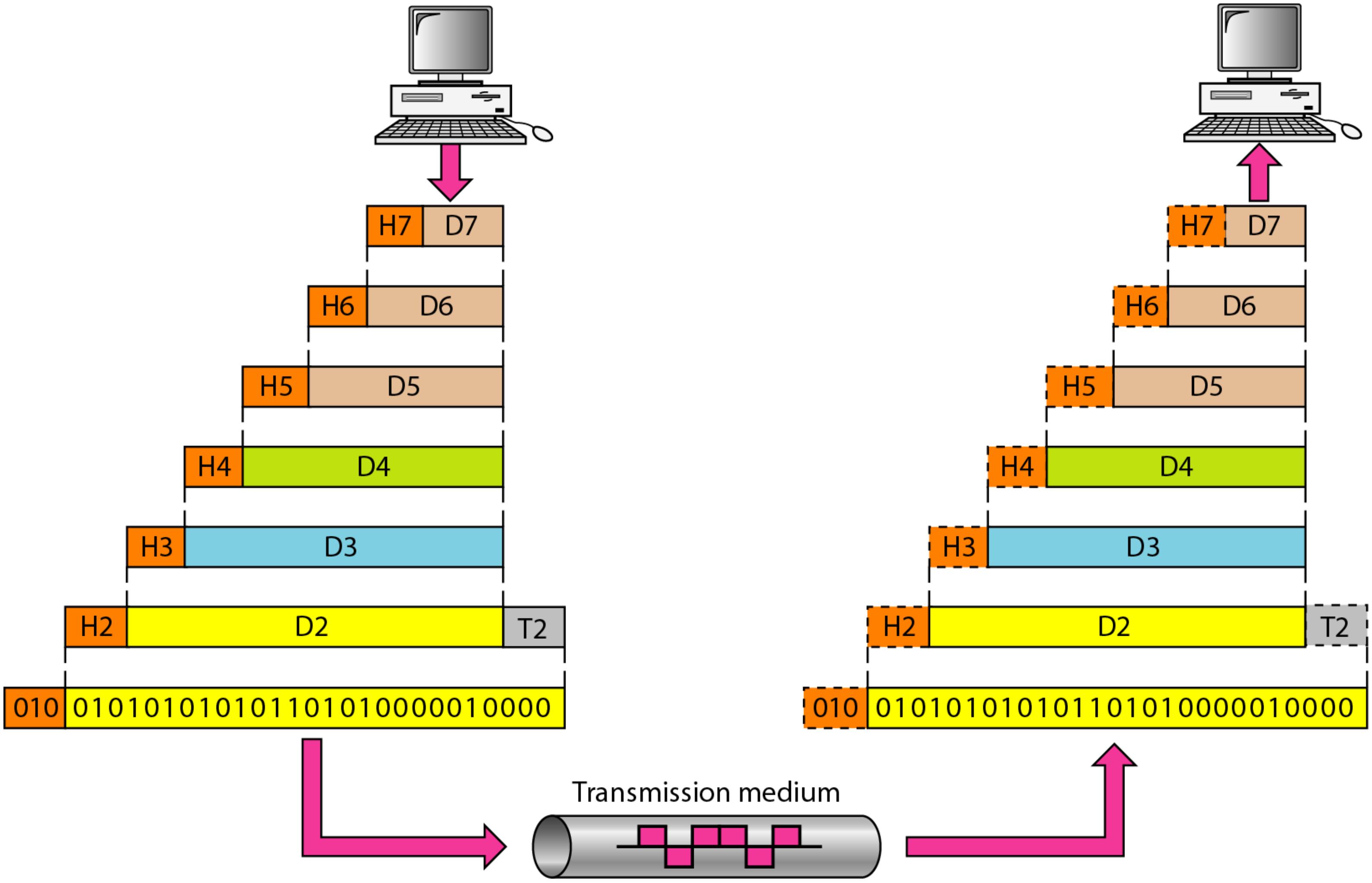
OSI Model

- OSI model is a layered framework for the design of network system that allows two different system to communicate irrespective of their underlying architecture.
- It consists of 7 separate but related layers each of which defines a segment of the process of moving information across a network.

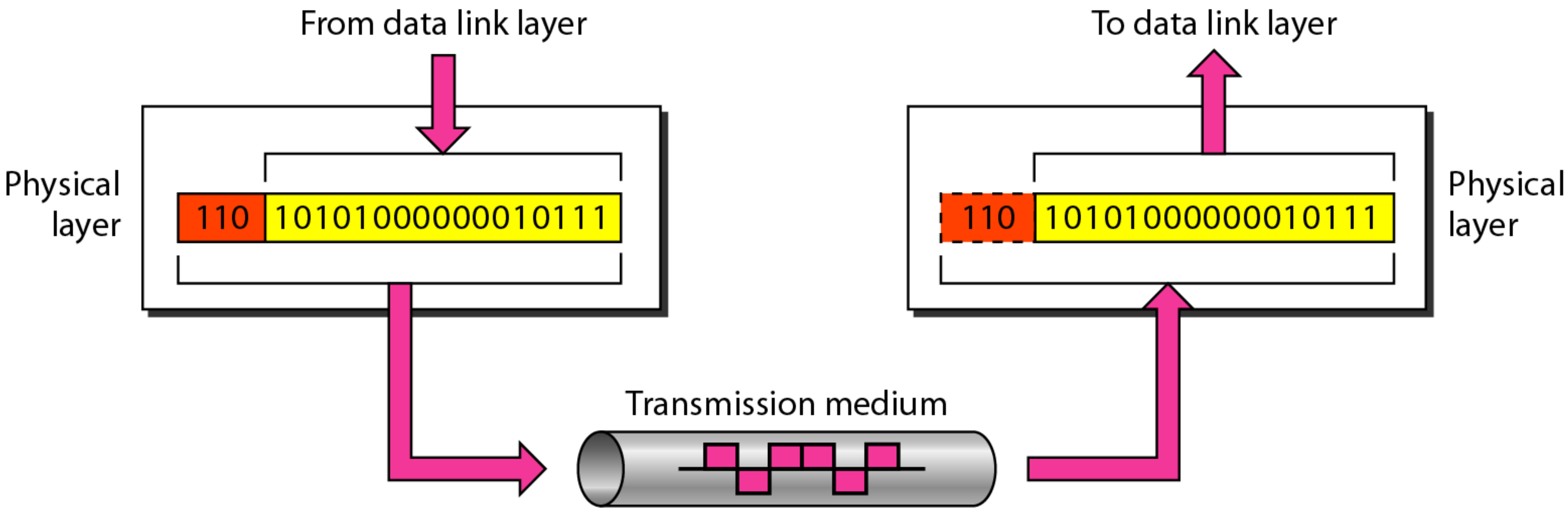
OSI Model


Device
A
Intermediate
node
Intermediate
node
Device
B
Peer-to-peer protocol (7th layer)
Peer-to-peer protocol (6th layer)
Peer-to-peer protocol (5th layer)
Peer-to-peer protocol (4th layer)
7
Application
7-6 interface
6
Presentation
6-5 interface
5
Session
5-4 interface
4
Transport
4-3 interface
3
Network
3-2 interface
2
Data link
2-1 interface
1
Physical
3rd
Network
3rd
Network
3rd
2nd
Data link
2nd
Data link
2nd
1st
Physical
1st
Physical
1st
Application
7-6 interface
Presentation
6-5 interface
Session
5-4 interface
Transport
4-3 interface
Network
3-2 interface
Data link
2-1 interface
Physical
7
6
5
4
3
2
1
Physical communication

OSI Model

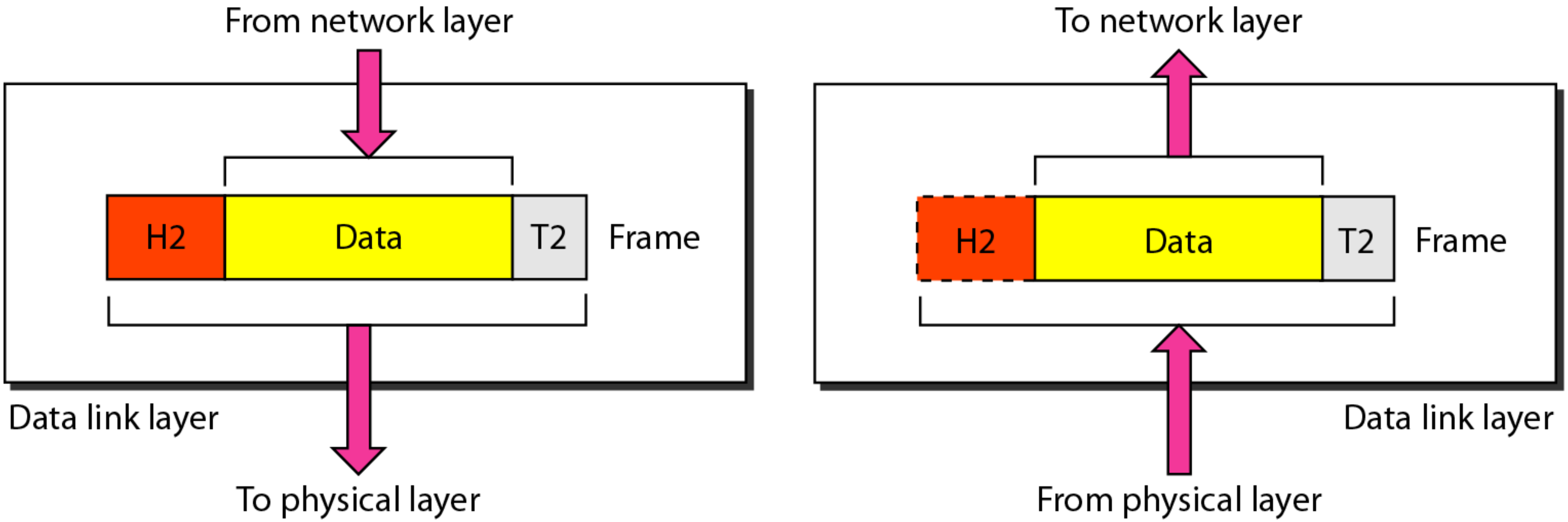

H7
D7
H6
D6
H5
D5
H4
D4
H3
D3
H2
D2
T2
010
0101010101011010100000010000
Transmission medium
H7
D7
H6
D6
H5
D5
H4
D4
H3
D3
H2
D2
T2
010
0101010101011010100000010000

Physical Layer



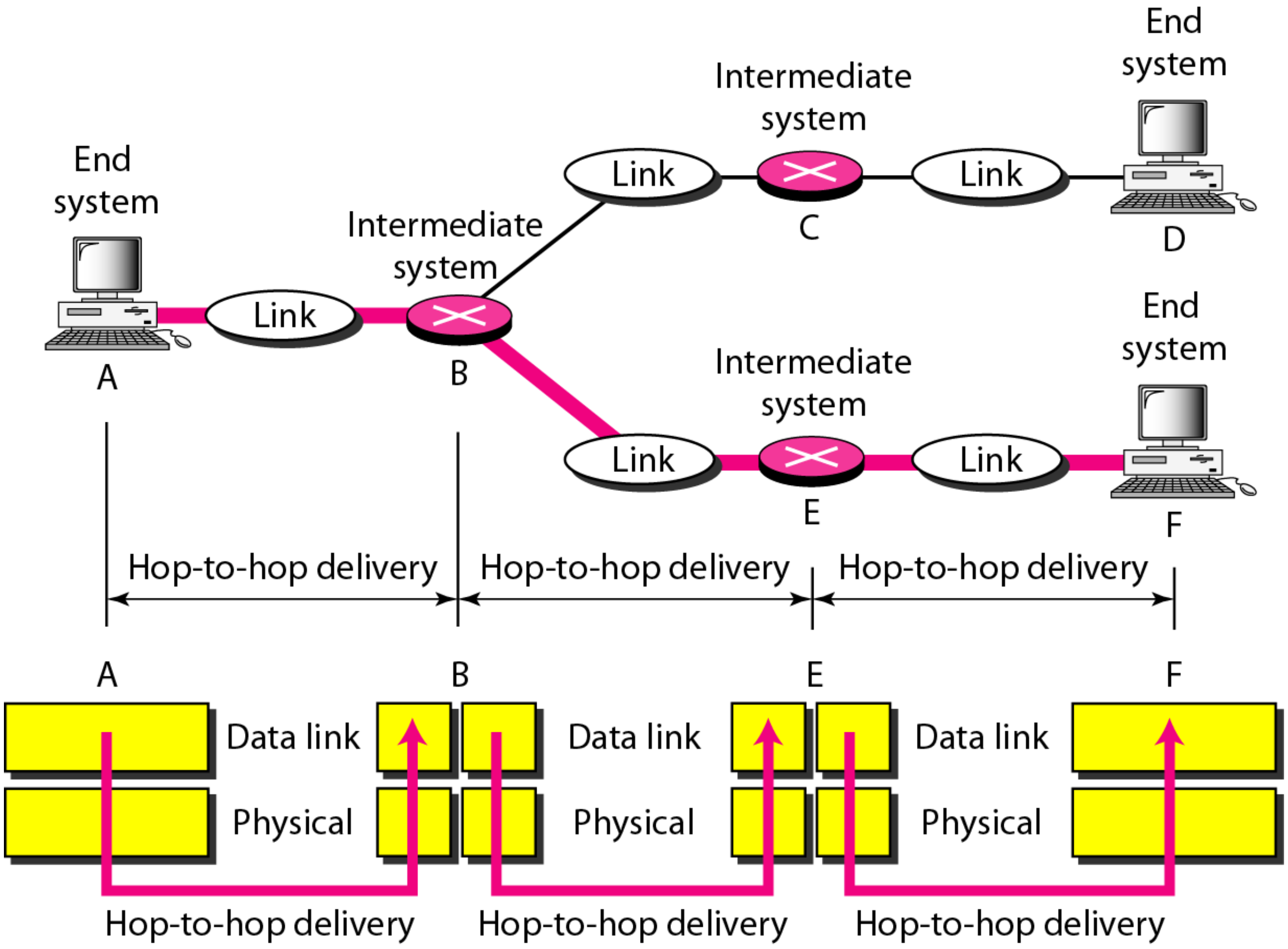
The physical layer is responsible for movements of individual bits from one hope (node) to the next node.

Data Link Layer

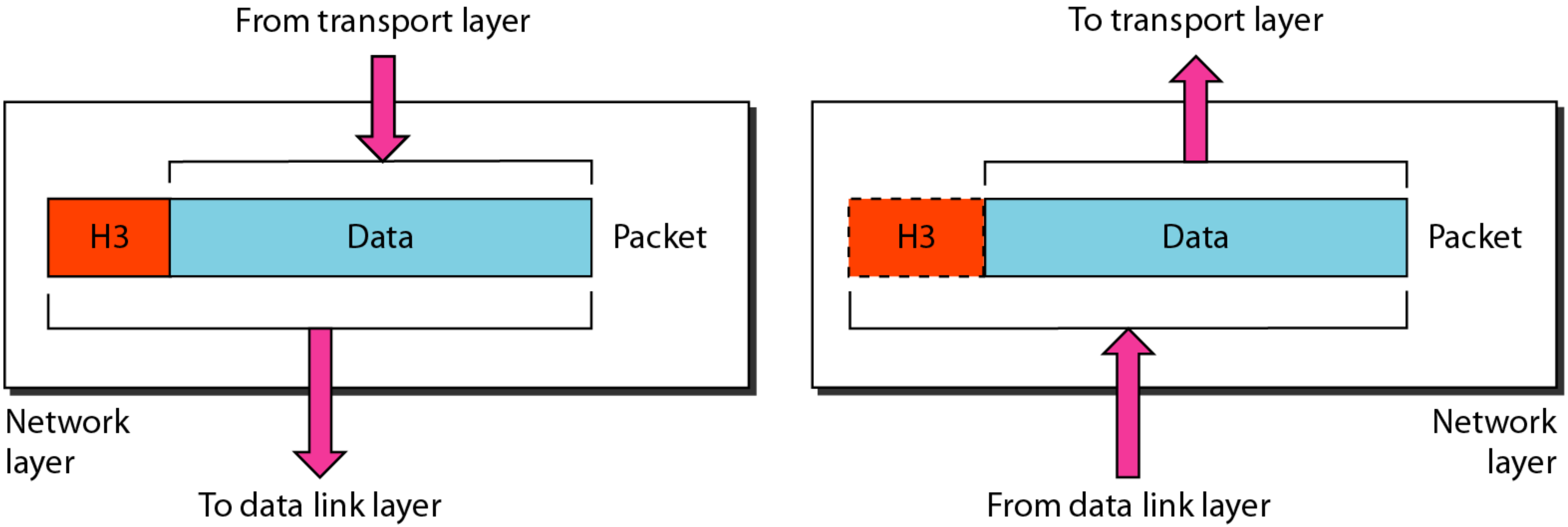


The data link layer is responsible for moving frames from one hop (node) to the next node.

OSI Model

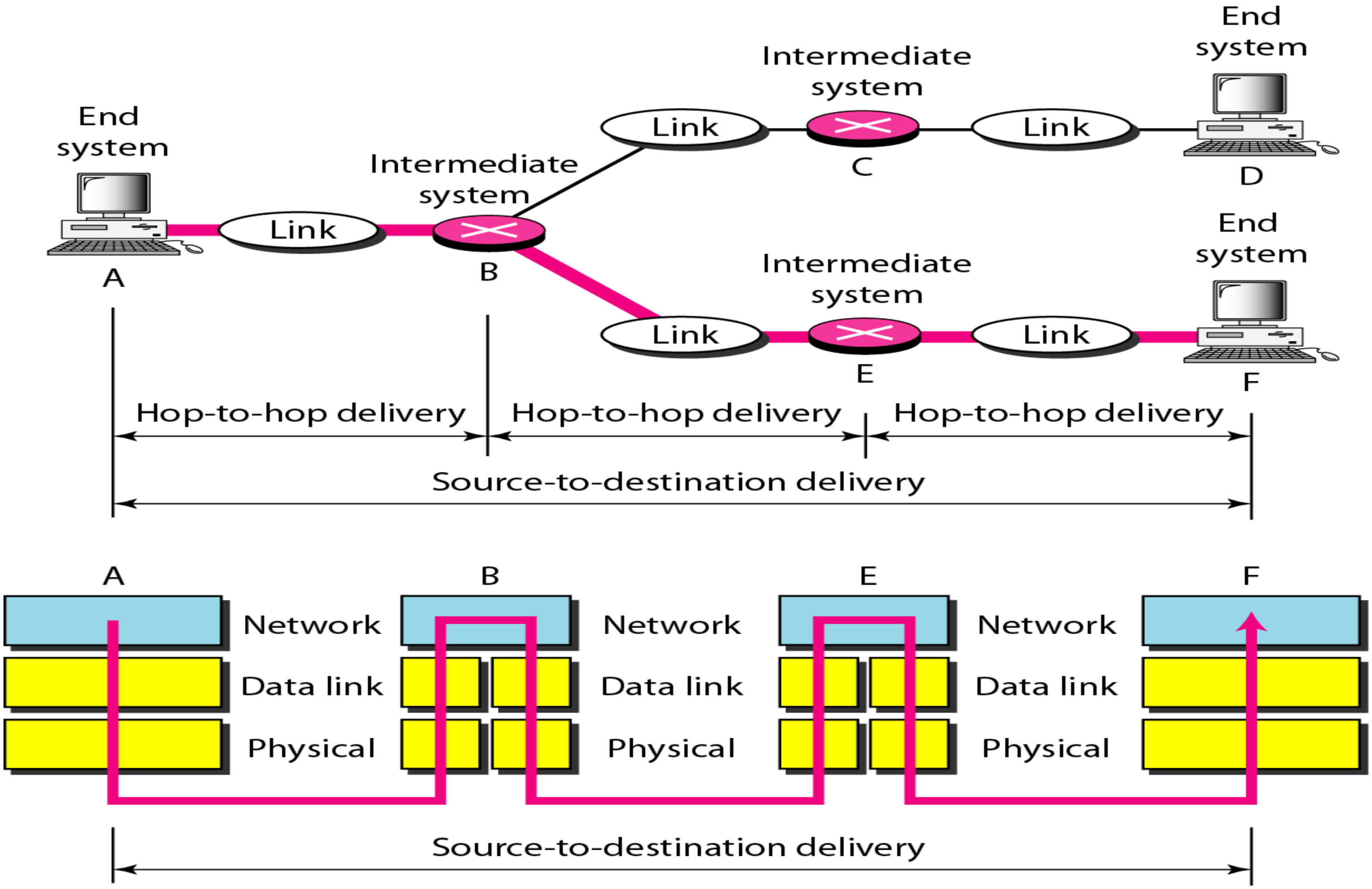

End system
Intermediate system
End system
Link
Link
C
D
End system
Intermediate system
Link
A
B
Intermediate system
End system
Link
Link
E
F
Hop-to-hop delivery
Hop-to-hop delivery
Hop-to-hop delivery
A
B
E
F
Data link
Data link
Data link
Physical
Physical
Physical
Hop-to-hop delivery
Hop-to-hop delivery
Hop-to-hop delivery

Network Layer

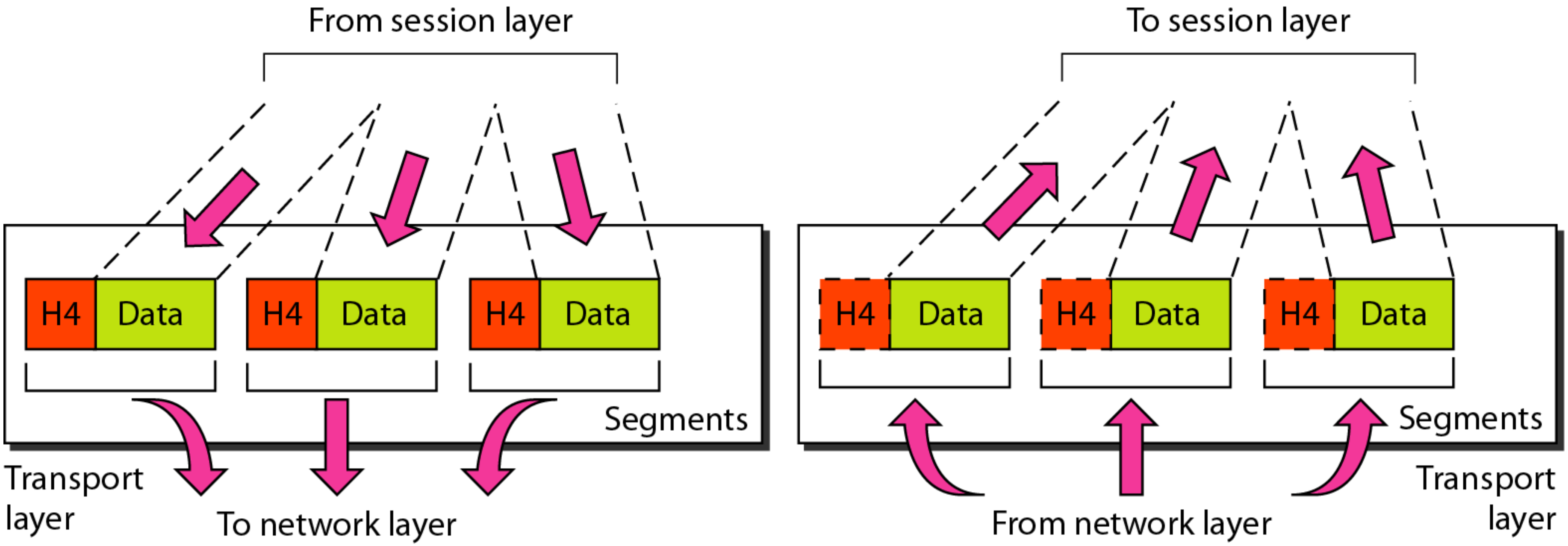


The network layer is responsible for the delivery of individual packets from the source host to the destination host.

OSI Model

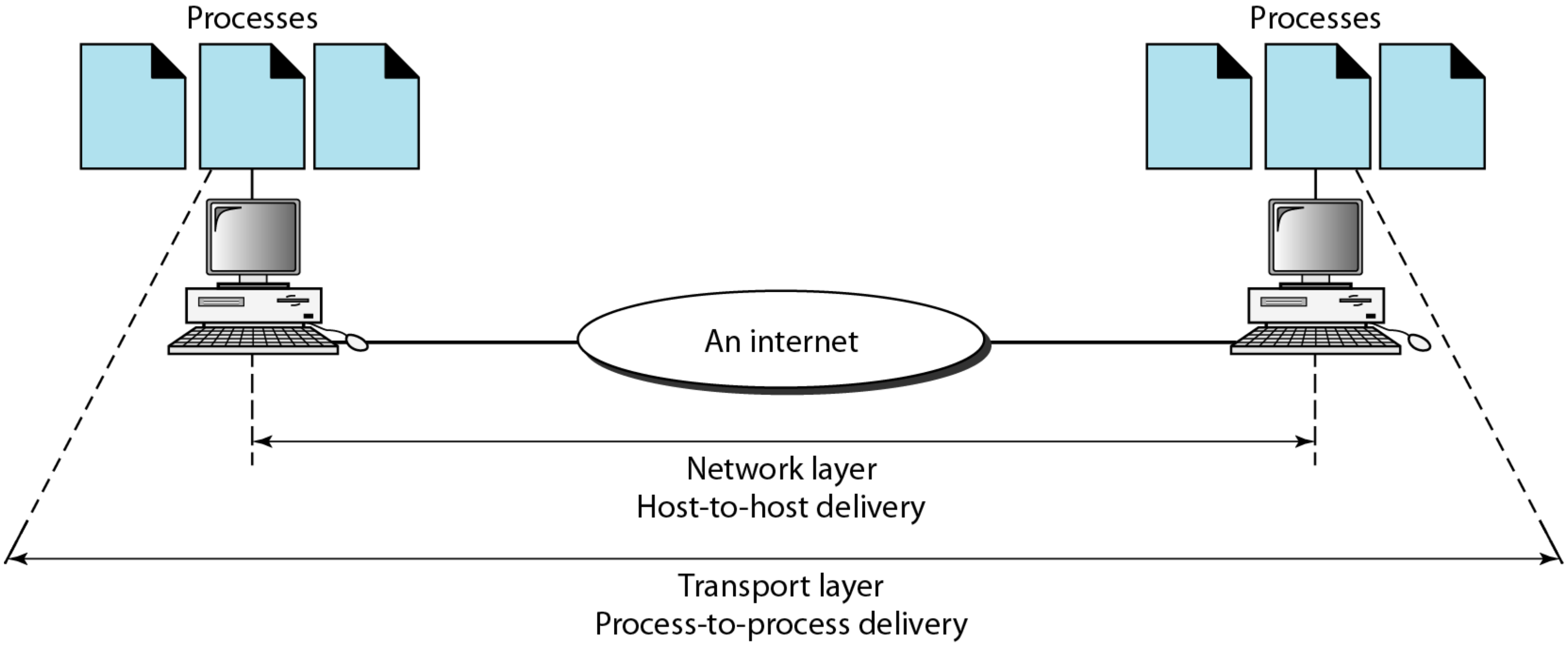

End system
Intermediate system
Intermediate system
End system
Link
Link
Link
Link
Link
C
D
A
B
Intermediate system
End system
E
F
Hop-to-hop delivery
Hop-to-hop delivery
Hop-to-hop delivery
Source-to-destination delivery
A
B
E
F
Network
Network
Network
Data link
Data link
Data link
Physical
Physical
Physical
Source-to-destination delivery

Transport Layer

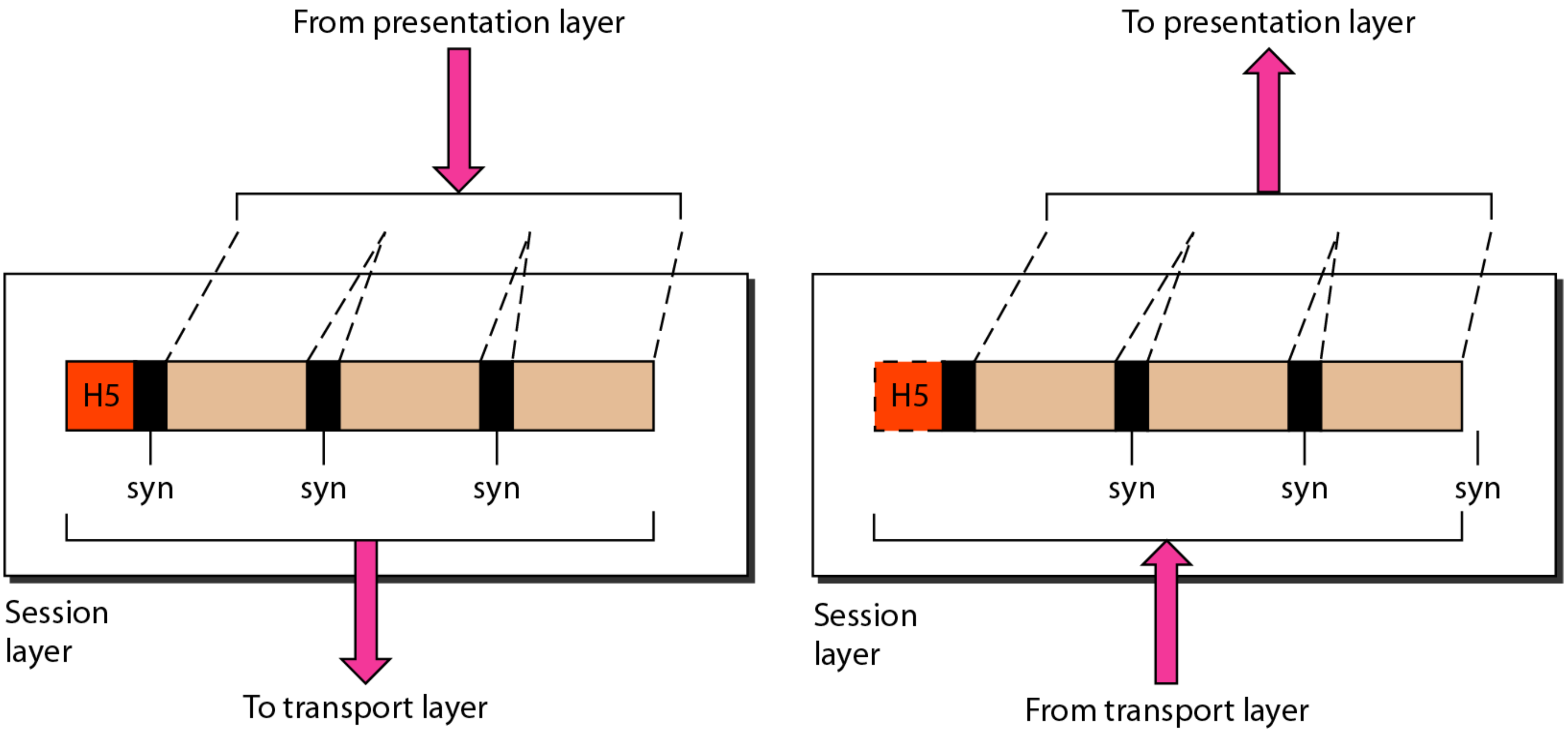


The transport layer is responsible for the delivery of entire message from one process to another.

Transport Layer

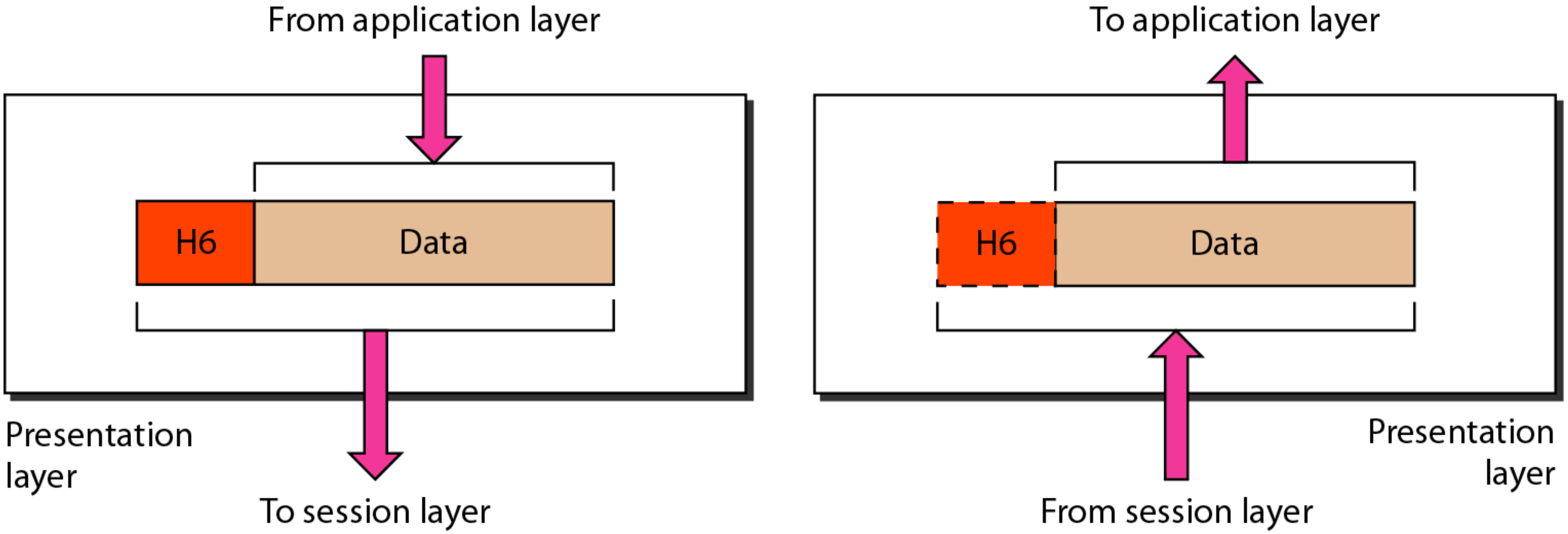


Session Layer



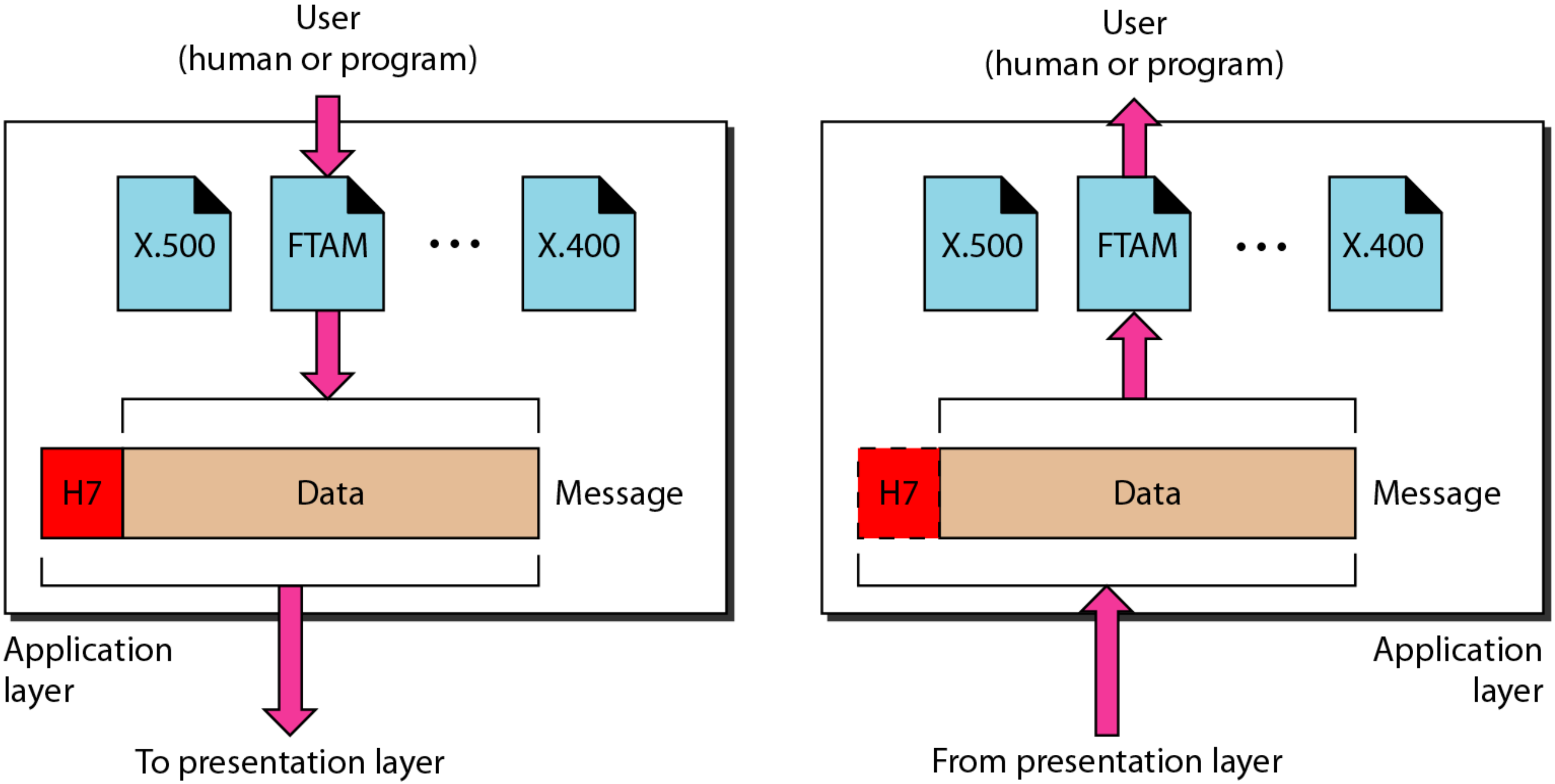
The session layer is responsible for dialog control and synchronization.

Presentation Layer



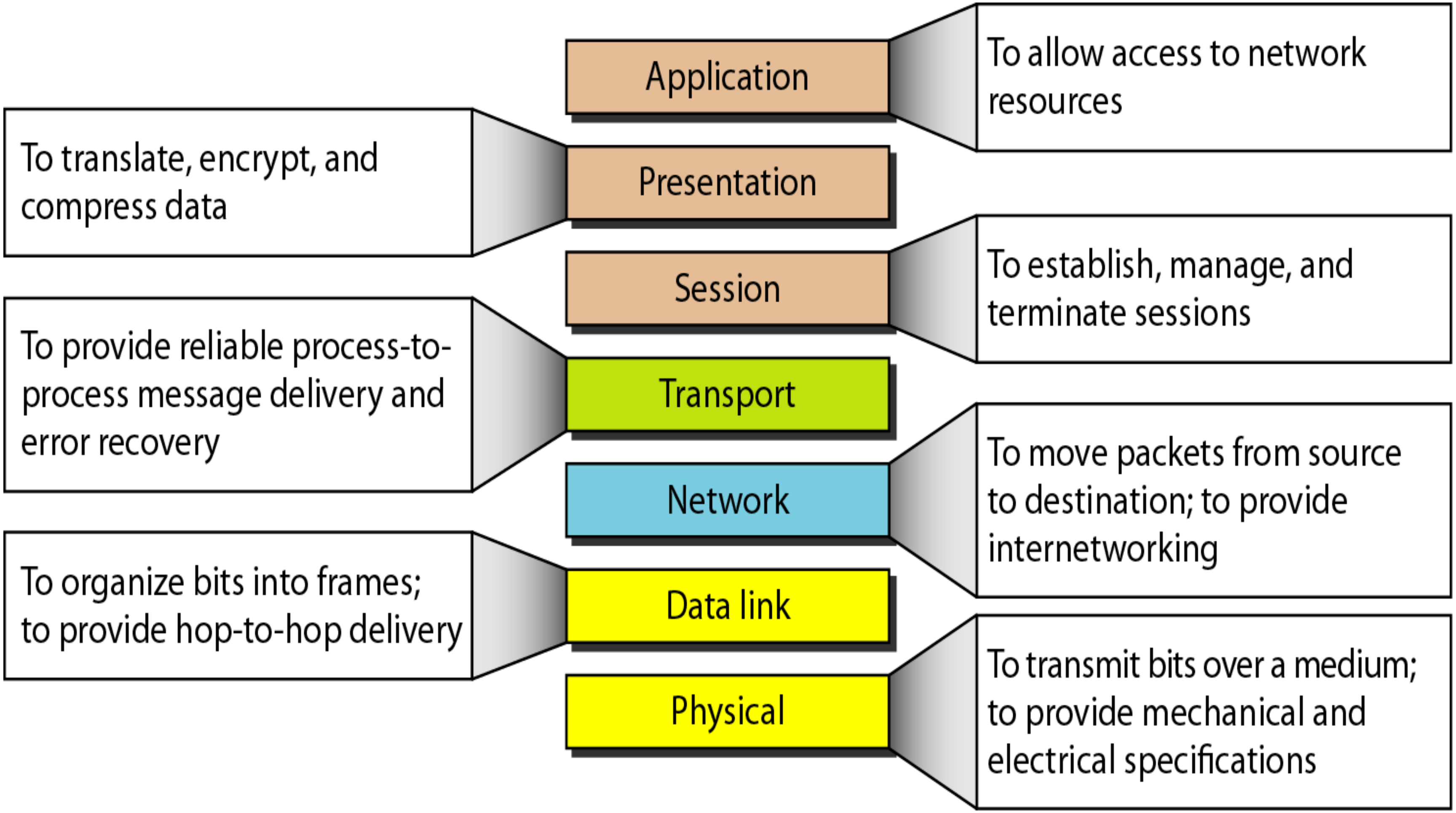
The presentation layer is responsible for translation, compression, and encryption.

Application Layer



The application layer is responsible for providing services to the user.

OSI Model



Application: To allow access to network resources

Presentation: To translate, encrypt, and compress data

Session: To establish, manage, and terminate sessions

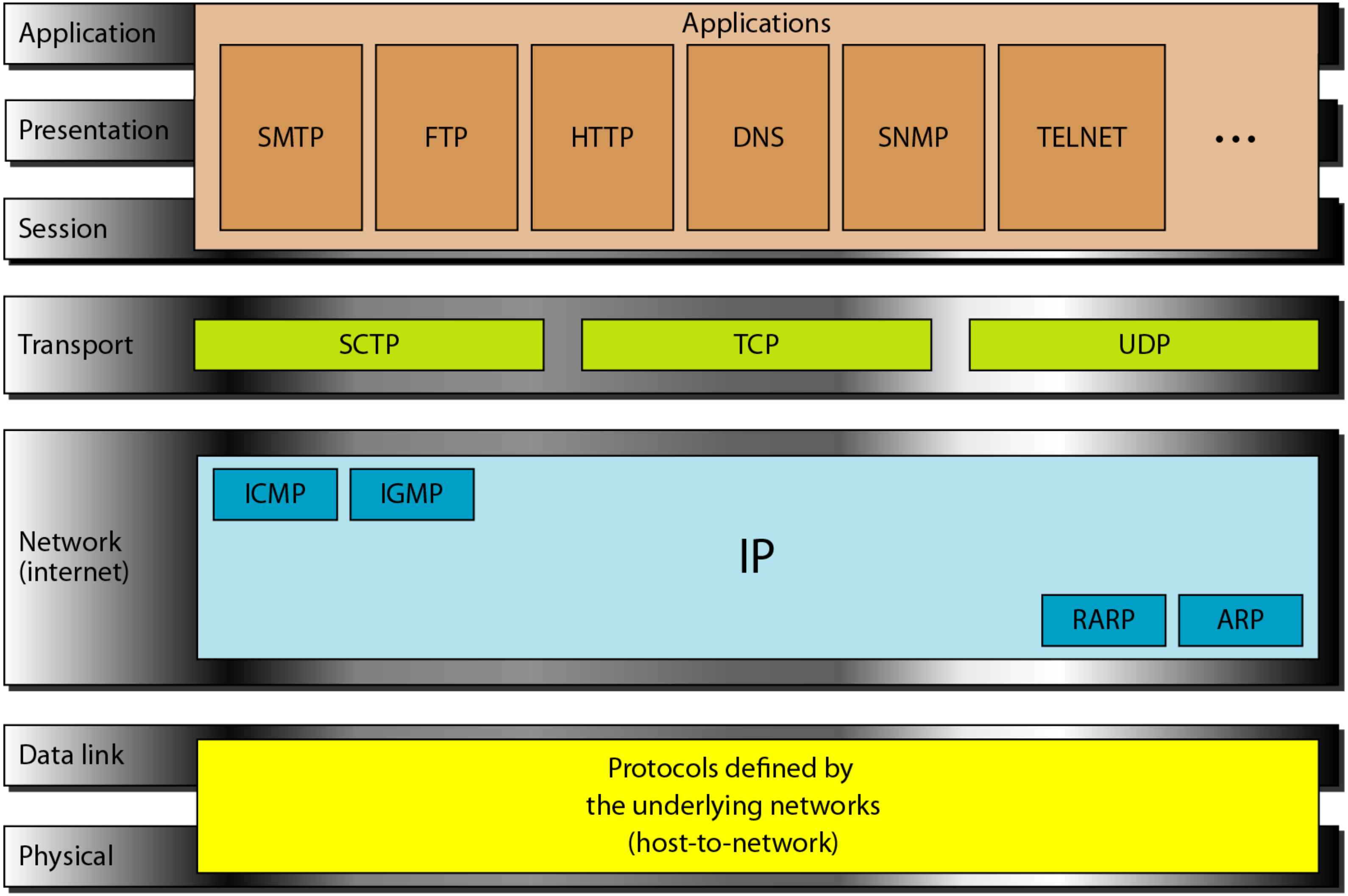
Transport: To provide reliable process-to-process message delivery and error recovery

Network: To move packets from source to destination; to provide internetworking

Data link: To organize bits into frames; to provide hop-to-hop delivery

Physical: To transmit bits over a medium; to provide mechanical and electrical specifications

TCP/IP & OSI Model

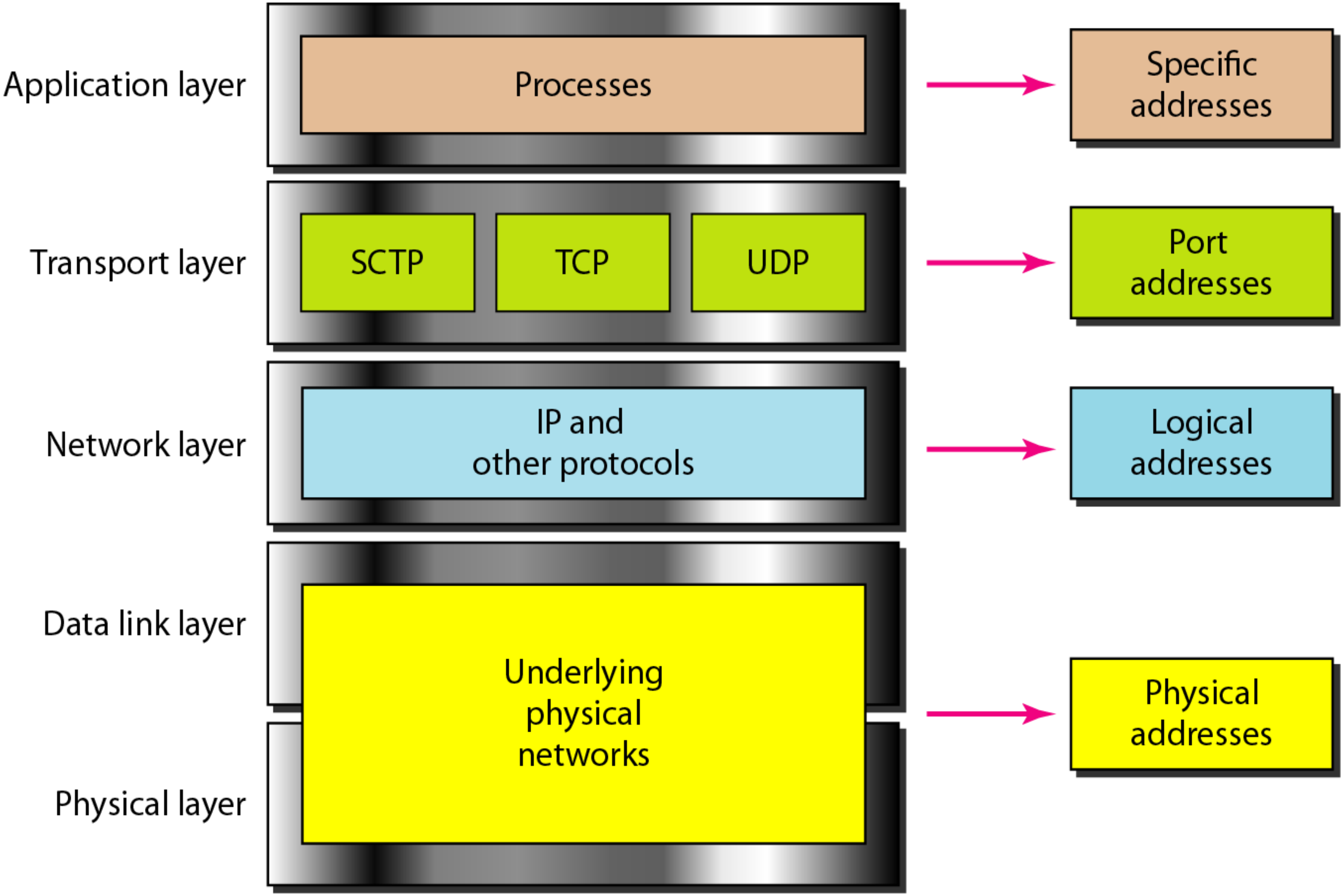


Addressing

Four types of addresses are used in an internet employing the TCP/IP protocols:

- Physical (MAC Address)
- Logical (IP address)
- Port
- Specific

Addressing

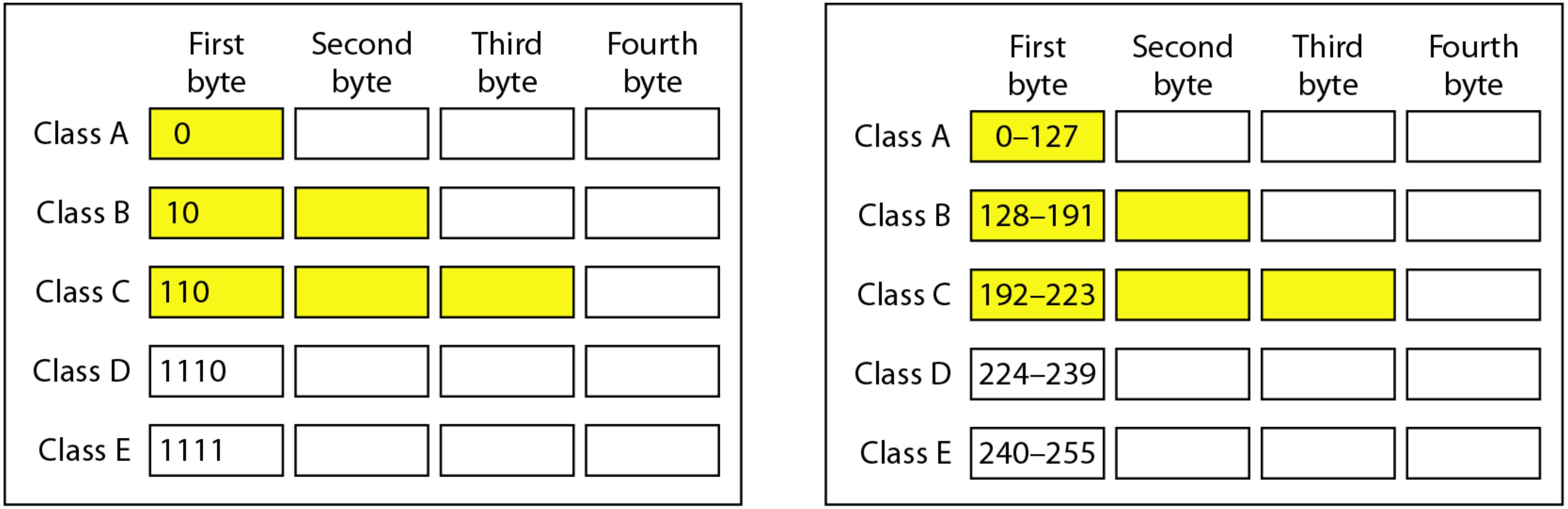

Application layer
Processes
Specific addresses
Transport layer
SCTP
TCP
UDP
Port addresses
Network layer
IP and other protocols
Logical addresses
Data link layer
Physical layer
Underlying physical networks
Physical addresses

Addressing

- Physical address identify the individual devices while logical address identify the connection of a host to its network.
- Each logical address is composed of 32 bits defining three fields:
  - Class type
  - Netid
  - hostid
- The IP addresses are unique and universal. The address space of IP is 2^{32} or 4,294,967,296.

Addressing

- In classful addressing, the address space is divided into five classes: A, B, C, D, and E.



	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–239			
Class E	240–255			

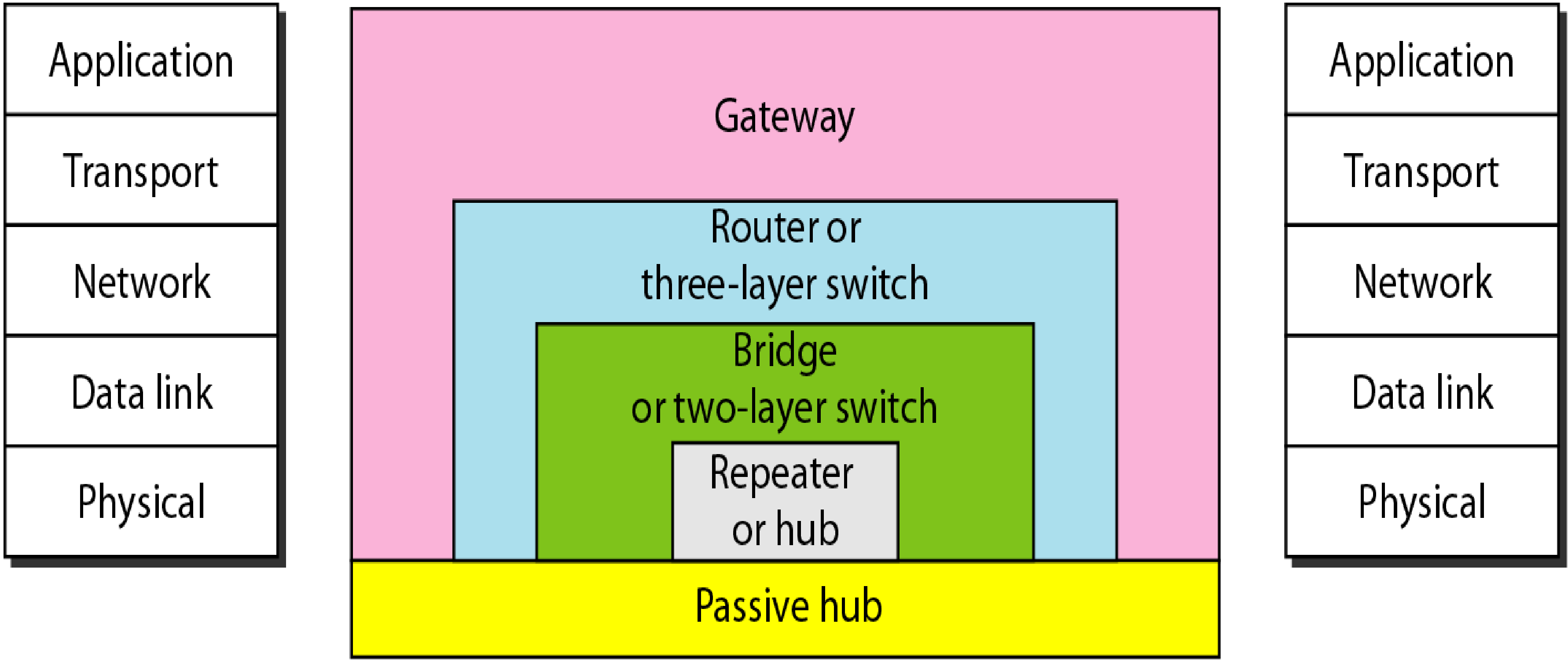
b. Dotted-decimal notation

Addressing

The physical addresses will change from node to node, but the logical addresses and port address remains usually remain the same.

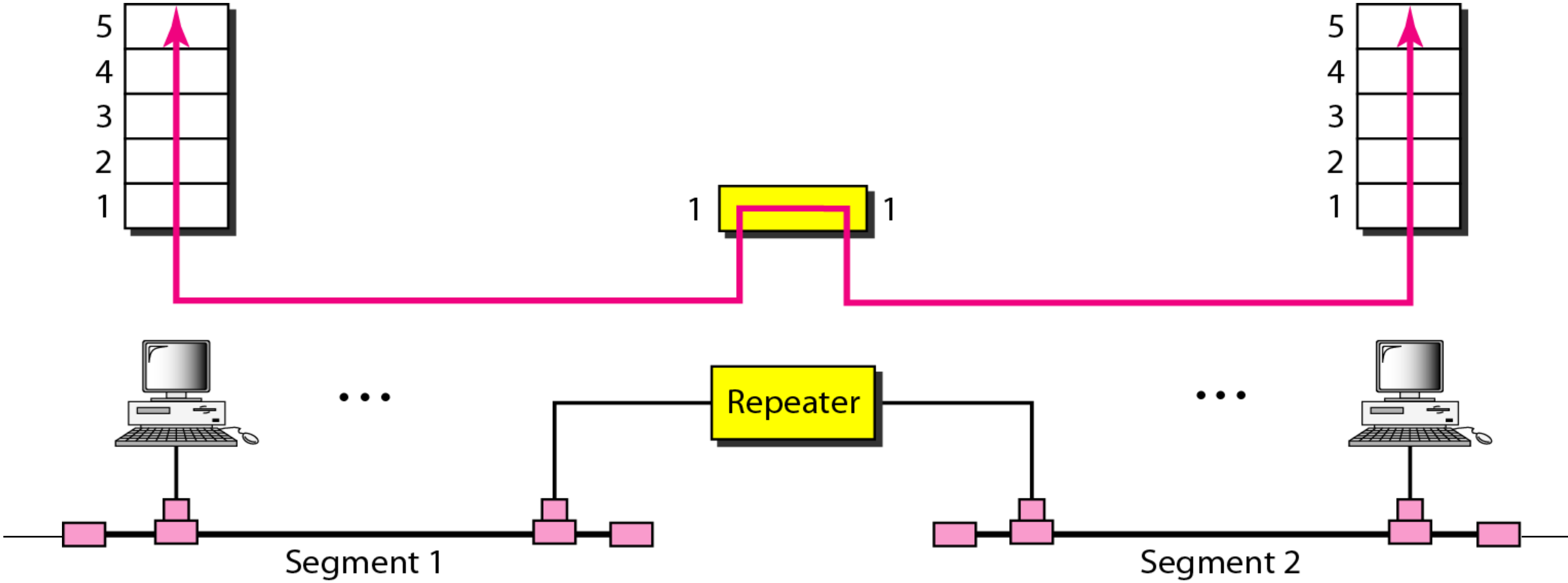
Networking Device

An internet is interconnection of individual networks which are connected by different devices. Based on the layer in which they operate in a network, connecting devices can be categorized into 5 different categories.



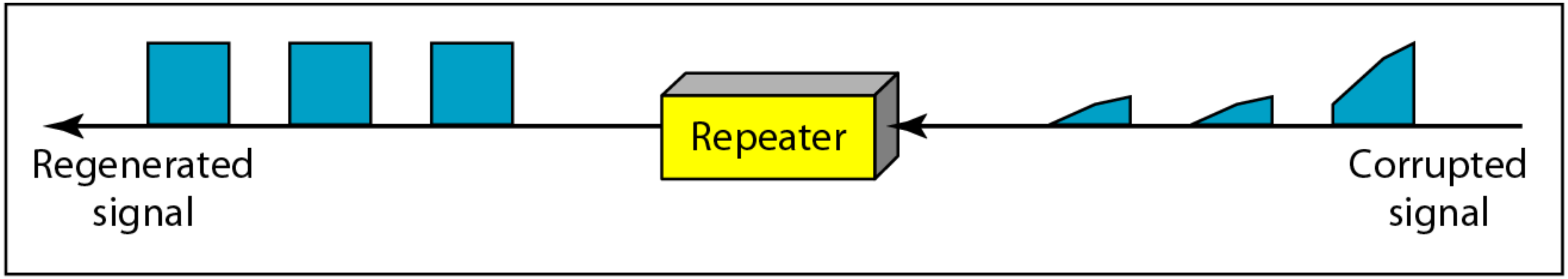
Networking Device

- Repeater act only upon the electrical components of a signal and are active only at the physical layer. Repeater allows us to extend the physical length of the network by regenerating the bit pattern. It does not have any intelligence (filter capability).

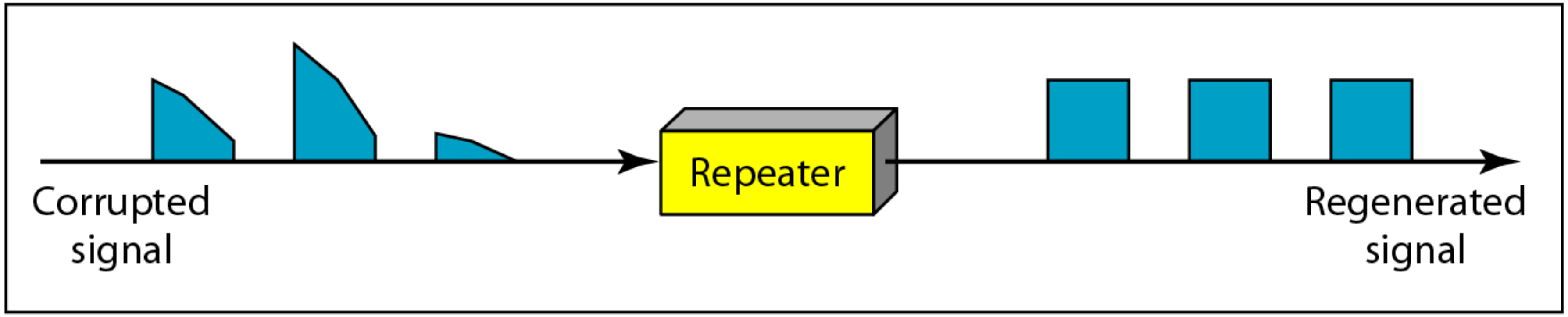


Networking Device

- Repeater is different from amplifier as it regenerates the signal while amplifier amplifies everything (signal & noise) fed to it.



a. Right-to-left transmission.

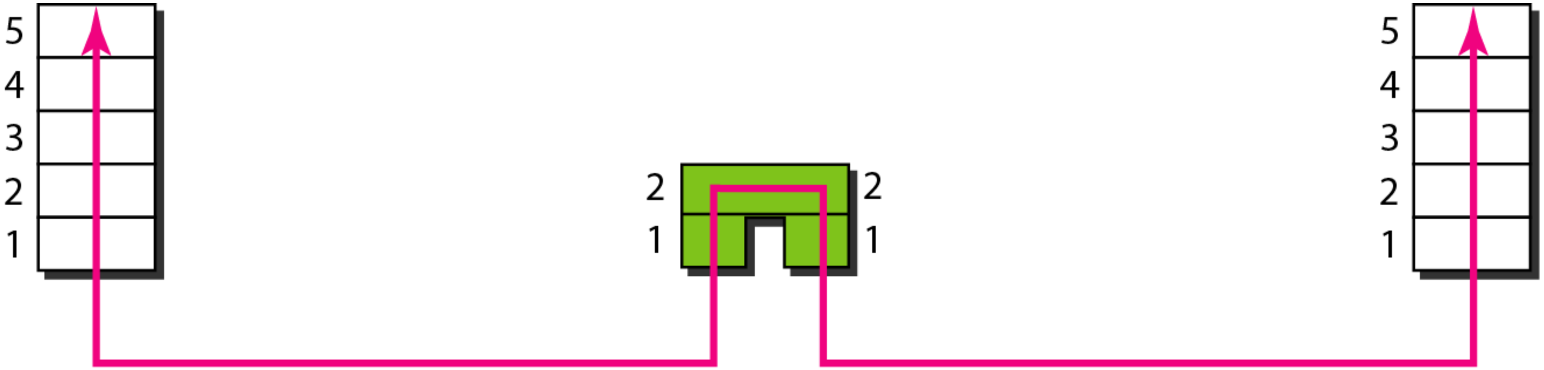


b. Left-to-right transmission.

Networking Device

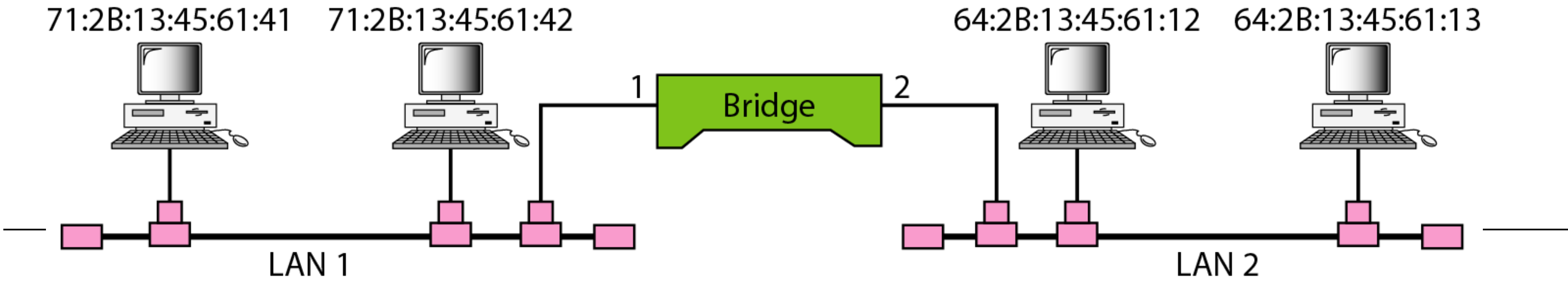
- Bridge uses the addressing protocol to access the physical address and most active at the data link layer.
- Bridge can divide a large network into smaller segments.
- Bridge contain logic (table used in filtering decision) that allows them to keep the traffic for each segment separate. This helps in congestion control and isolation.

Networking Device



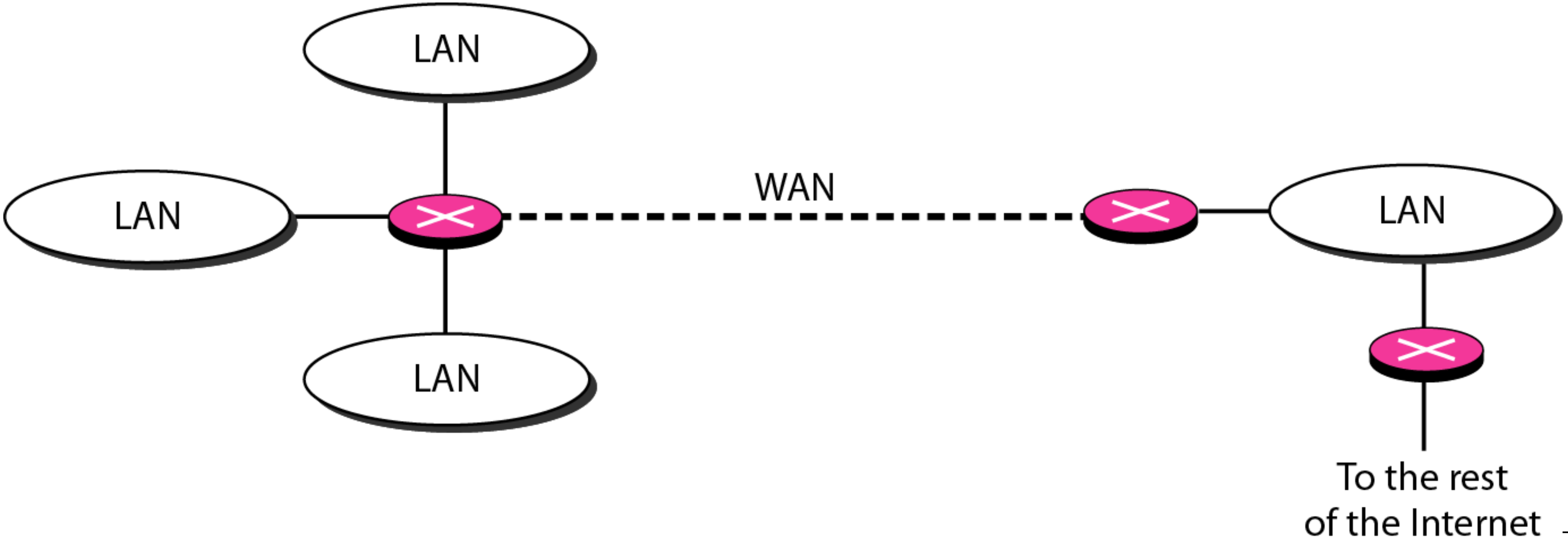
Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	1
64:2B:13:45:61:12	2
64:2B:13:45:61:13	2

Bridge Table



Networking Device

Router provides link between two separate networks using similar protocols and are most active at the network layer. They have access to network layer addresses (logical address) and contains software that enables them to determine which of several possible paths between those addresses is the best for a particular transmission.



Networking Device

Gateways provides translation service between incompatible networks or applications and are active in all the layers. Gateway is generally software installed within a router.

Networking Device

BASIS FOR COMPARISON	BRIDGE	SWITCH
Basic	A bridge can connect fewer LAN.	A switch can connect more networks compared to the bridge.
Buffer	Bridges do not have buffers.	Switch has a buffer for each link connected to it.
Types	Simple bridge, multiport bridge and transparent bridge.	Store-and-forward switch and cut-through switch.
Error	Bridges do not perform error checking.	Switches perform error checking.

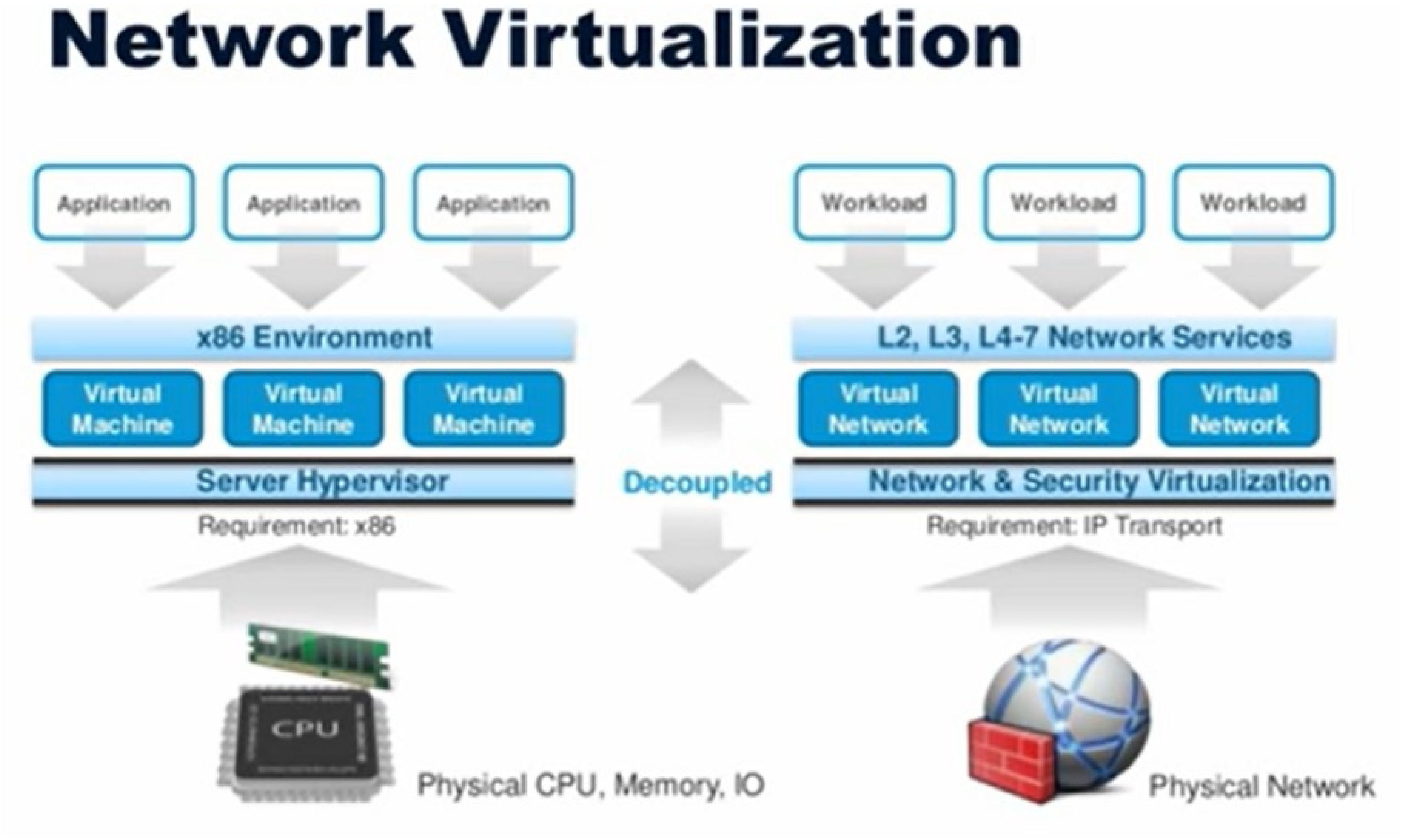
Networking Device

.No.	Hub	Switch
1.	It functions in a physical layer.	It functions in the data link layer.
2.	Switch allows packet switching.	There is a separate collision domain in the switch.
3.	Hub follows broadcast transmission.	Switch follows three i.e., multicast, unicast, and broadcast type transmission.
4.	In Hub, half duplex transmission technique is utilized.	In switch, full duplex transmission technique is utilized.
5.	Hub does not allow packet filtering.	Switch allows packet switching.
6.	There can be 4 ports in Hub.	24 to 28 ports contained by a Switch.

What is Network Virtualization (NV)

- Network Virtualization (NV) refers to abstracting network resources.
- Traditionally these resources are delivered in the form of hardware but through NV these resources are delivered in the form of software.
- It can also divide one physical network into separate, independent virtual networks.

What is Network Virtualization (NV)



Why Network Virtualization (NV)

- Network virtualization is rewriting the rules for the way services are delivered.
- This approach moves networks from static, inflexible, and inefficient to dynamic, agile, and optimized.
- Modern networks must keep up with the demands for cloud-hosted, distributed apps, and the increasing threats of cybercriminals while delivering the speed and agility you need for faster time to market for your applications.
- With network virtualization, you can forget about spending days or weeks provisioning the infrastructure to support a new application. Apps can be deployed or updated in minutes for rapid time to value.

Advantages of N/w Virtualization

Network virtualization helps organizations achieve major advances in speed, agility, and security by automating and simplifying many of the processes that go into running a data center network and managing networking and security in the cloud. Here are some of the key benefits of network virtualization:

- Flexibility
- Reduce network provisioning time from weeks to minutes
- Place and move workloads independently of physical topology
- Scalability
- Manageability
- Security & Isolation
- Programmability
- Heterogeneity

https://youtu.be/HFQdbOY8Ams

How does N/w Virtualization work

- Network virtualization decouples network services from the underlying hardware and allows virtual provisioning of an entire network.
- It makes it possible to programmatically create, provision, and manage networks all in software, while continuing to leverage the underlying physical network as the packet-forwarding backplane.
- Physical network resources, such as switching, routing, firewalling, load balancing, virtual private networks (VPNs), and more, are pooled, delivered in software, and require only Internet Protocol (IP) packet forwarding from the underlying physical network.

How does N/w Virtualization work

- Network and security services in software are distributed to a virtual layer (hypervisors, in the data center) and “attached” to individual workloads, such as your virtual machines (VMs) or containers, in accordance with networking and security policies defined for each connected application.
- When a workload is moved to another host, network services and security policies move with it.
- When new workloads are created to scale an application, necessary policies are dynamically applied to these new workloads, providing greater policy consistency and network agility.

How does N/w Virtualization work

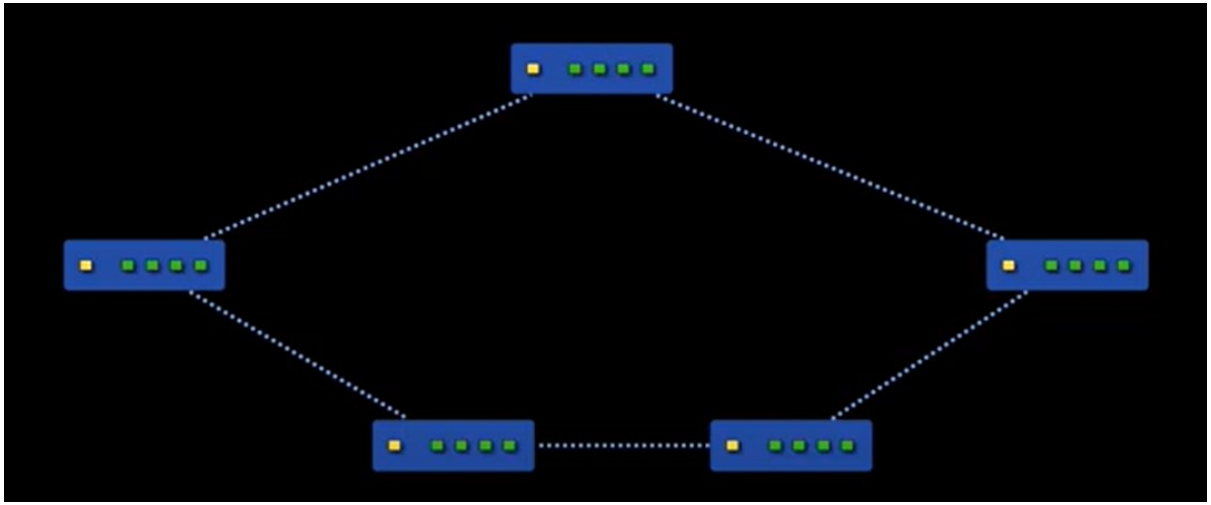
There are two ways to implement network virtualization:

- Software-defined networking (SDN) https://youtu.be/lfqQhRkL4Vo
- Network functions virtualization (NFV) https://youtu.be/xGZaZTnvR9A

Software-defined networking (SDN)

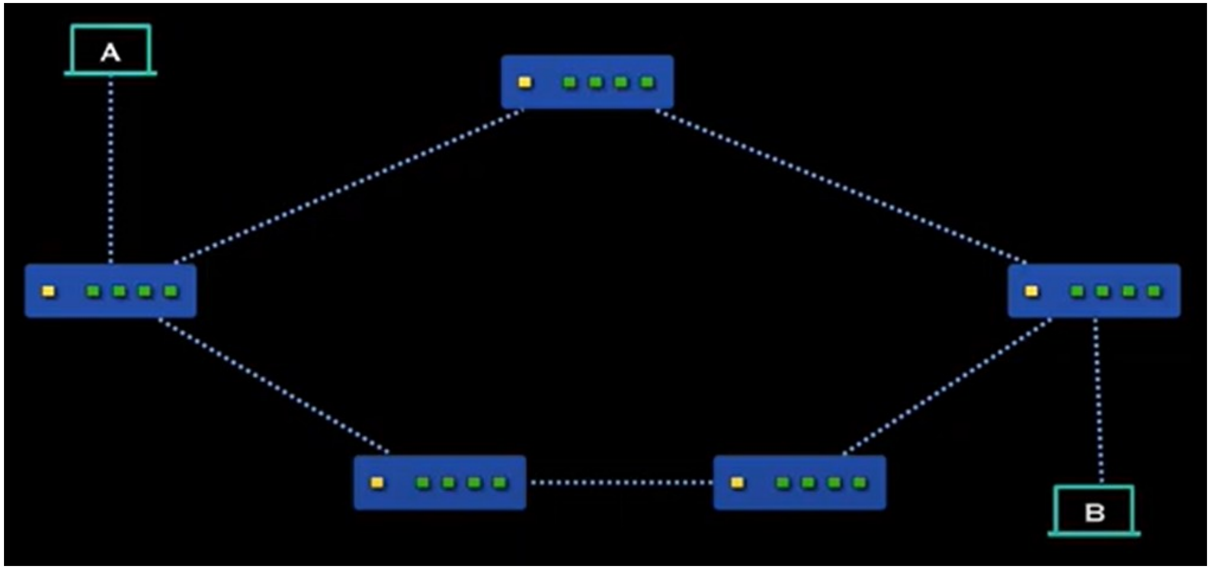
- Software-defined networking (SDN) manages networks by separating the **control plane** from the **data forwarding plane**.
- Architects and administrators use software to configure and manage network functions via a centralized **control plane**.
- This approach creates dynamic, agile, and scalable networks that use the virtualized infrastructure of modern data centers to respond rapidly to changing business requirements.

Software-defined networking (SDN)



- Scenario of traditional network connecting multiple networks using routers.

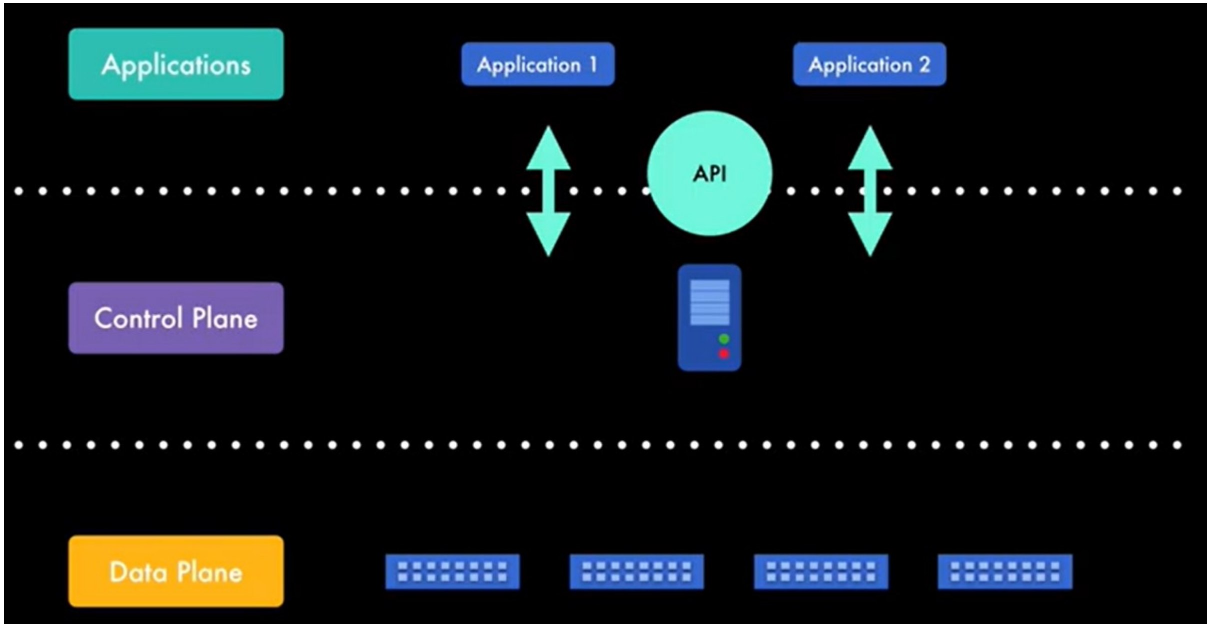
Software-defined networking (SDN)



Router does two important Functions:

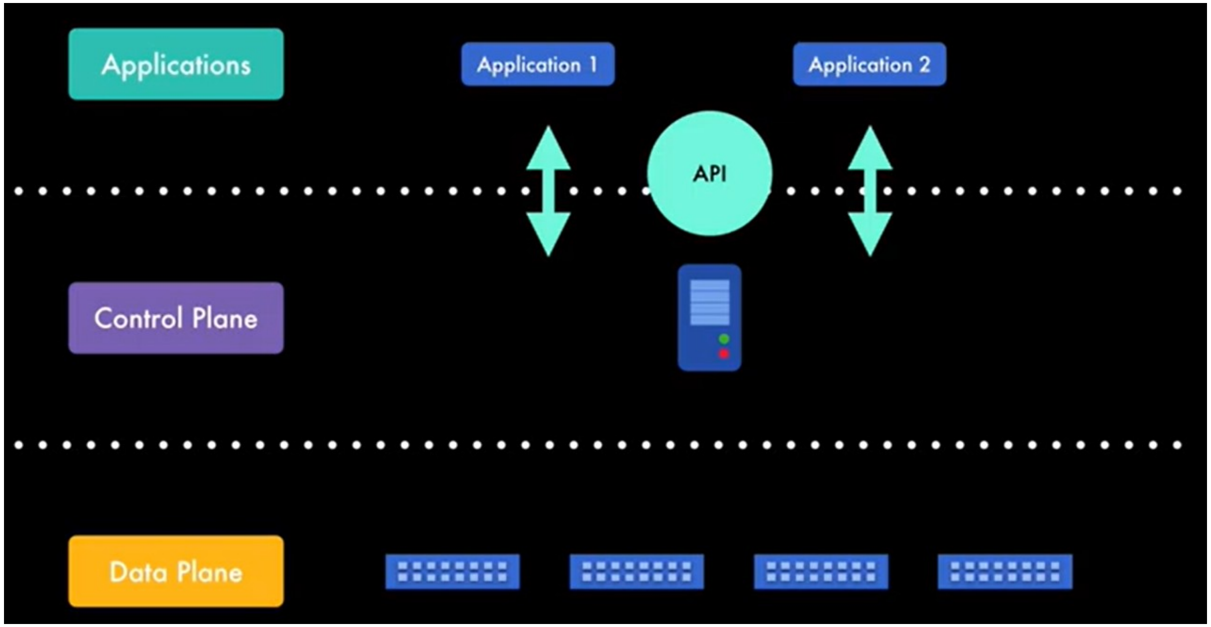
- Find the best path for taking data from computer A to computer B by learning the network topology and updating the routing table. This function is performed by the **control plane** of the router.
- Forward the actual data packets to the next device on the address of the destination machine. This function is performed by the **data plane** of the router.

Software-defined networking (SDN)



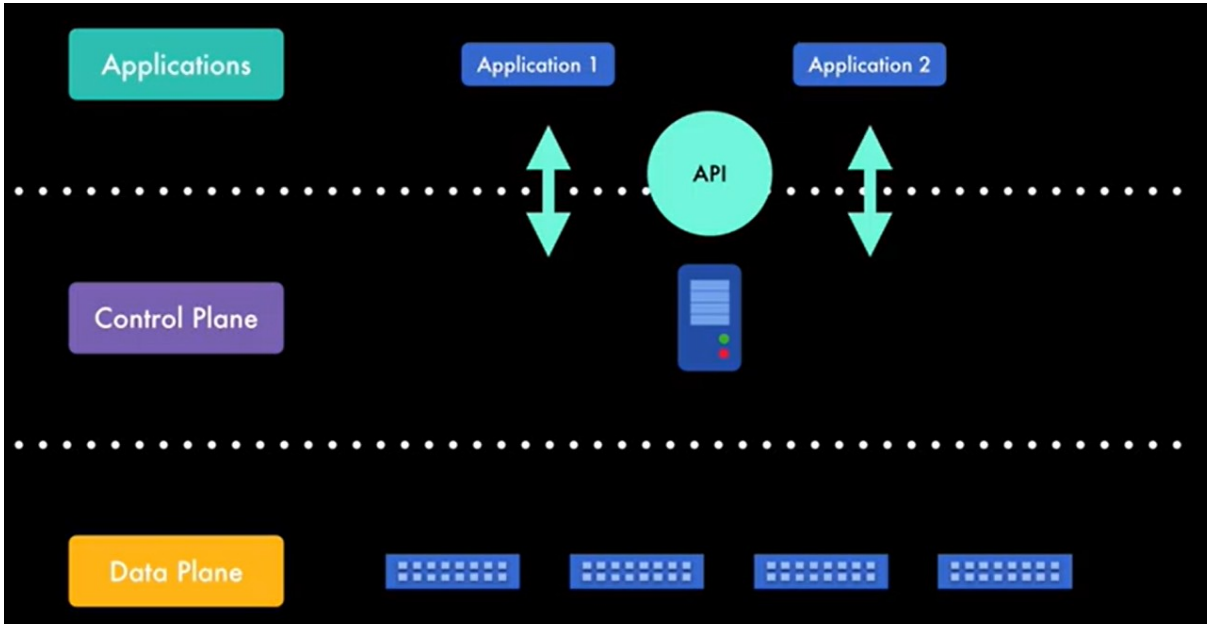
- Traditional routers have both data plane and control plane functionality running in the same hardware.
- In software defined network, control plant and data plane functionality are imparted in different devices.

Software-defined networking (SDN)



- Data plane functionality is imparted in the SDN switches. These are less expensive hardware then the traditional routers.
- Control plane functionality are provided by controller. The primary function of controller is to identify the route and update the flow table in SDN switches.

Software-defined networking (SDN)



- Controller talk to SDN switches through open flow API and it can update the flow table entries in each of these SDN switches. These APIs are called southbound API.
- Controller also provides API for the application to communicate. These APIs are called northbound APIs.
- Applications can dynamically provide the instruction to the controller and controller can update the flow table in SDN switches accordingly.

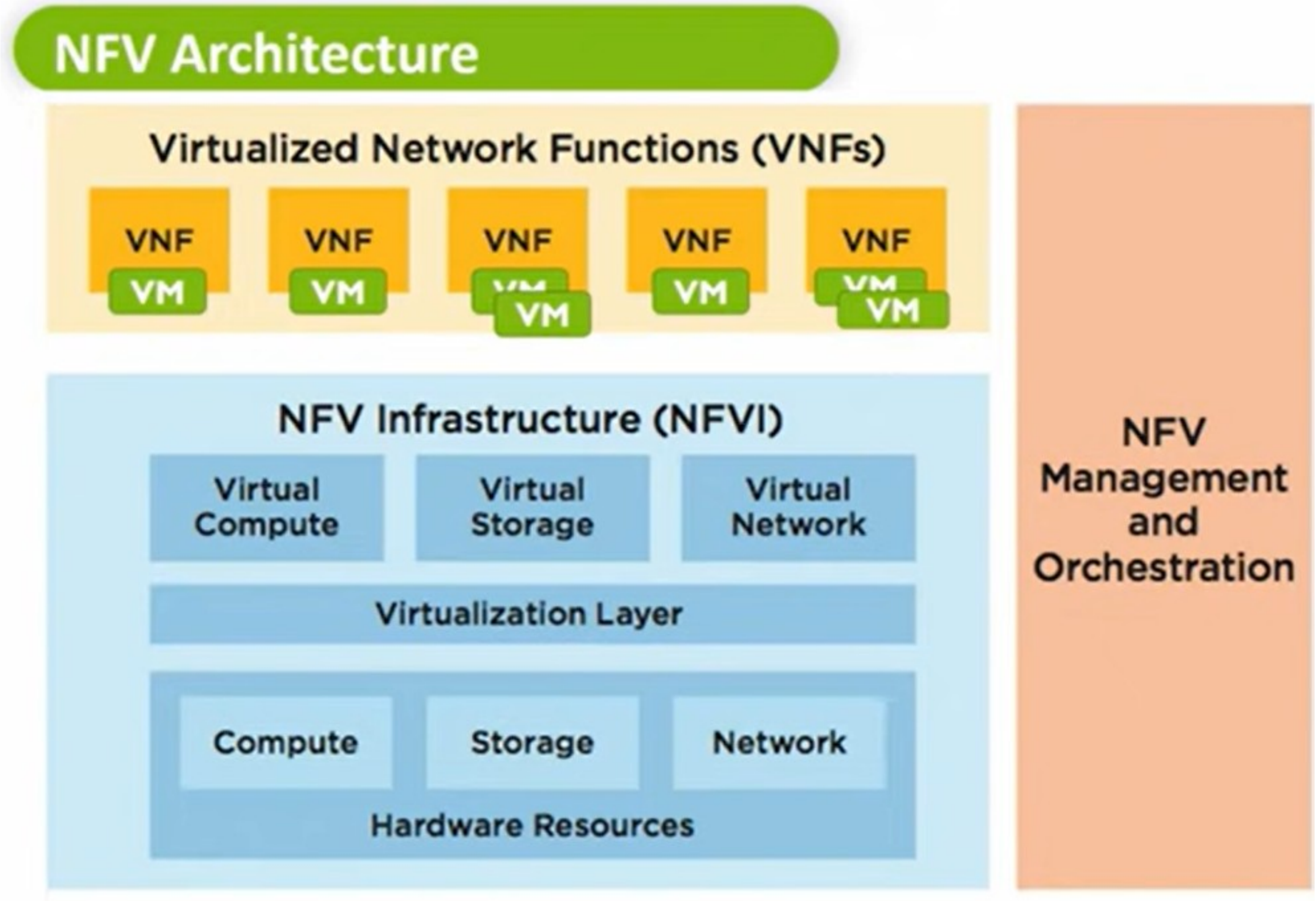
Network functions virtualization (NFV)

- Network functions virtualization (NFV) is a way to virtualize network services like routers, firewalls, load balancer etc. that have traditionally been run on the proprietary hardware.
- These services are packaged as virtual machine on commodity hardware, which allows the service provider to run their network on standard servers instead of proprietary ones.
- These virtual network functions (VNF) run on high-performance x86 servers and offer the distinct advantage of on-demand deployment.
- NFV provides the infrastructure on which SDN can run.

Network functions virtualization (NFV)

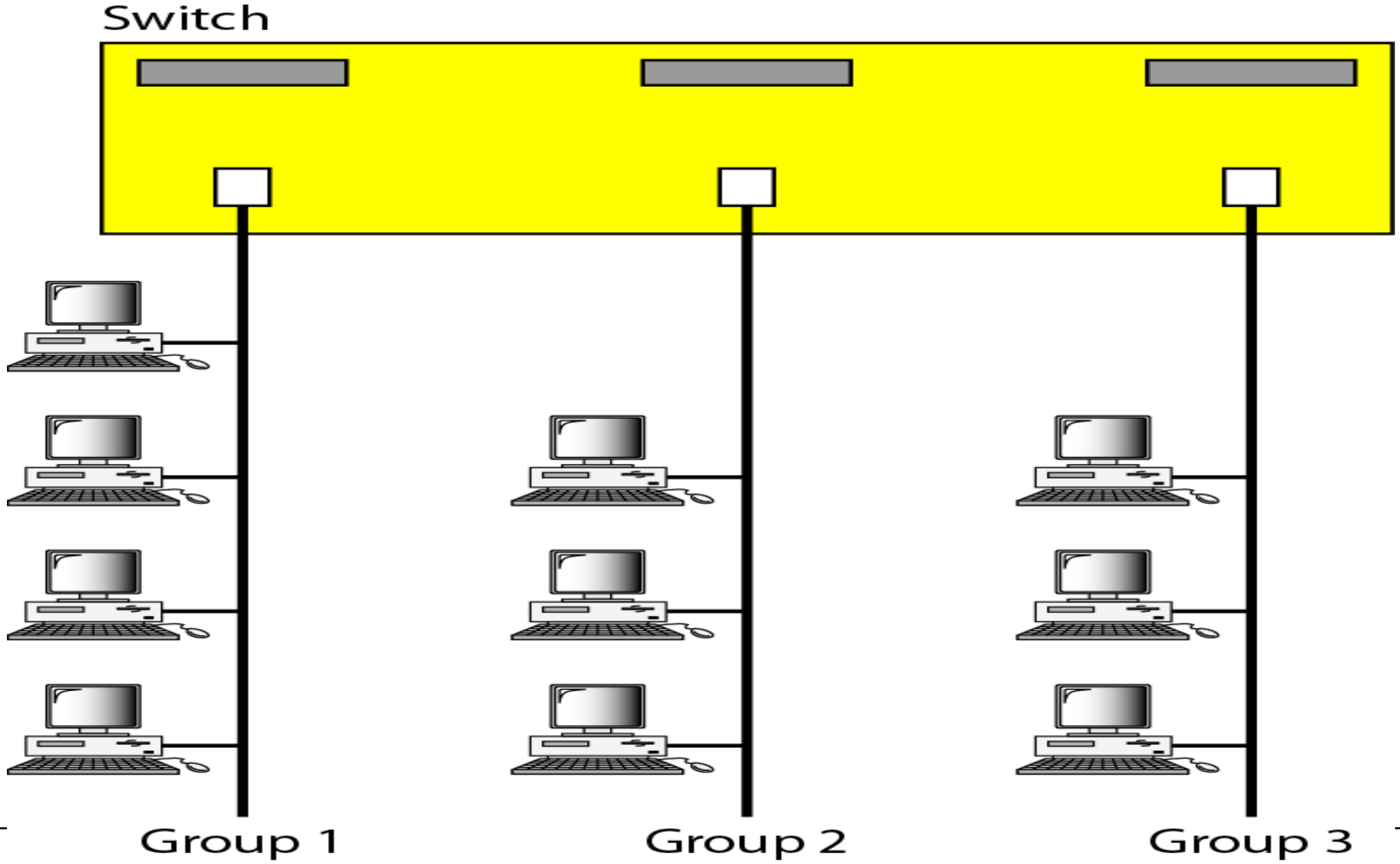
- NFC is composed of three main components:
  - **Virtualized Network Functions (VNF):** Provides the s/w implementation of network function which can run over NFVI
  - **NFV infrastructure (NFVI):** provide different resources like network, storage, compute in virtualized form
  - **NFV management & Orchestration**: IT deals with the virtualization management task which covers life cycle management of physical and/or s/w resources that supports infrastructure virtualization and life cycle management of VNFs.

Network functions virtualization (NFV)



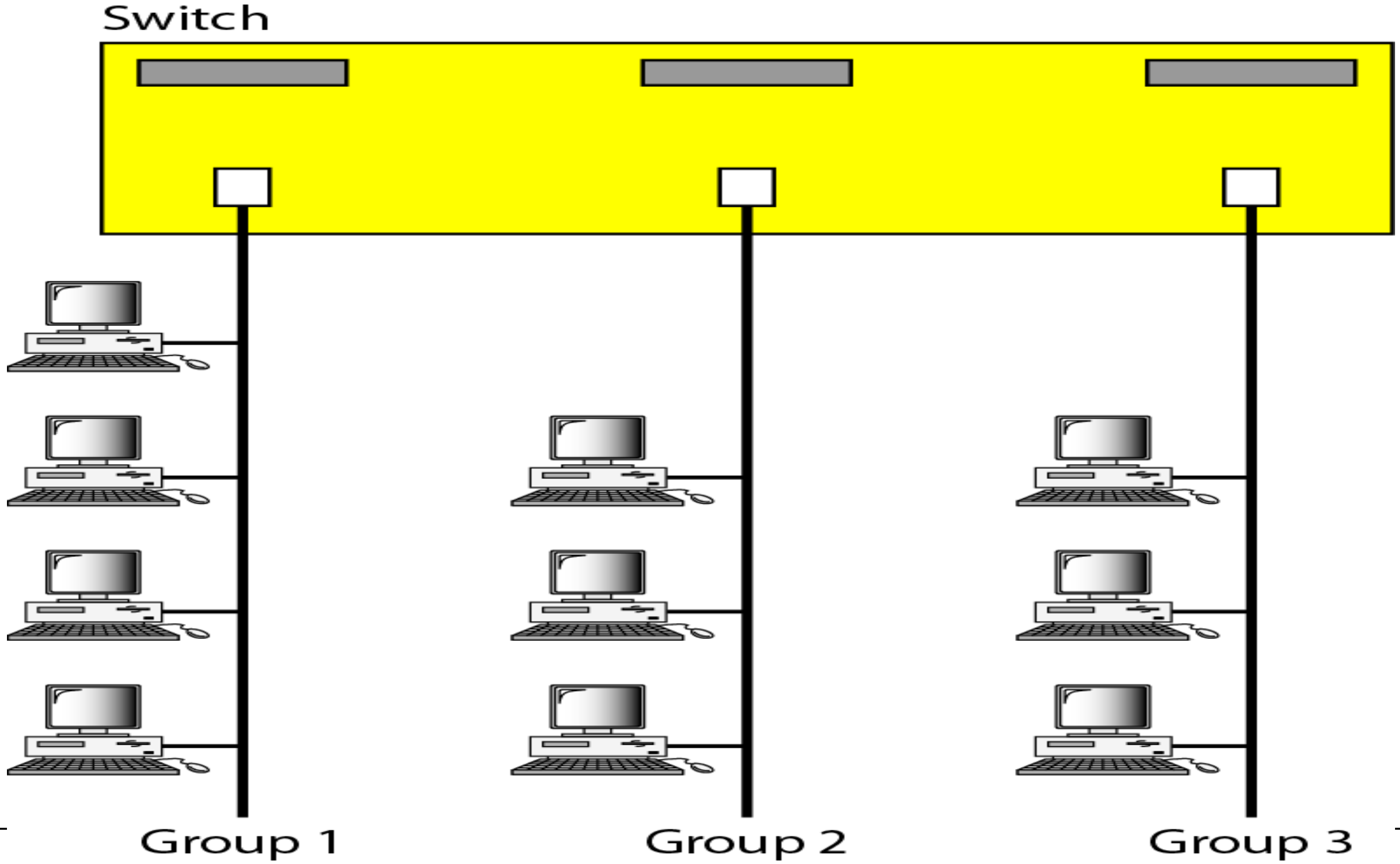
Virtual LAN (VLAN)

VLAN is a subnetwork or segment of LAN configured by software not by physical wiring.



Virtual LAN (VLAN)

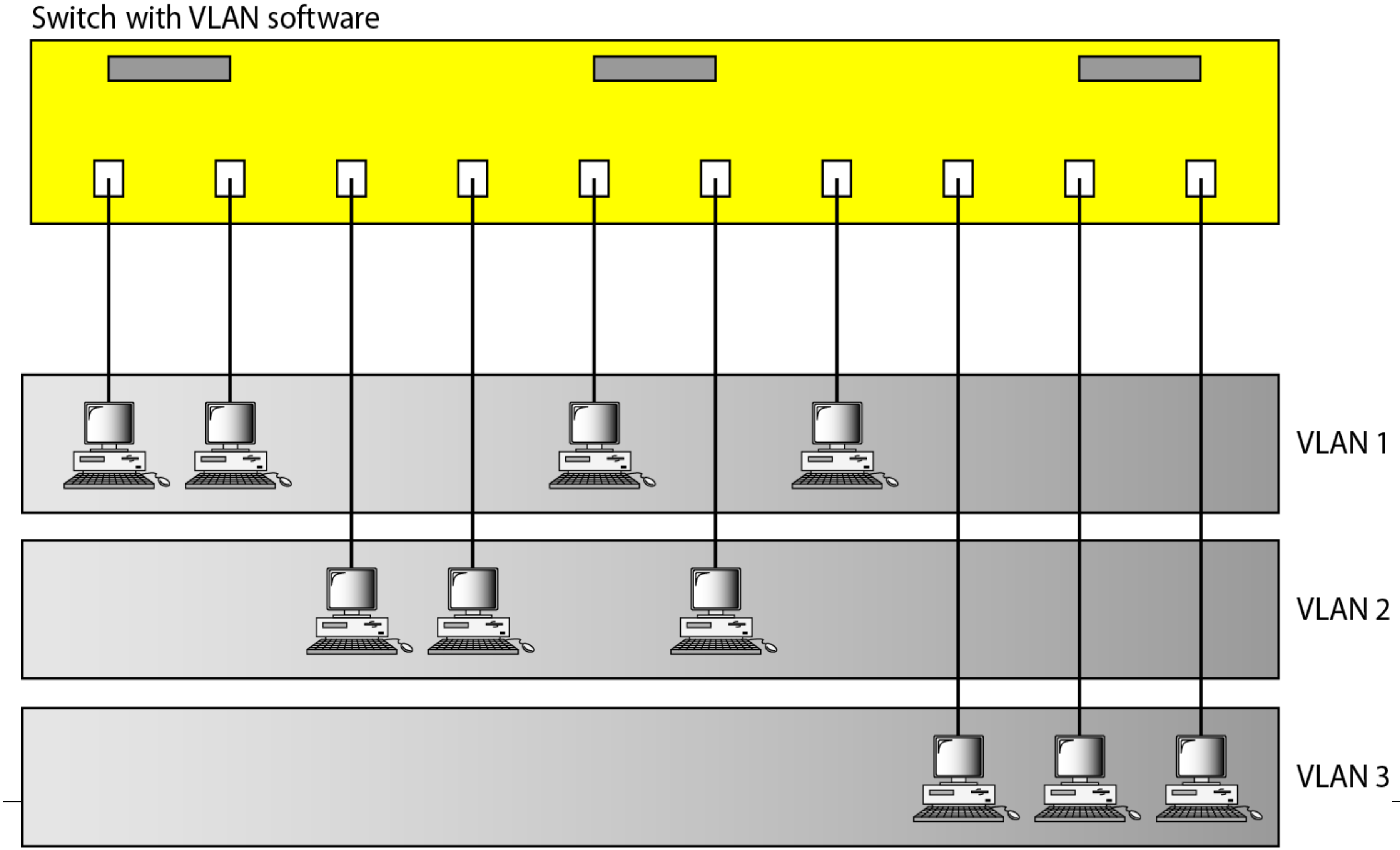
In a switched LAN, changes in the workgroup means physical changes in the network configuration.



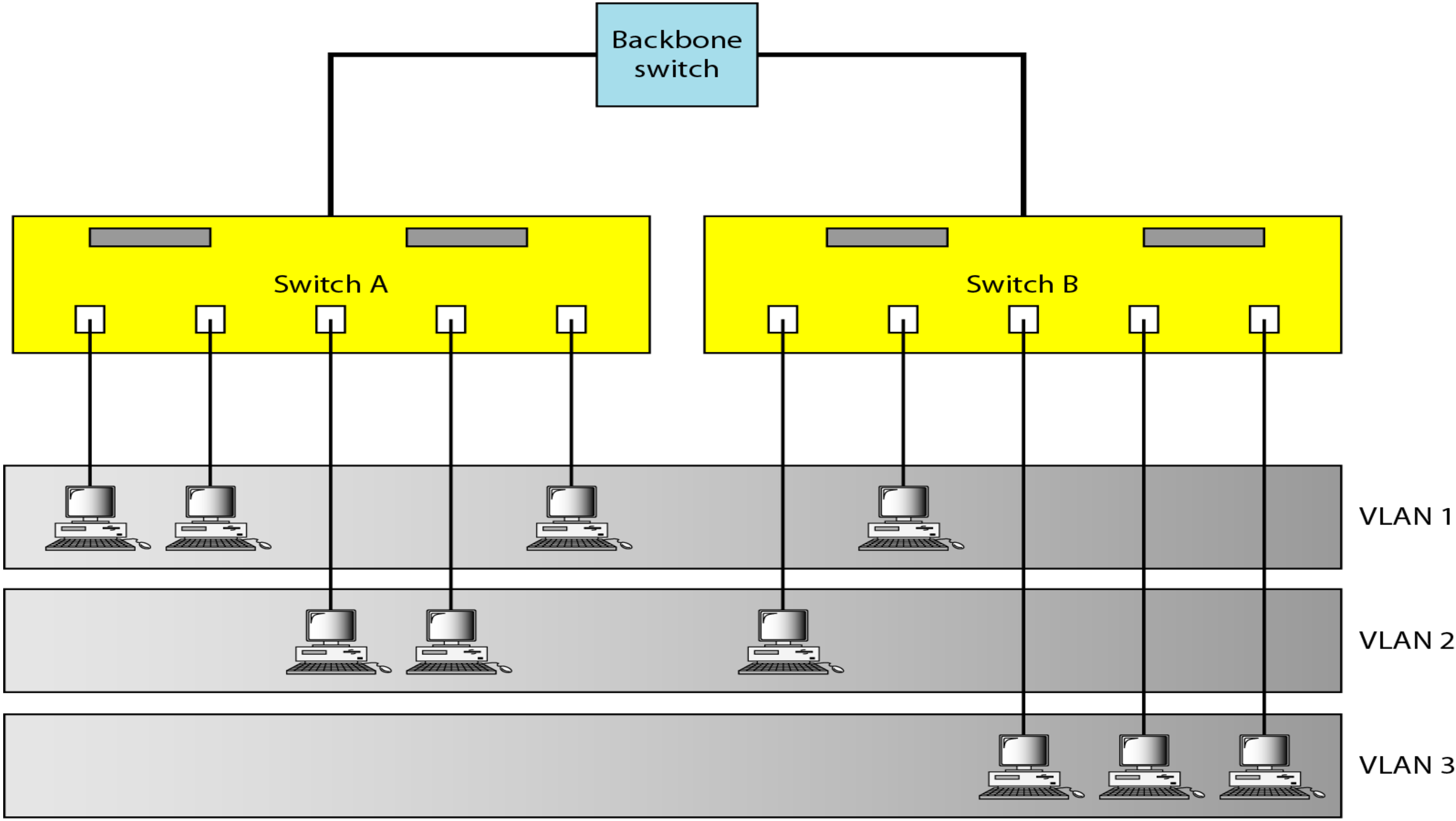
Virtual LAN (VLAN)

- The whole idea of VLAN technology is to divide a LAN into logical, instead of physical, segments.
- A LAN can be divided into several logical LANs called VLANs. Each VLAN is a work group in the organization.
- If a person moves from one group to another, there is no need to change the physical configuration. The group membership in VLANs is defined by software, not hardware.
- Any station can be logically moved to another VLAN. All members belonging to a VLAN can receive broadcast messages sent to that particular VLAN.
- VLAN creates broadcast domains.
- VLANs group stations belonging to one or more physical LANs into broadcast domains. T
- he stations in a VLAN communicate with one another as though they belonged to a physical segment.

Virtual LAN (VLAN)



Virtual LAN (VLAN)



https://youtu.be/jC6MJTh9fRE

Virtual LAN (VLAN)

- Membership: Vendors use different characteristics such as port numbers, MAC addresses, IP addresses, or a combination of two or more of these for grouping of stations in one VLAN.
- Configuration: How are the stations grouped into different VLANs? Stations are configured in one of three ways: manual, semiautomatic, and automatic.
- Advantages:
  - Cost & Time reduction
  - Security
  - Creating virtual workgroups

Virtual Private Network (VPN)

- Security is an important aspect of network communications.
- Information may be completely useless if it cannot be transmitted with the right levels of confidentiality.
- This kind of information includes but is not limited to confidential company data, sensitive private information, finance data, medical transactions and others.
- The public network is insecure. By default, all the data transmitted over the public network, or the internet can be seen or modified by anyone.
- The end-users or the communicating parties (communication endpoints) must take special steps to encrypt the communication at their end to ensure confidentiality of data.
- Also, the parties can setup a continuous encrypted channel to communicate or share data on a continuous basis.
- This channel is generally destroyed once the communication session is completed. The channel can be later established again between the parties to share information

Virtual Private Network (VPN)

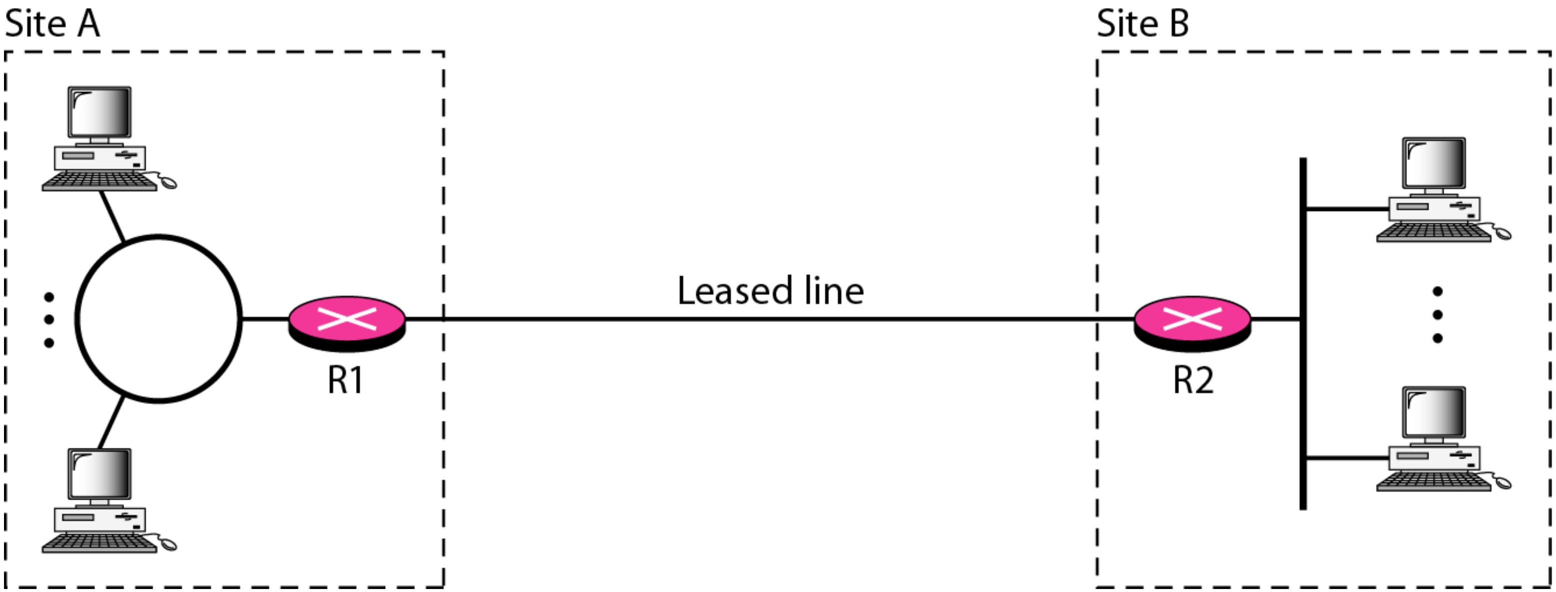
- Use of intermediate network hardware – routers to encrypt and decrypt the data on the channel. The end-user computers(or endpoints) do not require any special software or hardware to set up the secure channel.
- Use of end-user software or hardware clients – In this case, a secure server is set up at the destination and a secure client is set up at the client-end. The client can communicate or connect to the network at the server end by establishing a connection with the ecure-server.

Virtual Private Network (VPN)

- The security of this channel can be achieved in various ways.
- VPN is a technology to set up a secure channel over publicly insecure internet.
- VPN is a technology that is gaining popularity among large organizations that use the global internet as both intra and inter organization media but require privacy in their intra organization communication.
- Three strategies are there to achieve privacy during intra organization:
  - Private network
  - Hybrid network
  - VPN

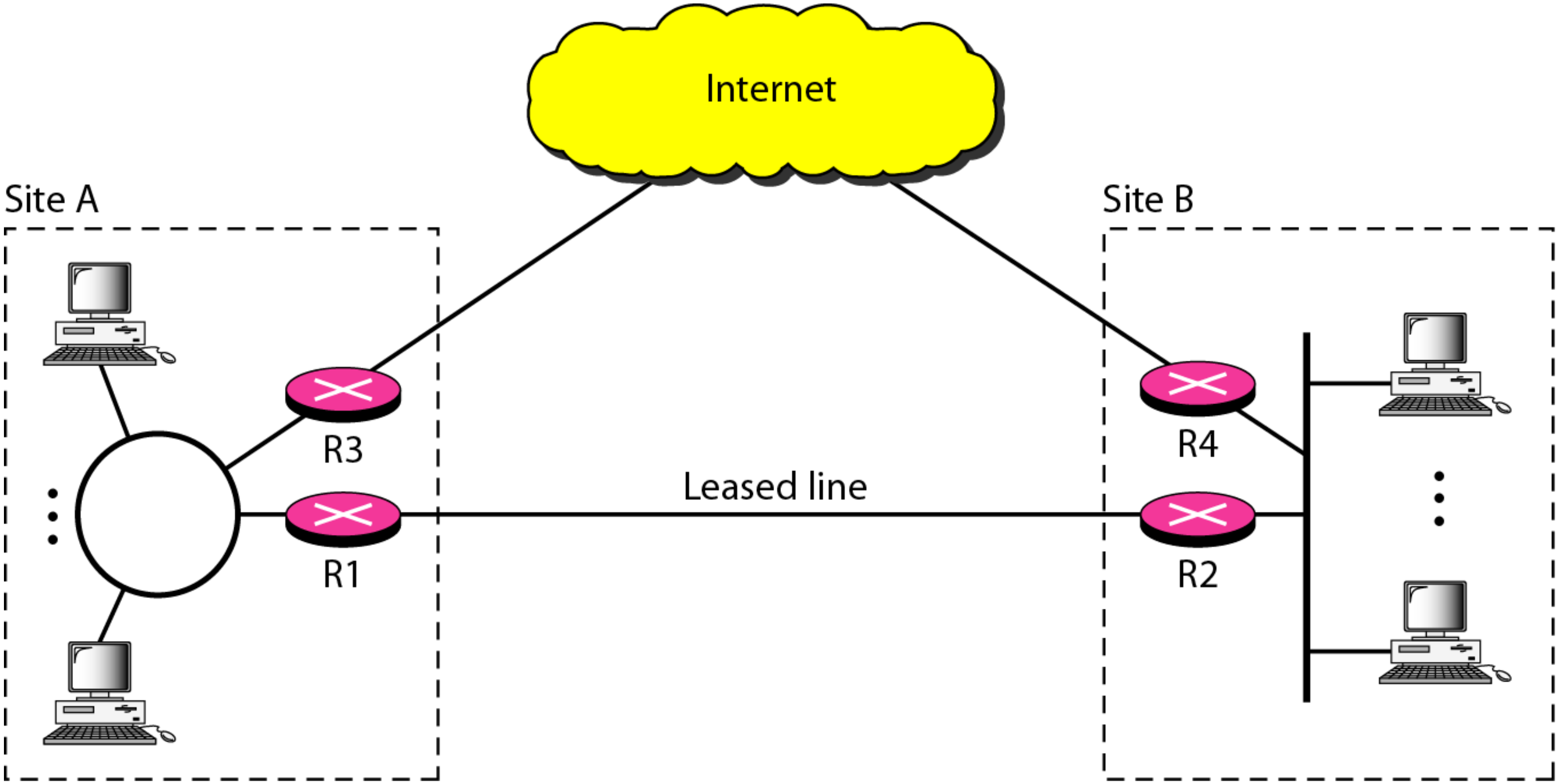
Virtual Private Network (VPN)

- Private network



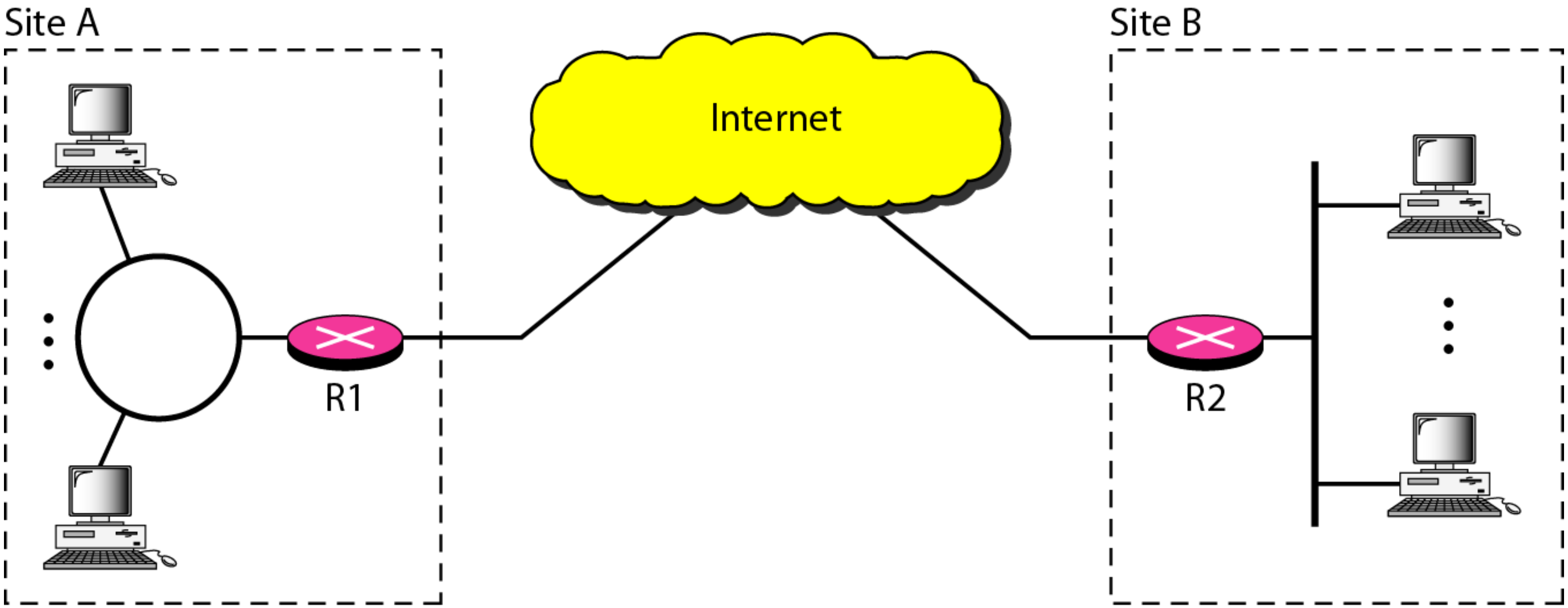
Virtual Private Network (VPN)

- Hybrid network



Virtual Private Network (VPN)

- VPN: Both private and hybrid networks have a major drawback of cost. One solution is to use VPN while using global internet for both private and public communication.



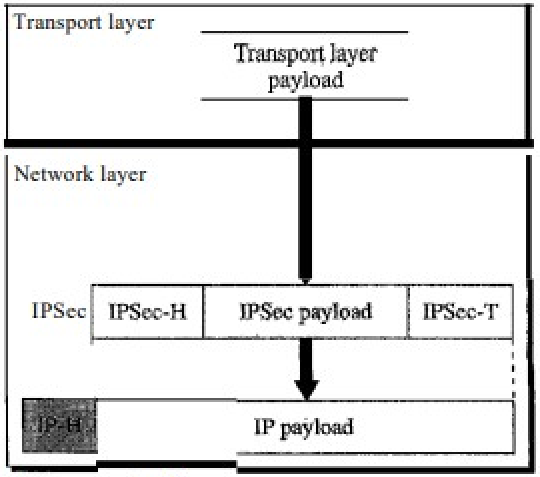
- VPN creates a network that is private but virtual.
- It is private because it guarantees privacy inside the organization.
- It is virtual because it does not use real private WAN, the network is physically public but virtually private.

Virtual Private Network (VPN)

- Using IPSec (IP security) protocol, we can ensure encryption, authentication, and tunneling in VPN.
- IPSec is a collection of protocols to provide security for a packet while transferring over Internet.
- IPSec does not stipulate the use of any specific encryption or authentication method. User can choose any encryption decryption protocol of their choice. It just provides a framework.
- IPSec can be implemented in two modes:
  - Transport mode
  - Tunneling mode

Virtual Private Network (VPN)

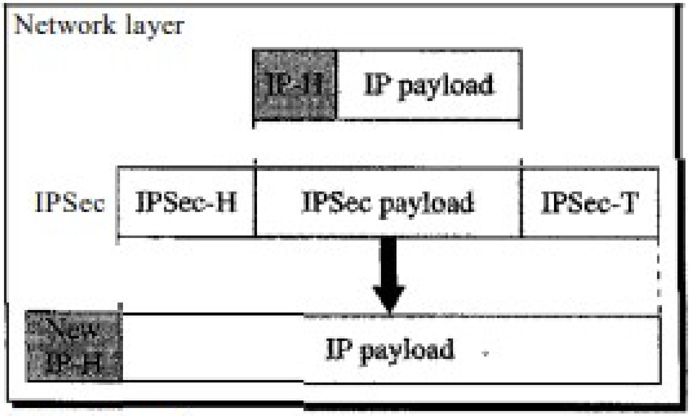
- IPSec in the transport mode does not protect the IP header; it only protects the information coming from the transport layer.
- The transport mode is normally used when we need host-to-host (end-to-end) protection of data.
- The sending host uses IPSec to authenticate and/or encrypt the payload delivered from the transport layer.
- The receiving host uses IPSec to check the authentication and/or decrypt the IP packet and deliver it to the transport layer



a. Transport mode

Virtual Private Network (VPN)

- In the tunnel mode, IPSec protects the entire IP packet. It takes an IP packet, including the header, applies IPSec security methods to the entire packet, and then adds a new IP header.
- The new IP header, has different information than the original IP header. The tunnel mode is normally used between two routers, between a host and a router, or between a router and a host.
- In other words, we use the tunnel mode when either the sender or the receiver is not a host. The entire original packet is protected from intrusion between the sender and the receiver.



b. Tunnel mode

- https://www.youtube.com/watch?v=sr2-K6AaHNI