

Module 1

Computer Networks Fundamentals

Prepared by Dr. Manal Mizher

Lecture 1



Network programming

Course ID: CYB615



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Our course (CYB615) Topics:

Module 1: Computer Networks Fundamentals.

Module 2: Computer Networks Protocols (TCP/UDP/IP/ICMP).

Module 3: Quality of Service.

Module 4: Middleboxes.

Module 5: Network Security.

Required Textbook: Goerzen J., Foundations of Python Network Programming, 2004, Course Technology, Apress, ISBN: 978-1-59059-371-4.

References:

- The official Python Tutorial: <http://docs.python.org/tut/>
- The Python Tutorial: <https://docs.python.org/3/tutorial/>



Our course (Network programming, Course ID: CYB615)

Explores network programming in the Python language. It covers the basic concepts, modules, and third-party libraries that you are likely to use when communicating with remote machines using the most popular Internet communication protocols.

The Building Blocks: Stacks and Libraries

1. **Protocol stack**, is a group of protocols that all work together to allow software or hardware to perform a function. The TCP/IP protocol stack is a good example.
2. Using **Python libraries** of previously written code—whether modules from the built-in standard library that ships with Python or packages from third-party distributions that you download and install—that already know how to speak the network protocol that you want to use.

The major purposes of this course are:

1. Introduce you to several key networking libraries available for Python.
2. Teaching you about the lower-level network services on which those libraries (point.1) are built.

Benefits: Knowing the lower-level material is useful:

1. understand how the libraries work.
2. will understand what is happening when something at a lower level goes wrong.

Module 1

Computer Networks Fundamentals

Lecture 1

PYTHON NETWORK PROGRAMMING



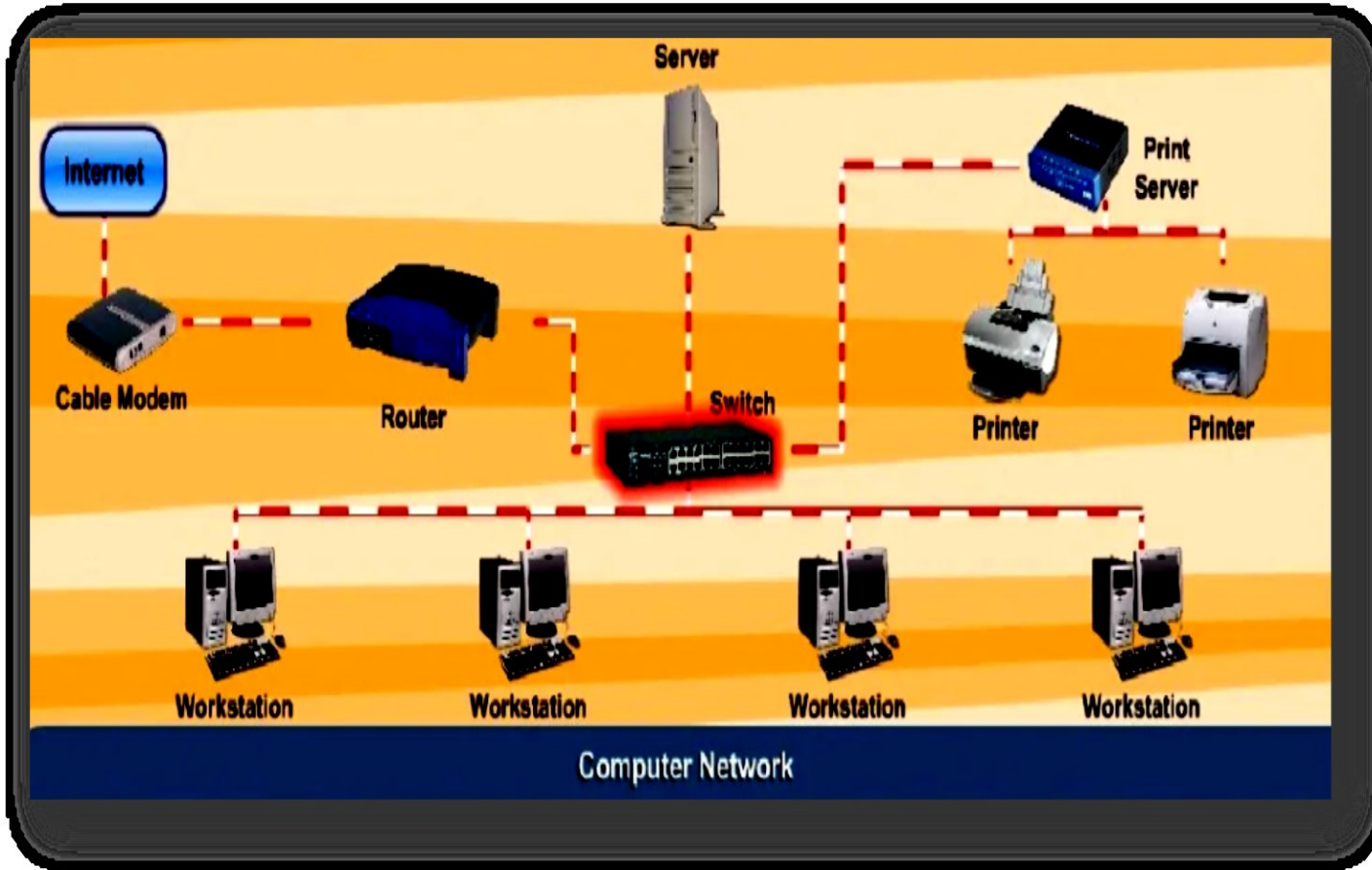
جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Module 1 (Computer Networks Fundamentals)

1. Definition of computer networks, communication
2. Importance of computer networks
3. Computer networks classifications (types, architectures, topologies, communications technology)
4. OSI model and communication through an internet
5. Mapping between OSI model and TCP/IP model
6. Data encapsulation and decapsulation
7. Network protocol (TCP, UDP)
8. Routing, Routing table, Routing protocols
9. Middleboxes
10. Throughput, Bandwidth, QoS, Bottleneck
11. Wireless networks (Technologies, types)
12. IEEE
13. Useful Windows Networking Commands

Module 1

Definition of computer networks



A computer network is a collection of **computers** and **devices**

connected together via **communication devices** and **transmission media**.

For examples it may connect computers, printers and scanners.

Devices – printer, scanner

Communication devices

NIC
Hub
??

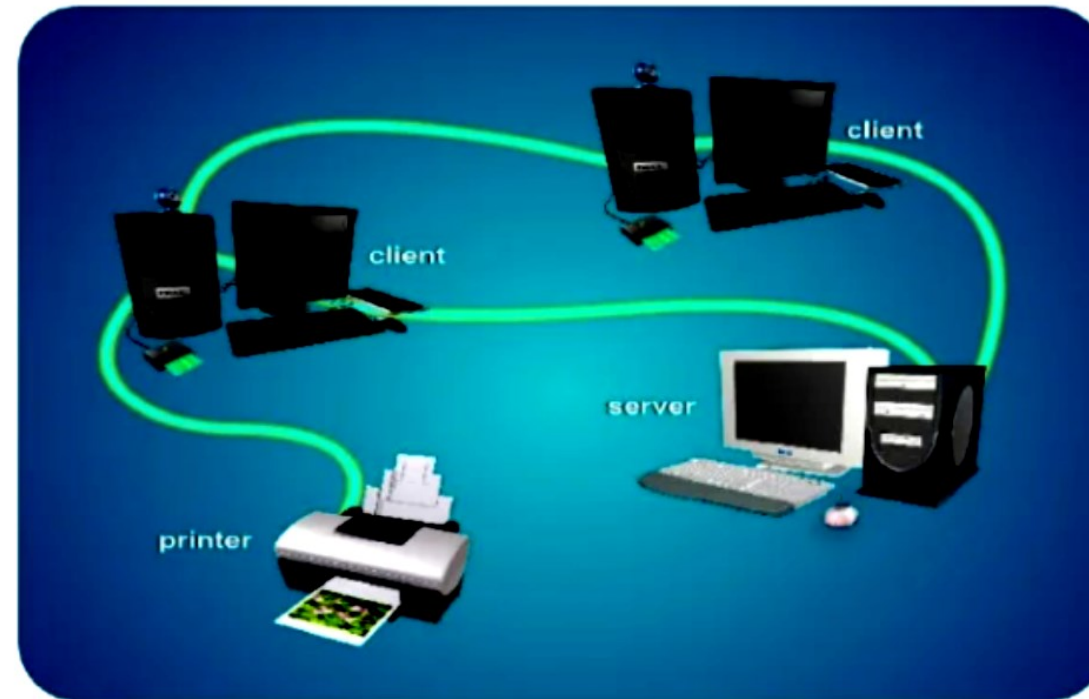
Router
??

Transmission Media

Physical

Infrared
Radiowave
Satellite

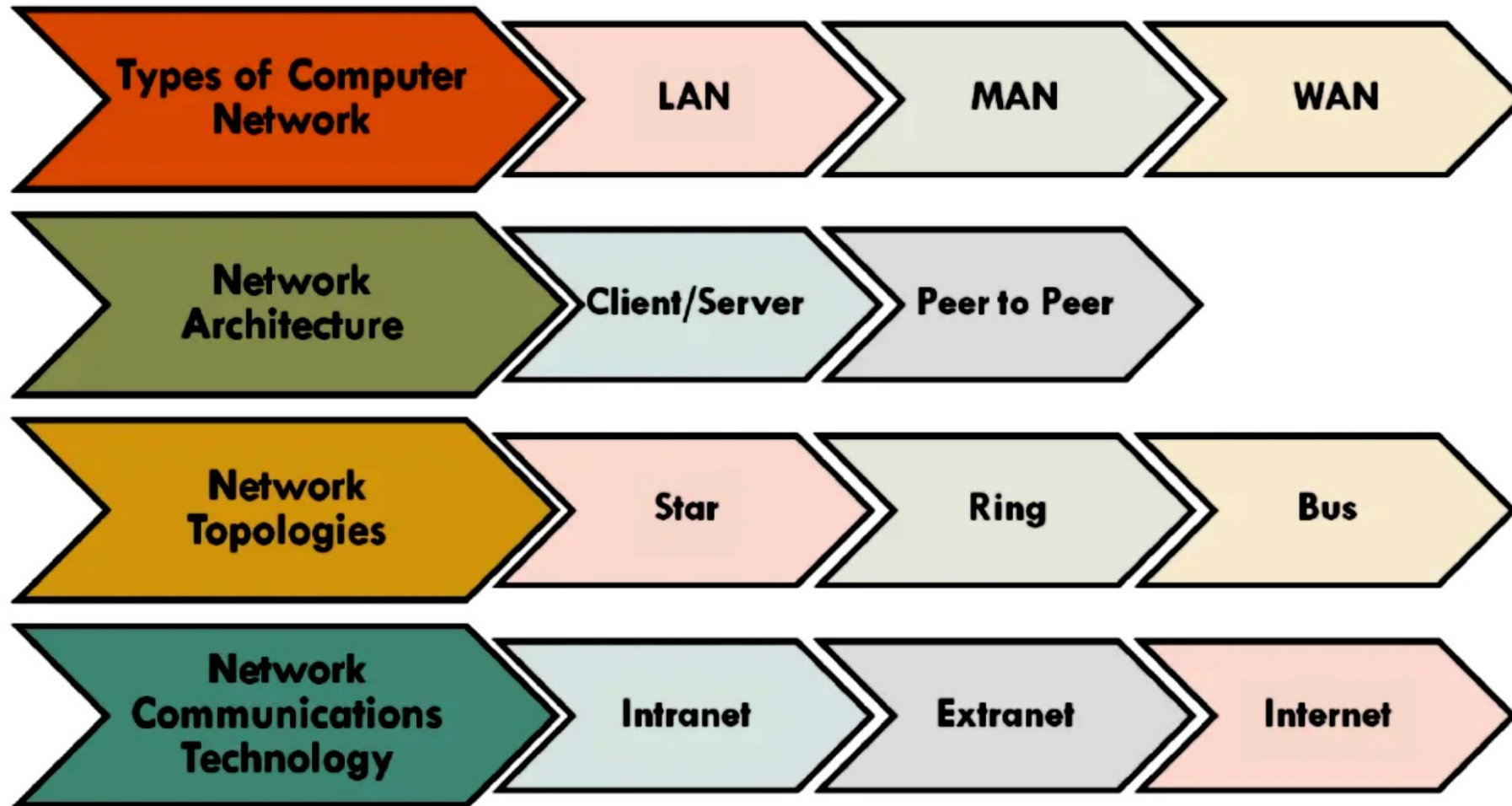
Communication describes a process in which two or more computer or **devices** transfer data, instructions and information.



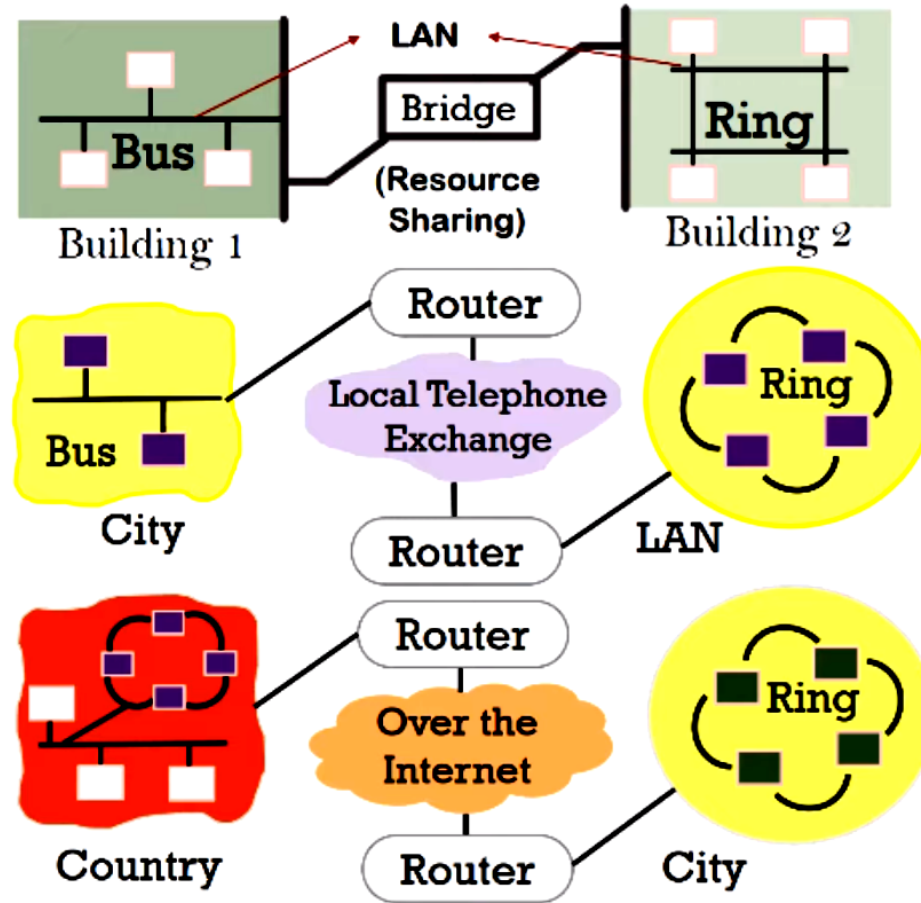
1. Sharing of **devices** such as printer and scanner
2. Sharing of **program**/software
3. Sharing of **files**
4. Sharing of **data**
5. Sharing of **information**
6. Sharing of **single high-speed internet connection**
Can access server centered **database**
7. **Better communication** using internet services such as email, mailing list and Internet Relat Chat (IRC)

Module 1

Computer networks classifications



LAN
MAN
WAN



Differences between Computer networks types

LAN (Local Area Network)

- LAN is a **Data network** that covers a **small** geographical area.
- Provides **high speed** of transmission.
- Mainly **implemented** at offices, home, school, etc.
- Uses **twisted pair** and **coaxial** cables.
- The information passed over a LAN is controlled by a set of **protocols**.

MAN (Metropolitan Area Network)

- Covers **large** physical area as compared to LAN.
- Maintained by single **operating entity**.
- Uses **protocols** such as ATM, FDDI, Fast Ethernet, etc.
- It is slower than LAN but faster than WAN.
- **Control of transmission** is also provided.
- Hard to snoop the data in a MAN as it uses **fiber optics cable**.

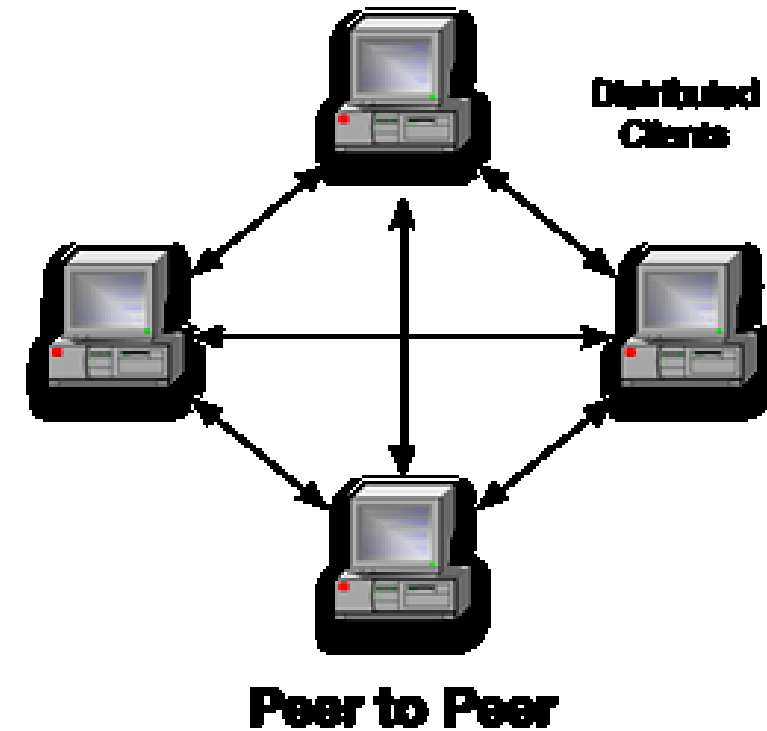
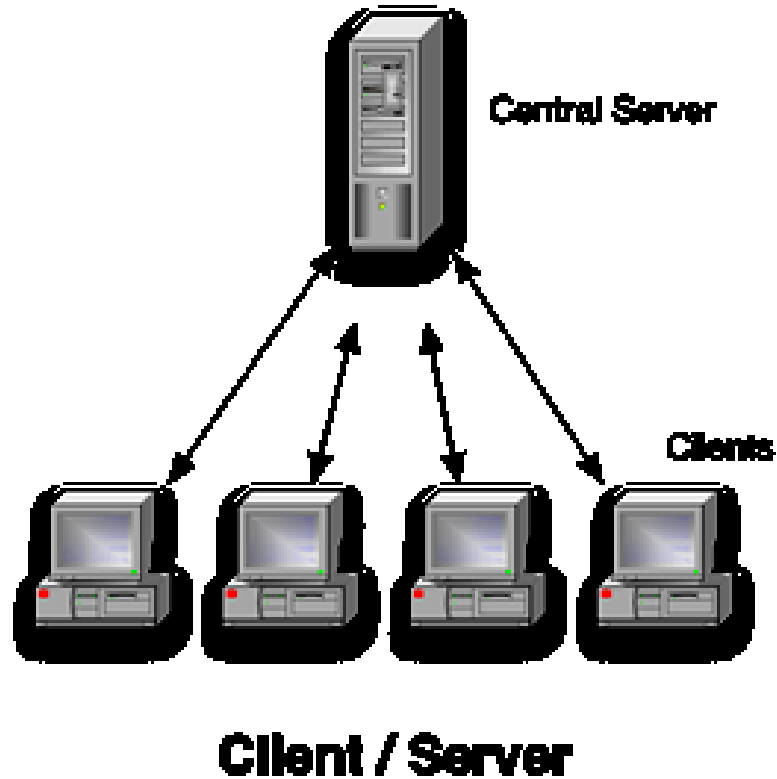
WAN (Wide Area Network)

- It covers the **largest** geographic area among LAN and MAN.
- It is part of a proprietary network but commonly we use it as a public network.
- Uses **protocols** such as TCP/IP for data delivery.
- ATM, Frame relay, POS and X.25 are used as **communication protocols**.
- May introduces issues like **noise** and **propagation delay**.



Module 1

Computer networks architectures



Differences between the two architectures

Client/Server

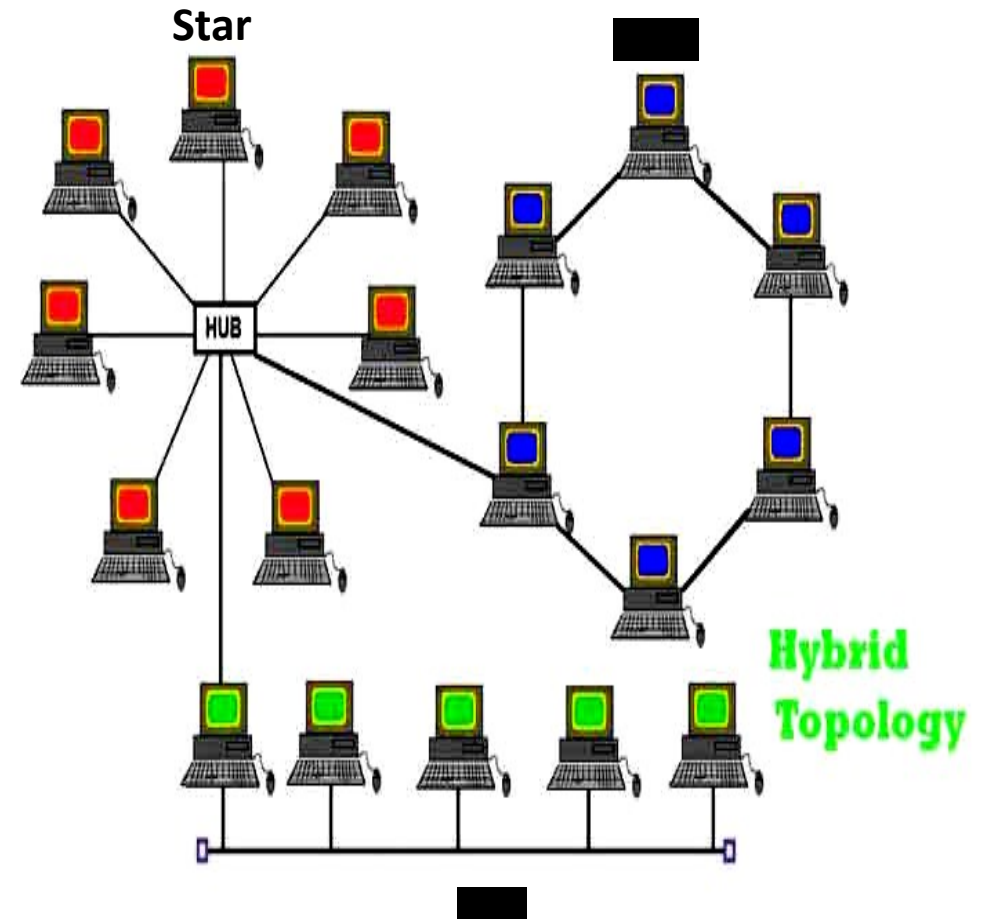
- 1) Server has to control ability while client's don't
- 2) Higher cabling cost
- 3) It is used in small and large networks
- 4) Easy to manage
- 5) Install software only in the server while the clients share the software
- 6) One powerful computer acting as server

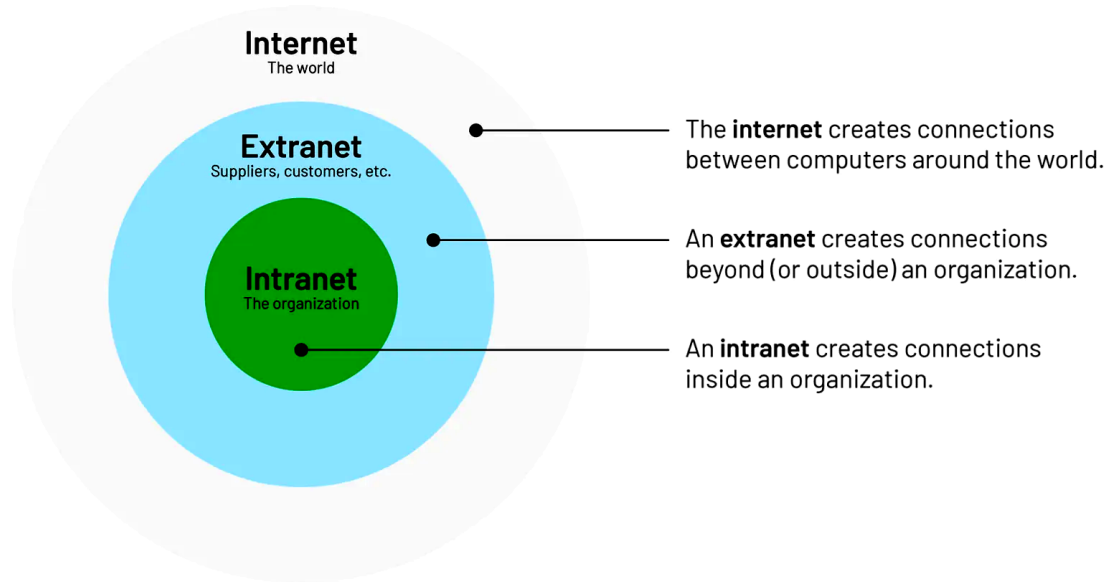
Peer-to-Peer

- 1) All computers have equal ability
- 2) Cheaper cabling cost
- 3) Normally used in small networks with less than 10 computers
- 4) Hard to manage
- 5) Install software to every computer
- 6) No server is needed



Physical Topology	Description	Advantages	Disadvantages
Bus	All computers are connected to a single cable	- Easy to install - Relatively inexpensive - Requires less cable than other topologies	- Media failure can bring down the entire network - Difficult to troubleshoot - Difficult to reconfigure
Star	Each computer is connected to a central point	- Easy to reconfigure - Easy to troubleshoot - Media failure does not bring down the entire network	- Failure of the hub brings the entire network down - Cost can be high due to the need for cabling
Ring	Each computer is connected to two other computers	- Cable faults are easy to identify - Even performance	- Media failure can bring down the entire network - Difficult to install and reconfigure - Cost can be high due to the need for cabling
Mesh	Each computer is connected to every other computer (point-to-point connections)	- Extremely fault tolerant - Provides redundant links	Expensive due to the need for large amounts of cabling





Difference Points	Internet	Intranet	Extranet
Network Accessibility Availability	Public Access It is a global system.	Private Access It is specific to an organization.	Private Access It makes use of the public network to share information with suppliers and vendors.
Coverage	All over the world.	Organizations Restricted area.	Restricted area only to an organization and a few of its stakeholders.
Content Accessibility	It is accessible to everyone connected.	It is accessible only to the members of the organization.	It is accessible only to the members of the organization and external members with logins credentials.
No. of computers connected	It is the largest in terms of connected devices.	The minimal number of devices are connected.	The connected devices are similar to the Intranet.
Owner	No one owns it.	Owned by Single organization.	Owned by Single/ Multiple organization.
Network Purpose	Its purpose is to share information throughout the world.	Its purpose is to share information throughout the organization.	Its purpose is to share information between members and external members.
Security	It is dependent on the user of the device connected to the network.	It is enforced via firewall.	It is enforced via firewall that separates the internet and extranet.
Users	The users are of the general public.	The users are employees of the organization.	The users are employees of the organization which are connected in the network.
Setup Policies	There is no hard and fast rule for policies.	Policies of the organization are imposed.	Policies of the organization are imposed.
Maintenance	It is maintained by ISP.	It is maintained by CIO, HR or communication department of an organization.	It is maintained by CIO, HR or communication department of an organization.
Economical	It is more economical to use.	It is less economical.	It is also less economical.
Relation	It is a network of networks.	It is derived from the Internet.	It is derived from the Intranet.
Example	What we are normally using is internet.	WIPRO using internal network for its business operations.	DELL and Intel are using the network for their business operations.

The OSI Model (Open Systems Interconnection Model)

- Was published in 1984 by the International Organization for Standardization (ISO).
- Conceptual framework used to describe the functions of a networking system (universal set of rules and *protocols* and requirements in order to support compatibility between different products and software).
- In the OSI reference model, the communications between a computing system are split into seven different abstraction layers.
- Still used today as a means to describe Network Architecture.

What is a Network Protocol?

Set of rules that governs the communications between computers on a network. These rules include guidelines that regulate the following characteristics of a network:

1. Access method
2. Allowed physical topologies
3. Types of cabling
4. Speed of data transfer.

Host Layers

Media Layers

OSI (Open Source Interconnection) 7 Layer Model

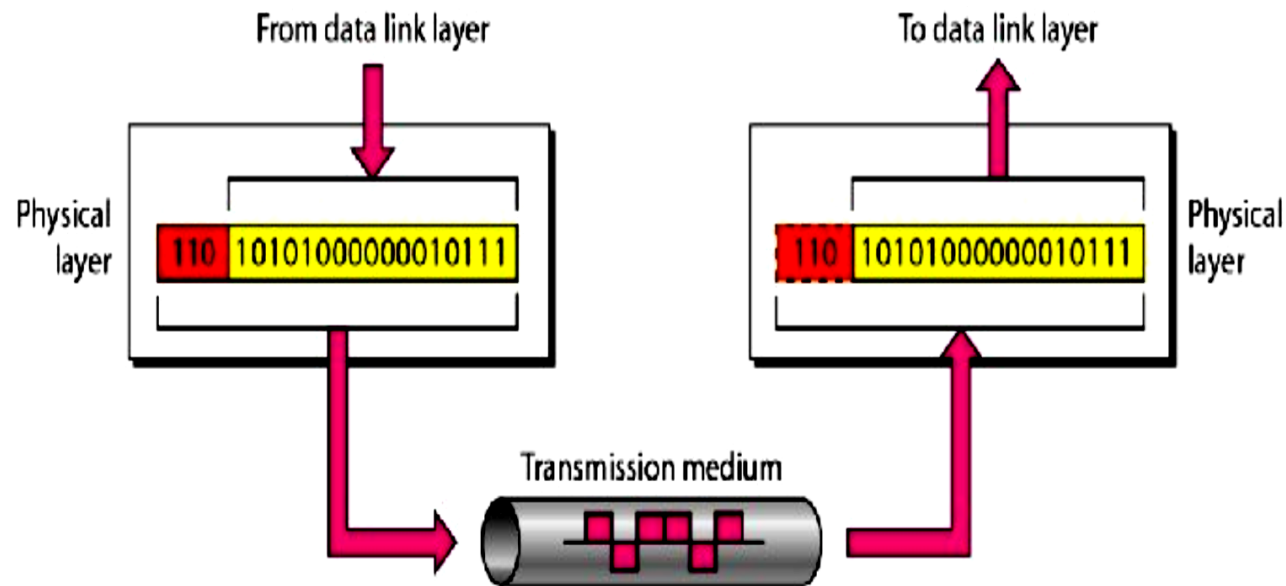
Layer	Application/Example	Central Device/ Protocols	DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	End User layer Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	User Applications SMTP	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	Syntax layer encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT	
Session (5) Allows session establishment between processes running on different stations.	Synch & send to ports (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	Logical Ports RPC/SQL/NFS NetBIOS names	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	TCP Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING TCP/SPX/UDP	Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	Packets ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	Frames ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	Switch Bridge WAP PPP/SLIP	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	Physical structure Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	Hub	

**G
A
T
E
W
A
Y**

Can be used on all layers

Land Based Layers

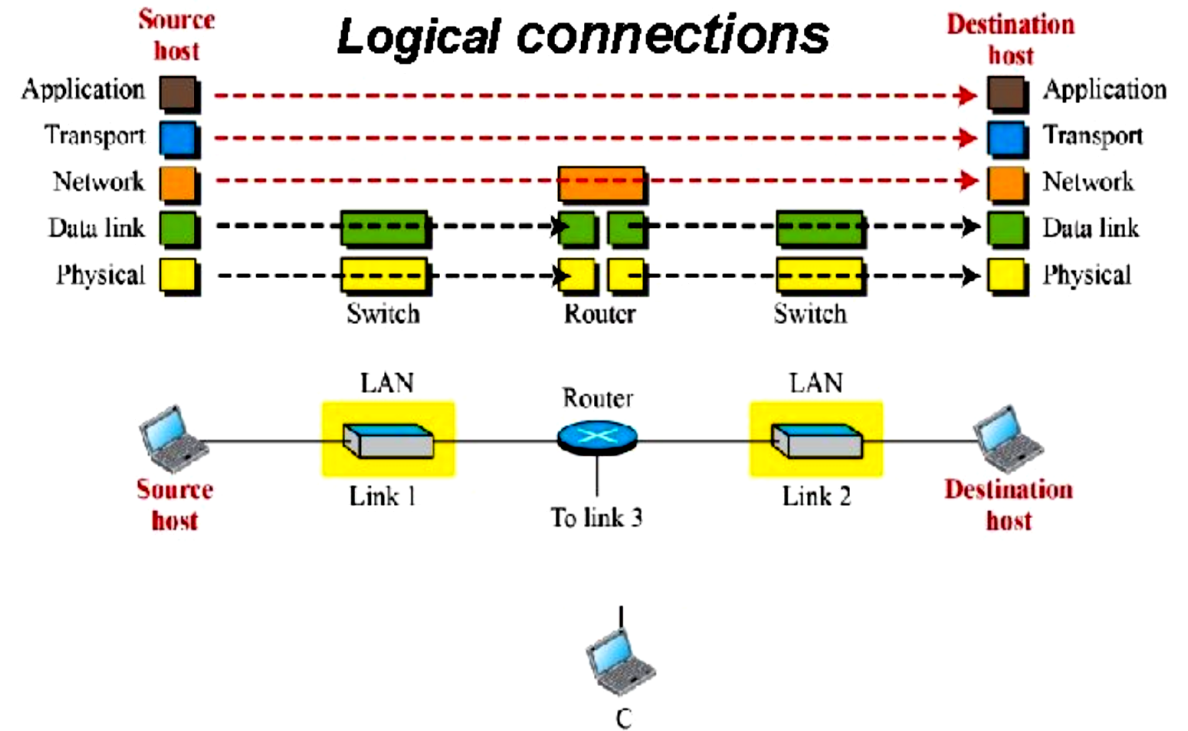
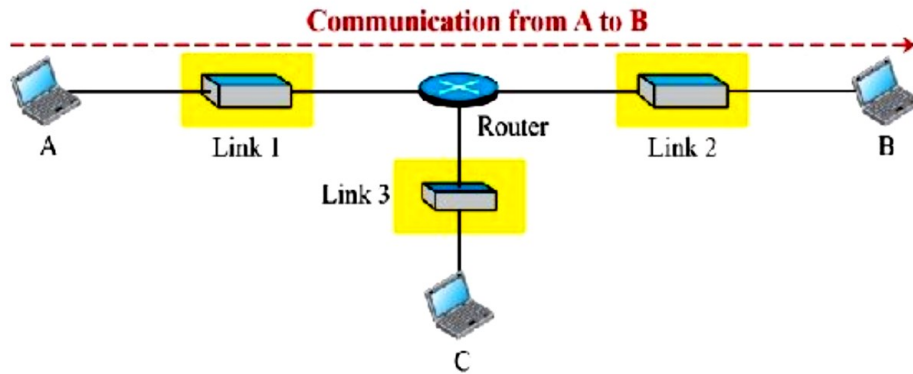
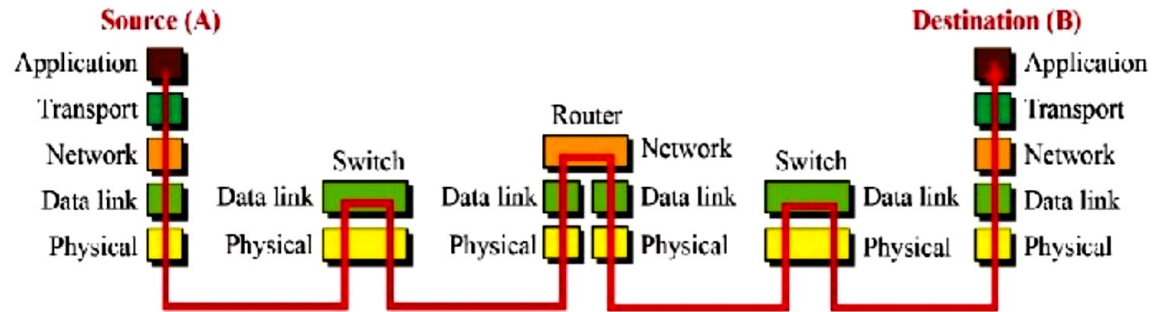
Hidden layer (transmission layer)



Note: Transmission Media is another hidden layer under
the Physical Layer

Module 1

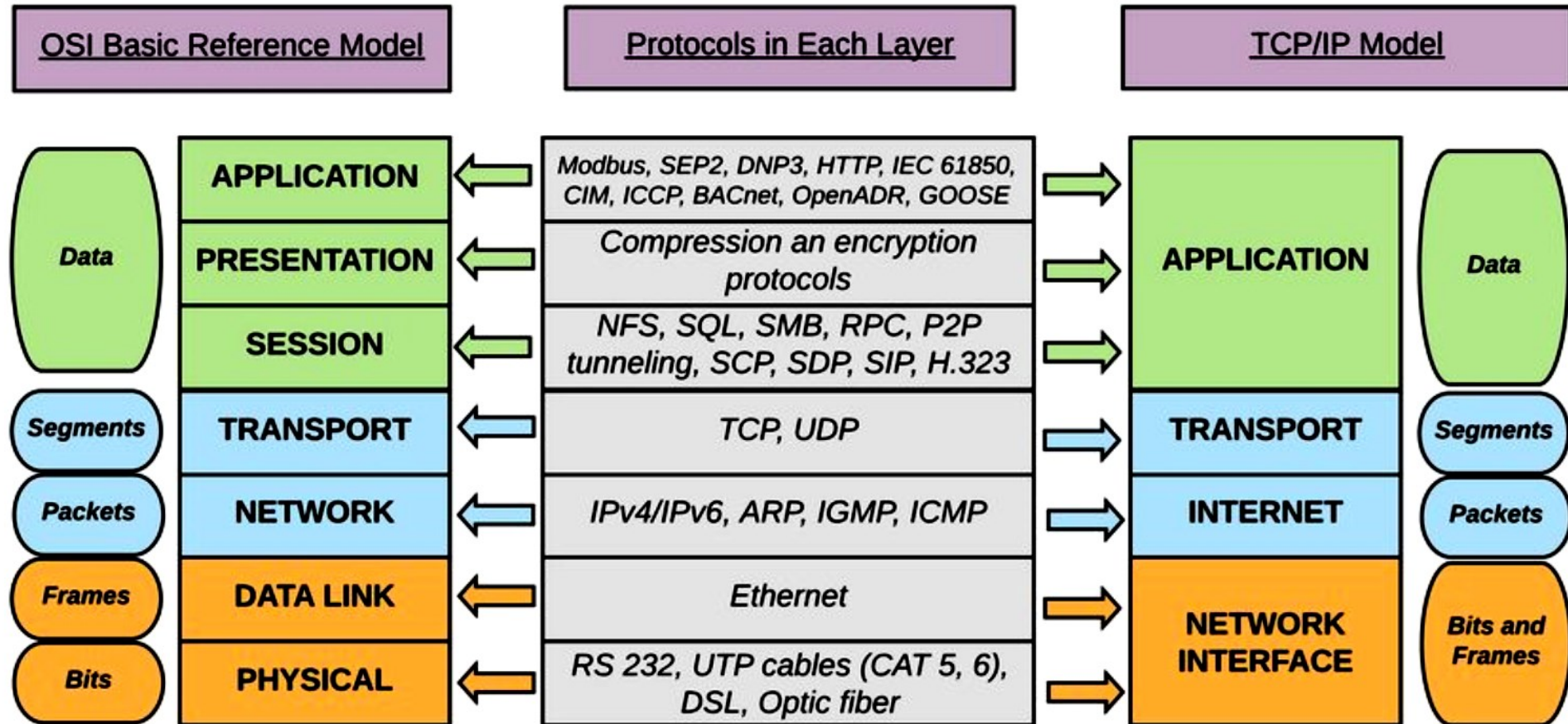
Communication through an internet

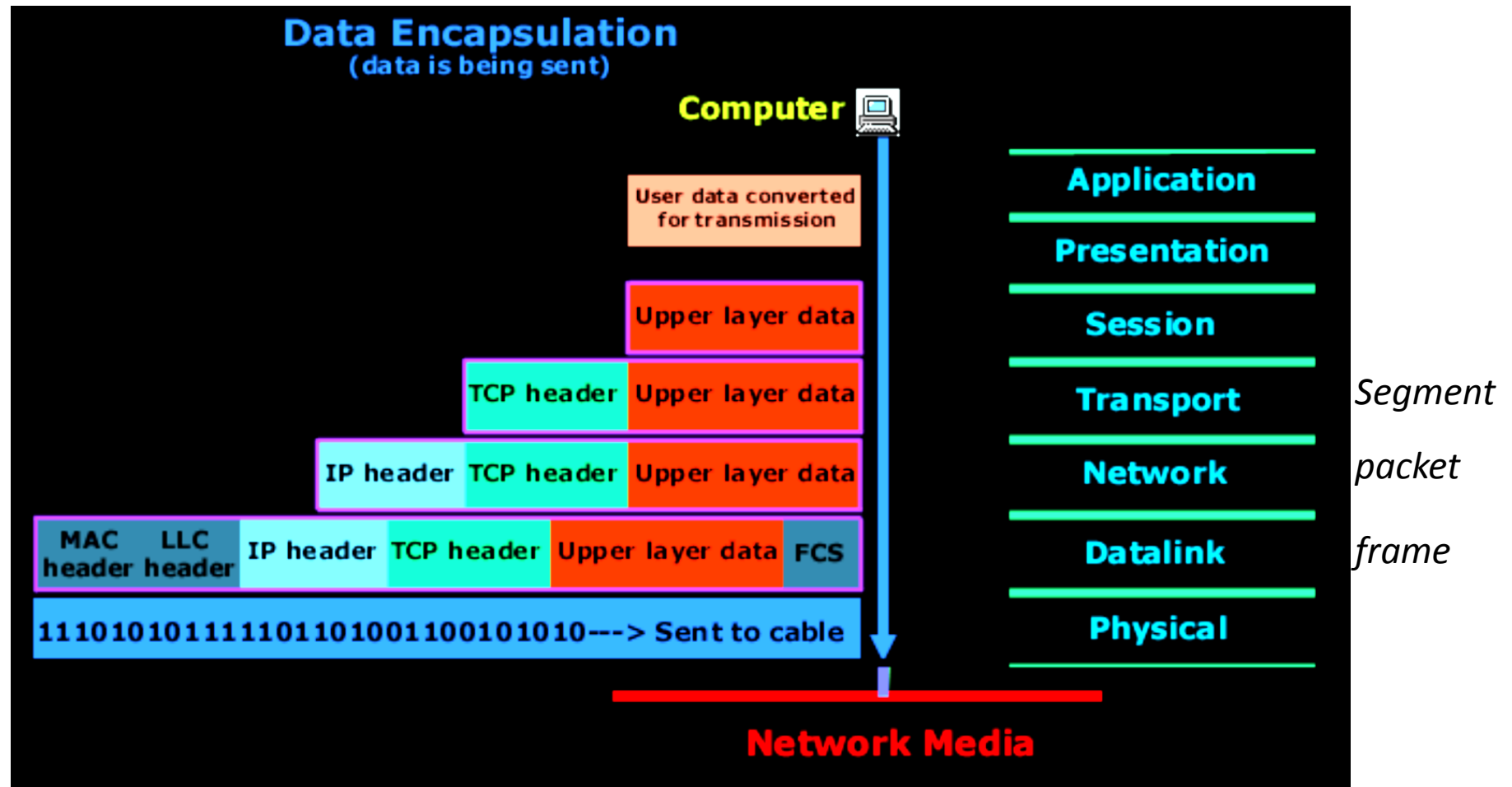


Remember: switches devices do not change data objects

Module 1

logical mapping between OSI model and TCP/IP model





TCP vs UDP

- | | |
|--|---|
| <ul style="list-style-type: none"> • Connected • State Memory • Byte Stream • Ordered Data Delivery • Reliable • Error Free • Handshake • Flow Control • Relatively Slow • Point to Point • Security: SSL/TLS | <ul style="list-style-type: none"> • Connectionless • Stateless • Packet/Datagram • No Sequence Guarantee • Lossy • Error Packets Discarded • No Handshake • No Flow Control • Relatively Fast • Supports Multicast • Security: DTLS |
|--|---|

TCP Segment Header Format

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Sequence Number							
64	Acknowledgment Number							
96	Data Offset	Res	Flags		Window Size			
128	Header and Data Checksum				Urgent Pointer			
160...	Options							

Transmission Control Protocol

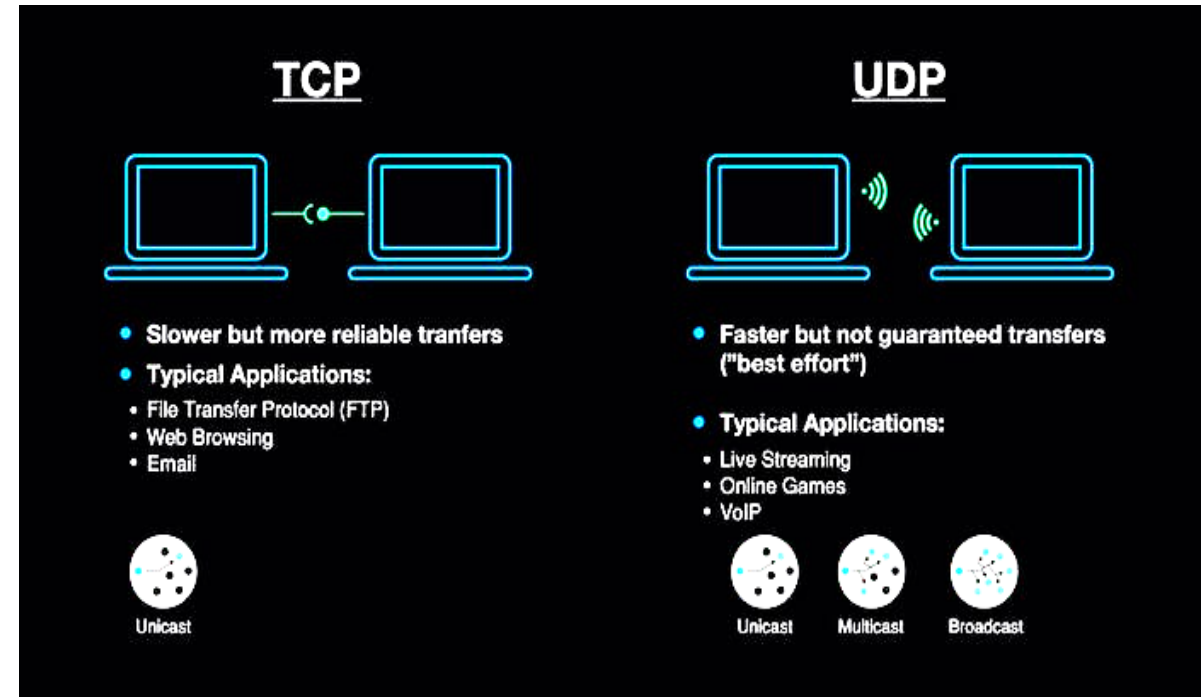
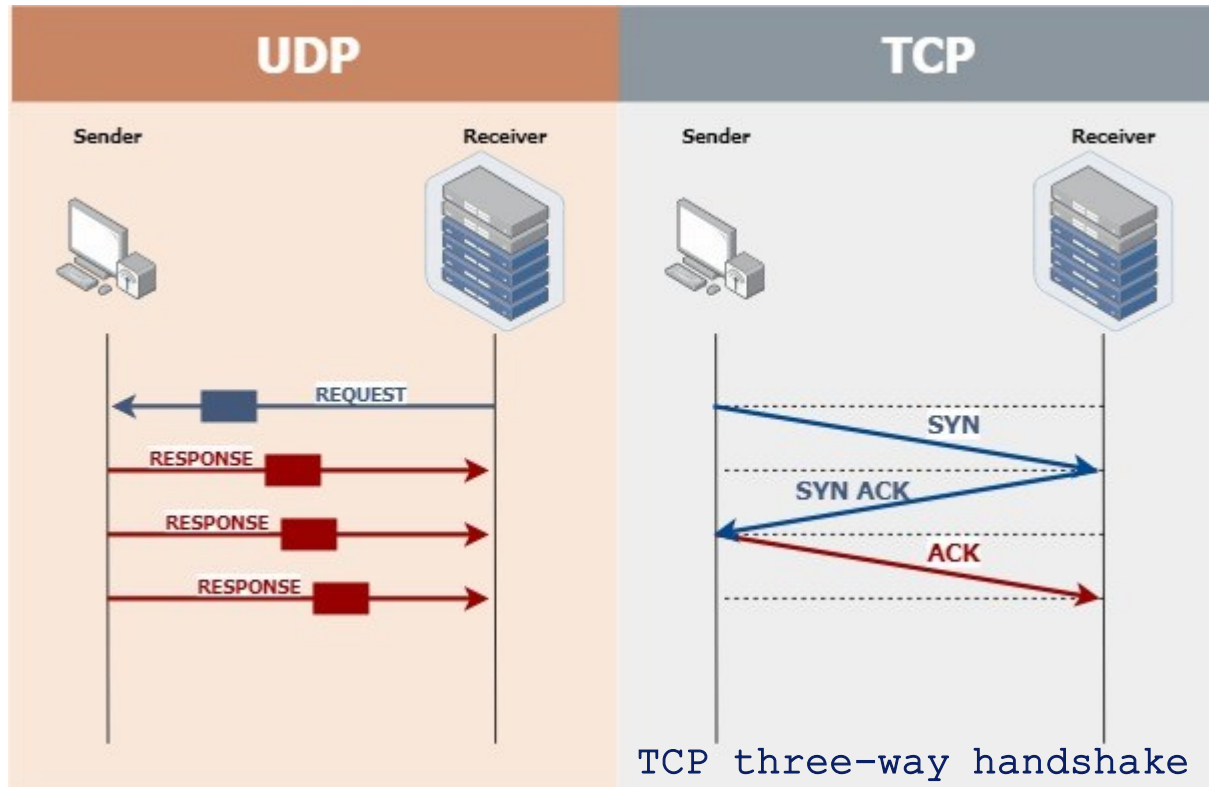
UDP Datagram Header Format

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Length				Header and Data Checksum			

User Datagram Protocol

Module 1

TCP/UDP protocols



Module 1

Encapsulation headers(IP) Internet protocol

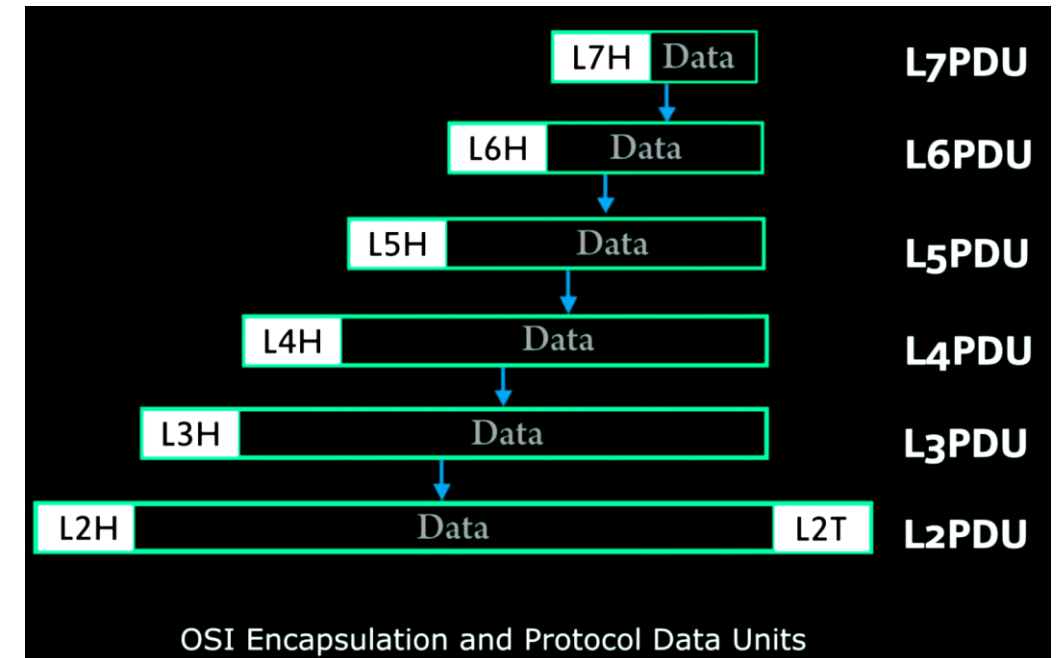
Method that governs how computers share data across the Internet.

When one computer sends data, such as an email or a web form, its message gets parsed into small packets that contain the sending computer's Internet address, the receiving computer's address, and part of the message (*packet*).

0	4	8	15	16	31
Version	IHL	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time to Live	Protocol		Header Checksum		
Source IP Address					
Destination IP Address					
Options					Padding

OSI uses a more generic term to refer to messages, rather than frame, packet, and segment. OSI uses the term *protocol data unit (PDU)*. A PDU represents the bits that include the headers and trailers for that layer, as well as the encapsulated data.

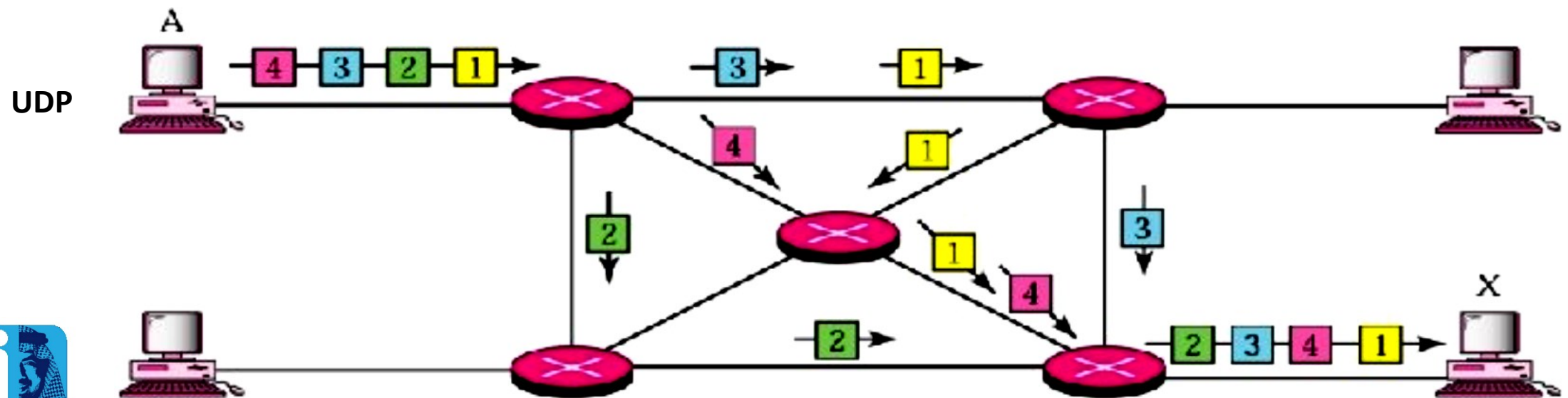
For example: A TCP segment of data using OSI terminology, is a PDU, more specifically a layer 4 PDU (abbreviated L4PDU) because TCP is Layer 4 protocol in the OSI model. In general, OSI refers to the layer x PDU (**LxPDU**), with x referring to the number of the layer.

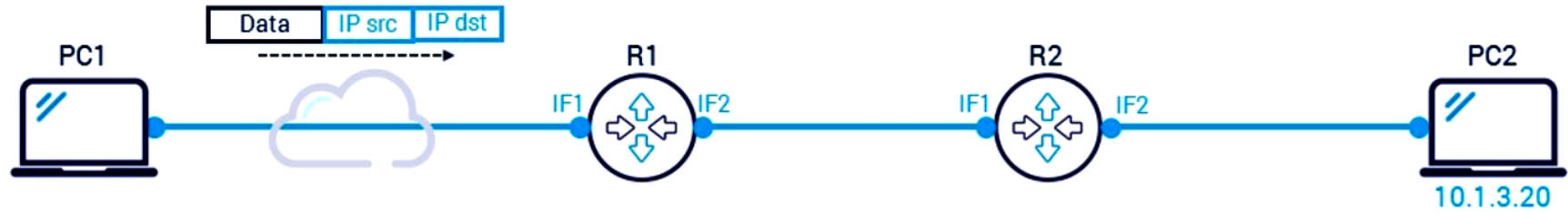


Encapsulation – Decapsulation comparison

ENCAPSULATION	DECAPSULATION
It occurs at source host computer	It occurs at destination host computer
Encapsulation is the process of wrapping the data	Decapsulation process is a process of opening packs
process starts from the uppermost layer (Application Layer) to the lowest layer	process starts from the lowest layer (Physical Layer) to the uppermost layer

- Process of selecting a path across one or more networks. The principles of routing can apply to any type of network, from telephone networks to public transportation.
- In packet-switching networks, such as the Internet, routing selects the paths for Internet Protocol (IP) packets to travel from their origin to their destination. These Internet routing decisions are made by specialized pieces of network hardware called routers.





RULE

- 1 Packet comes to ingress interface
- 2 Router looks into IP destination field in packet header
- 3 Router looks for **longest prefix that matches destination**

Example: IP dst: 10.1.3.20

Routing prefixes that has info about:

Ok	✓	10.0.0.0/8	via	IF2	
Ok	✓	10.1.0.0/16	via	IF2	
Ok	✓	10.1.3.0/24	via	IF2	
Not Ok	✗	192.168.0.0/16	via	IF1	R2_next hop
Longest match	Ok	✓	10.1.3.20/32	via	IF2 R2_next hop

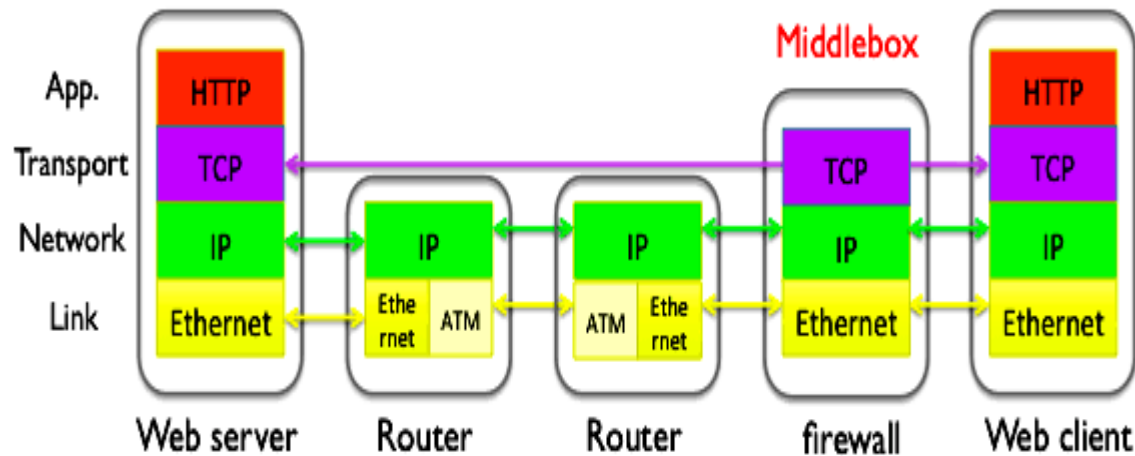
Module 1

Routing Protocols Comparison

PROTOCOL	INTERIOR OR EXTERIOR	TYPE	MATRIC	AD	HOP LIMIT	CONVERGE NCE	UPDATE TIMER	UPDATES	CLASSL ESS	VLSM SUPP.	ALGO.	UPDATE ADDR.	PROTOCOL/ PORT
RIPv1	INTERIOR	DV	HOP	120	15	SLOW	30 Sec	FULL	NO	NO	Dellman-ford	Broadcast	UPD/520
RIPv2	INTERIOR	DV	HOP	120	15	SLOW	30 Sec	FULL	YES	YES	Dellman-ford	224.0.0.0	UPD/520
IGRP	INTERIOR	DV	BANDWIDTH AND DELAY	100	255-100 Def	SLOW	90 Sec	FULL	NO	NO	Dellman-ford	224.0.0.0	IP/9
EIGRP	INTERIOR	HYBRIDE	BANDWIDTH AND DELAY	90(IN)- 170(EXT)	224-100 Def	VERY FAST	Whenever any changes happens	ONLY CHANGE	YES	YES	DUAL	224.0.0.0	IP/88
OSPF	INTERIOR	LINK STATE	COST	110	NONE	FAST	Whenever any changes happens (LSA-30mnt)	ONLY CHANGE	YES	YES	Disjkstra	224.0.0.0	IP/89
IS-IS	INTERIOR	LINK STATE	COST	115	NONE	FAST	Whenever any changes happens	ONLY CHANGE	YES	YES	Disjkstra		
BGP	EXTERIOR	PATH VECTOR	MULTIPLE ATTRIBUTES	20(EXT- 200(INT)	20 Ext 200 Int	AVRAGE	Whenever any changes happens	ONLY CHANGE	YES	YES	Best Path	Unicast	TCP/179



Middlebox is defined as any intermediary device performing functions other than the normal, standard functions of an IP router on the datagram path between a source host and destination host.



Primarily deployed for **security** and **performance** benefits.

Firewalls
Application Firewalls
Intrusion Detection Systems (IDS)
Intrusion Prevention Systems (IPS)
Proxy/Caches
WAN Optimizers
Protocol Accelerators

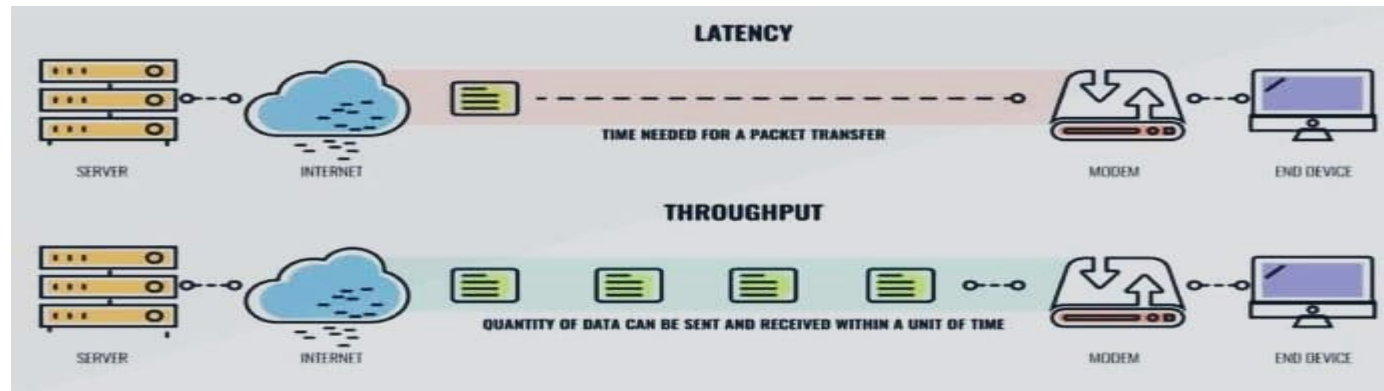
Many other uses too!

Billing and usage monitoring, asset tracking, Network Address Translation, protocol converters (6to4/4to6)...

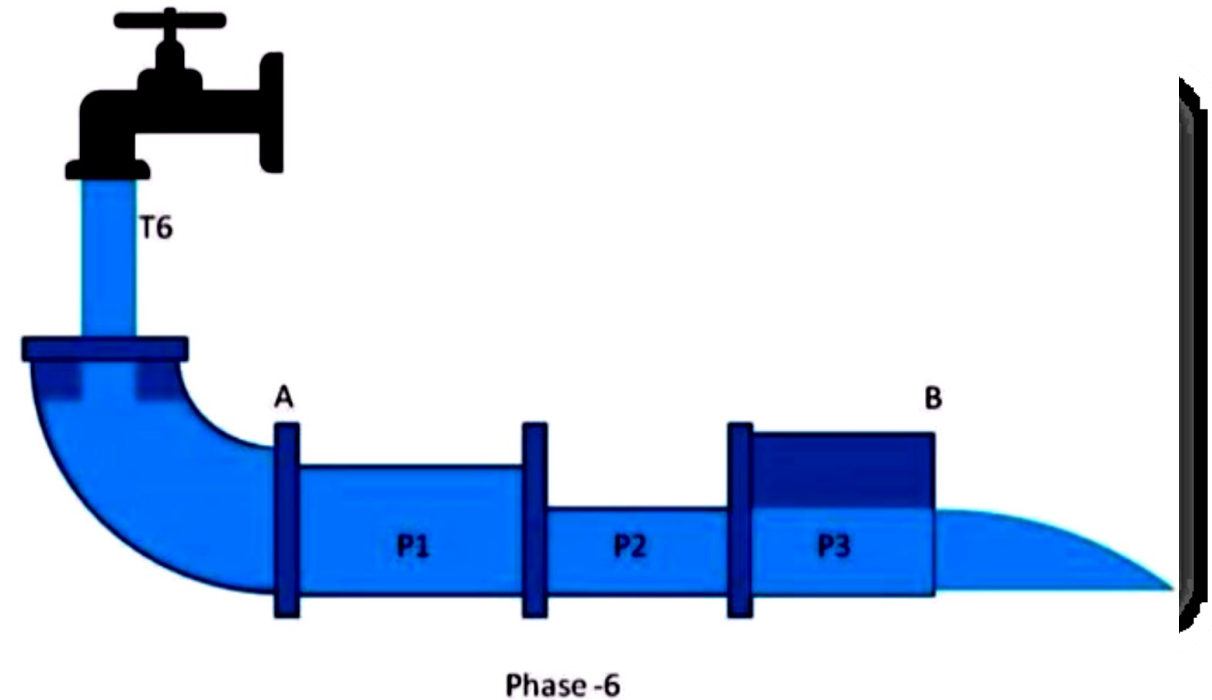
Throughput tells you how many packets arrive at their destinations successfully at any given time. For the most part, throughput capacity is measured in bits per second, but it can also be measured in data per second.

Bandwidth tells you how much data could theoretically be transferred from a source at any given time. Bandwidth is measured in bits, megabits, or gigabits per second.

It's important to remember high bandwidth doesn't necessarily equal high network performance. Substantial bandwidth won't matter if data throughput is still being dragged down by *latency*, *jitter*, or *packet loss*.



- ✓ You can think of bandwidth as a tube and data throughput as sand. If you have a large tube, you can pour more sand through it at a faster rate. Conversely, if you try to put a lot of sand through a small tube, it will go very slowly.



Quality of Service (QoS)

set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity. QoS technologies accomplish this by providing differentiated handling and capacity allocation to specific flows in network traffic.

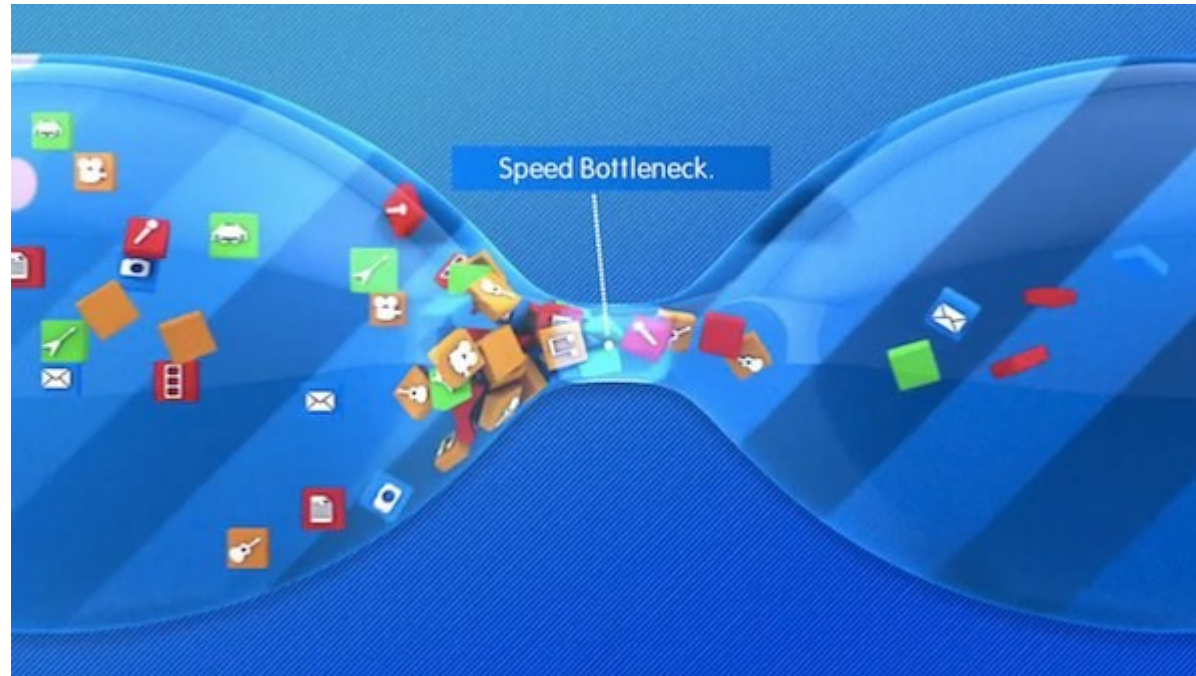
Bandwidth without QoS



Bandwidth with QoS

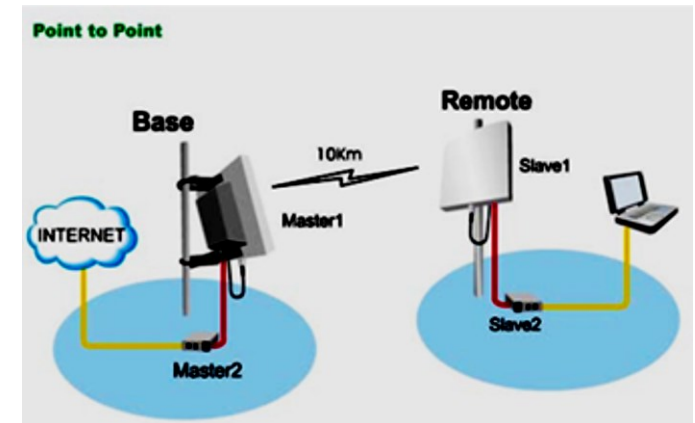
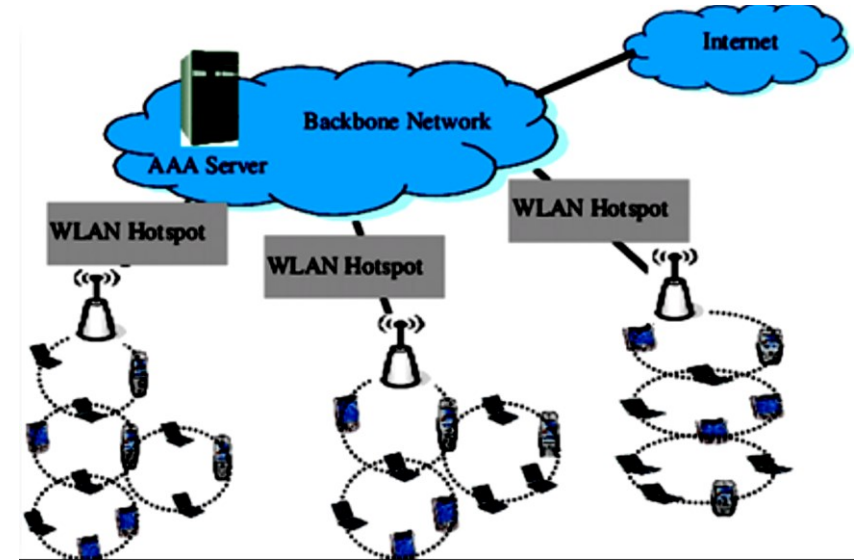


Bottleneck, in a communications context, is a point in the enterprise where the flow of data is impaired or stopped entirely. Effectively, a bottleneck results when there is not enough data handling capacity to accommodate the current volume of traffic.



Wireless network is a computer network that uses wireless data connections between network nodes.

- Avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.
- Admin telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical layer of the OSI model network structure.



Module 1

Wireless Communication technologies

1. Satellite Communication
2. Infrared Communication
3. Broadcast Radio
4. Microwave Communication
5. Wi-Fi
6. Mobile Communication Systems
7. Bluetooth Technology
8. Global Positioning System (GPS)
9. Paging
10. Radar
11. Radio Frequency Identification (RFID)



Wireless PAN

Wireless LAN

Wireless CAN

Wireless ad hoc network

Wireless MAN

Wireless WAN

Cellular network

Global area network

Space network

Table 1. Scope of IEEE 802 Wireless Subcommittees

Name	Subcommittee	Maximum Distances	Technology Consortia
WMAN (wireless metropolitan area network)	IEEE 802.16	Kilometers	WiMAX®
WLAN (wireless local area network)	IEEE 802.11	Hundreds of meters	Wi-Fi®
WPAN (wireless personal area network)	IEEE 802.15	Tens of meters	ZigBee® Bluetooth™ WiMedia™



What Does Institute of Electrical and Electronics Engineers (IEEE) Mean?

The Institute of Electrical and Electronic Engineers (IEEE) is a global association and organization of professionals working toward the development, implementation and maintenance of technology-centered products and services.

IEEE 802.12 will support both Ethernet and token ring frame types.

IEEE 802.1 Bridging (networking) and Network Management

IEEE 802.2 LLC inactive

IEEE 802.3 Ethernet

IEEE 802.4 Token bus disbanded

IEEE 802.5 Defines the MAC layer for a Token Ring inactive

IEEE 802.6 MANs disbanded

IEEE 802.7 Broadband LAN using Coaxial Cable disbanded

IEEE 802.8 Fiber Optic TAG disbanded

IEEE 802.9 Integrated Services LAN disbanded

IEEE 802.10 Interoperable LAN Security disbanded

IEEE 802.11 a/b/g/n Wireless LAN (WLAN) & Mesh (Wi-Fi certification)

IEEE 802.12 100BaseVG disbanded

IEEE 802.13 unused

IEEE 802.14 Cable modems disbanded

IEEE 802.15 Wireless PAN

IEEE 802.15.1 Bluetooth certification

IEEE 802.15.2 IEEE 802.15 and IEEE 802.11 coexistence

IEEE 802.15.3 High-Rate wireless PAN

IEEE 802.15.4 Low-Rate wireless PAN (e.g., ZigBee, WirelessHART, MiWi, etc.)

IEEE 802.15.5 Mesh networking for WPAN

IEEE 802.16 Broadband Wireless Access (WiMAX certification)

IEEE 802.16.1 Local Multipoint Distribution Service

IEEE 802.17 Resilient packet ring

IEEE 802.18 Radio Regulatory TAG

IEEE 802.19 Coexistence TAG

IEEE 802.20 Mobile Broadband Wireless Access

IEEE 802.21 Media Independent Handoff

IEEE 802.22 Wireless Regional Area Network

IEEE 802.23 Emergency Services Working Group New (March, 2010)



16 Useful Windows Networking Commands You Should Know

Command		Used For
1	PING	Troubleshooting network connection issues. (test whether one network host is able to communicate with another)
2	IPCONFIG	Quickly finding your IP address.
3	GETMAC	Quickly finding your MAC address.
4	ARP	Display and modify the Address Resolution Protocol cache; useful for resolving address resolution problems.
5	HOSTNAME	Quickly finding your hostname.
6	NSLOOKUP	Find the IP address of a device, find the domain name of an IP address of your device's DNS server and find mail servers for a domain.
7	NBTSTAT	Troubleshooting NetBIOS issues.
8	Route	Allow you to view the device's routing tables. To do so, simply type Route Print.

16 Useful Windows Networking Commands You Should Know

	Command	Used For
9	NET	Displaying available Net switches. (accounts to set password and logon requirements, file to show a list of open files and sessions to list, or even disconnect, sessions on the network)
10	NETSTAT	Displaying network statistics. NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]
11	NETSH	Displaying and configuring network adapters.
12	TASKKILL	Ending processes.
13	TRACERT	Trace the route a packet takes before reaching its destination, and see information on each "hop" along the route.
14	PATHPING	Combine that best of both ping and tracert into a single utility.
15	SYSTEMINFO	Displaying system information.
16	NET VIEW	Viewing devices connected to a network.

Q: Apply these windows networking commands, then send to me captured screen for commands (4-8) in your personal desktop computer (Pc) or laptop?

1. ipconfig
2. getmac
3. hostname
4. tracert esu.ac.ae
5. Ping esu.ac.ae
6. netstat -s
7. netstat -n
8. netstat -y