POLYTECHNIC UNIVERSITY OF THE PHILIPPINES

PARAÑAQUE CITY CAMPUS

INSTRUCTIONAL MATERIAL

FOR

CMPE 30114

DATA AND DIGITAL COMMUNICATIONS

COMPILED BY

ENGR. MARVIN DE PEDRO

Course Description and Learning Outcomes

This course includes the basic principles of network architecture, computer network design, services, technologies, and network security.

After completing the course, the student must be able to:

- Interpret the essential concepts in electronic communication systems, including the devices used and engineering processes involved;
- Illustrate the working principles of telecommunications, internet, and networks;
- Classify the different digital communication technologies, including digital and mobile telephony, terrestrial microwave communications, satellite communications, fiber optic communications, computer networks, and the internet;
- Appraise the significance of communication protocols and standards;
- Use engineering principles in considering the different functions and protocols of each layer in the OSI and TCP/IP reference models for data communications; and
- Develop an output that applies concepts of data communications systems.

Course Overview and Outline

Page

Chapter 1 (Introduction to Telecommunications)

Class Rules

Due to the restrictions brought by COVID-19 threats, there will still be no face-to-face class sessions for the 1st Semester of A.Y. 2021-2022, except probably for some hands-on activities. With that, we will use a “virtual classroom” method of distance learning instead. It’s a combination of online technology and home schooling type of class sessions wherein:

1. Class lectures will be done asynchronously through recorded videos. Students can get a copy of all lecture videos and other class materials (downloadable from a given Google Drive folder), and from time to time, check the updates on the class’ official FB group.
2. Oral assessments and class huddles will be done synchronously through a video conference (Zoom or Google Meet). There will be 2 synchronous class sessions for each chapter (4 modules) where students can also ask questions regarding the lessons, class requirements, and activities.
3. Students can have self-paced learning through the provided class materials. They can feel free to share it with other people at home and may take the lessons as a productive hobby during this season.
4. Those who can’t attend the scheduled synchronous class session as well as those who can’t participate or comply with certain class requirements must submit a formal letter

explaining his/her valid reason. This letter should be submitted as early as possible so that necessary adjustments or arrangements can be done ahead.

5. Some class requirements will be done as team tasks wherein each member is expected to cooperate and contribute to the team's output. **Please report anyone who does not*.

Knowing that some students may not have access to a reliable internet connection, your cooperation and resourcefulness are highly encouraged. Some of you may ask someone to download the materials on your behalf. Some may even ask to have the downloaded files saved in an SD card and send it to them via *Lalamove* or any courier services available. Same methods can be used for submitting the outputs to the leader who will upload the team's final output. These can be done without compromising safety.

Also, each one as an engineering student is encouraged and expected to:

- Practice self-discipline and time management in the individual and team tasks.
- Be responsible enough to cooperate with groupmates without the instructor's supervision and/or coercion.
- Take time to research and read beyond the given lecture materials.
- Be more serious in developing his/her own engineering skills and virtues.

Grading System

Class Standing		50%
• Quizzes / Laboratory Tasks	30%	
• Class Activities	20%	
Exam		30%
Performance Task		20%

		100%

Transmutation Table	
1.00	97 to 100
1.25	94 to 96.99
1.50	91 to 93.99
1.75	88 to 90.99
2.00	85 to 87.99
2.25	82 to 84.99
2.50	79 to 81.99
2.75	76 to 78.99
3.00	75 to 75.99
5.00	Below 75

Grades will be uploaded on the SIS right after the end of the first semester. A period of 3-5 days will be given for any necessary changes before the grades will be finalized.

Course Requirements

Class Activities (20%) + **Exam** (30%) – Team Task

- Perform *Activities 1-10* in the given Laboratory Manual PDF.
- Assigned team member(s) should have a video recording of themselves performing a laboratory activity (priority of the footage is the computer screen being used). You can use a video conferencing platform if multiple members work in an activity.
- Compile the video clips into a single AVP with just minimal editing effects (the simpler, the better). At least 5 members should appear in the entire AVP.
- All outputs to this requirement must be submitted within the last week of the semester, but it's best to start working on them early to avoid bottlenecking of the tasks at the said deadline period. Feel free to comment your queries on the dedicated FB group post or ask them during one of the synchronous class sessions.

Quizzes/Laboratory (30%) – Team Task

- All three teams will work together to perform a system study for a proposed *disaster risk reduction and management system* for Brgy. Sto Niño. Compile the information gathered in this study into a single 5-10 minute AVP and PDF documentation.
- Preferably, each team will assign representatives for each of the following tasks:
  - ✓ Discuss about the general information of the site, including its geography, demography, culture, economy, commercial activities, and governance.
  - ✓ Discuss the common disasters encountered within the site and the existing mitigation for such disasters. Gather information from residents and officials, and relate these with the discussed general information about the site.
  - ✓ Discuss the existing communications services and infrastructures installed within the site, and the possible technologies that could be part of risk mitigation for the said disasters. Apply concepts discussed in this course.
- All outputs to this requirement must be submitted within the last week of November. Feel free to comment your queries on the dedicated FB group post or ask them during one of the synchronous class sessions.

Performance Task (20%) – Team Task

- This grade component will come from the system proposal with feasibility study for the assigned project. It basically requires proper documentation and video presentation.
- See the given content outline document for the specific instructions.
- All “behind-the-scene” activities related to compliance to this requirement must also be documented by taking photos of group members performing the tasks, and by taking screenshots of the accomplished work in any necessary software tools as well as of the conversations, charts, and other project management details of the group.
- All outputs to this requirement must be submitted within the last week of the semester, but it’s best to start working on them early to avoid bottlenecking of the tasks at the said deadline period. Feel free to comment your queries on the dedicated FB group post or ask them during one of the synchronous class sessions.

Rubrics:

Criteria	Description	Weight Score
Substance	Output includes the expected key points and correct components.	50
Form	Output is presented accurately and systematically with minimum grammatical and formatting errors.	25
Compliance	Output meets the prescribed length, coverage, and other specified instructions.	25
	TOTAL	**100**

Introduction to Telecommunications

(CMPE 30114 – Data and Digital Communications)

1 Chapter

I. OVERVIEW

Telecommunications, also known as *telecom*, is the exchange of information over significant distances by electronic means, referring to all types of voice, data and video transmission. It is the transmission of information by various types of technologies over wire, radio, optical or other electromagnetic systems. It includes the means of electronic transmission of information over distances. The information may be in the form of voice telephone calls, data, text, images, or video. Today, telecommunications is used to organize more or less remote computer systems into telecommunications networks.

II. MODULE OBJECTIVES

After successful completion of modules 1-4 of Chapter 1, you should be able to:

1) Remember important concepts and terminologies in electronic communications;
2) Understand principles of digital and mobile telephony;
3) Evaluate the significance of terrestrial and satellite communications; and
4) Apply the best practices in designing, implementing, and maintaining fiber optic networks.

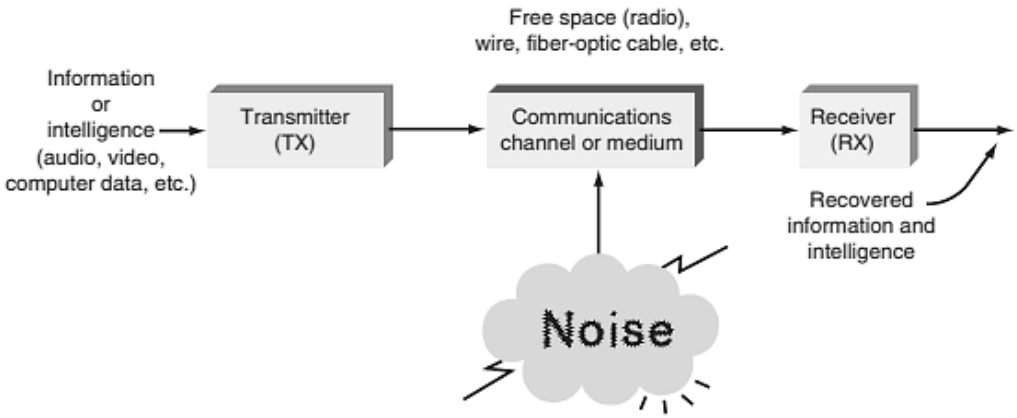
III. COURSE MATERIALS

Suggested Online Resources for Further Learning

- Downloadable Course AVPs: https://bit.ly/3lp25qa
- Downloadable Course PDFs: https://bit.ly/3FtitOt

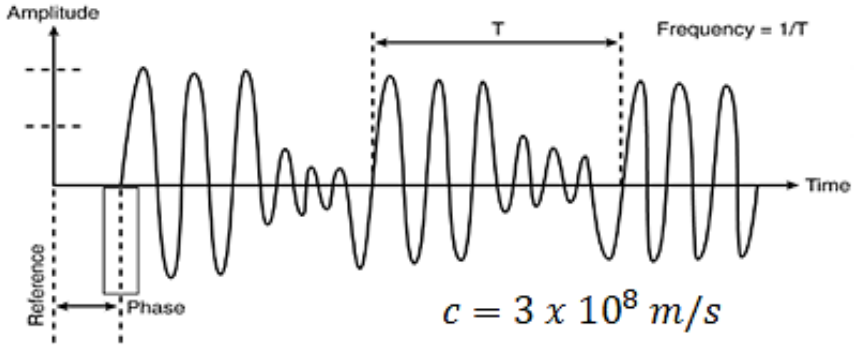
Module 1: **Principles of Communications Systems**

Electronic Communications refers to the transmission, reception, and processing of information or message (in the form of signals) between two or more locations with the use of circuits.



Signal is a time varying voltage, current or EM wave that conveys a message between observers, among other possibilities. It has the following properties:

- Amplitude – measure of the signal intensity, loudness, power, strength, or level
- Wavelength – distance between two identical points of neighboring cycles of a wave signal traveling in space or in any physical medium, measured in *meters* (m)
- Period – time it takes for a signal to complete one cycle, measured in *seconds* (s)
- Frequency – number of cycles per unit time, measured in *Hertz* (Hz)
- Bandwidth – range of frequencies within a given band, measured in *Hertz* (Hz)
- Phase – position of a point in time (an instant) on a signal cycle, measured in *radian degrees*



Transmitter Components

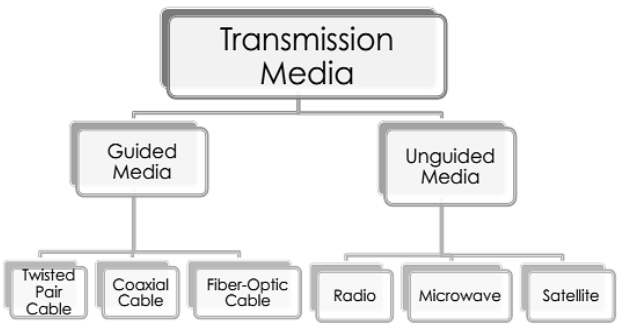
- Signal Input Interface
- Power Supply
- Local Oscillator
- Modulator
- RF Amplifier
- Impedance Matching Circuit

Receiver Components

- Signal Input Interface
- RF and IF Amplifiers
- Beat Frequency Oscillator
- Automatic Gain Control
- Phase Detector
- Bandwidth Filter
- Audio Limiter
- Power Supply
- Signal Output Interface

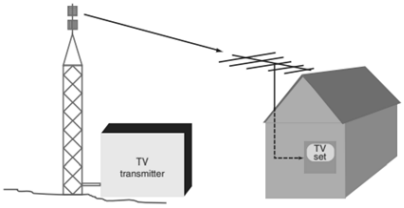
Generally speaking, a ***transceiver*** is a device that can both transmit and receive signals, whereas a ***transponder*** is a component programmed to monitor incoming signals and with a preprogrammed reply in the communication network.

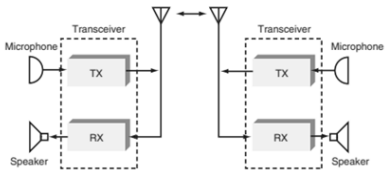
Transmission Media refers to a communication channel that carries the information from the sender to the receiver. It is the physical path between communication components that that can mediate the propagation of signals for the purposes of telecommunication

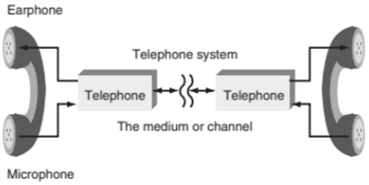


Transmission Modes

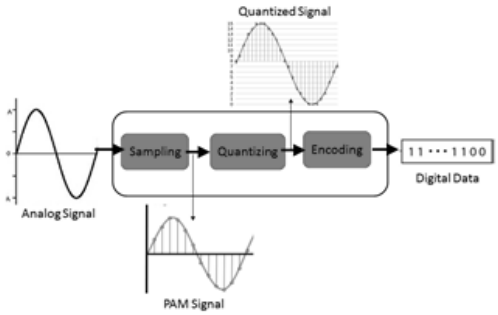
- Simplex – one-way communication, which is the simplest way to conduct electronic communication
- Half-Duplex – two-way communication in which only one party transmits at a time
- Full-Duplex – two-way communication in which each party can transmit and receive signals simultaneously with each other

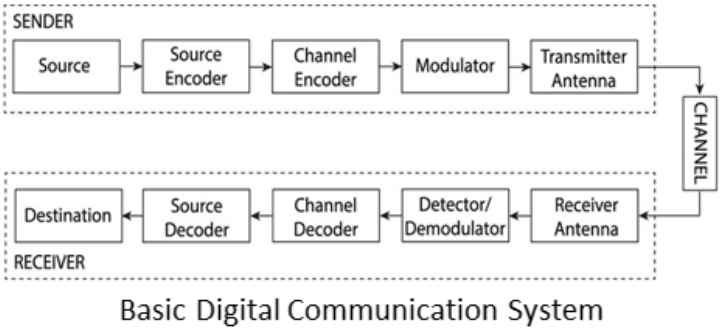






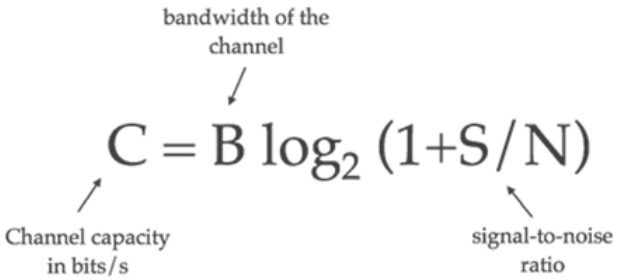
Digital Communications refers to the mode of communication where the information or the thought is encoded digitally as discreet signals and electronically transferred to the recipients.



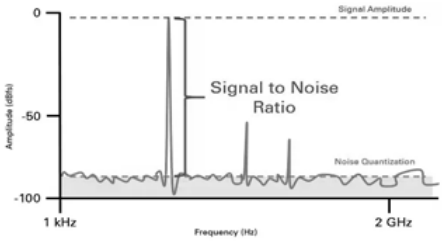


Basic Digital Communication System

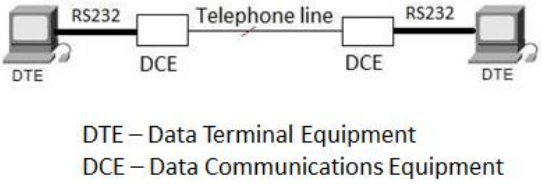
Information Theory studies the quantification, storage, and communication of information. It is the mathematical treatment of the concepts, parameters and rules governing the transmission of messages through communication systems



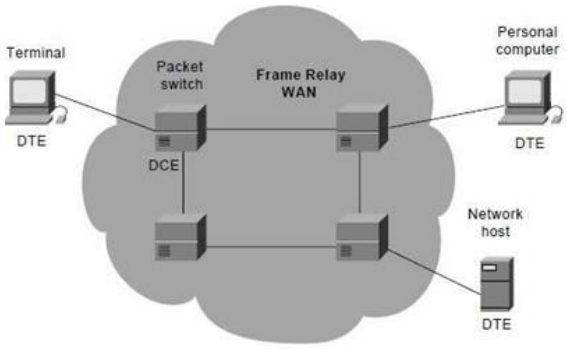
Shannon-Hartley Theorem



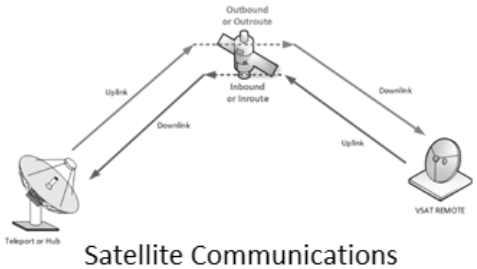
Data Communications mainly involves the process of using computing and communication technologies to transfer data from one place to another, and vice versa. It refers to the process of transmission of digital data between two or more computers.



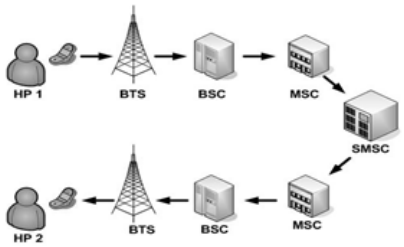
DTE – Data Terminal Equipment
DCE – Data Communications Equipment



Telecommunications is the exchange of information over significant distances by electronic means and refers to all types of voice, data and video transmission.

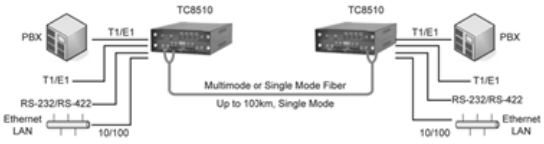


Satellite Communications



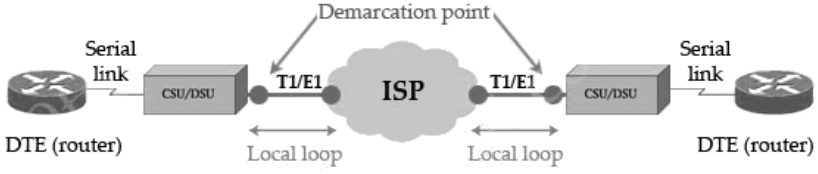
Cellular Communications

Terrestrial Microwave Communications



Fiber Optic Communications

Internet Communications allows sharing of information, ideas, or simply words over the Internet, which consists of a worldwide string of connected networks that exchanges data through packet switching using the standardized Internet Protocol Suite (TCP/IP).



ISP – *Internet Service Provider*

ASSESSMENT

Q&A

Answer what is asked in the following items. Each answer should be in a narrative form with at least 3 sentences and with normal formatting details.

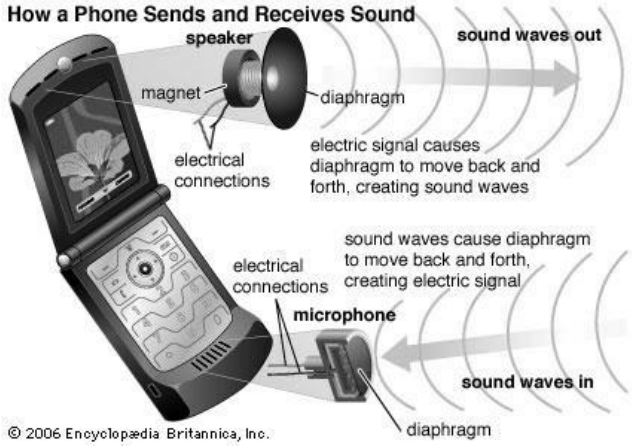
1. Explain the differences between signal and noise, including in terms of how they are generated.
2. How does a transceiver work, and how does it differ from a transponder?
3. Give examples of advantages and disadvantages of transmission lines, as well as of wireless technologies via antenna, for transmitting electronic signals.
4. In your own idea, what are the differences between digital communications and data communications? Mention the essential processes, techniques, and technologies involved.

Research Activity

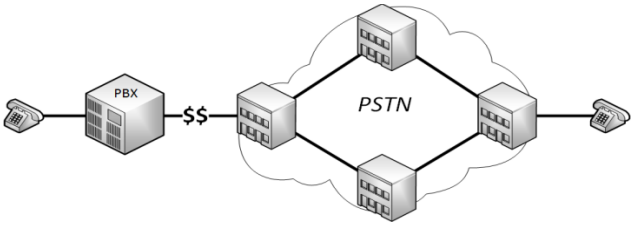
Watch the following YouTube tutorial about Cisco Packet Tracer:
Cisco Packet Tracer | Everything You Need to Know

Module 2: **Digital and Mobile Telephony**

Telephony is the collective term for the development, application, and deployment of telecommunication services for electronic transmission of voice, fax, or data, between distant parties. *Digital Telephony* uses computer hardware, software, and computer networks, that perform functions traditionally performed by telephone equipment.



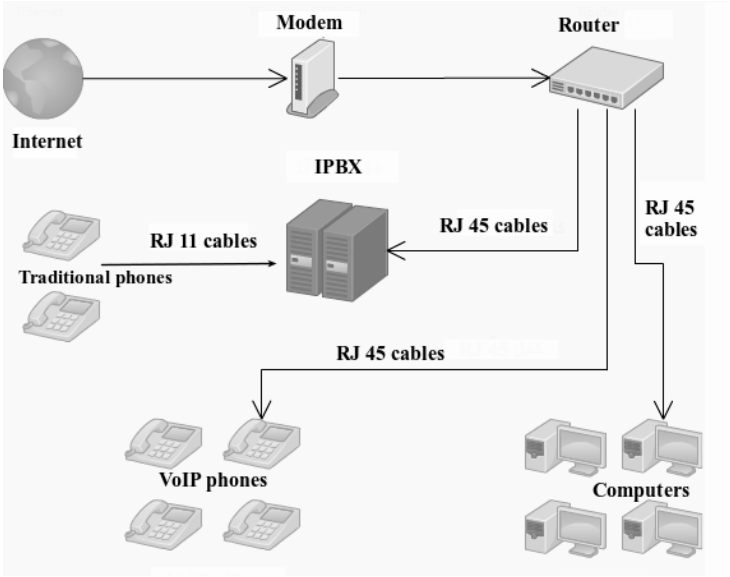
Public-Switched Telephone Network (PSTN) is the world's collection of interconnected voice-oriented public telephone networks. It is operated by national, regional, or local telephony operators, providing infrastructure and services for public telecommunication



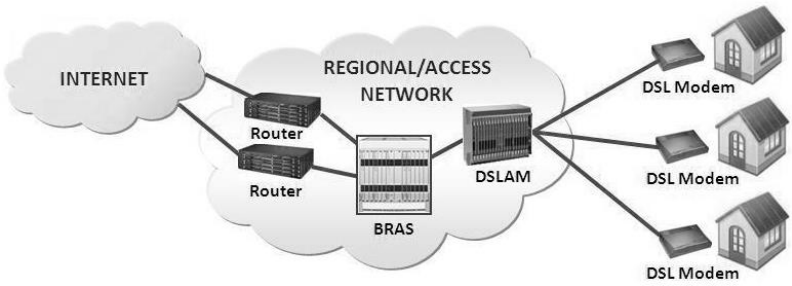
Private Branch Exchange (PBX) refers to the private telephone network used within a company or organization where the users of the phone system can communicate internally (within their company) and externally (with the outside world), using different communication channels like VoIP, ISDN or analog.

ITEM	PREMISE	HOSTED	Comments
Router	Common Industry Standard	Common Industry Standard	None
Switch/Power adapters	Either/or	Either/or	None
Cabling	Cat5/6, or Cat 3 if using digital devices	Cat5/6	Premise - if infrastructure critical
Key Service Unit/Server	Requires server	None required	Hosted means less equipment
Initial Investment	All Equipment paid upfront, or on lease	Options available for no upfront expense	Advantage-Hosted

Internet Protocol Private Branch Exchange (IP PBX) is a system that connects telephone extensions to the public switched telephone network (PSTN) and provides internal communication for a business.

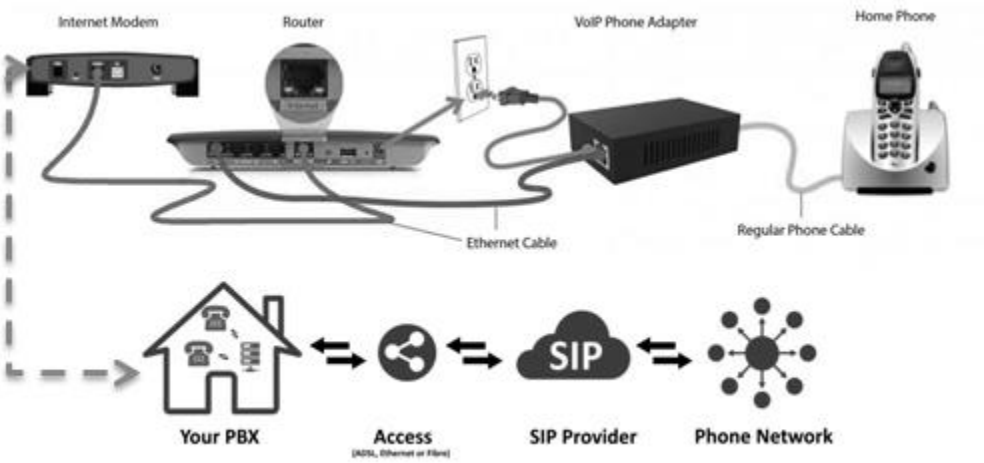


Digital Subscriber Line (DSL) is the technology that uses existing telephone lines to transport high-bandwidth *data*, such as multimedia and video, to service subscribers. It is a group of digital technologies that can provide high-speed digital signal transmission over the existing twisted-wire pair in local loops.

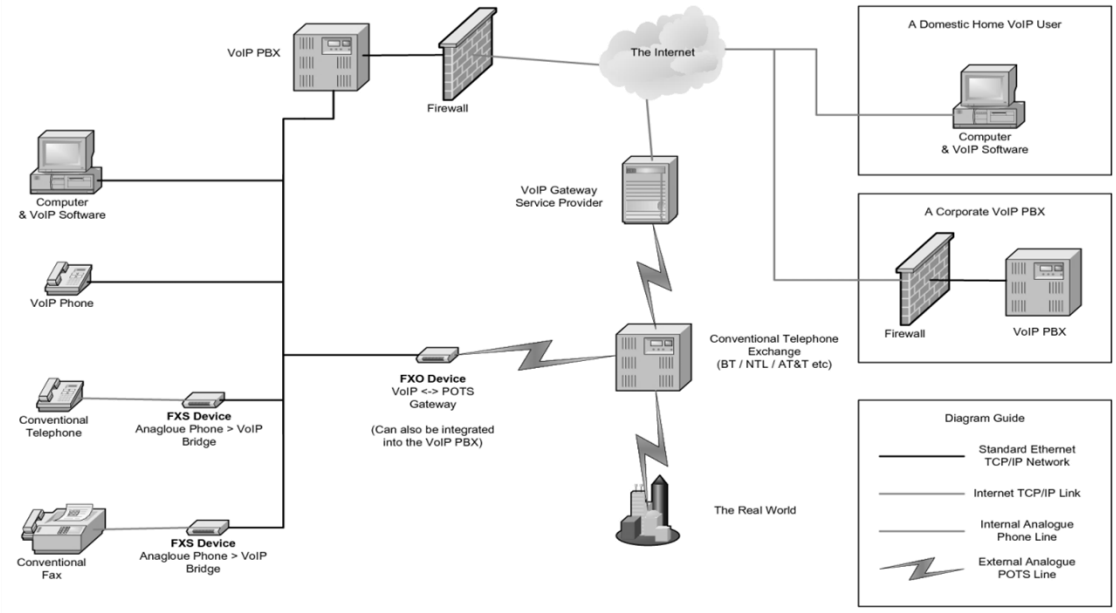


Type	Description	Data Rate Upstream Data Rate	Max Downstream Data Rate	Max Reach	POTS Support
HDSL	High Bit Rate - DSL	1.54Mbps	1.54Mbps	3650mtrs	No
ADSL	Asymmetric - DSL	800Kbps	8Mbps	5500mtrs	Yes
SDSL	Symmetric - DSL	2.3Mbps	2.3Mbps	6700mtrs	No
VDSL	Very High Bit Rate - DSL	16Mbps	52Mbps	1200mtrs	Yes
VDSL2	Very High Bit Rate - DSL (2nd Generation)	100Mbps	100Mbps	<1500mtrs	Yes

Voice over Internet Protocol (VoIP), also called *IP telephony*, is the method and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol networks, such as the Internet. ***Session Initiation Protocol*** (SIP) is a signaling protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video and messaging applications.

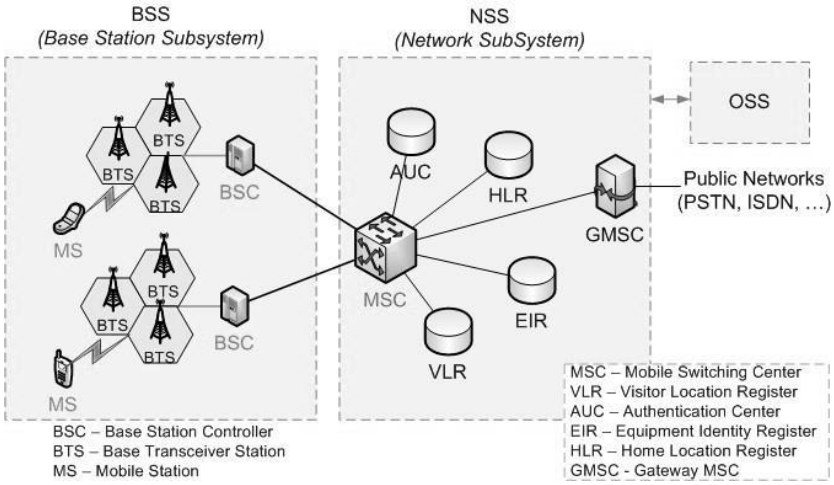


Basic VoIP Setup



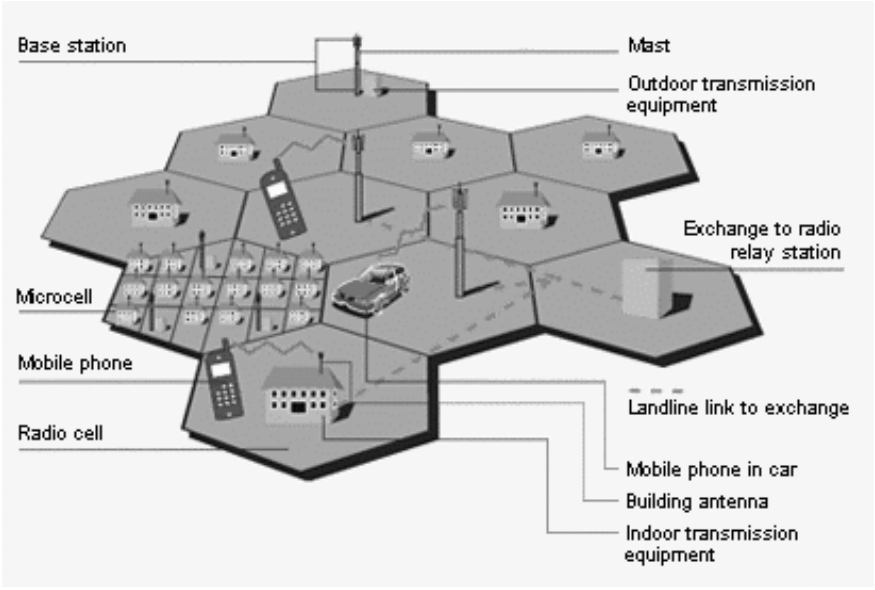
VoIP Gateway is the device that uses Internet Protocols to transmit and receive voice communications (VoIP).

Mobile Telephony or *cellular telephony* is the provision of telephone services to phones which may move around freely rather than stay fixed in one location



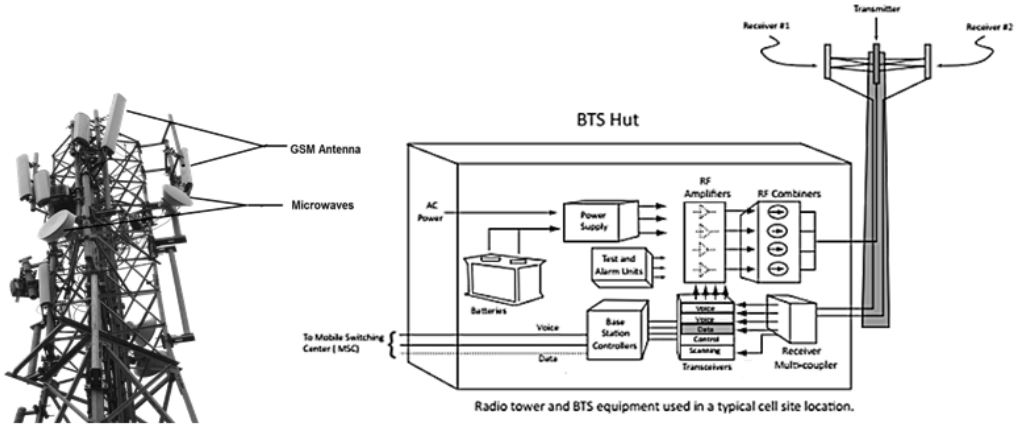
The "Cells"

Cellular communication is based on the geographic division of the communication coverage area into *cells*, and within cells. Each cell is allocated a given number of frequencies (or channels) that allow a large number of subscribers to conduct conversations simultaneously



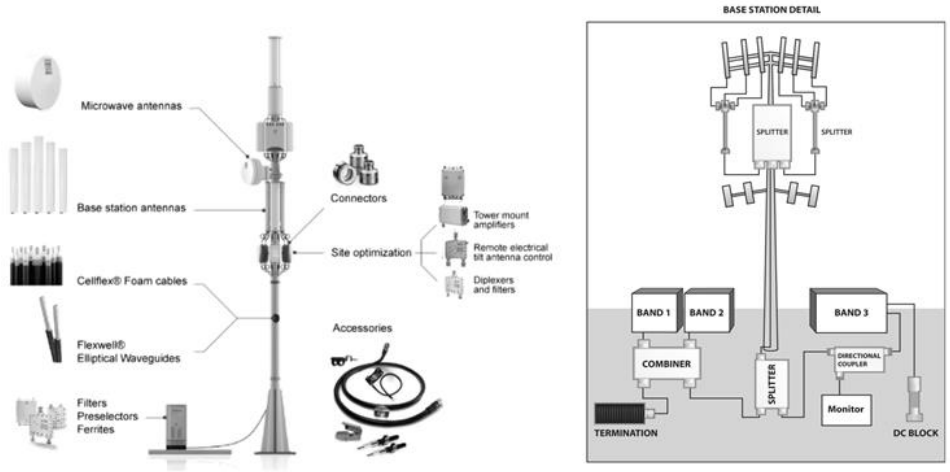
Global System for Mobile Communications (GSM) describes the protocols for second-generation digital cellular networks used by mobile devices such as mobile phones and tablets.

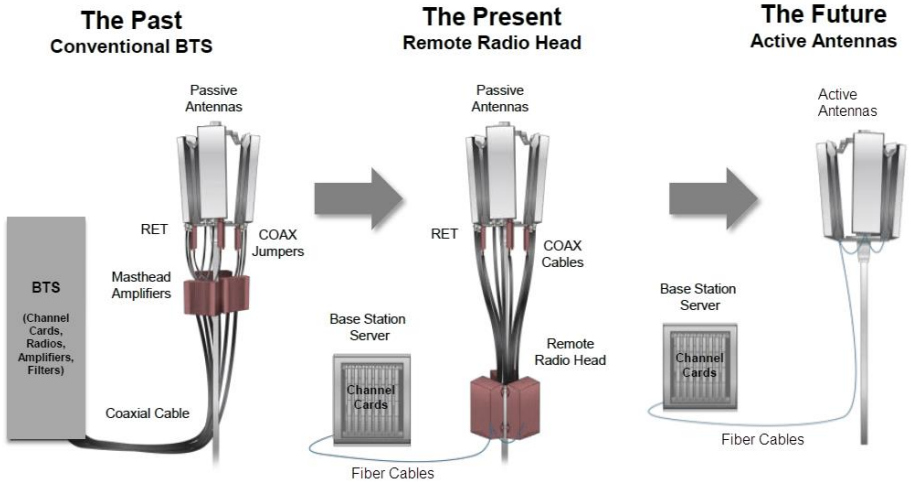
Base Transceiver Station (BTS) is the equipment that facilitates wireless communication between user equipment (UE) and a network.



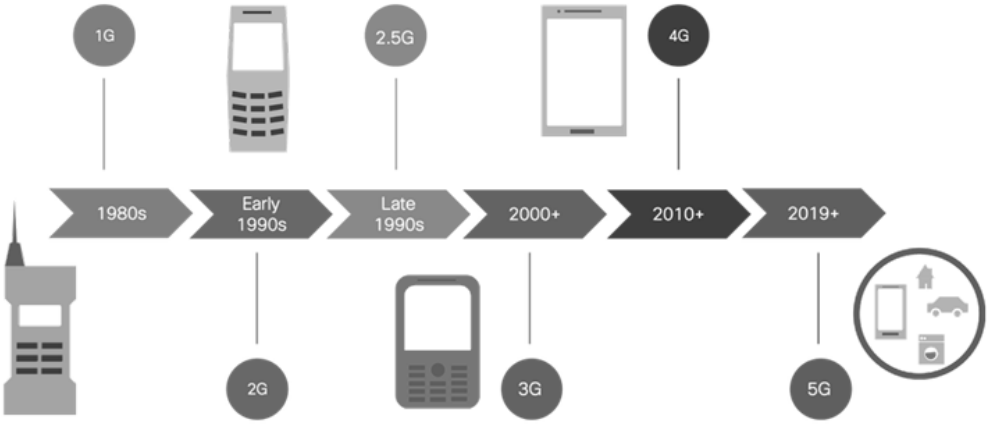
Radio tower and BTS equipment used in a typical cell site location.

The BTS Antenna

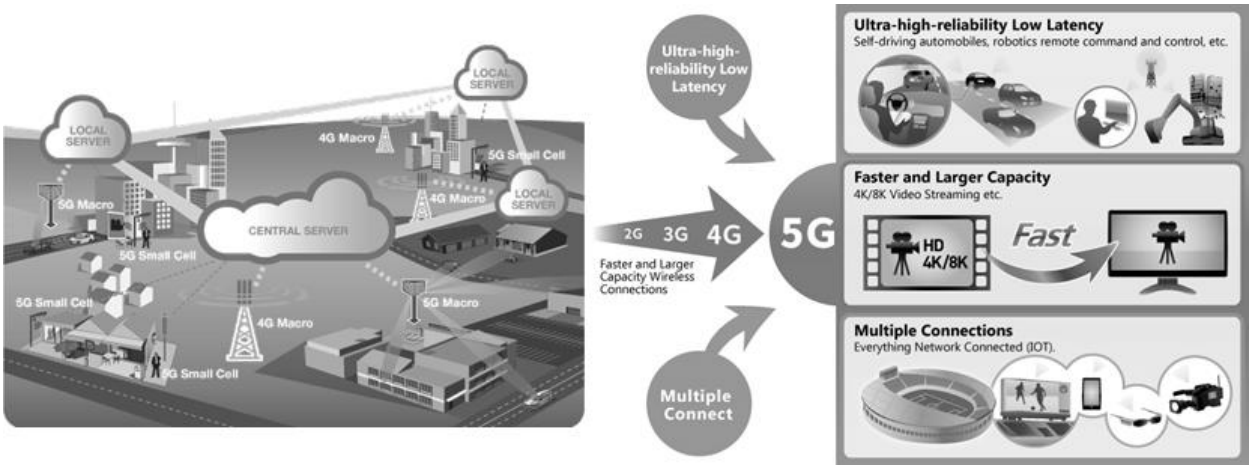


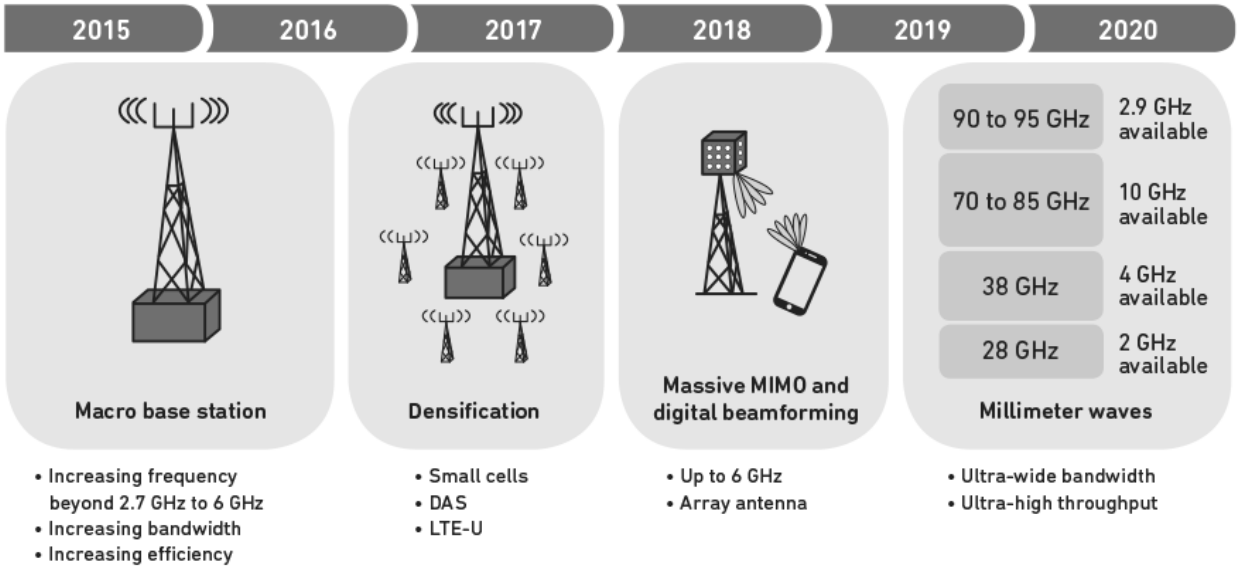


Evolution of Mobile Communications Technology



5G Mobile Technology





ASSESSMENT

Q&A

Answer what is asked in the following items. Each answer should be in a narrative form with at least 3 sentences and with normal formatting details.

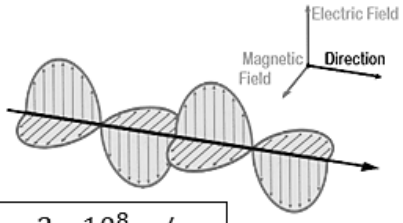
1. Discuss, in your own words, how does voice communication work using the processes and technologies involved in telephony.
2. What is the main difference between PSTN-based (or POTS) and IPBX telephone systems? Mention why VoIP telephone systems have become more preferred by corporations nowadays.
3. What is the reason behind mobile communications being also referred to as ‘cellular communications’?
4. In your own opinion, is it safe to build more BTSs and micro-stations within an urban area to enable and support 5G technologies? Defend your answer.

Research Activity

Watch the following YouTube tutorial about Cisco Packet Tracer:
Cisco Packet Tracer | Configuring VoIP Phones

Module 3: **Terrestrial and Satellite Communications**

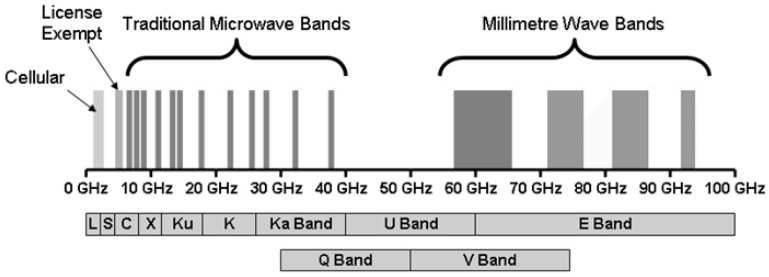
Radio Waves are electromagnetic (EM) waves best-known for their use in wireless communication technologies, such as TV, mobile phones and radios. They have frequencies as high as 300 gigahertz (GHz) to as low as 30 hertz (Hz).

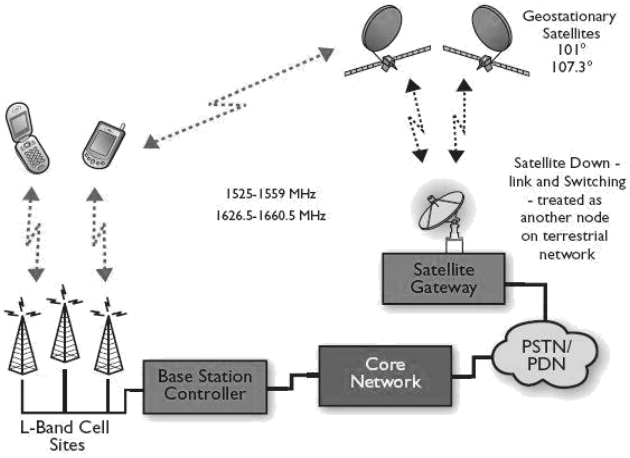


$$\lambda = \frac{c}{f} = \frac{3\ x\ 10^8\ m/s}{f}$$

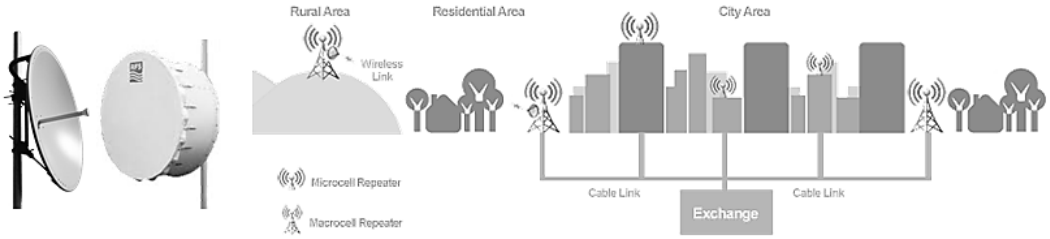
Name	Frequency	Wavelength
Extremely low frequencies (ELFs)	30–300 Hz	$10^7 - 10^6$ m
Voice frequencies (VFs)	300–3000 Hz	$10^6 - 10^5$ m
Very low frequencies (VLFs)	3–30 kHz	$10^5 - 10^4$ m
Low frequencies (LFs)	30–300 kHz	$10^4 - 10^3$ m
Medium frequencies (MFs)	300 kHz–3 MHz	$10^3 - 10^2$ m
High frequencies (HFs)	3–30 MHz	$10^2 - 10^1$ m
Very high frequencies (VHFs)	30–300 MHz	$10^1 - 1$ m
Ultra high frequencies (UHFs)	300 MHz–3 GHz	$1 - 10^{-1}$ m
Super high frequencies (SHFs)	3–30 GHz	$10^{-1} - 10^{-2}$ m
Extremely high frequencies (EHFs)	30–300 GHz	$10^{-2} - 10^{-3}$ m

Microwaves are radio waves with frequencies between 300 MHz (1 m) and 300 GHz (1 mm). They travel by line-of-sight (LOS); so terrestrial microwave communication links are limited by the visual horizon to about 40 miles (64 km). ***Microwave Transmission*** is an LOS wireless communication technology that uses high frequency beams of radio waves to provide high speed wireless connections that can send and receive voice, video, and data information.

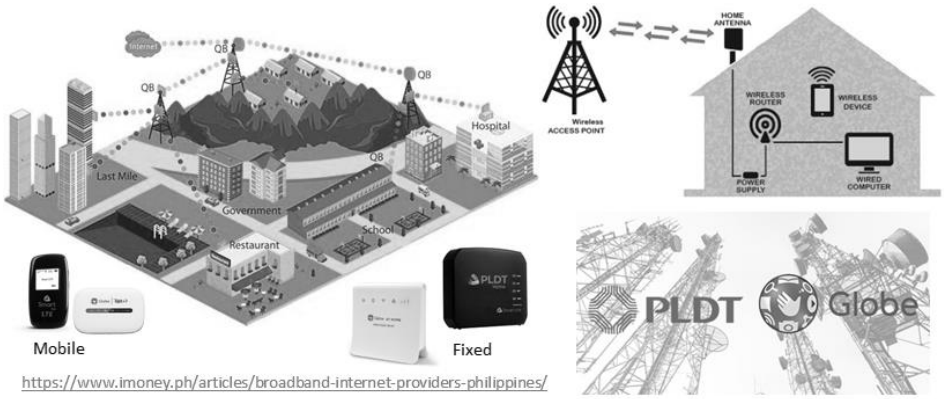




Microwave Terrestrial Communications (or *point-to-point communication*) is a wireless point-to-point connection between two communication endpoints or nodes. It employs Earth-based transmitters and receivers in the form of telephone relay towers, which are placed every few miles to relay telephone signals cross-country. Transmissions typically use a parabolic antenna that produces a narrow, highly directional signal, which is why LOS between the linked nodes must be maintained.

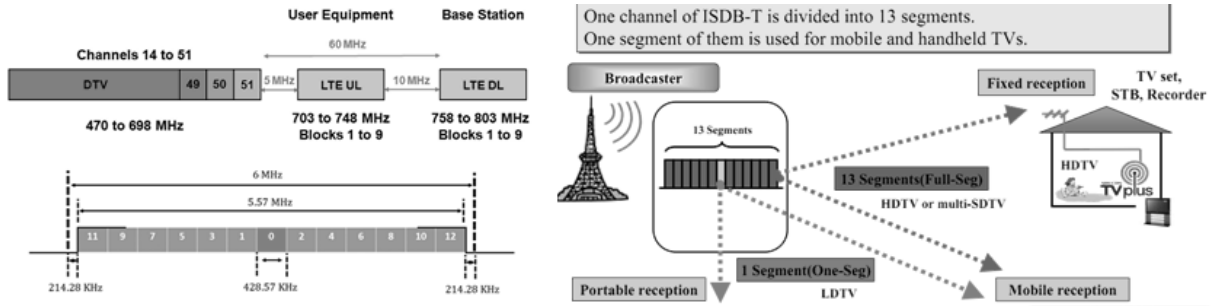


Wireless ISP



https://www.imoney.ph/articles/broadband-internet-providers-philippines/

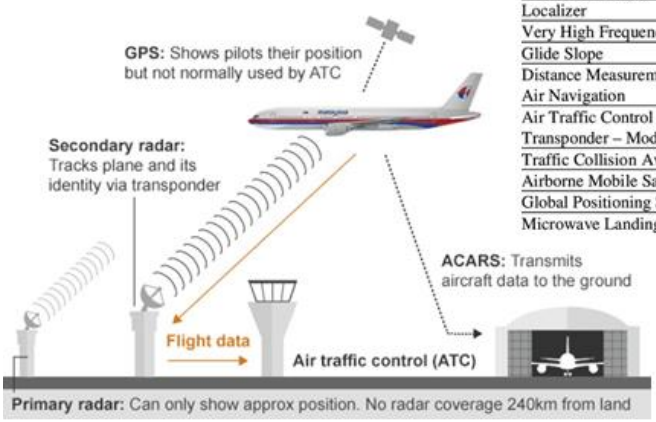
Digital Terrestrial TV (DTTV) Broadcast



DTTV Standards

- **Advanced Television Systems Committee** (ATSC) – *USA*
- **Digital Video Broadcast – Terrestrial** (DVB-T) – *Europe*
- **Integrated Services Digital Broadcasting – Terrestrial** (ISDB-T) – *Japan → Used in the Philippines*

Aircraft Navigation Systems

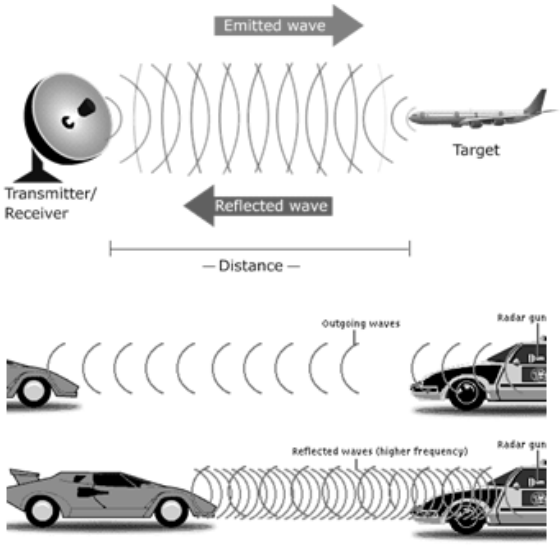


Aircraft Systems	Abbreviation	Receive Frequency Range (MHz)
HF Communications	HF	2.850-23.350
Marker Beacon	MB	74.8 –75.2
VHF Omni-Range	VOR	108 – 117.95
Localizer	LOC	108.1-111.95
Very High Frequency Communication	VHF	118 - 137
Glide Slope	GS	328.6 –335.4
Distance Measurement Equipment/ Tactical Air Navigation	DME/TACAN	962 - 1213
Air Traffic Control Transponder – Mode S	ATC Mode S	1030
Traffic Collision Avoidance System	TCAS	1090
Airborne Mobile Satellite Service	AMSS	1530 –1559
Global Positioning System	GPS	1575.42 +/- 2
Microwave Landing System	MLS	5031 - 5090.7

Main Navigational Aids:

- Instrument Landing System (ILS)
- Air Traffic Management (ATM)
- Radar and Pilot Position Reports
- Voice Communication

Radio Detection and Ranging (RADAR)

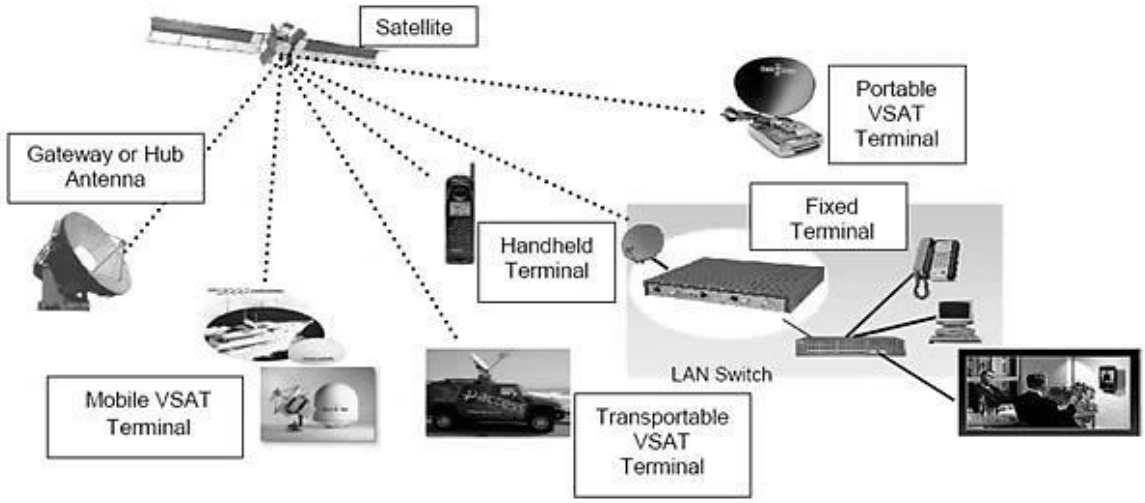


Band	Frequency (GHz)
L Band	1-2
S Band	2-4
C Band	4-8
X Band	8-12
KU Band	12-18
K Band	18-27
KA Band	27-40
V Band	40-75
W Band	75-110
E band	
E band Fixed Point to Point	71-76
Automotive radar	77-81
E band Fixed Point to Point	81-86
E band Fixed Point to Point	92-95

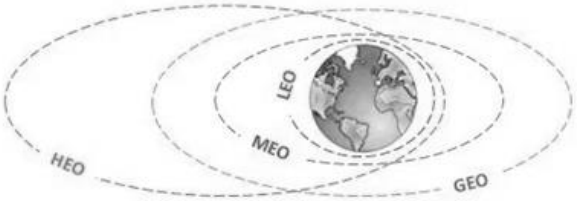
Slotted-Waveguide Radar Antenna

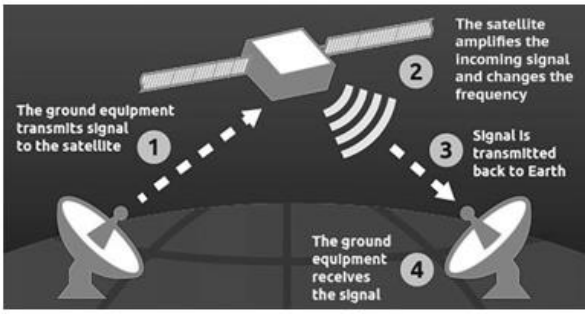
Parabolic Radar Antenna

Satellite Communications is the use of artificial satellites to provide communication links between various points on Earth. Telecommunication satellites are designed to relay several, or more usually many, signals simultaneously.



Parameter	LEO	MEO	GEO
Satellite Height	500–1500 km	5000–12000 km	35,800 km
Orbital Period	10–40 minutes	2–8 hours	24 hours
Number of Satellites	40–80	8–20	3
Satellite Life	Short	Long	Long
Number of Handoffs	High	Low	Least(none)
Gateway Cost	Very Expensive	Expensive	Cheap
Propagation Loss	Least	High	Highest



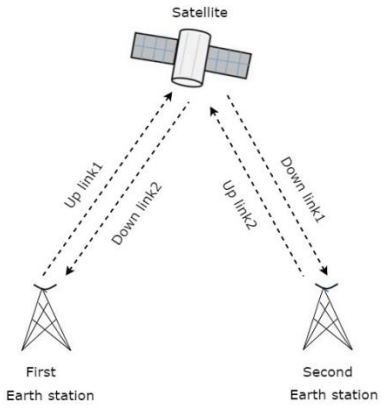


Advantages of Satellite

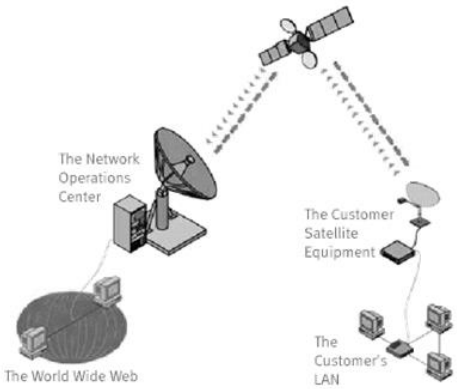
- ✓ Coverage area is very high.
- ✓ Transmission cost is independent of the coverage area.
- ✓ Higher bandwidths are possible.

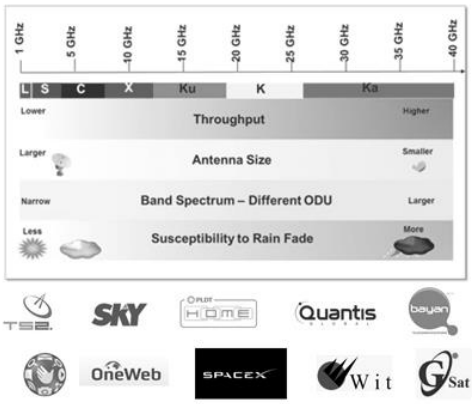
Disadvantages of Satellite

- ✓ Launching satellites into orbits is a costly process.
- ✓ Bandwidths are gradually used up.
- ✓ High propagation delay.

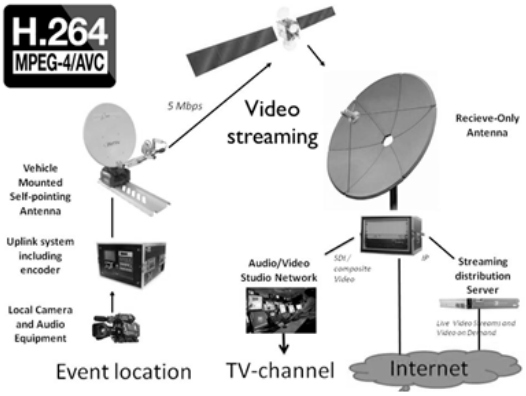


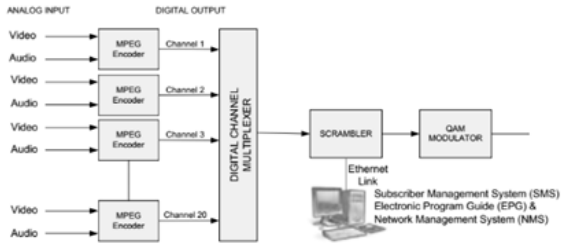
Satellite ISP and TV Broadcast (or Direct Broadcast TV, DBT)





IP and Satellite Streaming

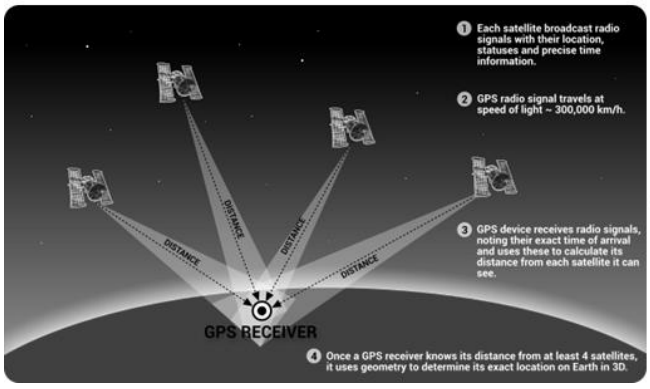


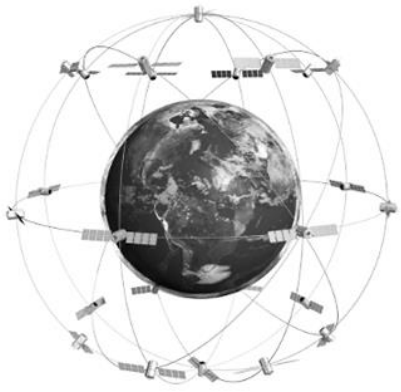


Band Designation	Deep Space Bands (for spacecraft greater than 2 million km from Earth)		Near Earth Bands (for spacecraft less than 2 million km from Earth)	
	Uplink (Earth to space)	Downlink (space to Earth)	Uplink (Earth to space)	Downlink (space to Earth)
S-band	2110–2120	2290–2300	2025–2110	2200–2290
X-band	7145–7190	8400–8450	7190–7235	8450–8500
K-band	*	*	*	25500–27000
Ka-band	34200–34700	31800–32300	*	*

* No allocation or not supported by the DSN.

Global Positioning System (GPS) is a US-owned utility that provides users with positioning, navigation, and timing (PNT) services. This system consists of three segments: the space segment, the control segment, and the user segment.





ASSESSMENT

Q&A

Answer what is asked in the following items. Each answer should be in a narrative form with at least 3 sentences and with normal formatting details.

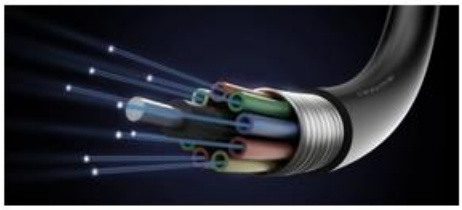
1. What are the pros and cons of microwave transmission compared to radio wave transmission using much lower frequencies?
2. Give at least 3 examples of practical applications of RADAR. Provide a brief explanation on each.
3. Research about satellite TV and satellite ISPs, and discuss their basic working principles.
4. Explain how does GPS work and why it has been essential in the Industry 4.0.

Research Activity

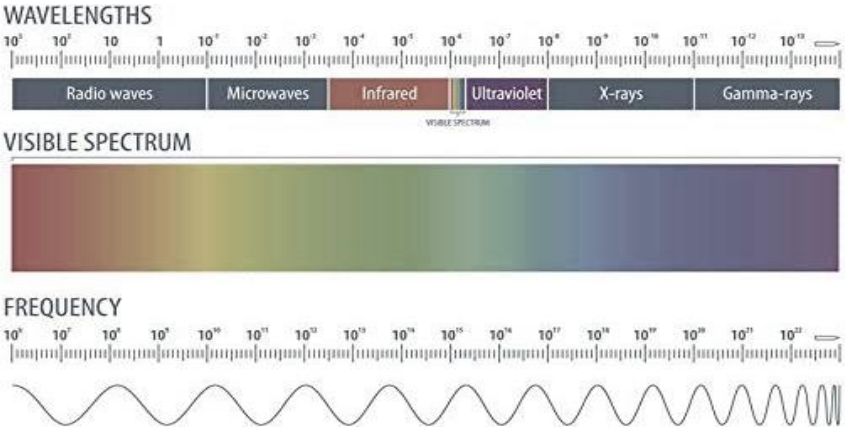
Watch the following YouTube tutorial about Cisco Packet Tracer:
Cisco Packet Tracer | Wireless Networking

Module 4: **Fiber Optics Systems and Technologies**

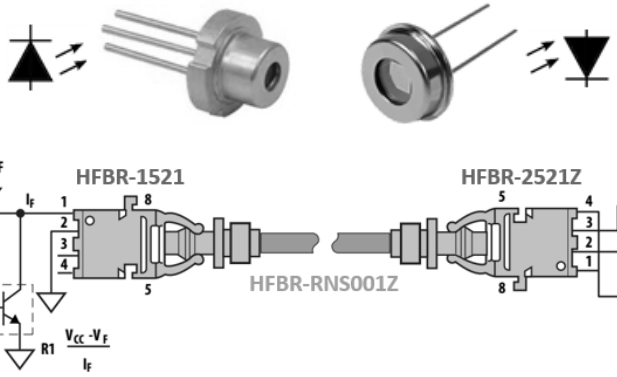
Fiber Optic Cable (FOC or OFC) is a high-speed data transmission medium consisting one or more strands of glass, each only slightly thicker than a human hair. It can support data transmissions rated at 10 Gbps, 40 Gbps, and 100 Gbps.



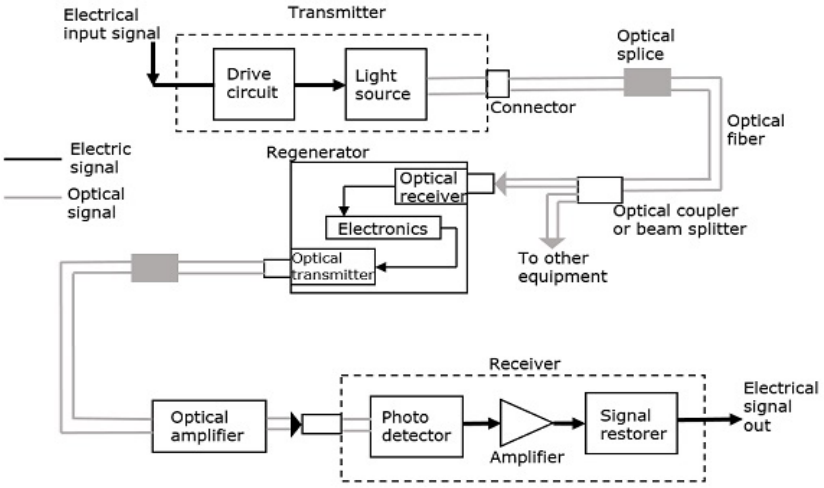
The Visible Light Spectrum



Laser diode (LD) module converts electronic signal into optical intensity signal for FOC transmission while ***photodiode*** (PD) module converts the transmitted light signal back into electronic signal.

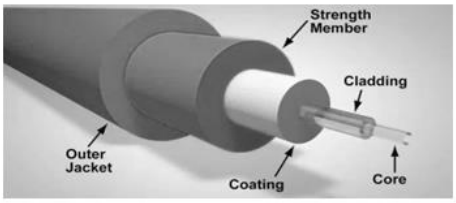


How Fiber Optics Work



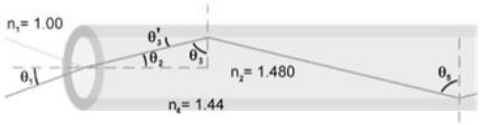
Physical Advantages of FOC

- ✓ much higher capacity and lighter weight
- ✓ no spark hazards
- ✓ more flexible and corrosion resistant
- ✓ raw material is cheaper
- ✓ lasts longer



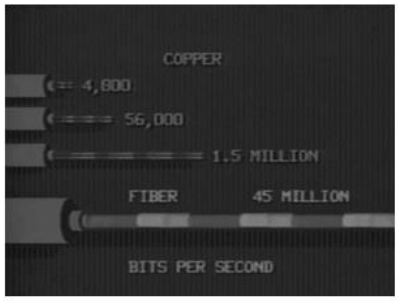
Functional Advantages of FOC

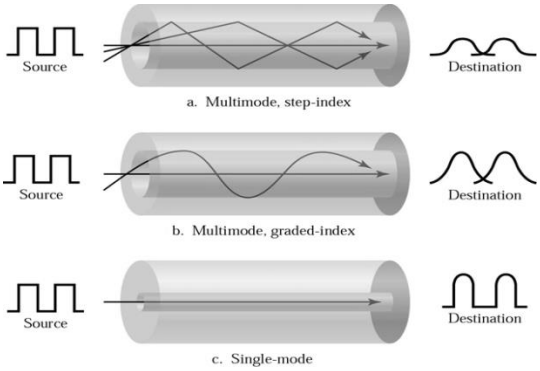
- ✓ higher bandwidth and amount of data
- ✓ very low power loss
- ✓ provides high transmission security
- ✓ immune to interferences and noise

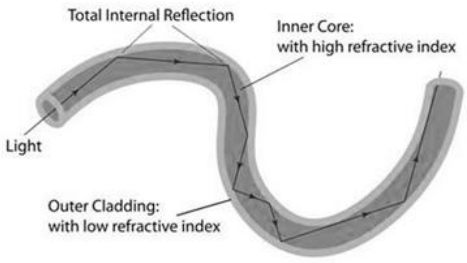


Physical Disadvantages of FOC

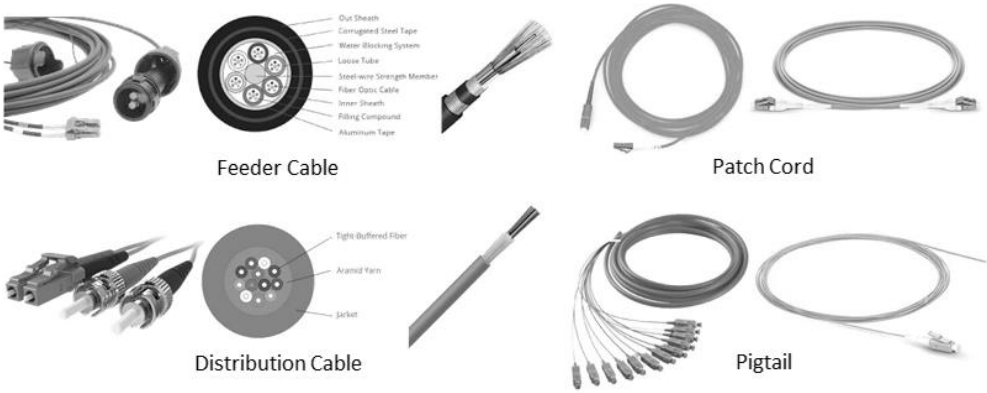
- ✓ fragile if not enclosed in a plastic sheath
- ✓ high installation cost
- ✓ no. of repeaters increases with distance



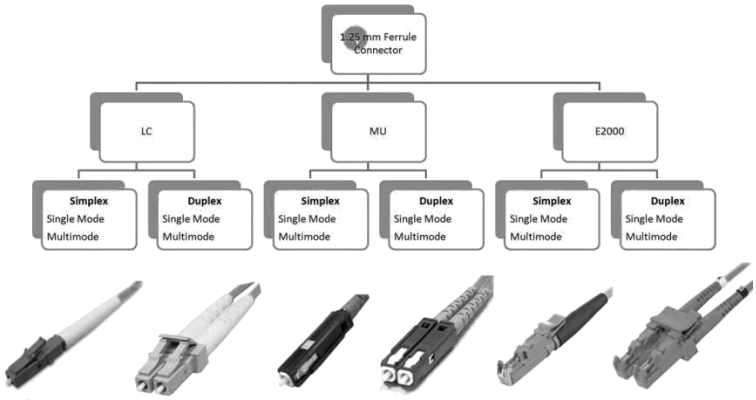


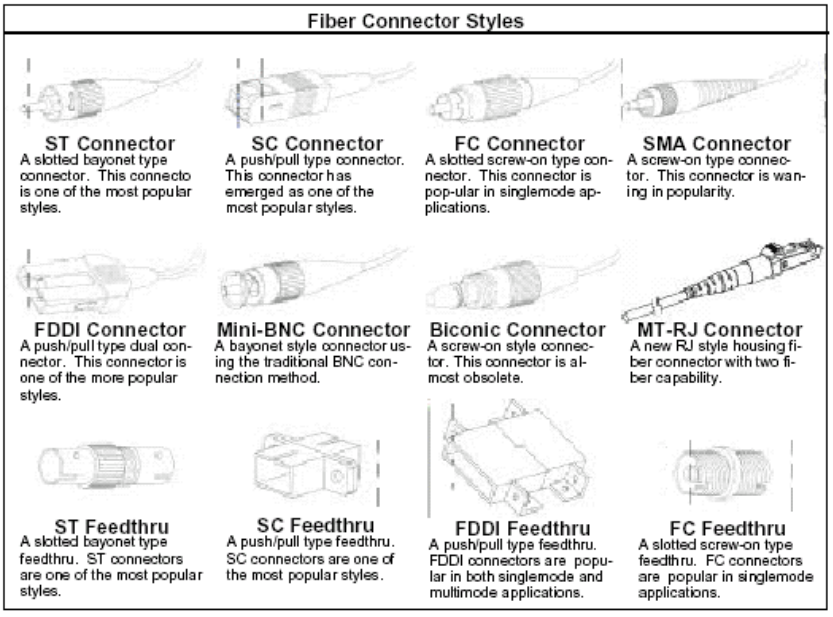


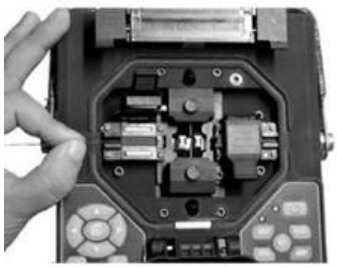
Classifications of FOC



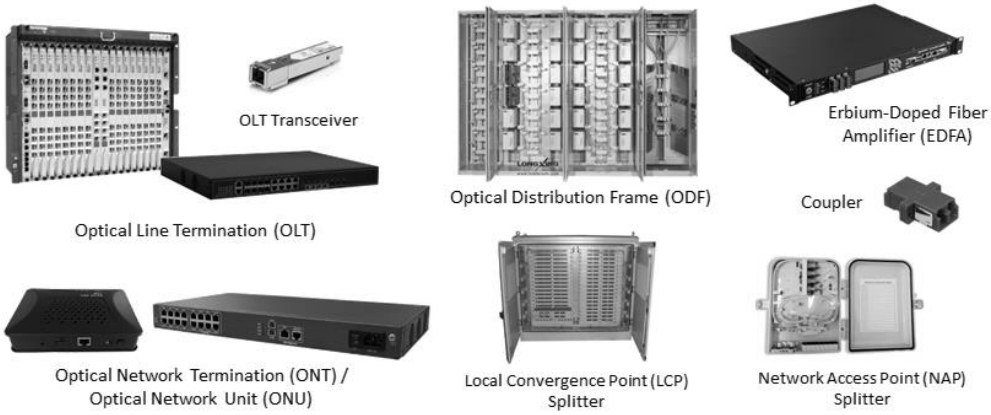
FOC Connectors



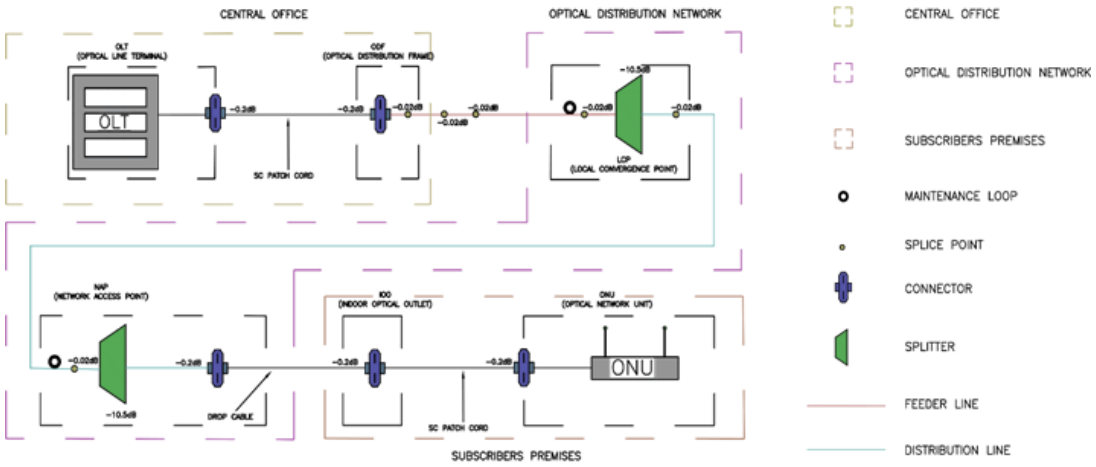




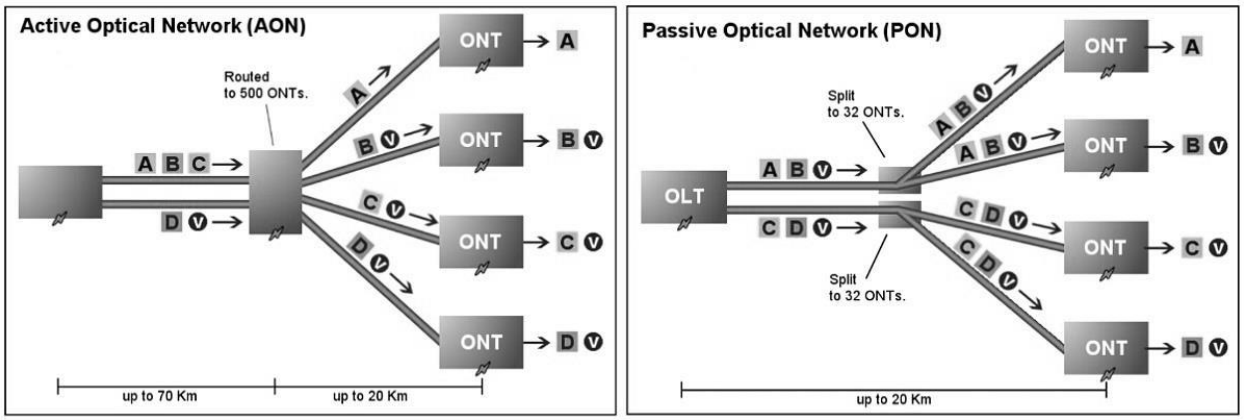
Key Components of an Optical Network



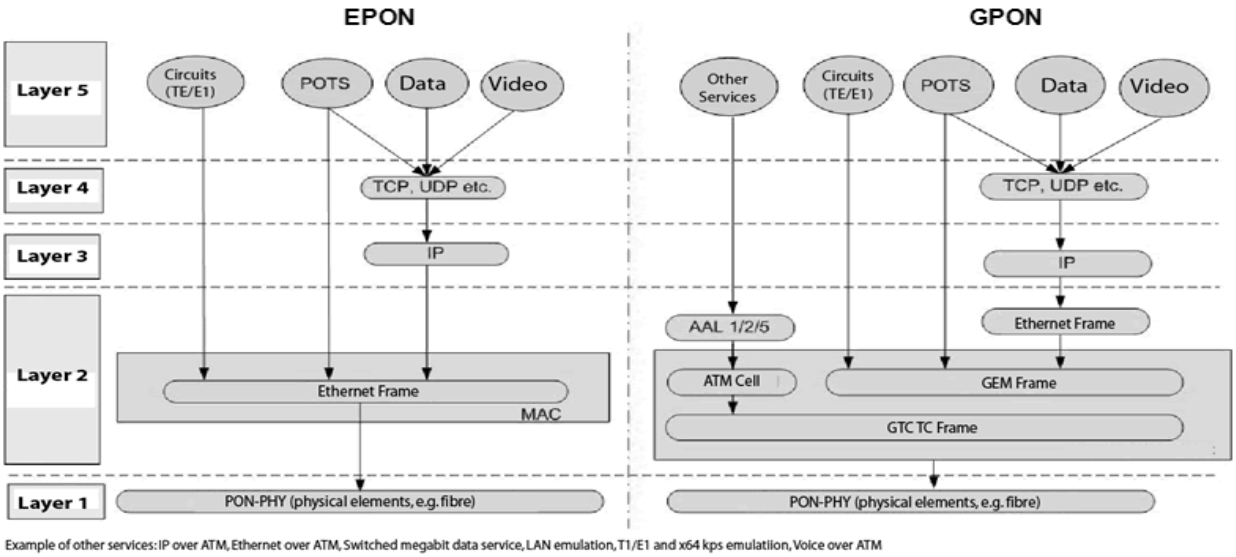
Example of an Optical Network Design



Two Types of Optical Network



Ethernet Passive Optical Network (EPON) and Gigabit Passive Optical Network (GPON)



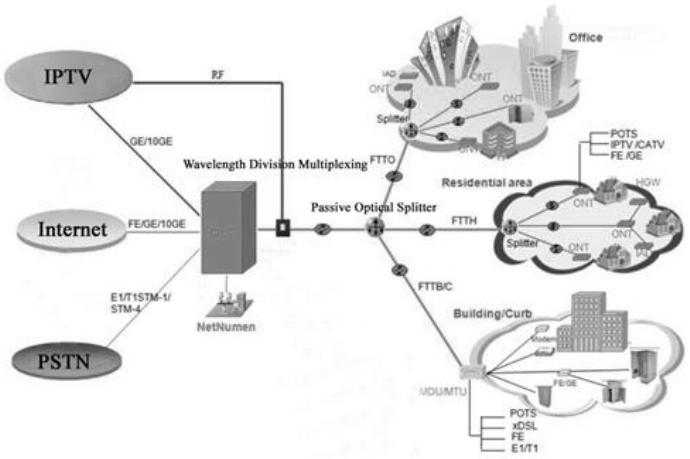
Category	EPON	GPON
standard	IEEE 802.3ah	ITU-T G.984
Upstream	1310nm	1310nm
Downstream	1550nm	1490&1550nm
Protocol	Ethernet	ATM, Ethernet, TDM, GEM
Bandwidth	Down ≤ 1.25Gbps UP ≤ 1.25Gbps	Down ≤ 2.4Gbps UP ≤ 2.4Gbps
Max Distance	10 or 20km	10 or 20km
Max Split Ratio	64 users	64 users

	IEEE 802.3ah (EPON)	ITU-T G.984 (GPON)
Downstream	1250 Mbps	2500 or 1250 Mbps
Upstream	1250 Mbps	1250 or 622 Mbps
Split ratio	1:32	1:32, 1:64, (1:128 planned)
Downstream Efficiency	~72% as a result of: 8B/10B encoding (20%) Overhead & Preamble (8%)	~92% as a result of: NRZ scrambling (no encoding) Overhead (8%)
Revenue BW	900 Mbps	2300 Mbps
OAM&P	OAM is optional and minimally supports: failure indication, loop-back and link monitoring to the ONT. Provisioning and services are out of scope.	OMCI is mandatory. Full FCAPS on ONT and services.
Security	None specified. AES used by various vendors.	AES is part of the standard.
Network Protection	None specified.	Optional 50 mS switching time.
TDM transport	Circuit Emulation over Ethernet (ITU-T Y.1413 or MEF or IETF)	Native via GEM or Circuit Emulation over Ethernet (ITU-T Y.1413 or MEF or IETF)
Interoperability	None specified	FSAN and ITU-T

GPON aims at transmission speeds of at least 1.2 Gbps, with speed combinations of:

- 1.2 Gbps up, 2.4 Gbps down
- 2.4 Gbps up, 2.4 Gbps down

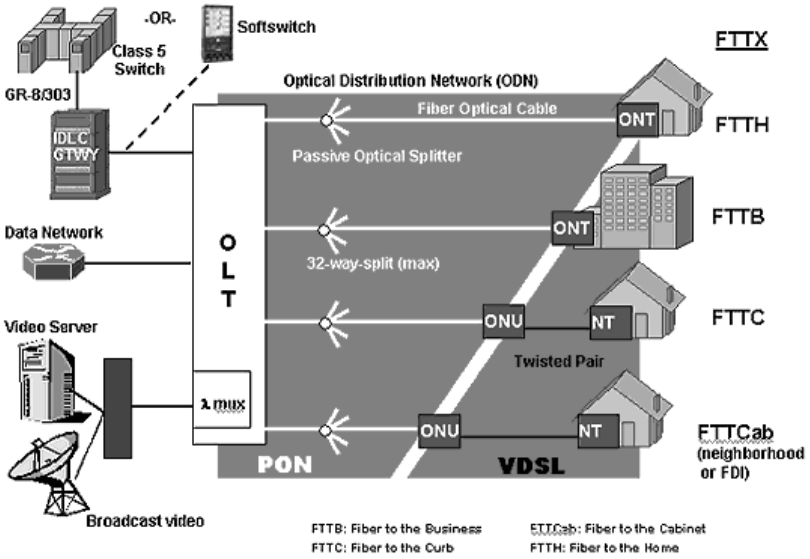
Services	Bandwidth
Data Download	10 Mbps
VoIP and video-conference	1 Mbps
Multimedia contents	2 Mbps
On-line Gaming	1 Mbps
SD Digital TV	3 Mbps
HD Digital TV	8 Mbps
Additional TV channels	16 Mbps



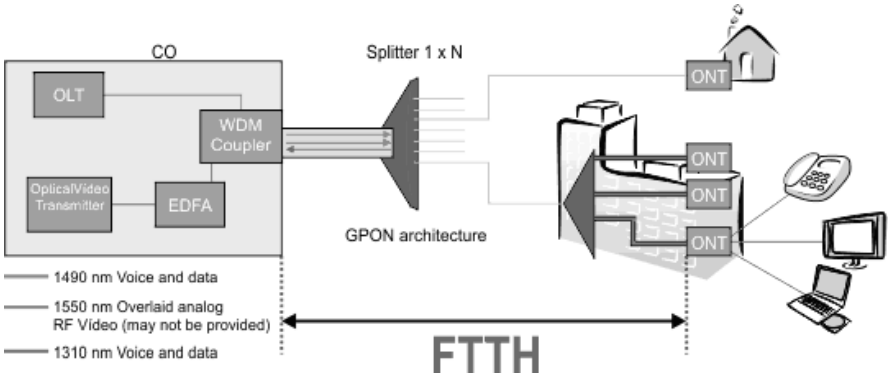
GPON Terminologies

- ***Service*** is defined as a network service required by the operators.
- ***Optical Access Network*** (OAN) is an access network towards the network side, it is also known as SNI (Service Network Interface).
- ***Optical Distribution Network*** is where all passive components from the PON Port of OLT to the PON Port of ONT come towards downstream side.
- ***Physical Reach*** is defined as the maximum physical distance between the ONU/ONT and the OLT. In GPON, two options are defined for the physical reach: 10km and 20km.
- ***Logical Reach*** is the maximum distance that can be covered for a particular transmission system, regardless of the optical budget. In GPON, the maximum logical reach is defined as 60 kms.
- ***Differential Fiber Distance*** (DFT) the difference in the distance between the nearest and the farthest ONU/ONT from the OLT. In GPON, the maximum differential fiber distance is 20 km.
- ***Mean Signal Transfer Delay*** is the average of the upstream and downstream delay values between reference points. This value is determined by measuring round-trip delay and then dividing by 2. GPON must accommodate services that require a maximum mean signal transfer delay of 1.5 ms.
- ***Split Ratio*** determines cost over optical power and bandwidth splitting, which creates the need for an increased power budget to support the physical reach. Split ratios of up to 1:64 are realistic for the physical layer, given current technology.

Fiber to the X (FTTX) or ***fiber-in-the-loop*** is a generic term for any broadband network architecture using optical fiber to provide all or part of the local loop used for last mile telecommunications.



Fiber-to-the-Home (FTTH)



Optical Fiber Communication Bands

Band name	Description	Range [nm]
O-band	Original	1260-1360
E-band	Extended	1360-1460
S-band	Short wavelength	1460-1530
C-band	Conventional	1530-1565
L-band	Long wavelength	1565-1625
U-band	Ultra-long wavelength	1625-1675

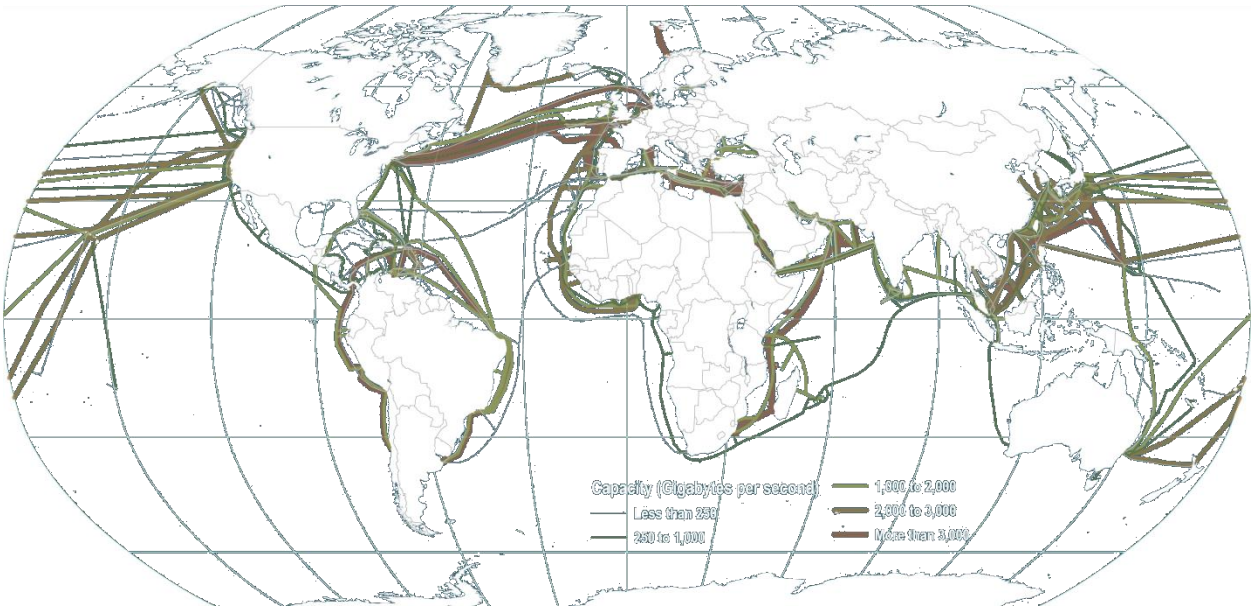
Splitting Ratio	Power per User (%)	Loss Calculation (dB)	Insertion Loss (dB)
1:2	50.00 %	- 3.01	- 3
1:4	25.00 %	- 6.02	- 6
1:8	12.50 %	- 9.03	- 9
1:16	6.25 %	- 12.04	- 12
1:32	3.13 %	- 15.04	- 15
1:64	1.56 %	- 18.07	- 18
1:128	0.78 %	- 21.08	- 21

DSL vs FTTH PON Data Rates

Transport	ADSL	ADSL2	ADSL2+	VDSL	VDSL2	FTTH PON
Max bandwidth	D:8M	12M	24M	55M	100M	100+
	U:1M	3.5M	1M	19M	100M	100+
Distance	3-5KM			<=1.3KM		<=100KM

- **ISDN**: 2B + D = 2 × 64 + 16 = 144 Kbps
- **HDSDN**: American standard 0.51mm, 2Mbps at max 5km.
- **ADSL**: 3-5 km 8 Mbps
- **ADSL2**: 3-5 km 12 Mbps
- **ADSL2+**: 3-5 km 24 Mbps
- **VDSL**: ≤ 1.3 km, 55 Mbps; VDSL2 upstream/downstream 100 Mbps

Global Submarine Cable Network



ASSESSMENT

Q&A

Answer what is asked in the following items. Each answer should be in a narrative form with at least 3 sentences and with normal formatting details.

1. What makes the visible light spectrum useful for fiber optic communications?
2. Telecommunications and Internet connection in the Philippines saw a great leap when the first transatlantic FOC link to other nations was installed. What do you think is the reason behind this statement?
3. Summarize the differences between EPON and GPON in terms of specifications and applications.
4. Why FTTH has now become the more preferred service over DSL? How does it work?

Research Activity

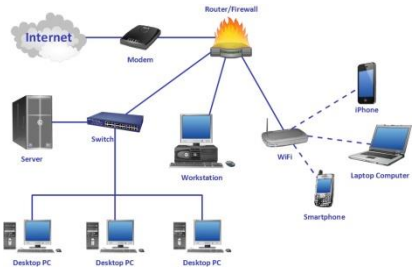
Watch the following YouTube tutorial about Cisco Packet Tracer:
Cisco Packet Tracer | Router to DSL Modem with ISP Configurations

Introduction to Network Engineering

(CMPE 30114 – Data and Digital Communications)

2 Chapter

I. OVERVIEW



Network engineering basically involves the design, implementation, and administration of computer infrastructures based on business needs, evaluating how information should flow throughout and outside the organization. It usually requires a significant amount of time charting data flow, especially as the network grows in size and complexity. Network engineers enable data to pass between computers in a network to facilitate communication between users. Their responsibilities include setting up, developing and maintaining computer networks within an organization or between organizations.

II. MODULE OBJECTIVES

After successful completion of modules 5-8 of Chapter 2, you should be able to:

1) Remember important concepts and principles in data communications;
2) Understand how the Ethernet and Wi-Fi work;
3) Evaluate the significance of the client-server architecture, IP addressing, and cybersecurity; and
4) Apply the processes in designing and managing computer networks in a real-world setup and also in engineering projects.

III. COURSE MATERIALS

Suggested Online Resources for Further Learning

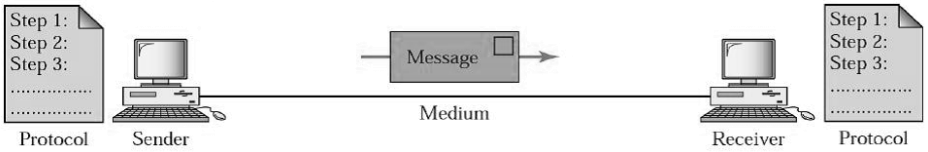
- Downloadable Course AVPs: https://bit.ly/3lp25qa
- Downloadable Course PDFs: https://bit.ly/3FtitOt

Module 5: **Principles of Data Communications**

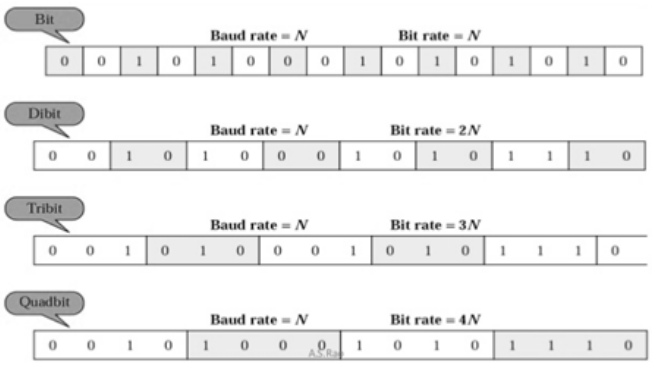
Data Communications is the transmission of digital data between two or more computers. It involves processes using computing and communication technologies to transfer data from one place to another, and vice versa. It aims to provide the highest possible transmission rate of digital data between two or more computers at the lowest possible power and with the least possible noise. It is intended to provide the rules (protocols) and regulations (standards) that will allow computers with different operating systems, languages, and locations to share resources.

Main Components of Data Communications

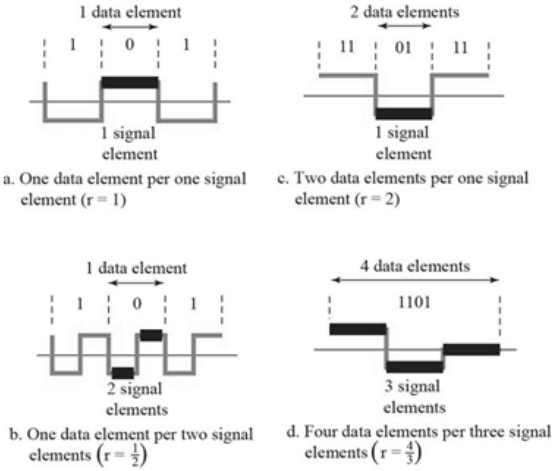
- Sender
- Receiver
- Medium
- Message
- Protocol



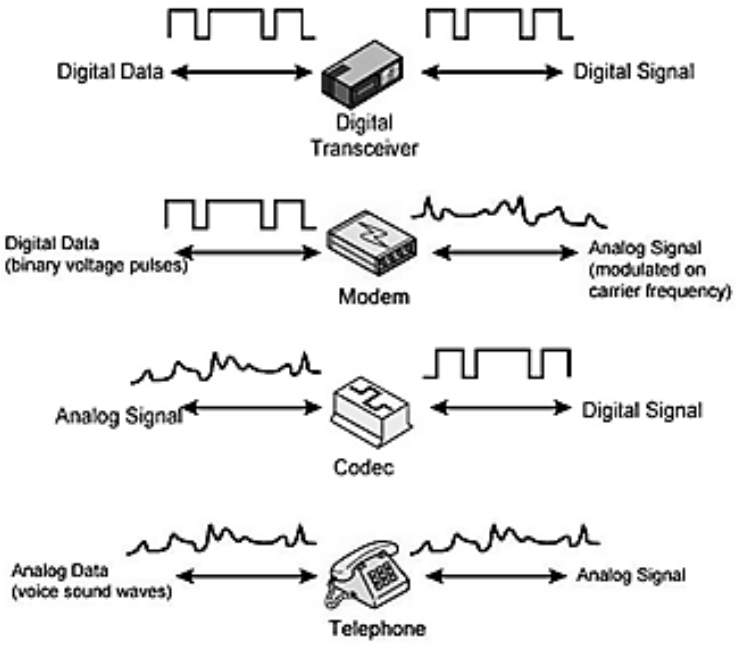
Data is information in numerical form that can be digitally transmitted or processed**,** while ***signal*** is a function that conveys information and can be used to transfer data from one device to another device. Both can have either an analog or a digital form.

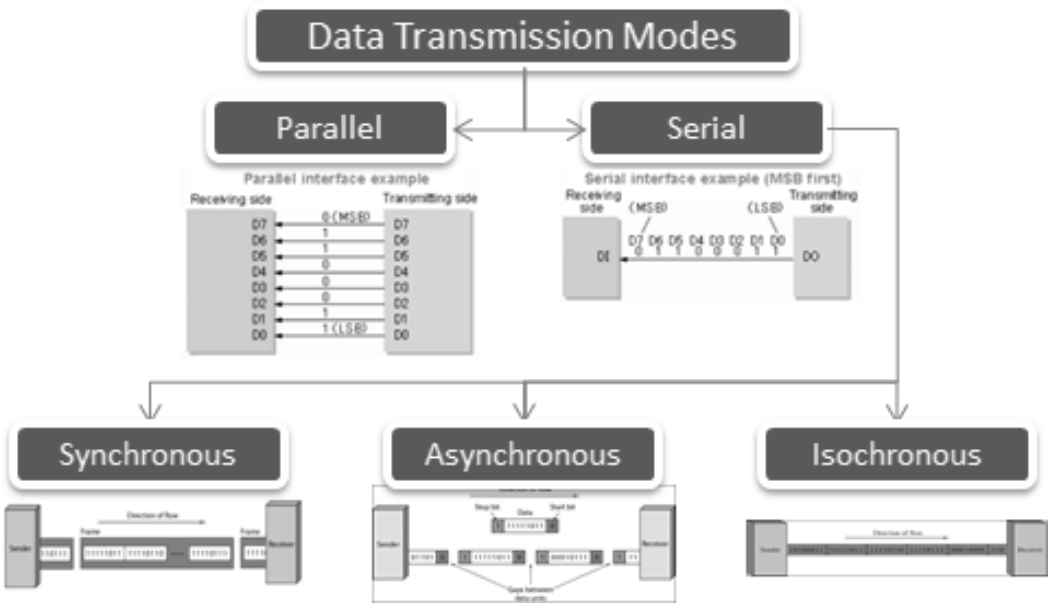


$$\text{transmission ratio } r = \frac{no.of\ data\ elements}{1\ signal\ element}$$

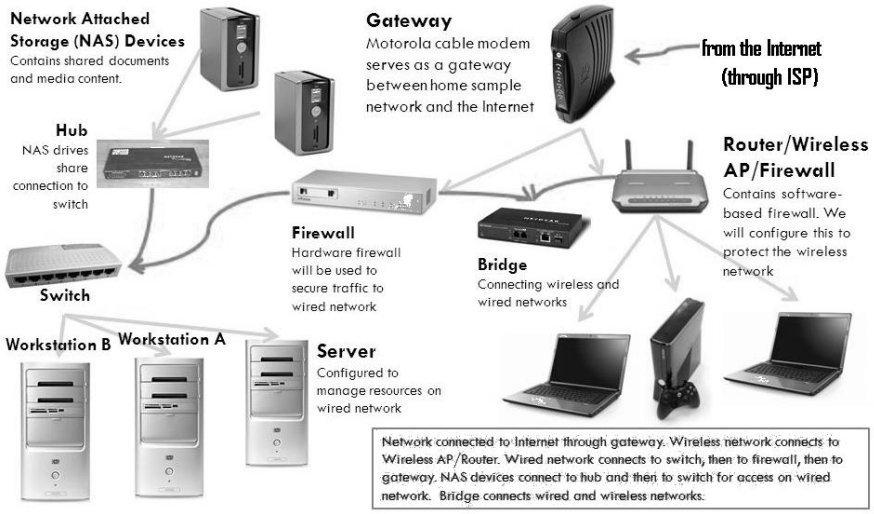


Data transmission is the process of transferring data between two or more digital devices. Data is transmitted from one device to another in analog or digital format. ***Throughput*** is an actual measure of transmission speed or how much data is successfully transferred per unit time, while ***bandwidth*** is a theoretical measure of how much data could be transferred from source to destination.

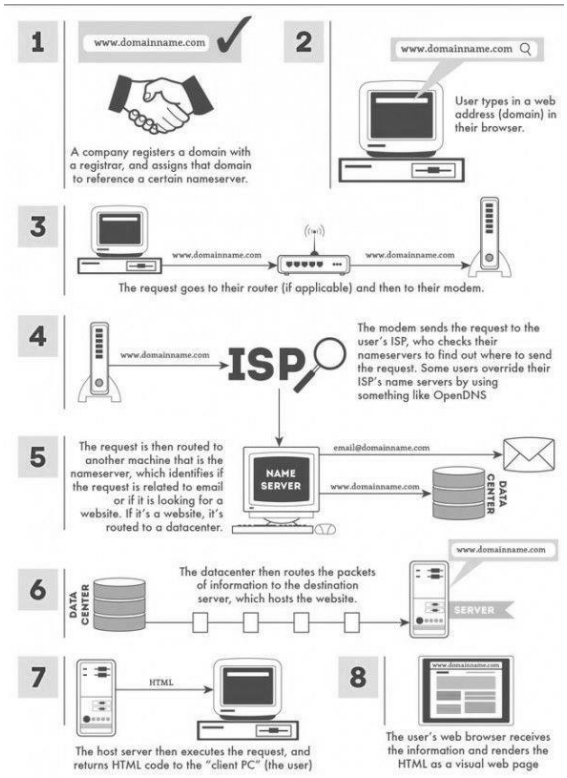




Computer Networks and the Internet



How the Internet Works

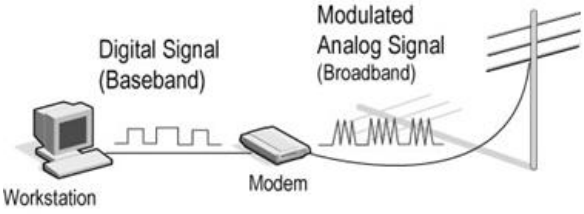


- Gateway – allows data to flow from one discrete network to another
- Modem – allows devices to communicate with other remote devices by converting digital data into analog data and transmitting it over an analog telephone line
- Firewall – prevents unauthorized use and access to the network
- Router – responsible for sending data from one network to another
- Switch – uses the MAC address of a device to send data only to the port the destination device is plugged into
- Bridge – creates a single aggregate network from multiple communication networks or network segments
- Hub – similar to a switch, but it broadcasts data to all ports
- Wireless Access Point – allows Wi-Fi devices to connect to a wired network

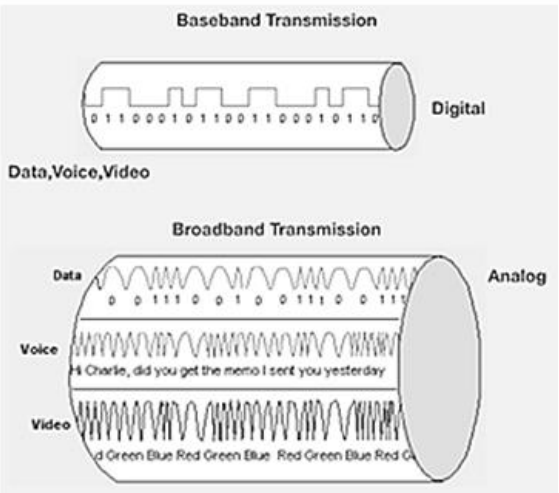
Wi-Fi vs Ethernet

	WiFi	Ethernet
Speed	Slow data transfer speed	Faster data transfer speed
Reliability	Suffers from signal interference due to many environmental factors	Delivers a consistent speed
Security	Data flow needs to be encrypted	Data doesn't require to be encrypted
Latency	Higher	Lower
Deployment	Easy to install and deploy	Cable installation infrastructure is required

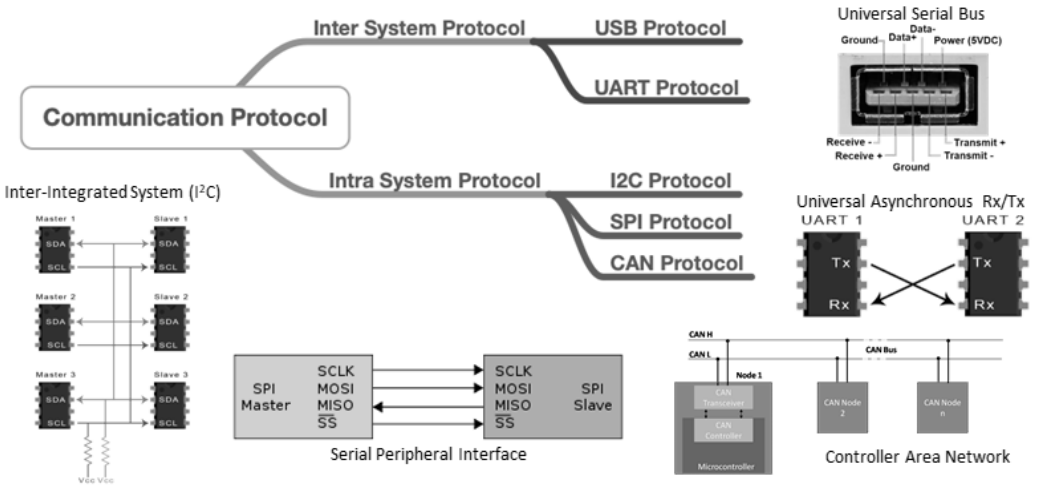
Baseband and Broadband Data Transmission



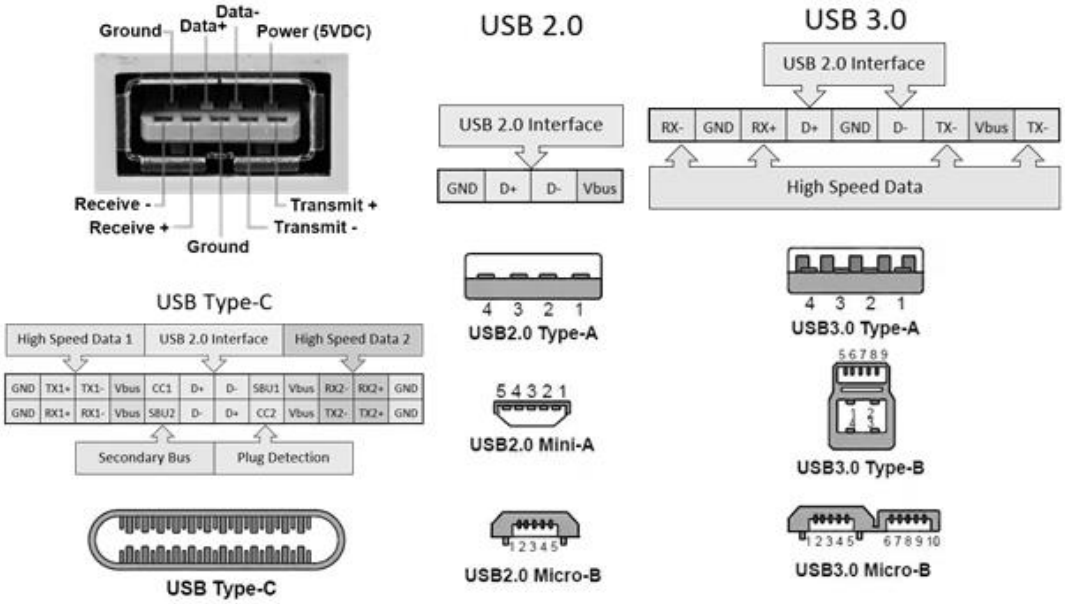
BASEBAND TRANSMISSION	BROADBAND TRANSMISSION
Baseband Transmission is a transmission technique that one signal requires the entire bandwidth of the channel to send data.	Broadband Transmission is a transmission technique that many signals with multiple frequencies transmit data through a single channel simultaneously.
Baseband Transmission uses digital signals.	Broadband Transmission uses analog signals.



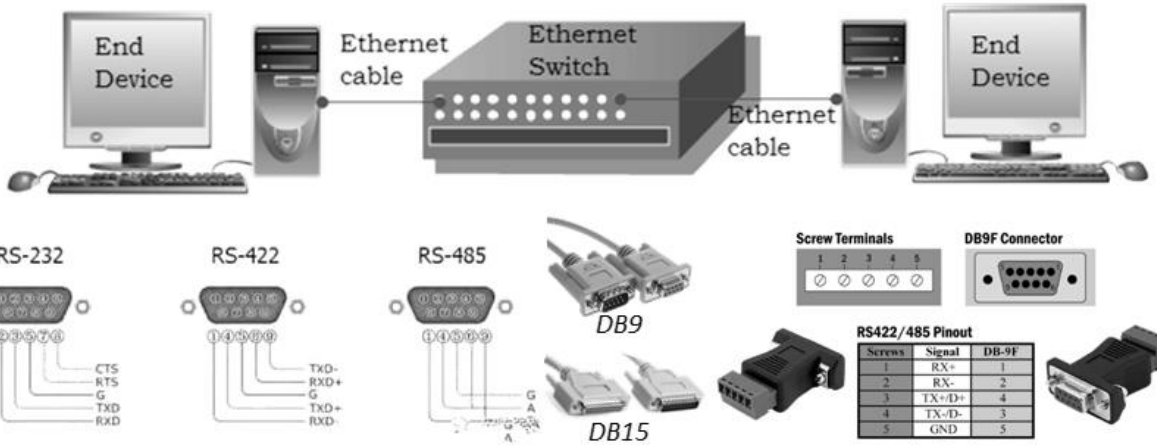
Short-Distance Data Transmission Technologies

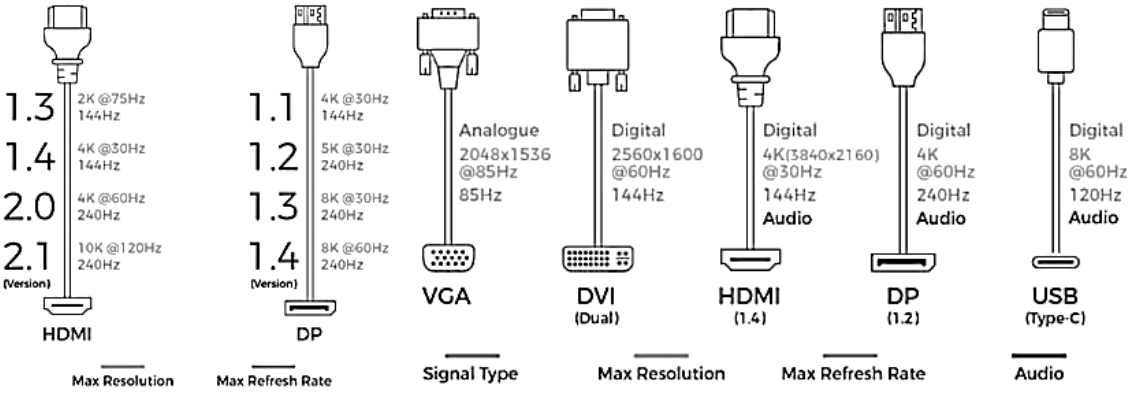


- Universal Asynchronous Receiver/Transmitter (UART) – device for asynchronous serial communication configurable data format and transmission speeds are
- Serial Peripheral Interface (SPI) – synchronous serial communication interface specification used for short-distance communication, primarily in embedded systems
- Inter-Integrated Circuit (I2C or I^2C) – serial protocol for 2-wire interface to connect low-speed devices like microcontrollers and other similar peripherals in embedded systems
- Universal Serial Bus (USB) – enables communication between devices and a host controller such as a personal computer; external bus standard that supports data transfer rates of 12 Mbps and can be used to connect up to 127 peripheral devices

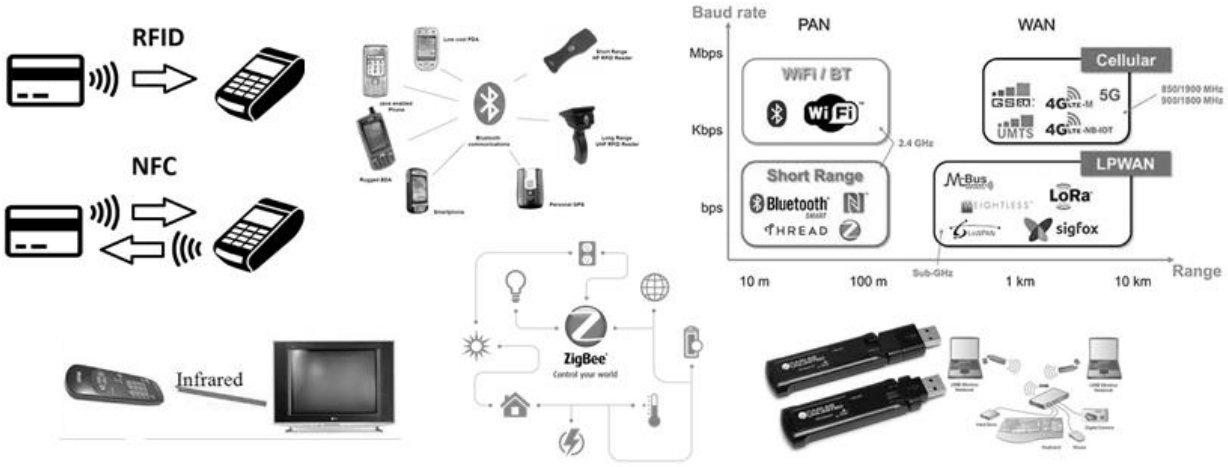


Wired Data Transmission Technologies





Wireless Data Transmission Technologies



Data Communication Standards

- ✓ American National Standards Institute (ANSI)
- ✓ Institute of Electrical and Electronics Engineers (IEEE)
- ✓ International Telecommunications Union (ITU)
- ✓ International Organization for Standardization (ISO)
- ✓ International Society (ISOC)
- ✓ Internet Society and the Internet Engineering Task Force (IETF)
- ✓ Electronic Industries Alliance and the Telecommunications Industry Association (EIA/TIA)

Example of Data Communications Standards

Signaling rate	Example bus standard	Fundamental frequency	Optimum antenna length
100 kbits/s	TIA/EIA-423	50 kHz	1,500 meters
1 Mbit/s	TIA/EIA-422	500 kHz	150 meters
10 Mbits/s	TIA/EIA-485	5 MHz	15 meters
200 Mbits/s	IEEE 1394 Firewire	100 MHz	75 cm
400 Mbits	ANSI TIA/EIA-644 LVDS	200 MHz	50 cm
2 Gbits/s	IEEE 802.3 Gbit Ethernet	1 GHz	7.5 cm

Standards body	Document number	Title	Approval date
IEEE 802.1	IEEE 802.1D	MAC Bridges	June 2004 (revised)
	IEEE 802.1Q	VLAN	Dec. 2005 (revised)
	IEEE 802.1ad	Provider Bridges	Dec. 2005
	IEEE 802.1ag	Connectivity Fault Management	Sept. 2007
	IEEE 802.1ah	Provider Backbone Bridges	Dec. 2008 (target)
	IEEE 802.1aj	Two Port MAC Relay	Dec. 2008 (target)
	IEEE 802.1aq	Shortest Path Bridging	Dec. 2009 (target)
	IEEE 802.1AS	Timing and Synchronization	Dec. 2010 (target)
	IEEE 802.1Qat	Stream Reservation Protocol	Dec. 2010 (target)
	IEEE 802.1Qav	Forwarding and Queuing Enhancements for Time-sensitive Streams	Dec. 2010 (target)
	IEEE 802.1Qay	Provider Backbone Bridge Traffic Engineering	Dec. 2011 (target)
IEEE 802.3	IEEE 802.3	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications (includes IEEE 802.3ae (10G Ethernet) and IEEE 802.3ah (Ethernet in the First Mile))	Dec. 2005 (revised)
	IEEE 802.3av	10G EPON	Mar. 2009 (target)
	IEEE 802.3ba	40G and 100G Ethernet	May 2010 (target)
ITU-T SG13	Y.1730	Requirements for OAM Functions in Ethernet-based Networks and Ethernet Services	Jan. 2004
	Y.1731	OAM Functions and Mechanisms for Ethernet-based Networks	May 2006
ITU-T SG15	G.8010	Architecture of Ethernet Layer Networks	Feb. 2008 (revised target)
	G.8011	Ethernet over Transport—Ethernet Services Framework	Aug. 2004
	G.8011.1	Ethernet Private Line Service	Aug. 2004
	G.8011.2	Ethernet Virtual Private Line Service	Sept. 2005
	G.8011.3	Ethernet Virtual Private LAN Service	Feb. 2008 (target)
	G.8011.4	Ethernet Virtual Private Rooted Multipoint Service	Feb. 2008 (target)
	G.8021	Characteristics of Ethernet Transport Network Equipment Functional Blocks	Under approval process (revised)
	G.8031	Ethernet Protection Switching	June 2006
	G.8032	Ethernet Ring protection	Feb. 2008 (target)

ASSESSMENT

Q&A

Answer what is asked in the following items. Each answer should be in a narrative form with at least 3 sentences and with normal formatting details.

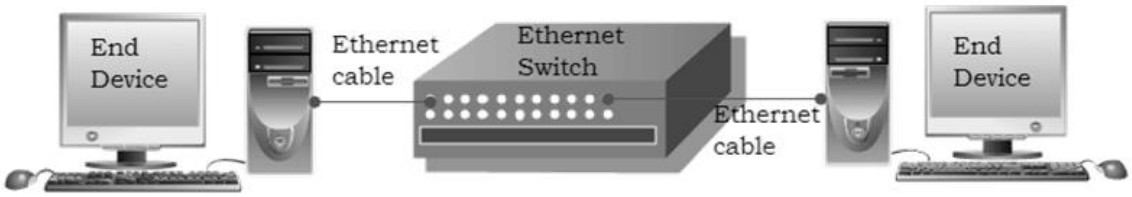
1. Discuss how a basic data communication system works by describing its main components.
2. What is the main difference between a codec and a modem in terms of data transmission? Which of them transmits analog signals, and which of them receives analog signals?
3. Explain the importance of selecting and configuring the right data transmission media and protocols for a data communication system.
4. Why do engineers need to be aware of the international data communications standards? Give examples of an international standards organization and some of the standards they established in the industry.

Research Activity

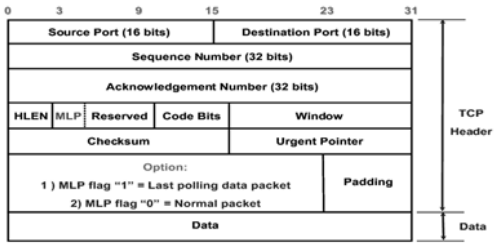
Watch the following YouTube tutorial about Cisco Packet Tracer:
Cisco Packet Tracer | Basic Tips and Tricks

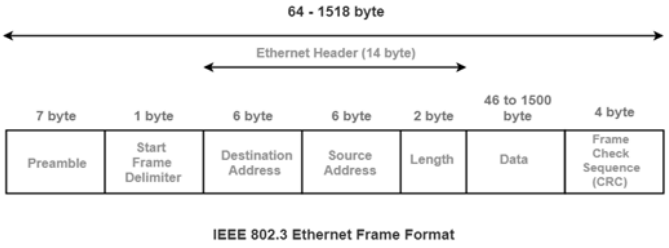
Module 6: **Ethernet and Wi-Fi Technologies**

Ethernet is a widely deployed LAN technology standardized in IEEE 802.3. Its connector is the *network interface card* (NIC) equipped with 48-bit MAC address, which helps other Ethernet devices to identify and communicate with remote devices in Ethernet.

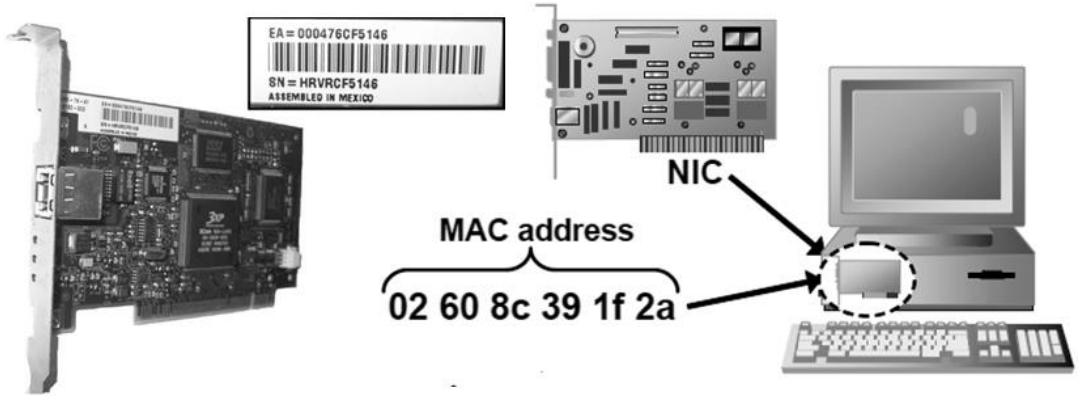


Network Packet is a formatted unit of data carried by a packet-switched network. It consists of control information and user data, which is also known as the *payload*. ***Ethernet Frame*** refers to the payload transported by a data unit on an Ethernet link. It is a data link layer protocol data unit that uses the underlying Ethernet physical layer transport mechanisms.

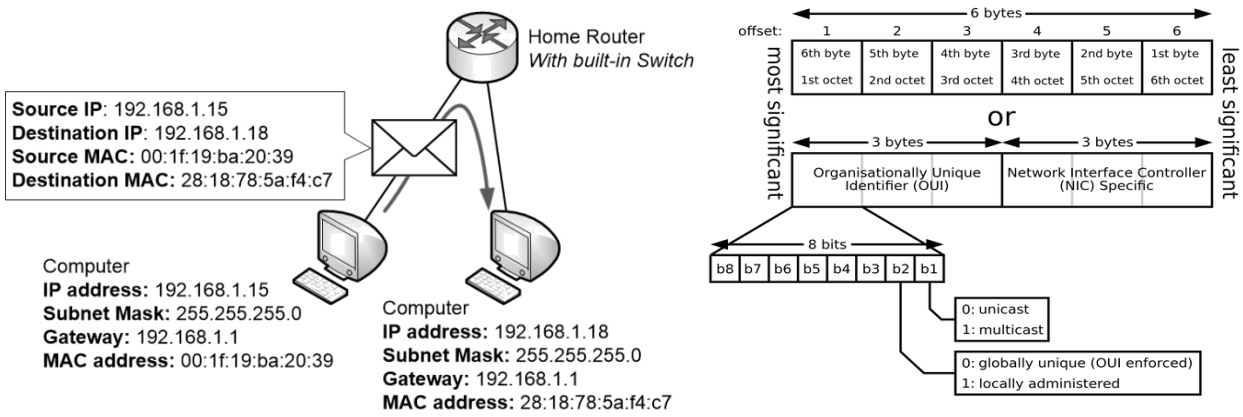




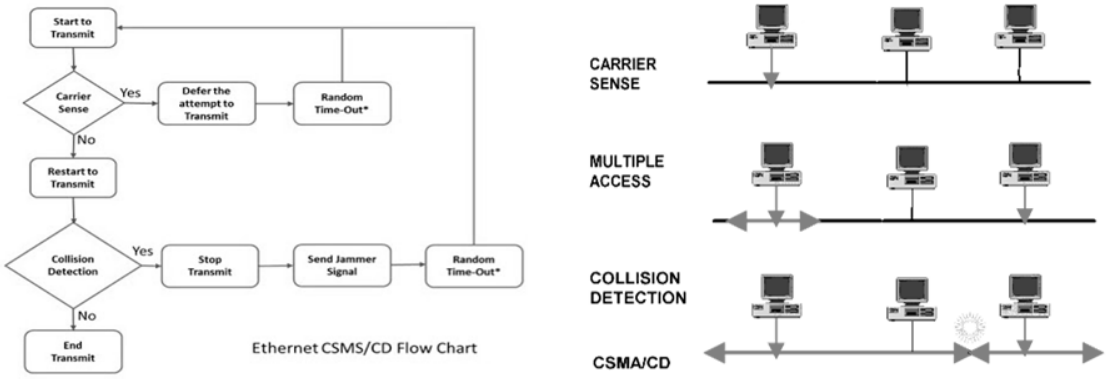
Media Access Control *(MAC)* ***Address***, which also known as *physical address*, is unique in each Network Interface Card.



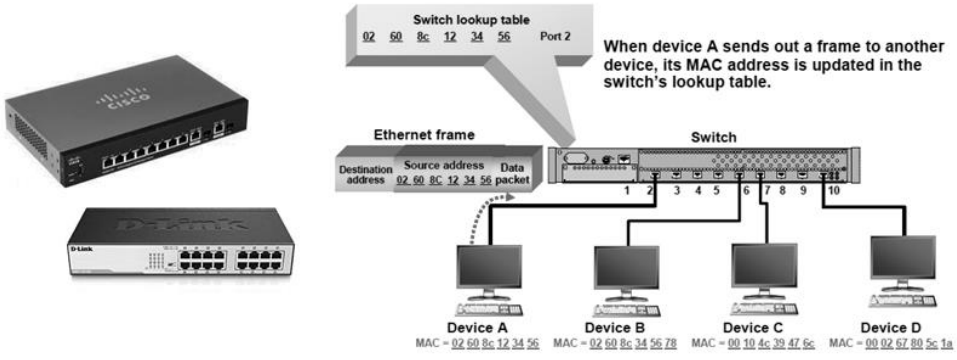
MAC Address



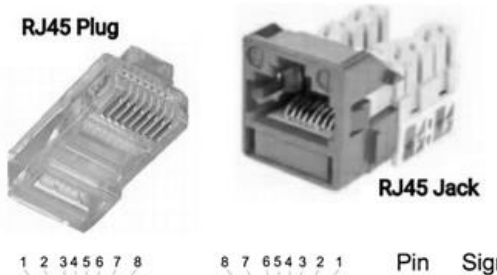
Carrier-Sense Multiple Access w/ Collision Detection (CSMA/CD) is a MAC method that defines how network devices respond when two devices attempt to use a data channel simultaneously and encounter a data collision/

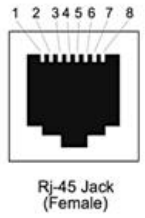


Ethernet Switch is a data link layer protocol data unit and uses the underlying Ethernet physical layer transport mechanisms. In this device, payload is transported by a data unit on an Ethernet link.



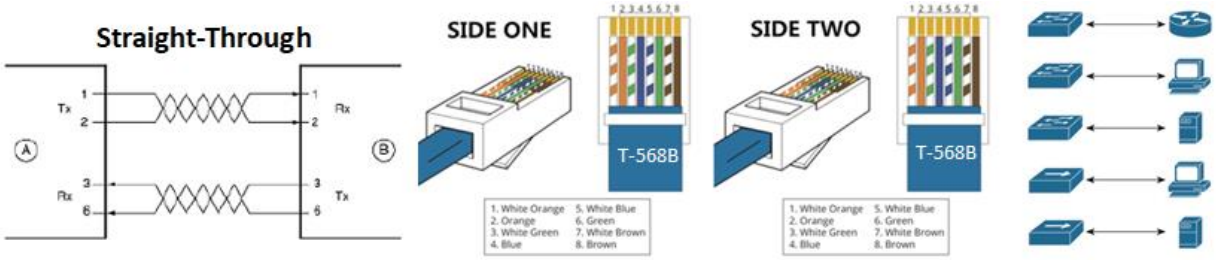
RJ-45 Connectors and Twisted-Pair Cables

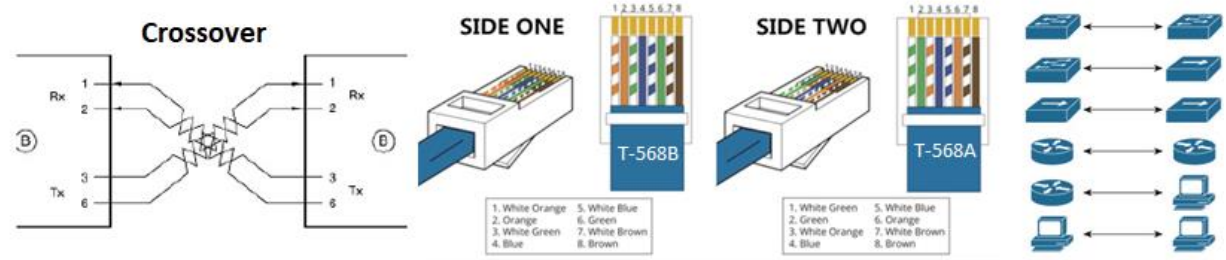




Pin	Signal
1	CTS
2	DTR
3	TXD
4	SGND
5	SGND
6	RXD
7	DSR
8	RTS

Parameters	UTP	STP
Full Form	Unshielded Twisted Pair	Shielded Twisted Pair
Structure	cable with wires that are twisted together.	Twisted pair cable enclosed in foil / shield.
Cost	Cheaper than STP	Costlier than UTP
Weight	Lighter than STP	Heavier than UTP
Noise & interference	Prone to Noise and interference	Less prone to noise and interference
Data Speed	Supports slower speed than on STP	Support higher speed than UTP
Grounding of cable	Not required	Required
Target deployments	Locations less prone to interference like offices and homes.	Locations prone to interference like factories and airports





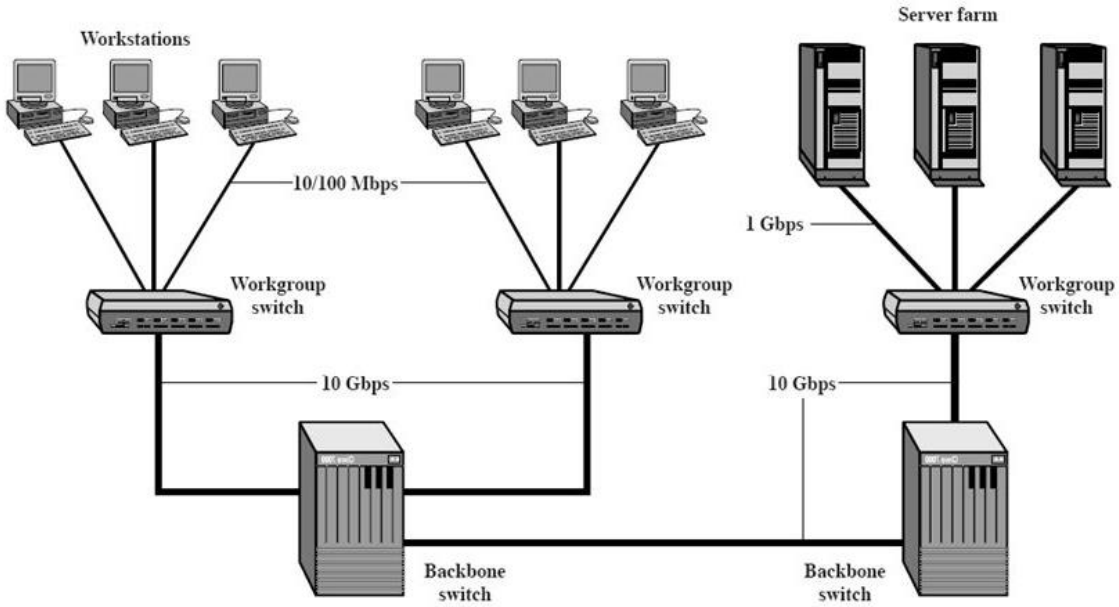
UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

Ethernet Type	Bandwidth	Cable Type	Max. Distance
10Base-T	10Mbps	Cat 3/Cat 5 UTP	100m
100Base-TX	100Mbps	Cat 5 UTP	100m
100Base-TX	200Mbps	Cat 5 UTP	100m
100Base-FX	100Mbps	Multi-mode fiber	400m
100Base-FX	200Mbps	Multi-mode fiber	2Km
1000Base-T	1Gbps	Cat 5e UTP	100m
1000Base-TX	1Gbps	Cat 6 UTP	100m
1000Base-SX	1Gbps	Multi-mode fiber	550m
1000Base-LX	1Gbps	Single-mode fiber	2Km
10GBase-T	10Gbps	Cat 6a/Cat 7 UTP	100m
10GBase-LX	10Gbps	Multi-mode fiber	100m
10GBase-LX	10Gbp	Single-mode fiber	10Km

Giga-Ethernet was introduced in 1995 and it quickly overtook Fast-Ethernet as it provides speed up to 1000 Mbits/seconds. IEEE802.3ab standardized Giga-Ethernet over UTP using Cat-5, Cat-5e and Cat-6 cables,l while IEEE802.3ah defines Giga-Ethernet over Fiber.

Cabling Standard	Cabling Type	Max Reach
10GBASE-SR	62.5µm OM3 multimode fiber	300m
	50µm OM4 multimode fiber	400m
10GBASE-LR	9µm single-mode fiber	10km
10GBASE-ER	9µm single-mode fiber	40km
10GBASE-ZR	9µm single-mode fiber	80km
10GBASE-LX4	9µm single-mode fiber	10km
	62.5µm multimode fiber	300m
	50µm multimode fiber	
10GBASE-LRM	9µm single-mode fiber	220m
10GBASE-T	Cat 6, Cat 6a or 7 twisted pair	30m
10G DAC/AOC	Copper RJ45	1-10m/up to 20m

Cable Type	Color
Multimode 50 µm and 62.5 µm (OM1, OM2)	Orange
Multimode 50 µm, laser optimized (OM3)	Aqua
Single-mode (OS1/OS2)	Yellow
Outside Plant (OSP) - MDPE	Black
Indoor/Outdoor (I/O)	Black

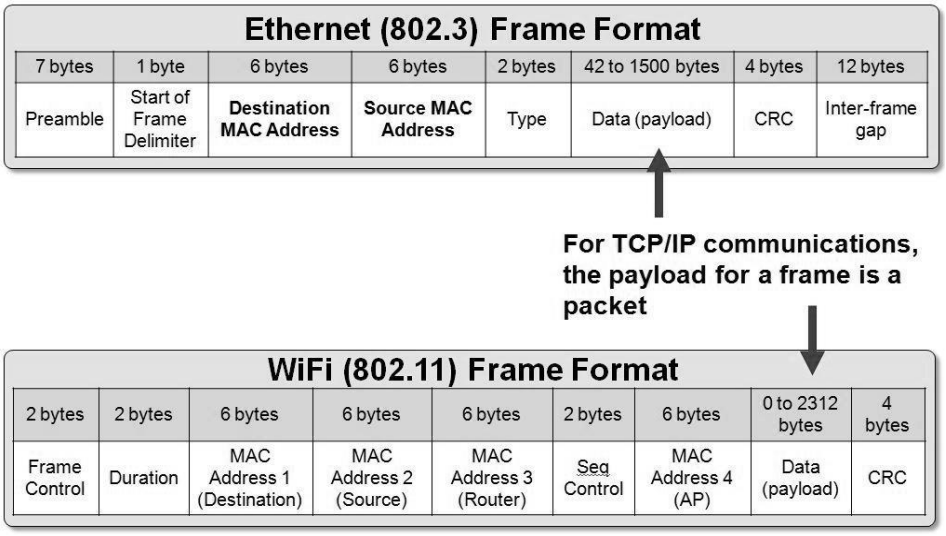


Example of a Giga-Ethernet Configuration

Wireless Fidelity (Wi-Fi) is a widely popular wireless networking technology that uses radio waves to provide wireless high-speed internet and network connections. It is based on the IEEE 802.11 family of standards and is primarily designed to provide in-building broadband coverage.

Technologies	Indoor/ Outdoor	Bitrate	Freq. bands	License	Bandwidth	Modulation	MIMO
IEEE 802.11	20m /100m	2 Mbps	2.4GHz	Unlicensed	20 MHz	FHSS and DSSS	—
IEEE 802.11b	35m/ 140m	11 Mbps	2.4GHz	Unlicensed	20 MHz	HR-DSSS	—
IEEE 802.11a	35m/ 119m	54 Mbps	5GHz	Unlicensed	20 MHz	OFDM	—
IEEE 802.11g	45m/ 90m	54 Mbps	2.4 GHz	Unlicensed	22 MHz	OFDM/ DSSS/ CCK	—
IEEE 802.11n	70m/ 250m	600 Mbps	2.4 GHz/ 5 GHz	Unlicensed	20 MHz/ 40 MHz	OFDM	4 X 4
IEEE 802.11ac wave	70m/ 250m	7000 Mbps	5 GHz	Unlicensed	80 MHz	64-QAM	MU-MIMO
IEEE 802.11ad	10m/ n/a	7000 Mbps	60 GHz	Unlicensed	2.16 GHz	Single Carrier/ OFDM	10 X 10
IEEE 802.11ac wave 2	70m/ 250m	7000 Mbps	5 GHz	Unlicensed	80 MHz/ 160 MHz	256-QAM	MU_MIMO 8 X 8

Ethernet vs Wi-Fi Frame Format



Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) is the protocol for carrier transmission in 802.11 (wireless) networks. It acts to prevent collisions before they happen, unlike in CSMA/CD that can only detect collisions.

Wi-Fi Adapters and Modules

Wireless Access Point (WAP) is a network device that acts as a portal for devices to connect to a local area network, while ***Wi-Fi Hotspot*** is created by installing an access point to an internet connection and it transmits a wireless signal over a short distance typically around 300 feet with IEEE 802.11b as the most common specification. The largest public Wi-Fi networks are provided by private internet service providers (ISPs), which charge a fee to the users who want to access the internet.

Different WAP Models

ASSESSMENT

Q&A

Answer what is asked in the following items. Each answer should be in a narrative form with at least 3 sentences and with normal formatting details.

1. How does Ethernet work? What is the role of MAC addresses and Ethernet frames in its working principles?
2. Explain the importance of CSMA/CD in Ethernet systems. How does it differ from CSMA/CA, which is used in Wi-Fi systems?
3. What are the main advantages and disadvantages of Wi-Fi over Ethernet?
4. In what ways do Wi-Fi hotspots and WAP networks differ from each other?

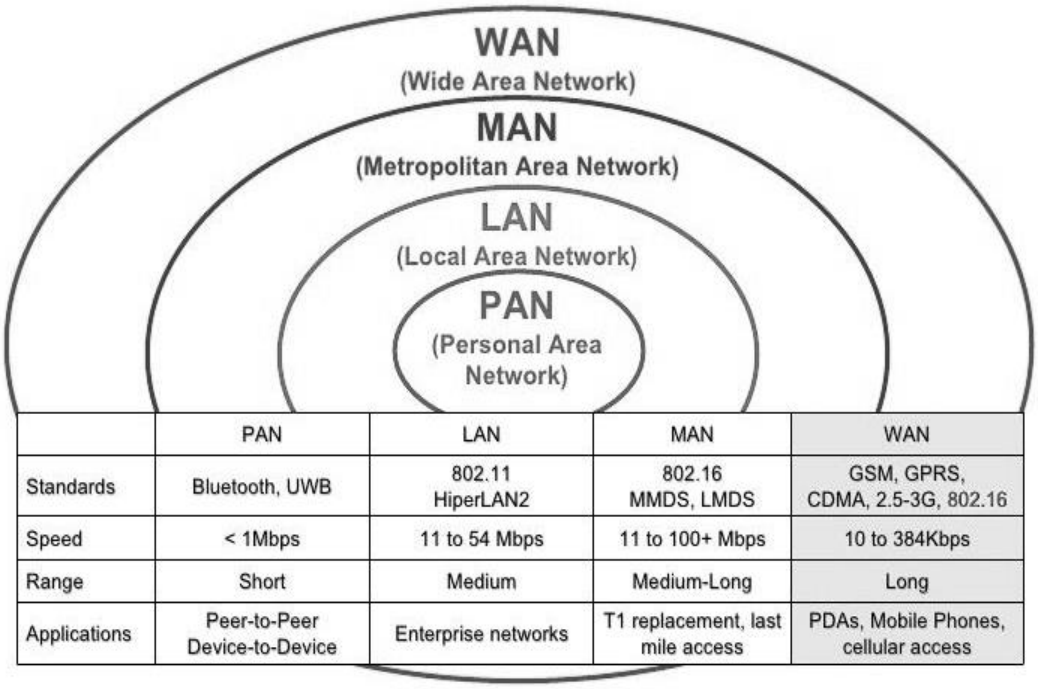
Research Activity

Watch the following YouTube tutorial about Cisco Packet Tracer:
Cisco Packet Tracer | Basic Switch Configuration

Module 7: **Computer Networks and the Internet**

Computer Network (or *data network*) is a system that transfers data between network access points (nodes) through data switching, system control, and interconnection transmission lines. The largest and most popular example is the ***Internet***.

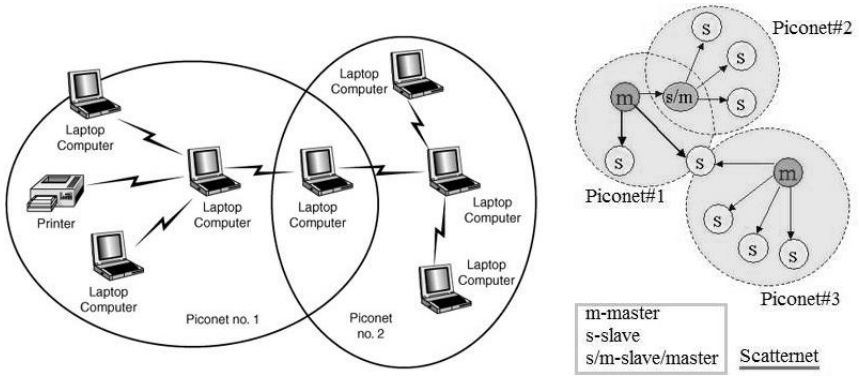
Types of Computer Networks



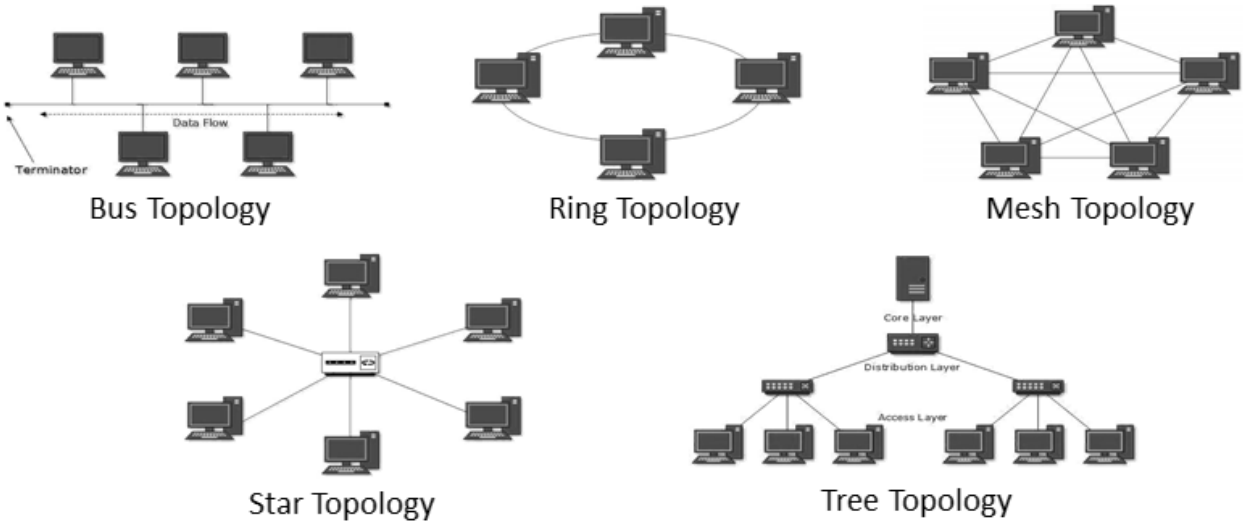
	PAN	LAN	MAN	WAN
Standards	Bluetooth, UWB	802.11 HiperLAN2	802.16 MMDS, LMDS	GSM, GPRS, CDMA, 2.5-3G, 802.16
Speed	< 1Mbps	11 to 54 Mbps	11 to 100+ Mbps	10 to 384Kbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise networks	T1 replacement, last mile access	PDAs, Mobile Phones, cellular access

LAN	WAN	MAN
Short for local area network.	Short for wide area network.	Short for metropolitan area network.
Connects a group of computers within a limited geographic area.	Covers a large geographical area such as a state, country or a continent.	Confined to a city or town. Distance coverage is larger than LAN and smaller than WAN.
High bandwidth for data transfer.	Low bandwidth for data transfer.	Bandwidth is moderate for data transfer.
Owned by private companies or individuals.	Established under distributed ownership.	Ownership can be private or public.
Limited to 100 to 1000 meters.	Spans a huge area of 100,000 kilometers.	Distance coverage is up to 100 kilometers.
Lower setup cost due to inexpensive devices.	Higher setup cost than LAN and MAN.	Moderate installation costs.
Higher data transfer speeds with 10, 100, and 1000 Mbps high-speed Ethernet.	Low data transfer rates between 10 to 20 Mbps.	Speed can go up to 100 Mbps.

Piconets and Scatternets



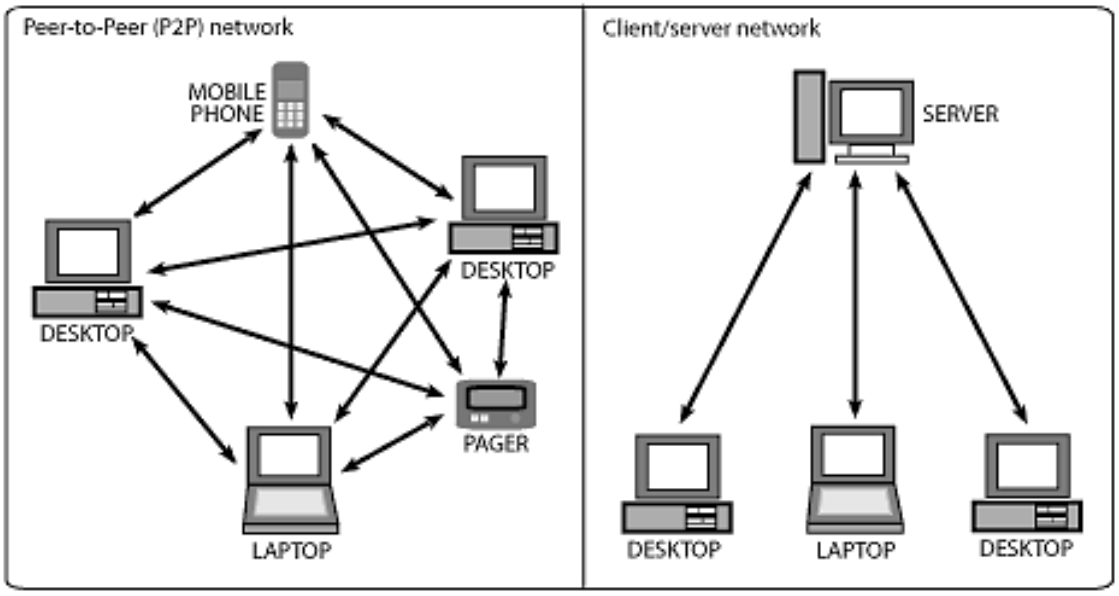
Computer Network Topologies

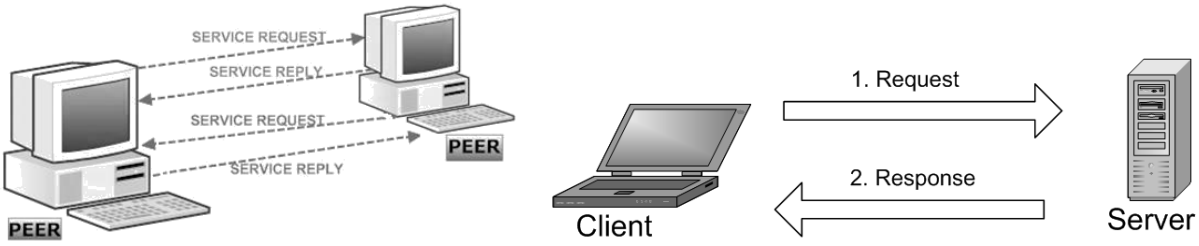


Topology	Advantages	Disadvantages
Mesh	Simplest and most fault tolerant.	Extremely difficult to reconfigure, extremely expensive, and very complex
Star/Tree	Cheap and easy to install, easy to reconfigure, and fault Tolerant	More expensive than bus
Ring	Efficient and easy to install.	Difficult to reconfigure and very expensive
Bus	Cheap and easy to install	Difficult to reconfigure, and break in bus disables entire network

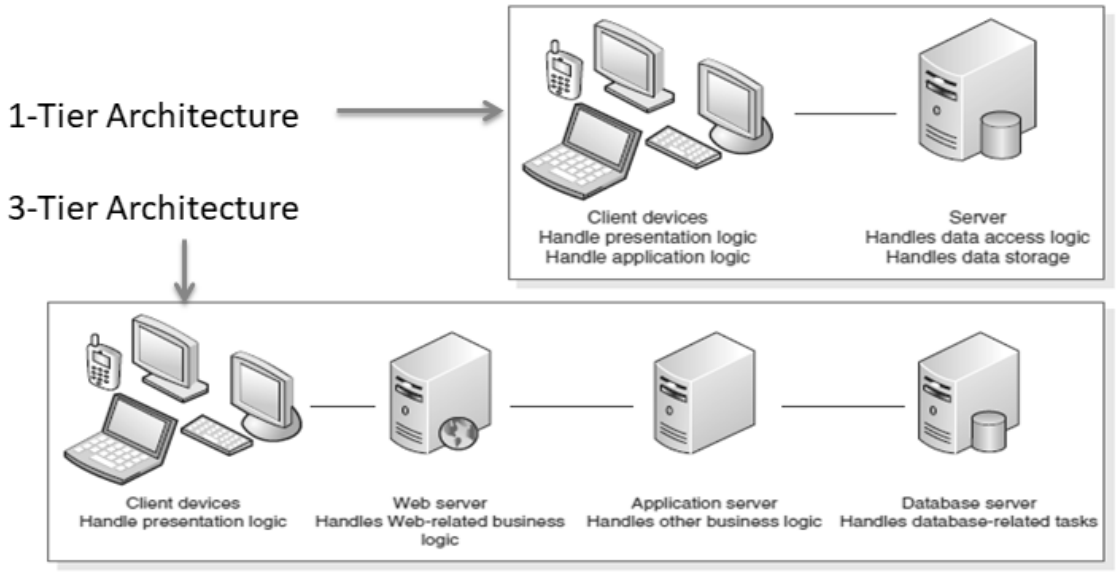
Usage / Factors	Very High	High	Moderate	Low	Very Low
Cost	**Mesh Topology**	**Tree Topology**	**Star Topology**	**Ring Topology**	**Bus Topology**
Security	**Mesh Topology**	**Tree Topology**	**Star Topology**	**Ring Topology**	**Bus Topology**
Privacy	**Mesh Topology**	**Tree Topology**	**Star Topology**	**Bus Topology**	**Ring Topology**
Use of cables	**Mesh Topology**	**Tree Topology**	**Star Topology**	**Bus Topology**	**Ring Topology**

Types of Computer Architecture





N-Tier Architecture



Types of Server

	Purpose	Examples		Purpose	Examples
Mail Server	E-mail Services	• Microsoft Exchange Server • IBM Lotus Domino	Proxy Server	Filtering And Caching	• Microsoft Forefront Threat Management Gateway (ISA Server) • Apache HTTP Server • Apache Traffic Server
Application Server	An Environment To Run Certain Applications	• Oracle WebLogic Server • Oracle Application Server • Oracle GlassFish Server • Zend Server	Print Server	Printer Services	• Microsoft Windows Storage Server (Built on the Microsoft Windows Server)
DNS Server	Translation of Domain Names Into IP Addresses	• Microsoft Windows Server • BIND	OTHER TYPES OF SERVERS: **FTP Server, Chat Server, Fax Server, Game Server, Audio/Video Server**		

Dynamic Host Configuration Protocol (DHCP) Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. ***IP Address*** is an identifier for devices on a TCP/IP network. It can be automatically assigned by the ISP (*dynamic IP address*) or manually assigned (*static IP address*). It has two versions: *IPv4* and *IPv6*.

DNS SERVER	DHCP SERVER
A device that locates the internet domain names and translates them into internet protocol (IP) addresses	A device that dynamically assigns IP address and other network configuration parameters to each device on a network so that they can communicate with each other
Stands for Domain Name System Server	Stands for Dynamic Host Configuration Protocol
Maps the domain names to the corresponding IP addresses	Assigns IP addresses automatically to the devices when they connect to the network
Uses port number 53	Works on port number 67 and 68
Works in a decentralized manner	Works in a centralized manner
Helps to map the domain names to IP addresses; user does not need to memorize the IP addresses	Helps to assign IP addresses to the devices automatically, making it easier to manage a large network

Visit www.PEDIAA.com

Server Form Factors and Roles

Tower:

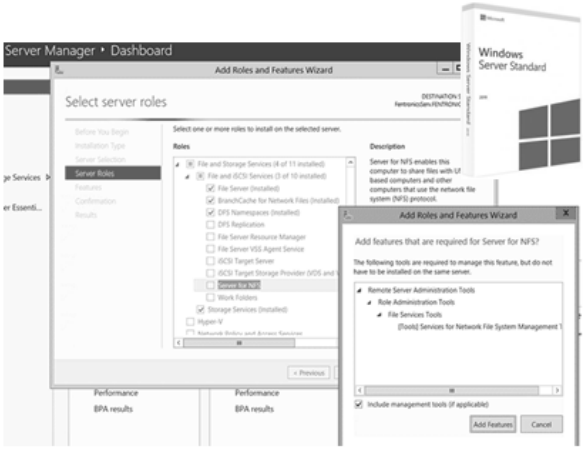
A tower server is a free-standing unit. similar to a large desktop pc in both size and shape.

Rack:

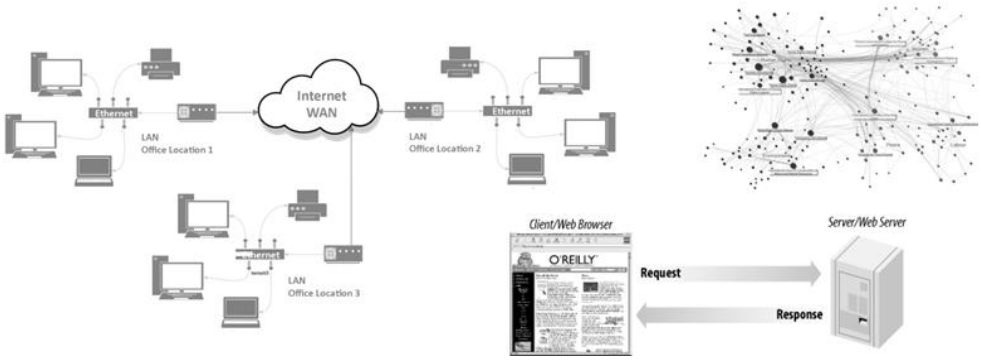
A rack server is specially designed to fit within a standardized 19" mounting rack.

Blade:

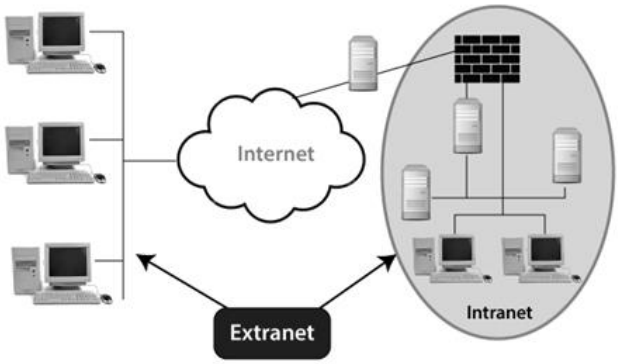
A blade servers are for use in blade enclosure that designed to fit within a standardized 19" mounting rack.



The ***Internet*** is the global system of interconnected computer networks that use the TCP/IP suite to link devices worldwide, while the ***World Wide Web*** (or web) is one of the services communicated over the Internet.

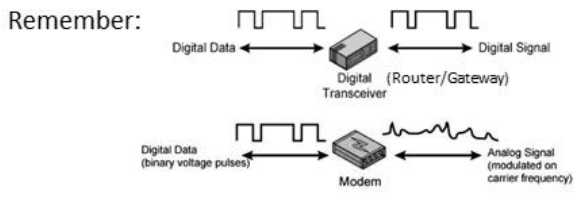


Intranet, Extranet, Internet



Parameter	Internet	Intranet	Extranet
Type of Network	Public	Private	Private/VPN
Size	Large number of connected devices	Limited number of connected devices	Limited number of connected devices over internet
Security	Depends on the device connected to the device	Firewall protected	Firewall separates Internet and Extranet
Policy	Internet Communication Protocols	Organizational Policies	Organizational policies, contractual policies and Internet Policies
Accessibility	Anyone	Authorized people	Authorized people
Information Sharing	Information can be shared across the world	Information can be shared securely within an Organization	Information can be shared between employees and external people
Owner	Not owned by anyone	Owned by a particular Organization	Owned by one or more Organizations
Example	World Wide Web, Email, Chat, Social Media	Internal Operations Network of an Organisation	Network of Collaboration between two Corporations

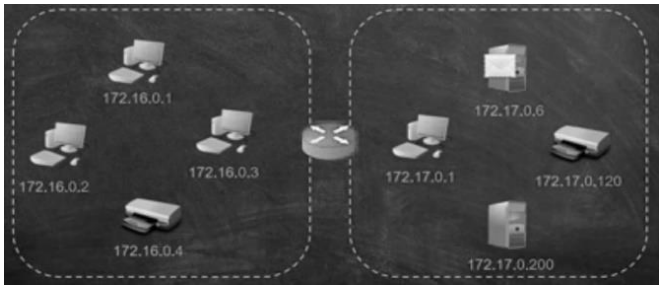
Modem and Gateway

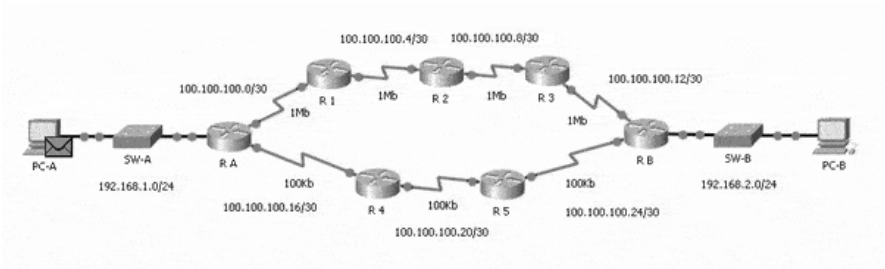


Gateway	Modem
A gateway is a network device that acts as an entry point to another network.	A modem is a hardware component that allows any networking device to connect to the Internet.
It is a device that combines the functionality of both a modem and a router on the same box.	It is mainly used as a border device that enables a computer to transmit data over cable lines.
A gateway serves as a link between computers using different protocols, platforms or operating systems.	It converts or modulates an analog signal from a cable or telephone line to digital data that a computer can easily recognize and understand.
It can be a router, a firewall, server, or any other networking device that enables traffic flow in and out of the network.	Examples of modem include a cable modem or a DSL modem.

Router is a device that forwards data packets connects both similar and dissimilar LANs with the same network protocols. It can provide modem, gateway, firewall, NAT, DNS, DHCP, and proxy server functions.

Routing is the process of selecting a path for traffic in a network or between or across multiple networks. It can be done in the form of *static routing* or *dynamic routing*.





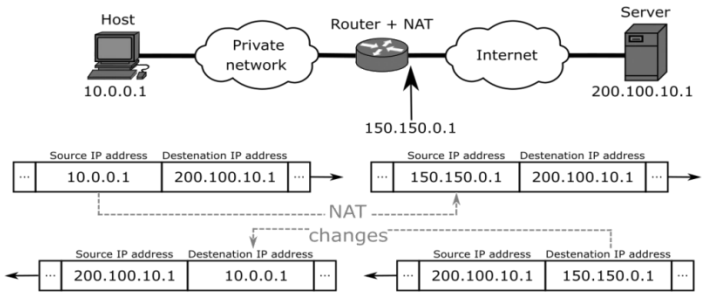
Static Routing (or *Non-Adaptive Routing*)

- occurs when a router uses a manually-configured routing entry rather than information from dynamic routing traffic
- the network administrator manually adds the routes in the routing table
- network is more secure and requires less bandwidth, but configuration is difficult

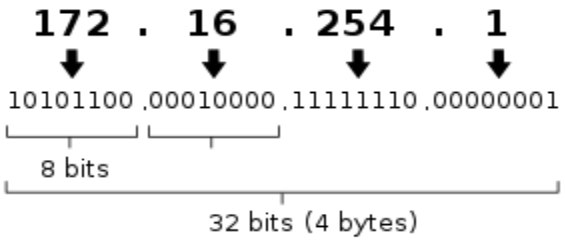
Dynamic Routing (or *Adaptive Routing*)

- where a router can forward data via a different route or given destination based on the current conditions of the communication circuits within a network
- routes are automatically according to the changes in the network
- configuration is easy but requires more bandwidth and network is less secure

Network Address Translator (NAT) translates private IP addresses into public, and vice versa.



IPv4 Address and Classful Addressing



CLASS	1ST OCTET	BINARY RANGE	PUBLIC ADDRESS RANGE	PRIVATE ADDRESS RANGE	APPLICATION
A	0 – 127	00000000 – 01111111	0.0.0.0 – 126.255.255.255	10.0.0.0 – 10.255.255.255	Government Networks
B	128 – 191	10000000 – 10111111	128.0.0.0 – 191.255.255.255	172.16.0.0 – 172.31.255.255	Medium Companies
C	192 – 223	11000000 – 11011111	192.0.0.0 – 223.255.255.255	192.168.0.0 – 192.168.255.255	Small Companies
D	224 – 239	11100000 – 11101111	224.0.0.0 – 239.255.255.255	N/A	For Testing
E	240 – 255	11110000 – 11111111	240.0.0.0 – 254.255.255.255	N/A	For Testing and Future Use

Types of IP Address

- Network Address – uniquely identifies a network; the first address of a class
- Host Address – uniquely identifies a host or node (computer or any IP-based device); somewhere between the network address and broadcast address of a class
- Broadcast Address – enables transmission to every node in a local network
- Loopback Address – special IP address (127.X.X.X) reserved for use in testing network cards

CLASS	NO. OF NETWORKS	NO. OF HOSTS	HOST ASSIGNMENT RANGE	N-H Representation	SUBNET MASK
A	$2^7 = 128$	$2^{24} - 2 = 16,777,214$	1.0.0.1 – 126.255.255.254	N – H – H – H	255.0.0.0
B	$2^{14} = 16,384$	$2^{16} - 2 = 65,534$	128.0.0.1 – 191.255.255.254	N – N – H – H	255.255.0.0
C	$2^{21} - 1 = 2,097,151$	$2^8 - 2 = 254$	192.0.0.1 – 223. 255.255.254	N – N – N – H	255.255.255.0

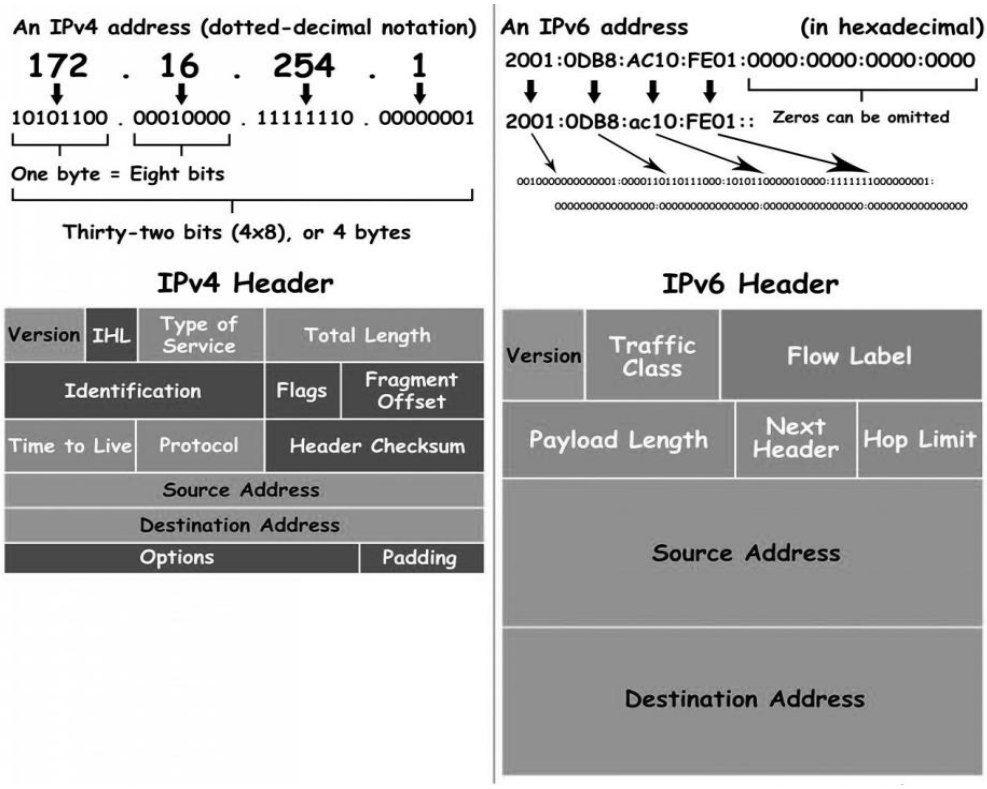
Subnetting is a process that allows to create multiple *subnetworks* (*subnets*) or logical networks or that exist within a single Class A, B, or C network. It uses a *subnet mask* to determine what subnet an IP address belongs to. ***Classless Inter-Domain Routing*** (CIDR) is the set of IP standards used to create unique identifiers for networks and individual devices.

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

Special IP Addresses

Address block	Present use
0.0.0.0/8	"This" network
14.0.0.0/8	Public-data networks
24.0.0.0/8	Cable television networks
39.0.0.0/8	Reserved but subject to allocation
128.0.0.0/16	Reserved but subject to allocation
169.254.0.0/16	Link local
191.255.0.0/16	Reserved but subject to allocation
192.0.0.0/24	Reserved but subject to allocation
192.0.2.0/24	Test-Net 192.88.99.0/24 6to4 relay anycast
198.18.0.0/15	Network interconnect device benchmark testing
223.255.255.0/24	Reserved but subject to allocation
224.0.0.0/4	Multicast
240.0.0.0/4	Reserved for future use

IPv4 vs IPv6



ASSESSMENT

Q&A

Answer what is asked in the following items. Each answer should be in a narrative form with at least 3 sentences and with normal formatting details.

1. Research about the best practices in selecting a network topology and its corresponding technologies. Summarize and discuss the key points.
2. In your own idea, why is it important to select the right server tier, type, and form factor when designing a client-server network?
3. Explain, in your own words, how the internet works. Mention also the role played by routers in it.
4. What is the purpose of IP addresses? Why do network engineers or IT technicians need to perform IP addressing and subnetting?

Research Activity

Watch the following YouTube tutorial about Cisco Packet Tracer:
Cisco Packet Tracer | Basic Router Configuration

Module 8: **Cybersecurity and Industry 4.0**

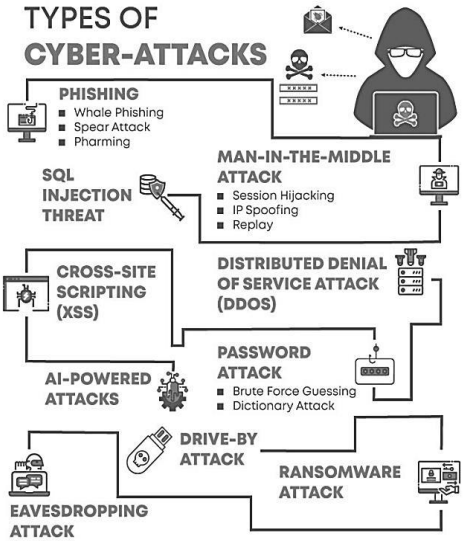
Cybersecurity refers to the measures for protecting computer systems, networks, and information systems from disruption or unauthorized access, use, disclosure, modification, or destruction. It basically involves assessing, managing, and mitigating the risk, which are all continuous activities as long as the protected system exists. Its basic objectives are to ensure the data confidentiality, integrity, and availability.

Required Soft Skills

- Attention to Detail
- Creative Problem Solving
- Clear Communication

Required Hard Skills

- Information Management
- Computer Science Basics
- Specialization in a Subset



Assessing Cybersecurity Risks

Point of Sale (POS) intrusions
Where retail transactions are conducted, specifically where card – present purchases are made.

Physical Theft and Loss
Any incident where an information asset went missing, whether through misplacement or malice.

Cyber Extortion
Crime involving an attack or threat of attack against your IT infrastructure , couple with demand for money to stop the attack.

Insider and Privilege Misuse
Any unapproved or malicious use of organisations resources. Mainly insider misuse or external (through collusion)

Miscellaneous Errors
People make mistakes! Unintentional actions directly compromised a security attribute of an information asset.

Web App Attacks
This includes exploits of a code – level vulnerabilities in the application as well as thwarting authentication mechanisms.

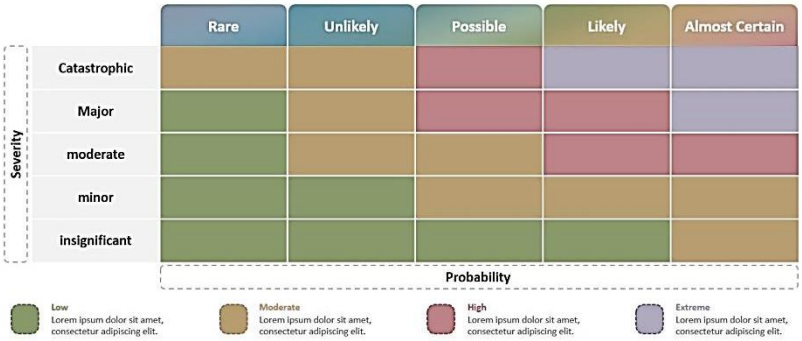
Cyber Espionage
Unauthorised network or system access linked to state affiliated actors and / or exhibiting the motive of espionage.

Payment Card Skimmers
Where a skimming device is physically implanted on an asset that reads magnetic stripe data from a payment card

Denial of Service
Intended to compromise the availability of networks and systems. Includes both network and application layer attacks.

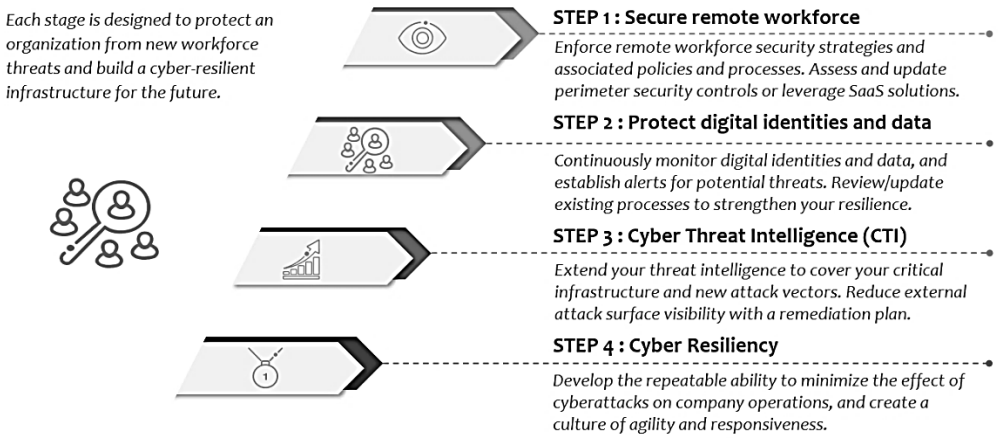
Crimeware
A form of malware. Primary goal is to gain control of systems to steal credentials

Assessing Cybersecurity Risks

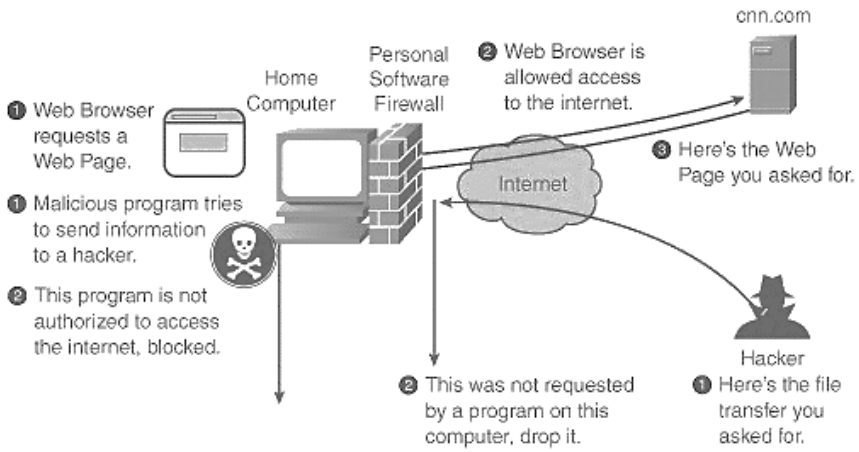


Example of a Risk Management Matrix

Mitigating Cybersecurity Risks



Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.



Encryption is a process that encodes a message or file so that it can be only be read by certain people. It uses an algorithm to scramble, or encrypt, data and then uses a key for the receiving party to unscramble, or decrypt, the information. ***Decryption*** is the process of converting the encoded or encrypted text back into its original form.

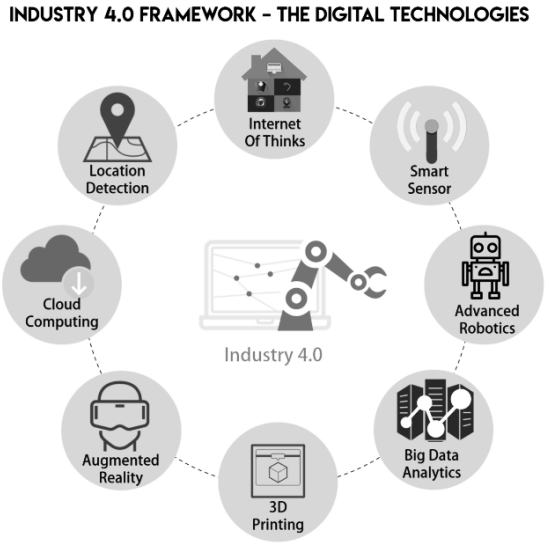
Ethical Hacking describes an act of intruding/ penetrating into system or networks to find out threats, vulnerabilities in systems which a malicious attacker may find and exploit causing data loss, financial loss or other major damages. It is done to improve the security of the network or systems by fixing the identified vulnerabilities.

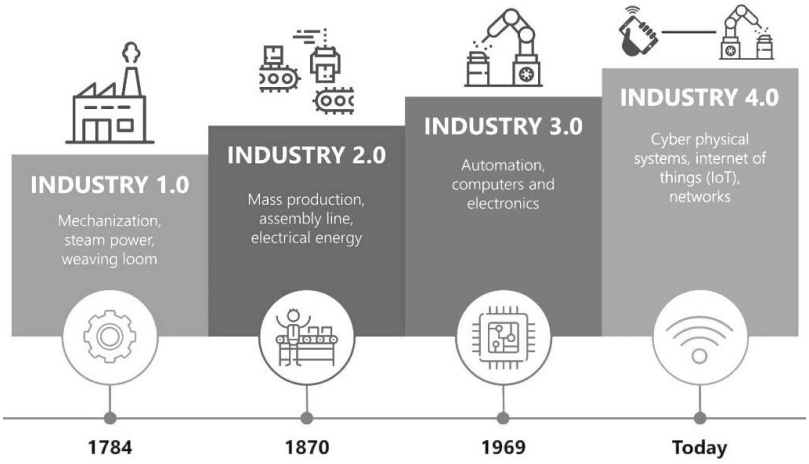
CpE-Related Laws

- ✓ RA 10844 – Department of Information and Communications Technology Act of 2015
- ✓ RA 10173 – Data Privacy Act of 2012
- ✓ RA 10175 – Cybercrime Prevention Act of 2012
- ✓ RA 8792 – Electronic Commerce Act of 2000
- ✓ RA 8293 – Intellectual Property Code of the Philippines
- ✓ RA 11058 – Occupational Safety and Health Act

  (Click the hyperlink for presentation and more information)

Industry 4.0, also known as the *Fourth Industrial Revolution* (4IR or FIRe), refers to the digital transformation of manufacturing/production and related industries and value creation processes. This new phase in the Industrial Revolution focuses heavily on interconnectivity, automation, machine learning, and real-time data.





Technologies under Industry 4.0

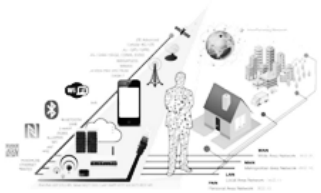
- Internet-of-Things (IoT)
- GPS and Smart Sensors
- Robotics and Artificial Intelligence (AI)
- Mixed Reality
- Nanotechnology and Biomaterials
- 3D Printing
- Cloud Computing and Big Data
- Blockchain

Internet of Things (IoT) is a system of interrelated computing devices and machines provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. It creates opportunities for more direct, integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions.

Components of IoT (3 Cs)

Components

Connecting the Real World to the Internet

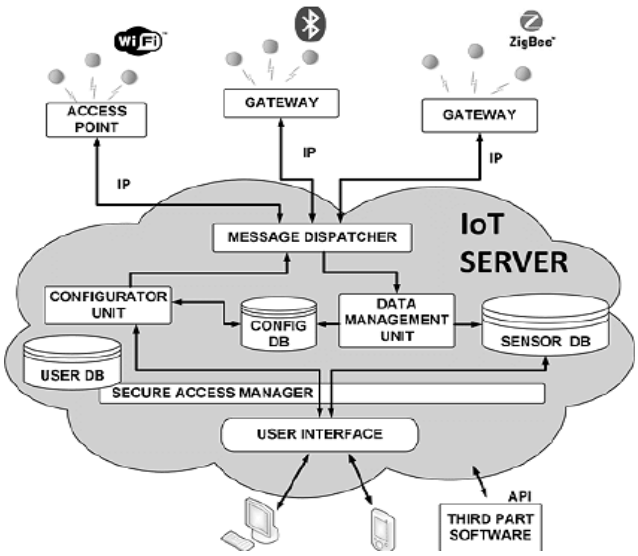


Connections

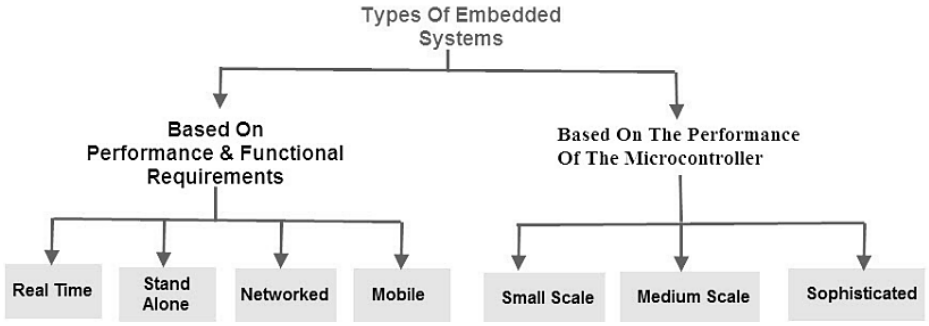
Holding the System Parts Together

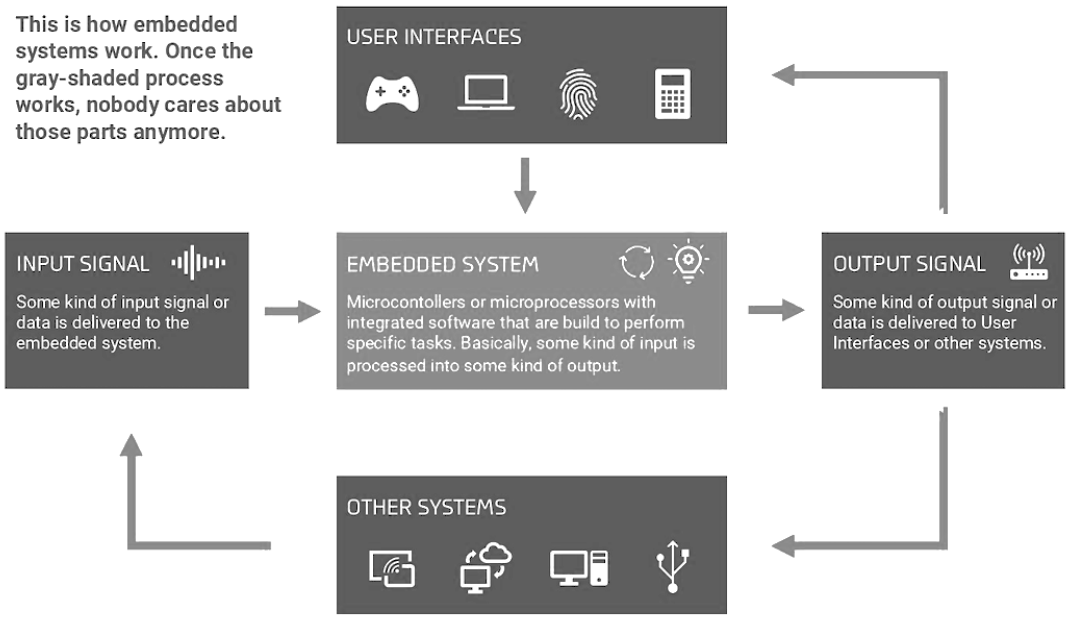
Cloud

Storing and securing all the System Data

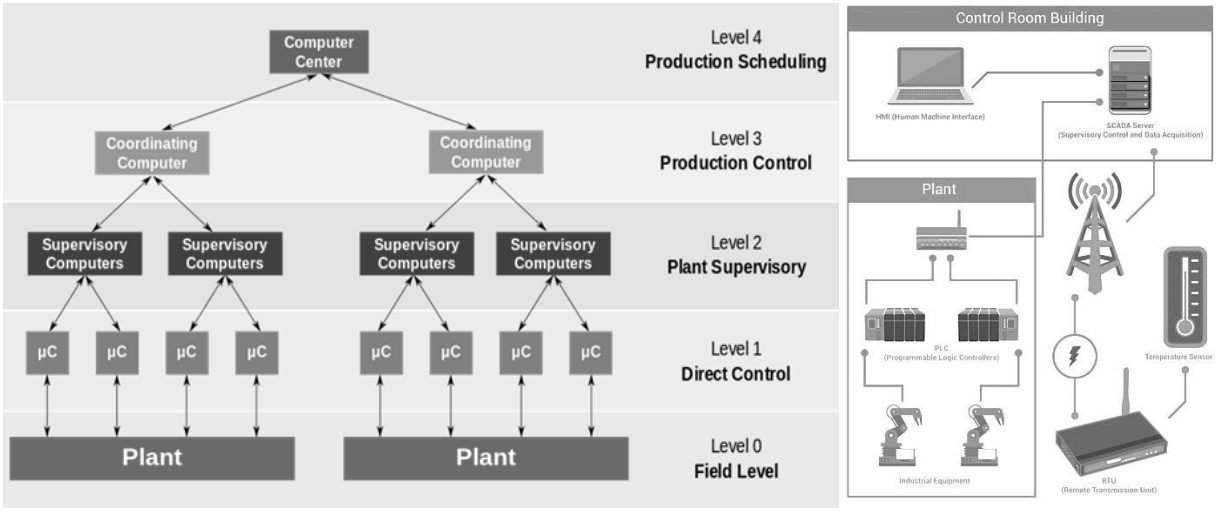


Embedded System is basically a controller with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. It is embedded as part of a complete device often including hardware and mechanical parts.

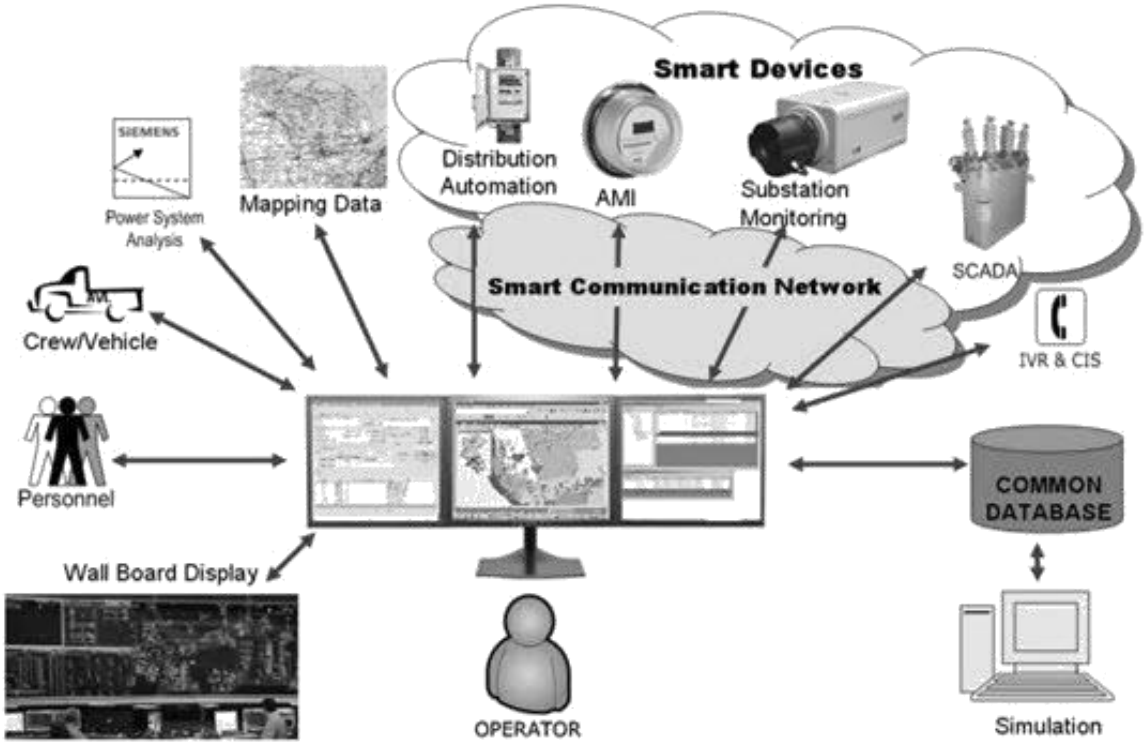




Industrial Control Systems

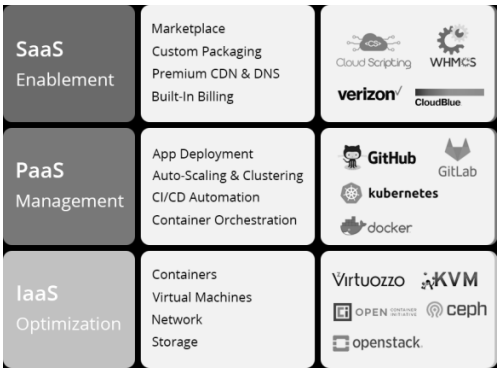


Supervisory Control and Data Acquisition Systems (SCADA) is the basis of any real-time control system. The system collects data from multiple sources and pre-processes and stores the data. The data is transferred to a data base where it's available for various users and applications.



Cloud Computing is everything, from computing power to computing infrastructure, applications, business processes to personal collaboration— can be delivered as a service wherever and whenever needed. The "*cloud*" is a set of hardware, networks, storage, services, and interfaces that combine to deliver computing as a service. *Cloud services* include the delivery of software, infrastructure, and storage over the Internet based on user demand.

- Public Clouds – services provided via Internet
- Private Clouds – services deployed via a hosted data center or a company intranet
- Hybrid Clouds – combine the power of both public and private clouds

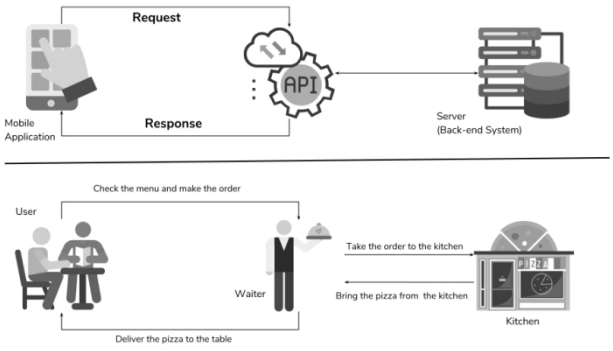


Advantages of Cloud Computing

- Elasticity – makes the cloud scalable so that the resources allocated can be increased or decreased based upon demand.
- Efficiency – cloud resources can be obtained in a straightforward fashion and can be released if no longer required.
- Standardized APIs – communication among programs or data sources and linkages between cloud services is easier
- Resources Billing – usage is measured and customers pay only for resources used

Application Programming Interface (API) is a set of routines, protocols, and tools for building software applications, as well as for communication among various components and interaction among software components.

Web APIs are the defined interfaces through which interactions happen between an enterprise and applications that use its assets, which also is a *Service Level Agreement* (SLA) to specify the functional provider and expose the URL or service path for its API users.



ASSESSMENT

Q&A

Answer what is asked in the following items. Each answer should be in a narrative form with at least 3 sentences and with normal formatting details.

1. Discuss, in your own words, the purpose of assessing, managing, and mitigating cybersecurity risks in a computer system or network.
2. How does ethical hacking work and how can it help improve the cybersecurity measures of an organization?
3. What is the relevance of cybersecurity in IoT systems and other various Industry 4.0 technologies?
4. In your own idea, what is the common denominator among the various Industry 4.0 technologies that make them part of the fourth industrial revolution?

Research Activity

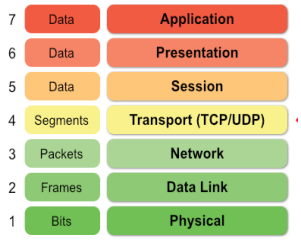
Watch the following YouTube tutorial about Cisco Packet Tracer:
Cisco Packet Tracer | Setting Up IoT

Introduction to Communication Protocols

(CMPE 30114 – Data and Digital Communications)

3 Chapter

I. OVERVIEW



Communication protocols are formal descriptions of digital message formats and rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity. They define the rules, syntax, semantics and synchronization of communication and possible error recovery methods. The *OSI model* is a generic model that is based upon functionalities of each layer. It distinguishes the three concepts, namely, services, interfaces, and protocols. It also gives guidelines on how communication needs to be done. Meanwhile, the *TCP/IP* model is a protocol-oriented standard that does not have a clear distinction between the three concepts, but its protocols layout standards on which the Internet was developed. So, TCP/IP is a more practical model. In the TCP/IP suite, the protocols were developed first and then the model was developed.

II. MODULE OBJECTIVES

After successful completion of modules 9-12 of Chapter 3, you should be able to:

1) Remember the purpose of communication protocols, as well as the important concepts of the OSI and TCP/IP models;
2) Understand the principles behind the physical and data link layer protocols;
3) Evaluate the different protocols in the network, transport, session, presentation, and application layers; and
4) Apply the analysis of TCP/IP protocols when designing, implementing, or managing computer networks.

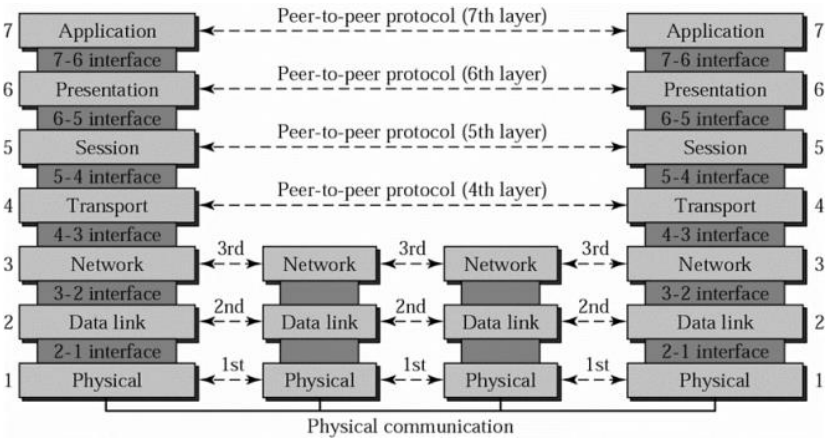
III. COURSE MATERIALS

Suggested Online Resources for Further Learning

- Downloadable Course AVPs: https://bit.ly/3lp25qa
- Downloadable Course PDFs: https://bit.ly/3FtitOt

Module 9: **Basic Concepts and the Physical Layer**

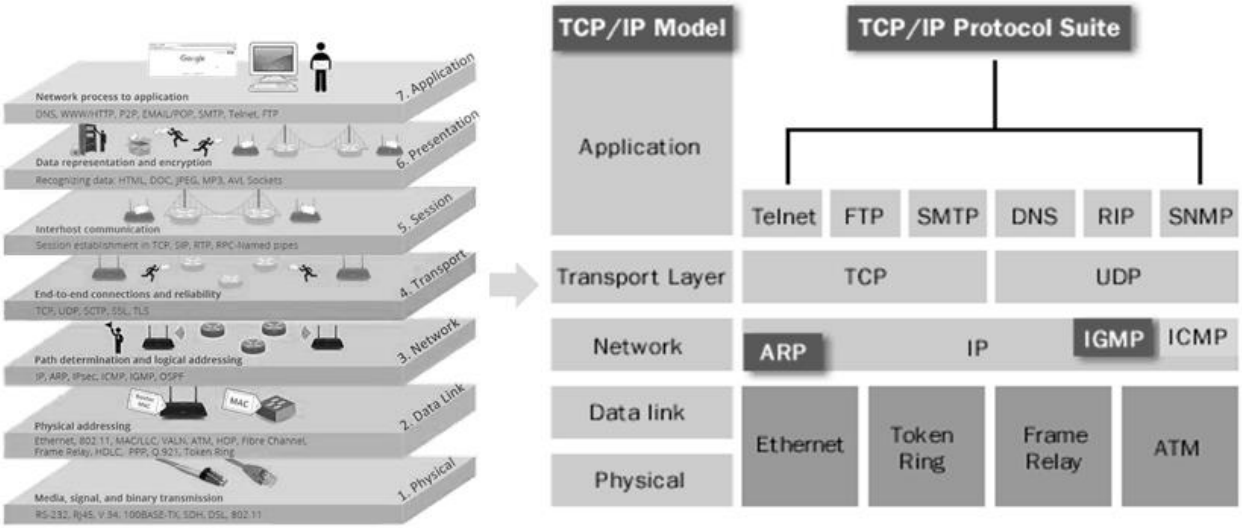
Communication Protocols are formal descriptions of digital message formats and rules required to exchange messages in or between computing systems and are required in telecommunications. These are a set of rules, syntax, semantics and synchronization of communication and possible error recovery methods, as well as cover authentication, error detection and correction, and signaling.



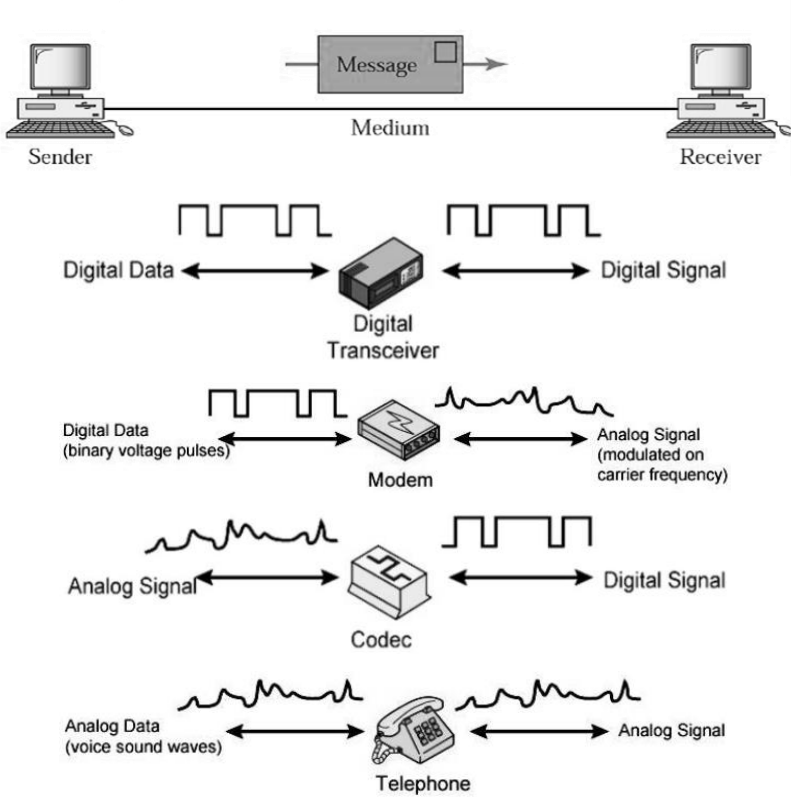
Open System Interconnect (OSI) is a conceptual model that enables diverse communication systems to communicate using standard protocols. The OSI reference model guides developers and vendors so the digital communication and software products they create can interoperate, and to facilitate a clear framework that describes the network functions or a telecommunication system. Additionally, it is used trace how data is sent or received over a network.

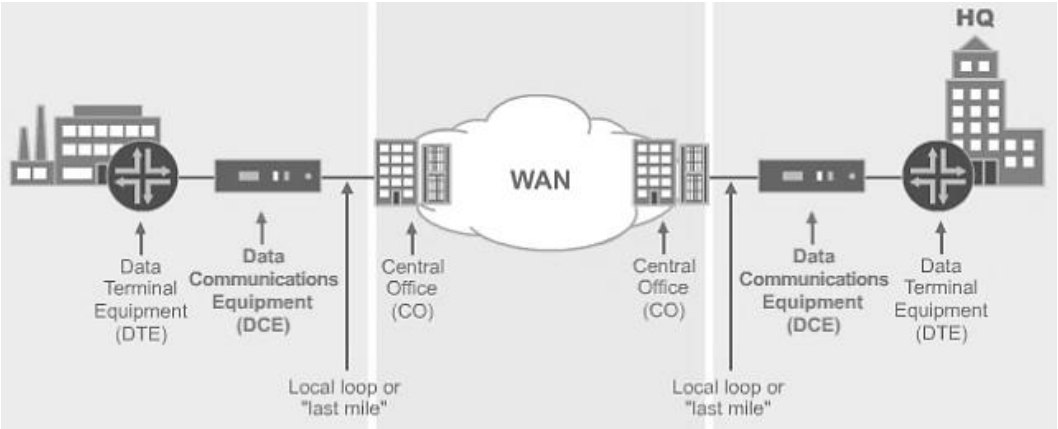
Transmission Control Protocol / Internet Protocol (TCP/IP) is a conceptual model and set of communications protocols used in the Internet and similar computer networks. It is composed of 4 layers (not including/separating the physical layer) instead of 7. The ***TCP/IP suite*** is a set of protocols for an end-to-end connectivity by specifying how data should be packetized, addressed, transmitted, routed and received on a TCP/IP network. This model helps:

- determine how a specific computer should be connected to the internet and how data should be transmitted between them
- create a virtual network when multiple computer networks are connected together
- allow communication over large distances

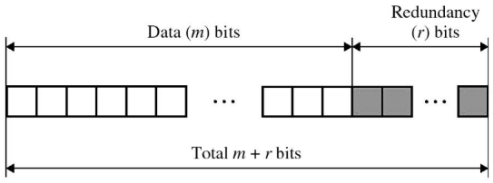


The ***Physical Layer*** plays the role of interacting with actual hardware and signalling mechanism (defines the hardware equipment, cabling, wiring, frequencies, pulses used to represent binary signals etc.). It provides its services to the *Data Link Layer*, which hands over *frames* to the physical layer; these frames are then converted by the physical layer to electrical pulses, which represent binary data that is then sent over the transmission media.



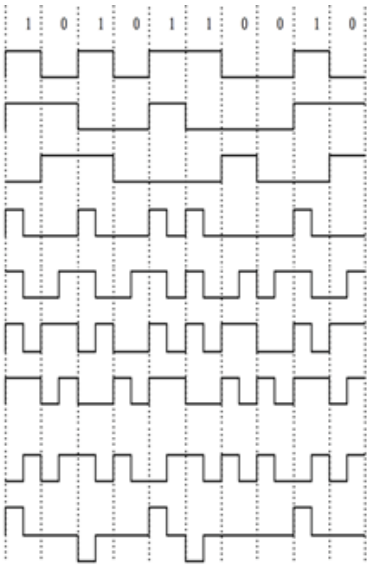


Digital transmission of digital data basically involves the ***line coding*** and ***block coding*** processes. Line coding is the process for converting digital data (binary bits) into digital signal. Furthermore, to ensure accuracy of the received data frame, block coding is done wherein ***redundant bits*** are used. For example, in even-parity, one parity bit is added to make the count of 1s in the frame even and so the original number of bits is increased. Overall, line coding is necessary while block coding is optional,

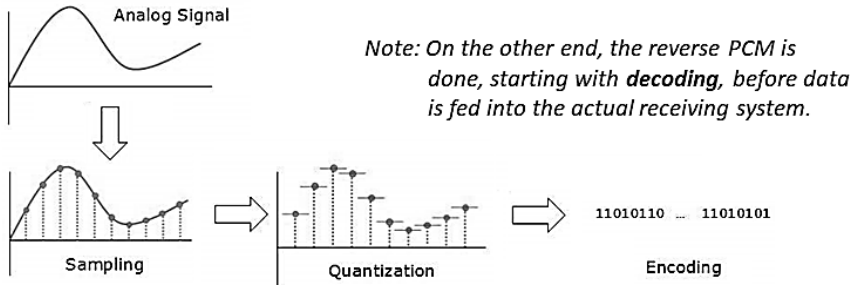


Common Line Coding Schemes

Signal	Comments	1 state	0 state
NRZ–L	Non-return-to-zero level. This is the standard positive logic signal format used in digital circuits.	forces a high level	forces a low level
NRZ–M	Non-return-to-zero mark	forces a transition	does nothing (keeps sending the previous level)
NRZ–S	Non-return-to-zero space	does nothing (keeps sending the previous level)	forces a transition
RZ	Return to zero	goes high for half the bit period and returns to low	stays low for the entire period
Biphase–L	Manchester. Two consecutive bits of the same type force a transition at the beginning of a bit period.	forces a negative transition in the middle of the bit	forces a positive transition in the middle of the bit
Biphase–M	Variant of Differential Manchester. There is always a transition halfway between the conditioned transitions.	forces a transition	keeps level constant
Biphase–S	Differential Manchester used in Token Ring. There is always a transition halfway between the conditioned transitions.	keeps level constant	forces a transition
Differential Manchester (Alternative)	Need a Clock, always a transition in the middle of the clock period	is represented by no transition.	is represented by a transition at the beginning of the clock period.
Bipolar	The positive and negative pulses alternate.	forces a positive or negative pulse for half the bit period	keeps a zero level during bit period



In digital transmission of analog data, digitization must be done first. ***Pulse Code Modulation*** (PCM) is the most common method used and it comes in three steps:

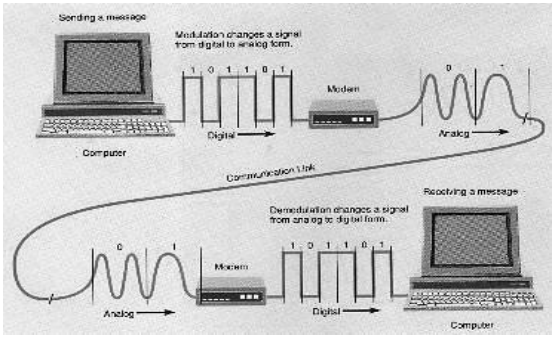


*Note: On the other end, the reverse PCM is done, starting with **decoding**, before data is fed into the actual receiving system.*

The same process with Line Coding happens in the encoding stage of PCM.

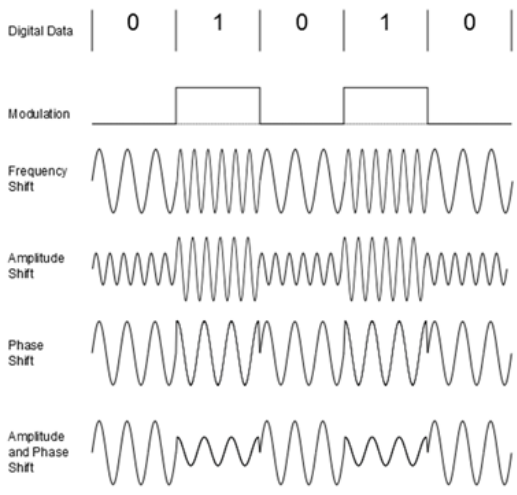
To transmit the digital data over an analog media, it must go through a digital-to-analog converter (DAC) first. It can be through bandpass filters (BPF) that allow only the frequencies of interest to pass, or through low-pass filters that allow to pass only frequencies that are below the cut-off. Analog carrier signals are modified to reflect digital data. Thus, ***digital modulation*** or analog transmission of digital data can be in the form of:

- Amplitude Shift Keying (ASK)
- Frequency Shift Keying (FSK)
- Phase Shift Keying (PSK)
- Quadrature Amplitude Modulation (QAM)



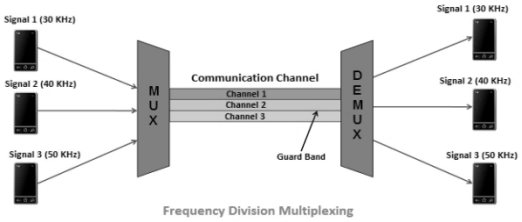
Types of Digital Modulation

Modulation	Units	Bits/Baud	Baud rate	Bit Rate
ASK, FSK, 2-PSK	Bit	1	N	N
4-PSK, 4-QAM	Dibit	2	N	2N
8-PSK, 8-QAM	Tribit	3	N	3N
16-QAM	Quadbit	4	N	4N
32-QAM	Pentabit	5	N	5N
64-QAM	Hexabit	6	N	6N
128-QAM	Septabit	7	N	7N
256-QAM	Octabit	8	N	8N

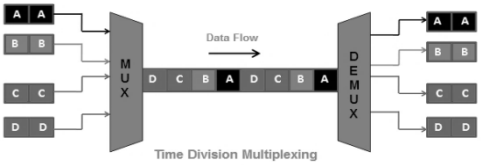


Multiplexing is a technique by which different streams of transmission can be simultaneously processed over a shared link. It divides the high capacity medium into low capacity logical medium which is then shared by different streams. The reverse of this process is called ***demultiplexing***.

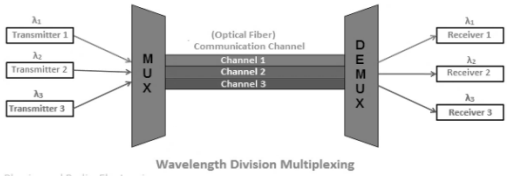
Frequency Division Multiplexing is used in analog TV and radio broadcast systems where the carrier bandwidth is divided into logical channels and allocates one user to each channel



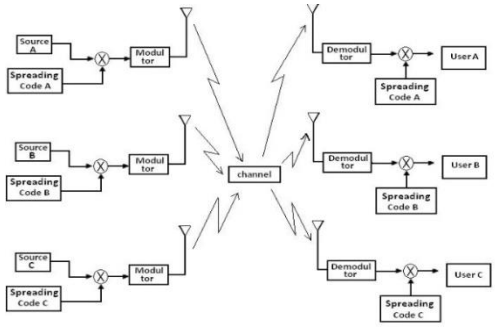
Time Division Multiplexing is used in telephone systems where shared channel is divided among its users by means of time slot where each user transmit data within the provided time slot only



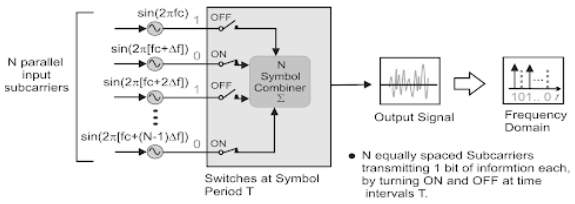
Wavelength Division Multiplexing is used in fiber optic systems where multiple optical carrier signals are multiplexed by using different wavelengths



Code Division Multiplexing is applied in TCP/IP communication to transmit multiple data signals over a single frequency but allows its users to full bandwidth and transmit signals all the time using an orthogonal code to spread the signals

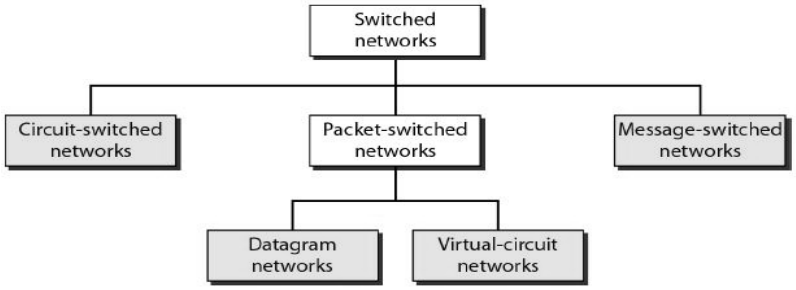


Orthogonal Frequency Division Multiplexing is where single data stream is split across several separate narrowband channels at different frequencies to reduce interference and crosstalk. It is used in digital TV and audio broadcasting, DSL internet access, wireless networks, power line networks, and 4G/5G mobile communications

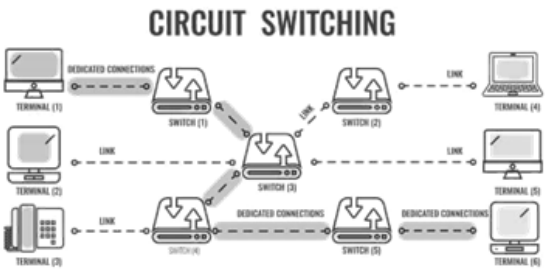


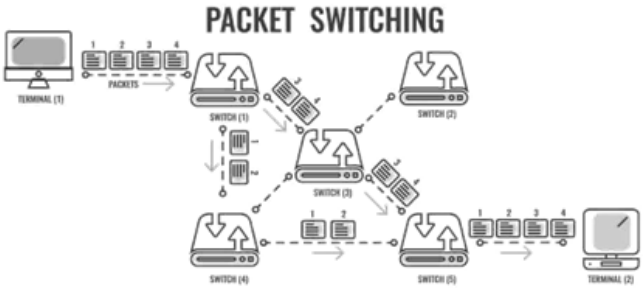
Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called *ingress*, and when data leaves a port or goes out it is called *egress*. A communication system may include number of switches and nodes. At broad level, switching can be divided into two major categories:

- Connectionless – data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- Connection-Oriented – Before switching data to be forwarded to destination, a pre-establish circuit along the path between both endpoints is required. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.



Parameter	Message switching	Circuit switching	Packet switching
Application	Telegraph network for transmission of telegrams	Telephone network for bi-directional, real time transfer of voice signals	Internet for datagram and reliable stream service between computers
End terminal	Telegraph, teletype	Telephone, modem	Computer
Information type	Morse, Baudot, ASCII	Analog voice or PCM digital voice	Binary information
Transmission system	Digital data over different transmission media	Analog and digital data over different transmission media	Digital data over different transmission media





ASSESSMENT

Q&A

Answer what is asked in the following items. Each answer should be in a narrative form with at least 3 sentences and with normal formatting details.

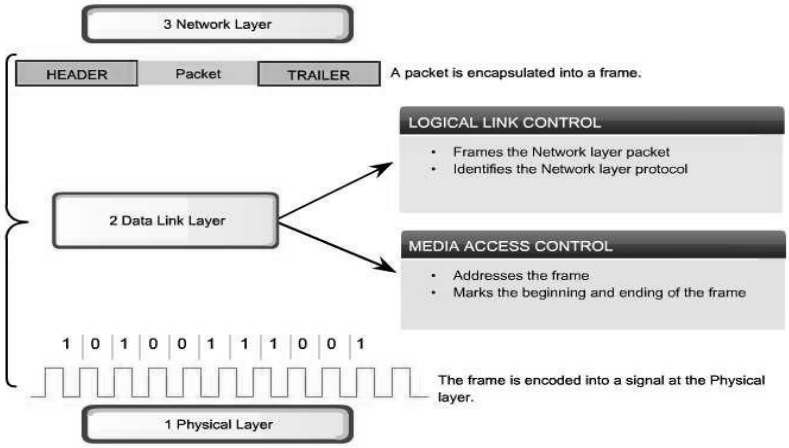
1. Discuss the differences and similarities between the OSI Model and TCP/IP Model in terms of their layers and functions.
2. What is the overall role of the physical layer in the OSI Model? Discuss some of the key processes and technologies involve in it.
3. Explain the difference between ‘digital transmission of analog data’ and ‘analog transmission of digital data’.
4. Which type of switching is used in Internet services? Explain why.

Research Activity

Watch the following YouTube tutorial about Cisco Packet Tracer:
Cisco Packet Tracer | Structured Cabling

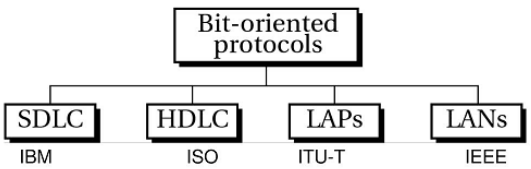
Module 10: **The Data Link and Network Layers**

The ***Data Link Layer*** is responsible for the exchange of frames between nodes over a physical network media and ensures that all packets of information are passed on free of errors. It works between two hosts which are directly connected in some sense that could be point to point or broadcast; systems on broadcast network are said to be on same link. Its work tends to get more complex when it deals with multiple hosts on single collision domain.



Important Data Link Technologies:

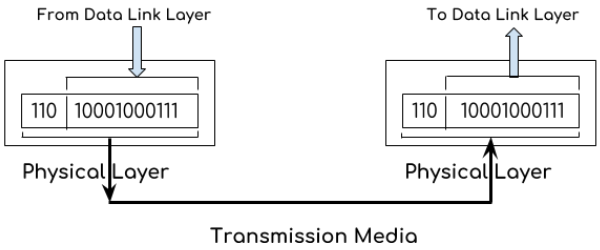
- Frame Relay – telecommunication service designed for cost-efficient data transmission for intermittent traffic between LANs and between endpoints in WANs
- Token Ring – networking technology used to build local area networks; it uses a special 3-byte frame (*token*) that travels around a logical ring of workstations or servers
- Asynchronous Transfer Mode (ATM) – switching technique used by telecommunication networks that uses asynchronous TDM to encode data into small, fixed-sized cells
- Point-to-Point Protocol (PPP) – provides a standard method for transporting multi-protocol datagrams over PPP links, as well as connection authentication, transmission encryption, and compression.



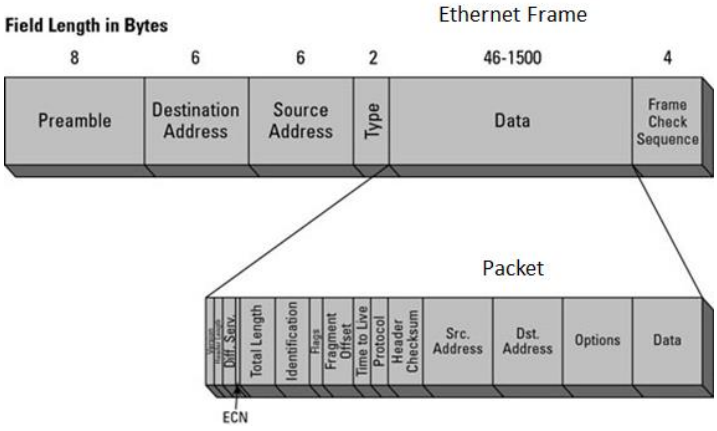
SDLC – Synchronous Data Link Control
HDLC – High-Level Data Link Control
LAPs – Link Access Protocols
LAN – Local Area Nelwork

Services in the Data Link Layer

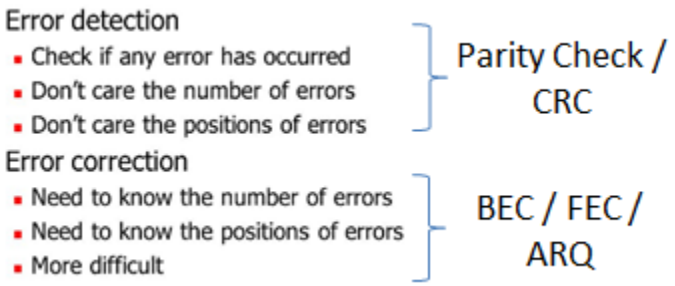
1. Framing – packets are taken from the network layer and encapsulated into ***frames***, which are then sent bit-by-bit to the physical layer

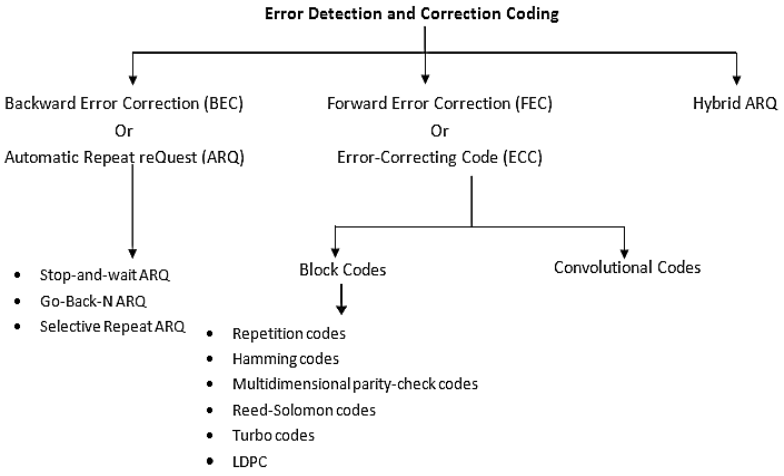


2. Addressing – data-link layer provides layer-2 hardware addressing mechanism in the form of MAC addresses
3. Synchronization – when data frames are sent on the link, both machines must be synchronized in order to transfer to take place

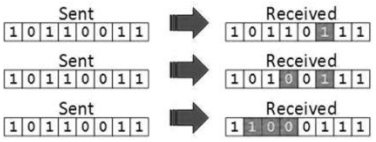


4. Error Control – signals may have encountered problem in transition and the bits are flipped; these errors are detected and the actual data bits are attempted to be recovered with an error reporting mechanism



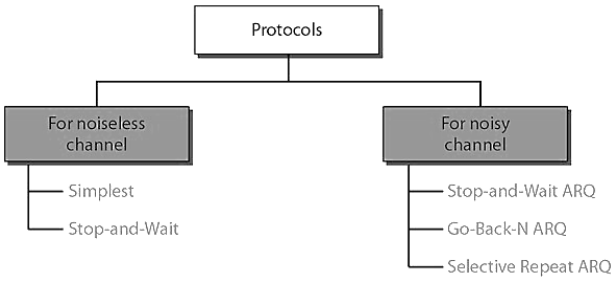


3 Types of Error

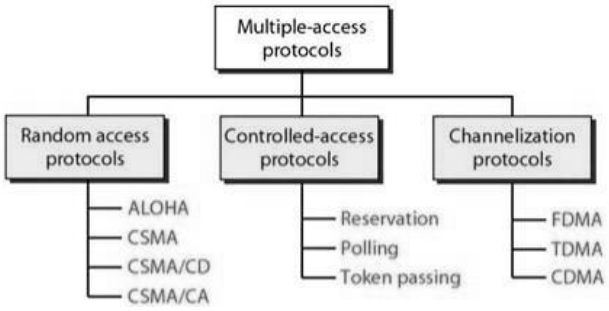


- Single-Bit Error
- Multiple-Bit Error
- Burst Error

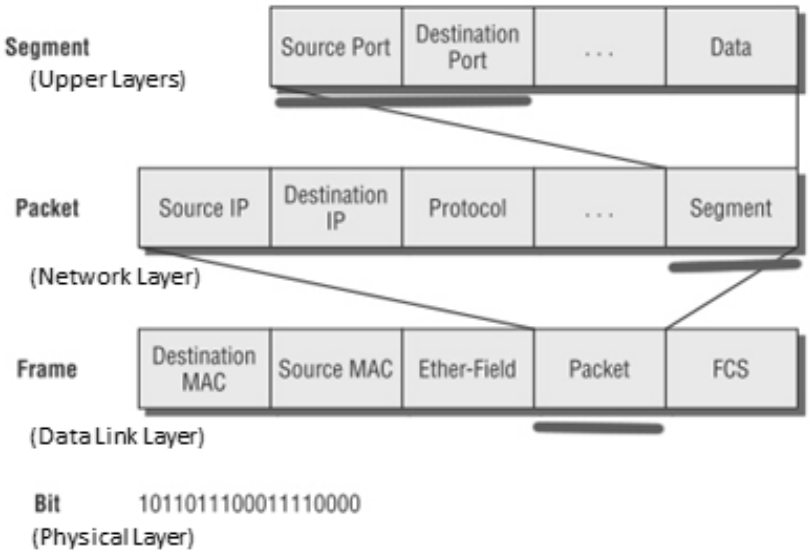
5. <u>Flow Control</u> – stations on same link may have different speed or capacity, and so the data-link layer ensures that both machine to exchange data on same speed



6. <u>Multi-Access</u> – when host on the shared link tries to transfer the data, it has a high probability of collision and hence, mechanism such as *CSMA/CD* and *CSMA/CA* are provided to equip capability of accessing a shared media among multiple systems



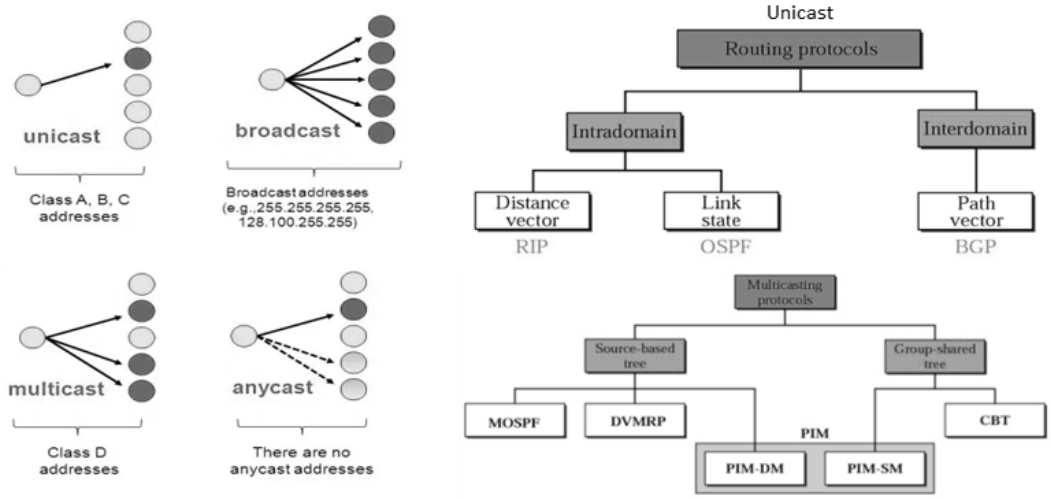
The ***Network Layer*** provides services to allow end devices to exchange data across the network. It manages options pertaining to host and network addressing, managing sub-networks, and internetworking. It takes the responsibility for routing packets from source to destination within or outside a subnet, and also divides the outgoing messages into packets and to assemble incoming packets into messages for higher levels.



Services in the Network Layer

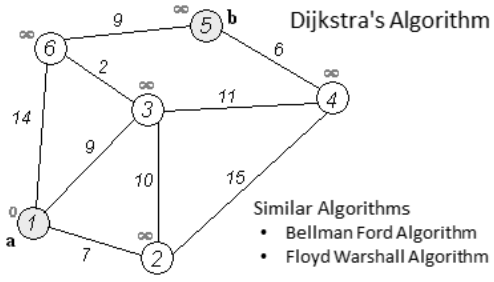
1. Addressing End Devices – in the same way that a phone has a unique number, end devices must be configured with a unique IP address for identification on the network as a *host* (or *node*)
2. Encapsulation – the network layer receives a *protocol data unit* (PDU) from the transport layer and in a process called *encapsulation*, it adds IP header information and the PDU becomes a *packet*
3. Routing – the network layer directs packets to a destination host on another network through a *routing* process wherein a router selects paths for and directs packets toward the destination host, and each route the packet takes to reach the destination host is called a *hop*
4. De-encapsulation – when the packet arrives at the network layer of the destination host, the host checks the packet's IP header and if the destination IP address within it matches its own IP address, the header is removed and the resulting Layer 4 PDU is passed up to the appropriate service at the transport layer

IP Routing Modes



Routing Algorithms

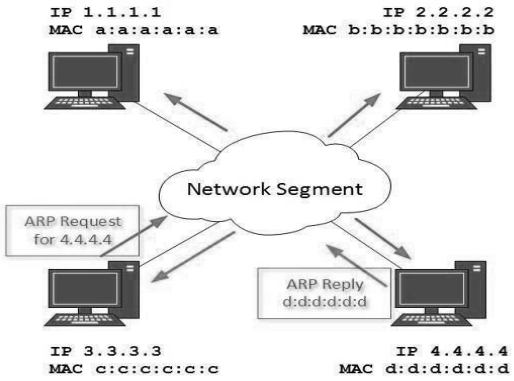
- Flooding – simplest method packet forwarding; when a packet is received, the routers send it to all the interfaces except the one on which it was received.
- Shortest Path – routing decision in networks are mostly taken on the basis of cost between source and destination, considering the *hop count*;



Network Layer Protocols

1. Internet Protocol (IP) – enables every host on the TCP/IP network to be uniquely identifiable; connectionless, best-effort, and media-independent protocol that provides only the necessary functions for delivering a packet from a source to a destination over an interconnected system of networks
2. Internet Control Message Protocol (ICMP) –network diagnostic and error reporting protocol that belongs to IP protocol suite and uses IP as carrier protocol to send back to the originating host any feedback about network such as *ICMP-echo* and *ICMP-echo-reply* messages encapsulated in an IP packet

3. Address Resolution Protocol (ARP) – used to send out an ARP broadcast message asking, "Who has this IP address?" to know the MAC address of remote host on a broadcast domain; also includes the IP address of destination host (the sending host wishes to talk to) into a packet, so that when a host receives an ARP packet destined to it, it replies back with its own MAC address

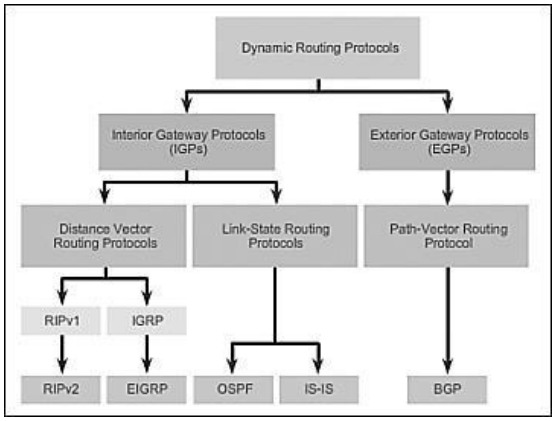


4. IP Routing Protocols – specify how routers talk to each other to distribute information so they can select routes between any two nodes on a network; ***Routing Information Protocol*** (RIP) is one the most common of these protocols

Protocol	Type	Scalability	Metric	IP classes
RIP-1	Distance vector	Small	Hop count	Classful
RIP-2	Distance vector	Small	Hop count	Classless
OSPF-2	Link state	Large	Cost	Classless
IS-IS	Link state	Very large	Cost	Classless
IGRP	Distance vector	Medium	Bandwidth, delay, load, MTU, reliability	Classful
EIGRP	Dual	Large	Bandwidth, delay, load, MTU, reliability	Classless
BGP	Distance vector	Large	Vector of attributes	Classless

Features	RIP		OSPF
	Version 1	Version 2	
Algorithm	Bellman-Ford		Dijkstra
Path Selection	Hop based		Shortest Path
Routing	Classful	Classless	Classless
Transmission	Broadcast	Multicast	Multicast
Administrative Distance	120		*110*
Hop Count Limitation	15		No Limitation
Authentication	No	MD5	MD5
Protocol	UDP		IP
Convergence Time	RIP>OSPF		

Dynamic routing protocols are a solution that is used in large networks so as to reduce the complexity in configuration that would be occasioned by having to configure static routes. These are used to enable the routers exchange routing information, they allow routers to learn about remotely connected networks dynamically. This information is then added to their routing tables as a basis for forwarding packets.



IP Packets

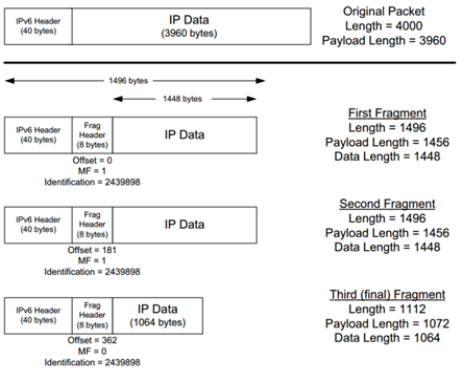
- Payload (IP Data) - contains the Layer 4 segment information and the actual data
- IP Header - identifies the packet characteristics; contains significant fields

Original IP Packet

Sequence	Identifier	Total Length	DF	MF	Fragment Offset
0	345	5140	0	0	0

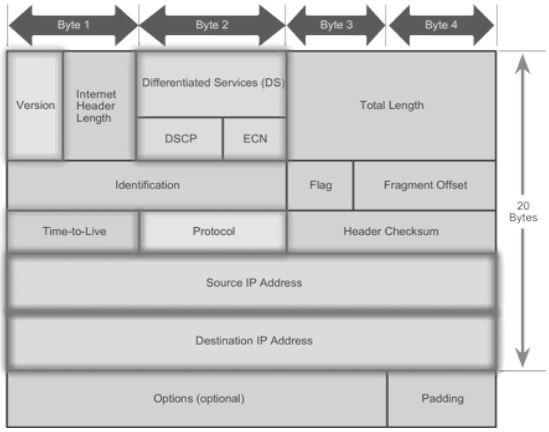
IP Fragments

Sequence	Identifier	Total Length	DF Flag	MF Flag	Fragment Offset
0-0	345	1500	0	1	0
0-1	345	1500	0	1	185
0-2	345	1500	0	1	370
0-3	345	700	0	0	555



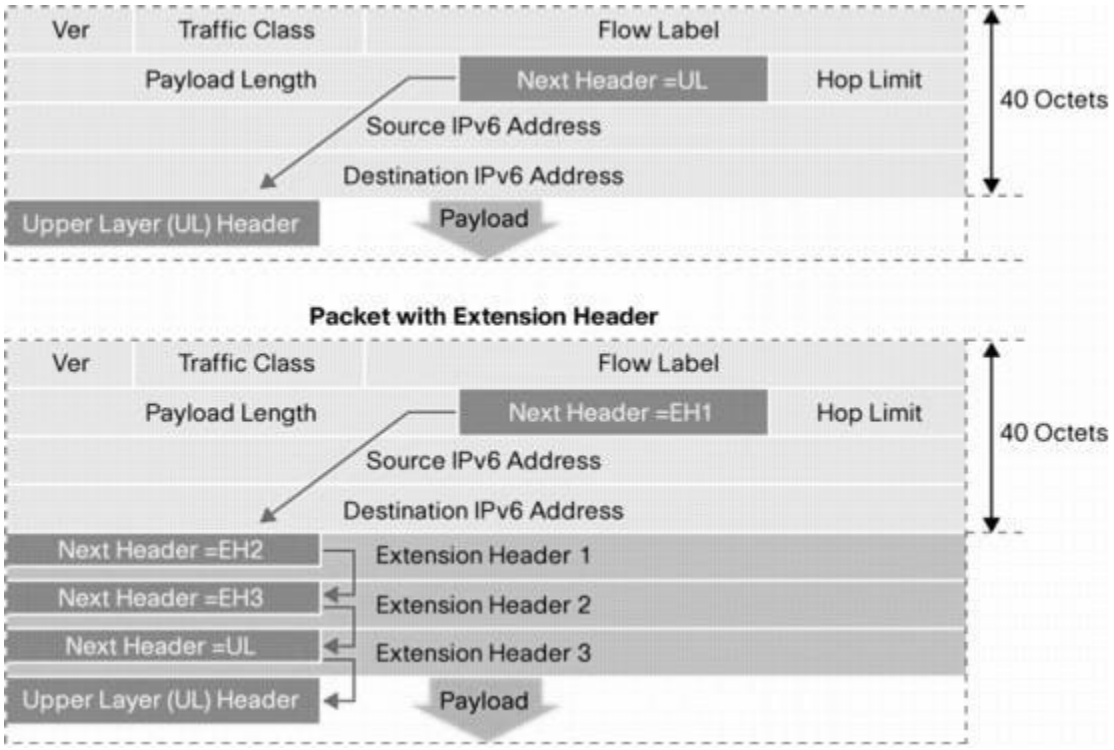
Significant Fields in an IPv4 Packet Header

- Version – contains a 4-bit binary value identifying the IP packet version; set to 0100
- Differentiated Services (DS) – 8-bit field used to determine the priority of each packet; the first 6 bits identify the *Differentiated Services Code Point* (DSCP) value used by a *quality of service* (QoS) mechanism, while the last 2 bits identify the *explicit congestion notification* (ECN) value that can be used to prevent dropped packets during times of network congestion; formerly called the *Type of Service* (ToS) field
- Time-to-Live (TTL) - contains an 8-bit binary value used to limit the lifetime of a packet; specified in seconds but commonly referred to as *hop count;* the *traceroute* command uses this field to identify the routers used between the source and destination
- Protocol – 8-bit binary value that indicates the data payload type that the packet is carrying, which enables the network layer to pass the data to the appropriate upper-layer protocol; common values include ICMP (1), TCP (6), and UDP (17)
- Source IP Address – contains a 32-bit binary value that represents the source IP address of the packet.
- Destination IP Address – contains a 32-bit binary value that represents the destination IP address of the packet.



Significant Fields in an IPv6 Packet Header

- Version – contains a 4-bit binary value identifying the IP packet version; always set to 0110.
- Traffic Class – 8-bit field equivalent to the IPv4 DS field (contains 6-bit DSCP and 2-bit ECN)
- Flow Label – 20-bit field provides a special service for real-time applications
- Payload Length –16-bit field equivalent to the TL field in the IPv4 header that defines the entire packet (fragment) size, including header and optional extensions.
- Next Header – 8-bit field equivalent to the IPv4 Protocol field that indicates the data payload type that the packet is carrying, enabling the network layer to pass the data to the appropriate upper-layer protocol
- Hop Limit – 8-bit field that replaces the IPv4 TTL field
- Source Address –128-bit field that identifies the IPv6 address of the sending host
- Destination Address – 128-bit field identifies the IPv6 address of the receiving host



ASSESSMENT

Q&A

Answer what is asked in the following items. Each answer should be in a narrative form with at least 3 sentences and with normal formatting details.

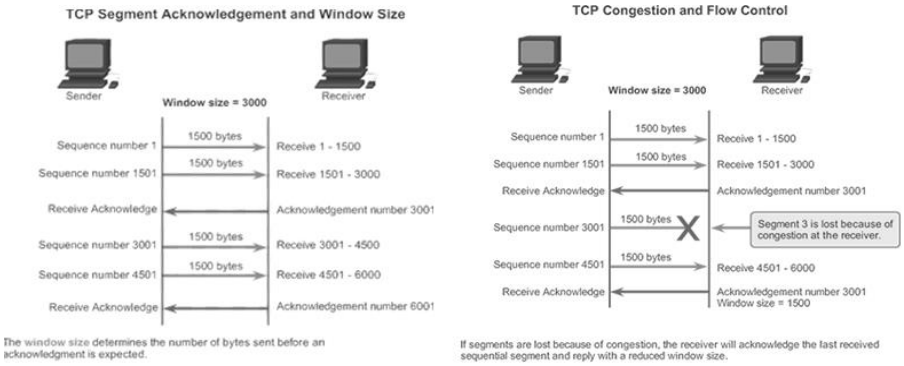
1. Summarize the services of the data link layer. Mention the protocols that make those services possible.
2. What is the difference between error detection and error correction? Explain in terms of the techniques and protocols involved.
3. Discuss the role of the network layer in data communications by describing its four types of services.
4. How does the Internet Protocol work and what are IP packets?

Research Activity

Watch the following YouTube tutorial about Cisco Packet Tracer:
Cisco Packet Tracer | Identify MAC and IP Addresses

Module 11: **The Transport and Session Layers**

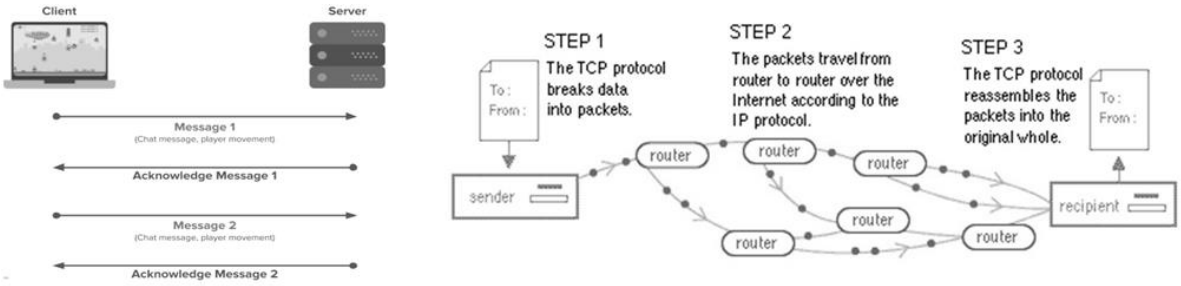
The ***Transport Layer*** offers peer-to-peer and end-to-end connection between two processes on remote hosts. Its main role is to categorize all modules and procedures pertaining to transportation of data or data stream. It takes data from the upper layer (i.e. Application layer) and then breaks it into smaller size segments, numbers each byte, and hands over to network layer for delivery. It also controls the reliability of communications through flow control, segmentation, and error control.



Services in the Transport Layer

1. Connection-Oriented Communication – hosts establish a ***handshake*** protocol to ensure a connection is robust before data is exchanged, but the repeated requests involved cause significant slowdown of network speed when defective byte streams are sent
2. Same Order Delivery – ensures that packets are always delivered in strict sequence by assigning them a number to fix any discrepancies in sequence
3. Data Integrity – using checksums, the data transmitted is guaranteed the same as the data received and that is not corrupt or missing
4. Flow Control – data can end up being sent faster than the speed at which the receiving device is able to buffer or process it, but this service ensures that the data is sent at a rate that is acceptable for both sides by managing data flow
5. Error Control – the transport layer can identify the symptoms of overloaded nodes and reduced flow rates and take the proper steps to remediate these issues
6. Multiplexing – allows the use of simultaneous applications over a network such as when different internet browsers are opened on the same computer
7. Byte orientation – allows applications that require to receive byte streams instead of packets

Transmission Control Protocol (TCP) is the most widely used protocol for data transmission in communication network such as internet. It provides reliable communication between hosts.



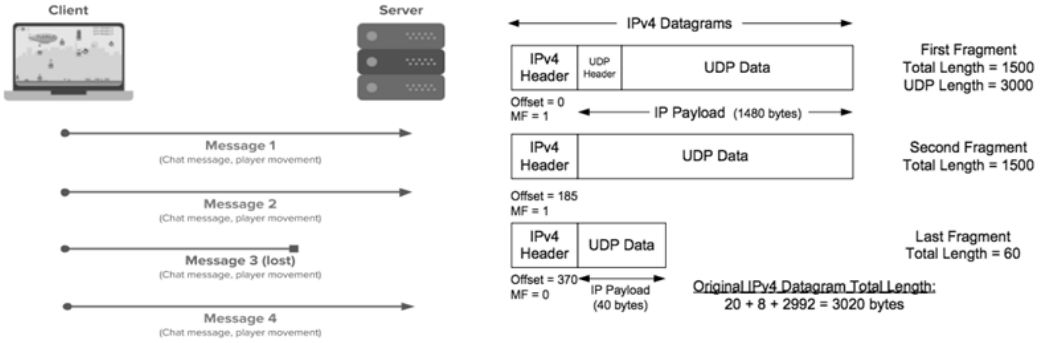
Fields in the TCP Header

- Source Port (16-bits) – identifies the sender's application process source port
- Destination Port (16-bits) – identifies the receiver's application process destination port
- Sequence Number (32-bits) – sequence number of data bytes of a segment in a session
- Acknowledgement Number (32-bits) – contains the next sequence number of the data byte expected when *ACK* is set, and works as acknowledgement received previous data
- Data Offset (4-bits) – implies both, the TCP header size (32-bit words) and the offset of data in current packet in the whole TCP segment
- Reserved (3-bits) – reserved for future use and all are set zero by default
- Flags (1-bit each) – indicate a particular state of connection or provide some additional useful information like troubleshooting or control purposes
- Windows Size – used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment
- Checksum – contains the checksum of *Header*, *Data* and *Pseudo Headers*
- Urgent Pointer – points to the urgent data byte if *URG* flag is set to 1
- Options – facilitates additional options which are not covered by the regular header; always described in 32-bit words (if less than 32-bit, padding is used)

TCP Header

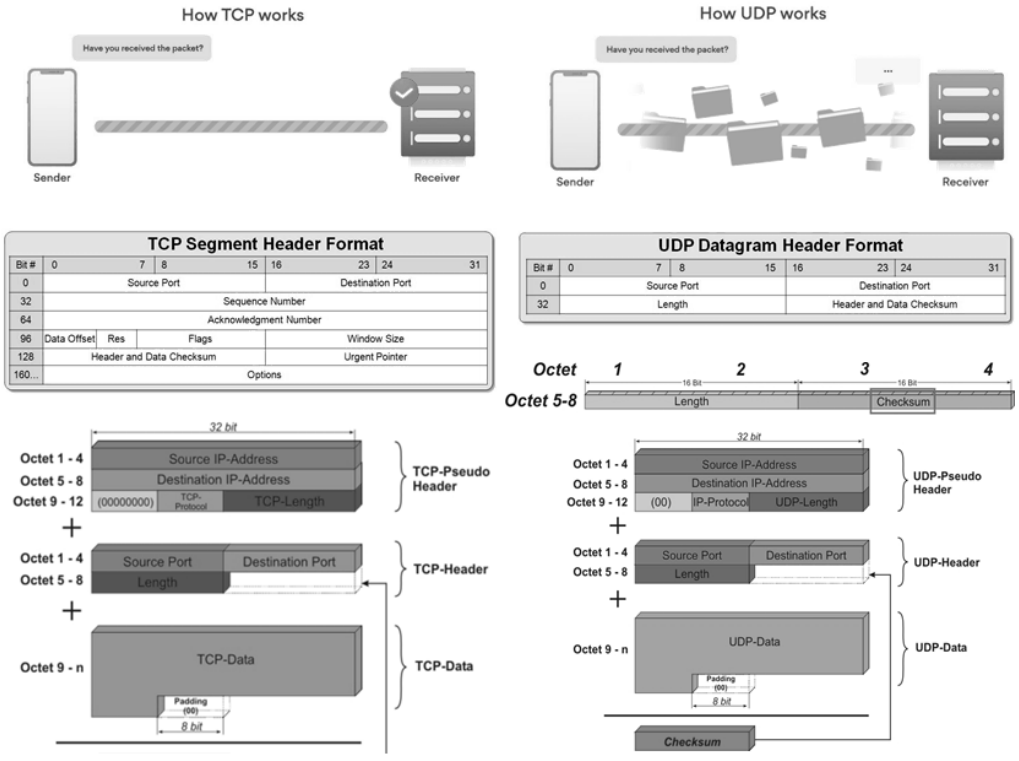
Offsets Octet		0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	**0**	Source port																Destination port															
4	**32**	Sequence number																															
8	**64**	Acknowledgment number (if ACK set)																															
12	**96**	Data offset				Reserved 0 0 0			NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
16	**128**	Checksum																Urgent pointer (if URG set)															
20 ...	**160** ...	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																															

User Datagram Protocol is the simplest Transport Layer communication protocol available of the TCP/IP protocol suite. It involves minimum amount of communication mechanism. Though said to be unreliable, it uses IP services which provides best effort delivery mechanism.



Fields in the UDP Header

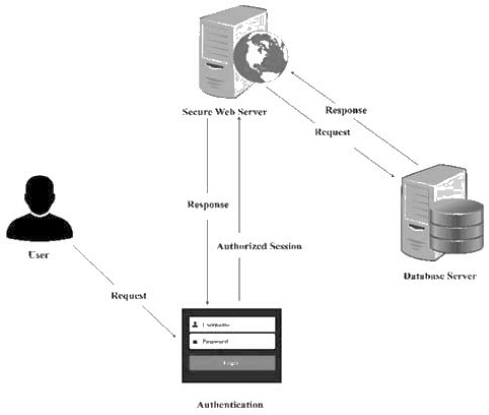
- Source Port (16-bits) – used to identify the source port of the packet
- Destination Port (16-bits) – used to identify destination's application level service
- Length (16-bits) – specifies the entire length of UDP packet (including header)
- Checksum (16-bits) – stores the checksum value generated by the sender before sending; IPv4 has this field as optional so when checksum field does not contain any value it is made 0 and all its bits are set to zero



Other Transport Layer Protocols

1. Stream Control Transmission Protocol (SCTP) – ensures reliable, in-sequence transport of data and provides multi-homing support for transparent failover between redundant network paths
2. Datagram Congestion Control Protocol (DCCP) – minimal, general-purpose transport protocol that provides the establishment, maintenance and tear-down of an unreliable packet flow, as well as congestion control of that packet flow
3. Secure Sockets Layer (SSL) – encryption-based Internet security protocol for ensuring privacy, authentication, and data integrity in Internet communications
4. Transport Layer Security – successor of SSL designed to provide communications security over a computer network and all communications between their servers and web browsers

The ***Session Layer*** controls the connections between multiple computers and tracks the dialogs between computers, called *sessions*. This layer is particularly useful for multimedia applications for which it is necessary to coordinate the timing of two or more types of data, such as voice and moving images, with a high degree of precision.



Services in the Session Layer

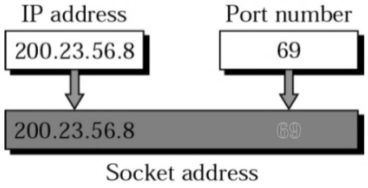
1. Dialog Control – the session layer behaves as a *dialog controller* that allows two communication machines to enter into a dialog in either half-duplex or full-duplex mode
2. Synchronization – process to add checkpoints which are referred to as *synchronization points* into the stream of data
3. Token Management – through prevents the two users to simultaneously attempt access of the same critical operation by managing ***tokens***, which are basically *session IDs*

Network Layer Protocols

1. X.225 (or ISO 8327) – tries to recover lost connection, and refreshes one that is not used for a long period; also provides synchronization points in the stream of exchanged messages
2. Session Control Protocol (SCP) – method of creating multiple light-duty connections from a single TCP connection
3. Zone Information Protocol (ZIP) – AppleTalk protocol that coordinates the name binding process and maintains mappings of zone names to network numbers on internet routers
4. Message Queue Telemetry Transport (MQTT) – protocol used for remote monitoring in IoT to collect statistics of many devices and the delivery of its infrastructure
5. Secure MQTT (SMQTT) – extended form of MQTT that uses encryption based on lightweight attribute-based encryption for a more secure data transmission
6. Advanced Message Queuing Protocol (AMQP) –designed for the financial industry, which also runs on TCP and provides a publishing/subscription architecture, but the broker is broken into two main components: *exchange* and *queues*.

These session-layer tools are normally provided to higher layer protocols through command sets often called ***application program interfaces*** (API). Common APIs include *NetBIOS*, *TCP/IP Sockets*, and *Remote Procedure Calls* (RPCs).

- Network Basic Input/Output System (NetBIOS) – allows applications on different computers to communicate within a local area network (LAN)
- TCP/IP Sockets – internal endpoint for sending or receiving data within a node on a computer network; combination of IP address plus port
- Remote Procedure Call (RPC) – used to request a service from a program located in another computer on a network without having to understand the network's details.



A TCP ***socket*** is an endpoint instance defined by an IP address and a ***port*** in the context of either a particular TCP connection or the listening state. ***Kernel space*** is where the *kernel* (i.e., the core of the operating system) runs and provides its services where the user is not allowed to interfere with.

ASSESSMENT

Q&A

Answer what is asked in the following items. Each answer should be in a narrative form with at least 3 sentences and with normal formatting details.

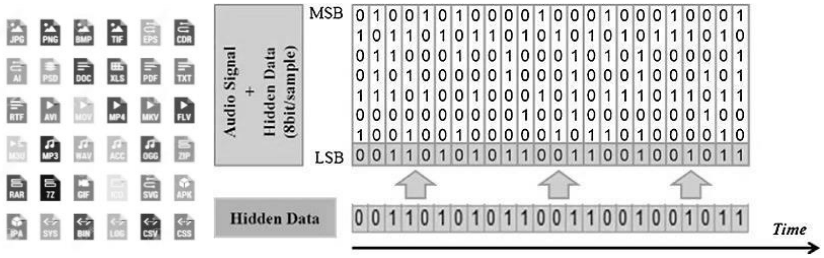
1. Explain the importance of the transport layer through a summary of its services.
2. What are the advantages and disadvantages of TCP compared to UDP, especially with regards to data transmission reliability and speed?
3. How does the session layer work in providing a secure connection in data communications? Which of its services are responsible for it?
4. Research about APIs and discuss how they play a part in the services of the session layer.

Research Activity

Watch the following YouTube tutorial about Cisco Packet Tracer:
Cisco Packet Tracer | TCP and UDP

Module 12: **The Presentation and Application Layers**

The ***Presentation Layer*** is responsible for the delivery and formatting of information to the application layer for further processing or display. It deals with syntactical differences in *data representation* within the end-user systems; hence, it's sometimes called the *syntax layer*. It is responsible for data encryption/decryption and for data compression/decompression. Many of its protocols also belong to the application layer.



Services in the Presentation Layer

1. Translation – process of ensuring interoperability between encoding methods as different computers use different encoding methods
2. Encryption – process that encodes a message or file so that it can be only be read by certain people or program
3. Compression – process of modifying, encoding, or converting the bits structure of data in such a way that it consumes less space on disk or transmission bandwidth

Data Representation refers to the form in which data is stored, processed, and transmitted. It also describes how data types are structured such as how signs are represented in numerical values and how strings are formatted (enclosed in quotes, terminated with a null, etc.). Data representation as text:

- ASCI (American Standard Code for Information Interchange)
- UTF-8 (8-bit Unicode Transformation Format)

Characters:	h	o	p	e
Binary Values:	01101000	01101111	01110000	01100101

File extension	File type name
Text files	
Microsoft Word (Office 97-2003)	
.DOC	Word document
.DOT	Word document template
.WBK	Word backup document
Microsoft Word Open XML (introduced in Office 2007)	
.DOCX	Word document
.DOCM	Word macro-enabled document
.DOTX	Word document template
.DOCB	Word binary document
Other types of text files	
.ODT	OpenDocument text document
.PAGES	Pages document
.RTF	Rich text format file
.TXT	Plain text file
.WPD	WordPerfect document
.WPS	Microsoft Works word processor file
Data files	
.CSV	Comma-separated values file
.ODC	Office data connection file
.ODF	Apache OpenOffice math file

A ***computer file*** is a computer resource for recording data discretely in a computer storage device. A ***file type*** or a *filename extension* is an identifier specified as a suffix to the name of a computer file.

The ASCII Code

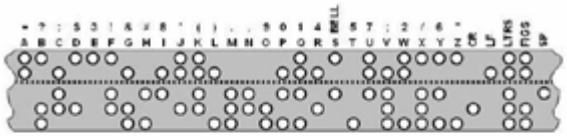
Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	`
1	1	1		33	21	41	!	65	41	101	A	97	61	141	a
2	2	2		34	22	42	"	66	42	102	B	98	62	142	b
3	3	3		35	23	43	#	67	43	103	C	99	63	143	c
4	4	4		36	24	44	$	68	44	104	D	100	64	144	d
5	5	5		37	25	45	%	69	45	105	E	101	65	145	e
6	6	6		38	26	46	&	70	46	106	F	102	66	146	f
7	7	7		39	27	47	'	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(	72	48	110	H	104	68	150	h
9	9	11		41	29	51	)	73	49	111	I	105	69	151	i
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	j
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	k
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	l
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	m
14	E	16		46	2E	56	.	78	4E	116	N	110	6E	156	n
15	F	17		47	2F	57	/	79	4F	117	O	111	6F	157	o
16	10	20		48	30	60	0	80	50	120	P	112	70	160	p
17	11	21		49	31	61	1	81	51	121	Q	113	71	161	q
18	12	22		50	32	62	2	82	52	122	R	114	72	162	r
19	13	23		51	33	63	3	83	53	123	S	115	73	163	s
20	14	24		52	34	64	4	84	54	124	T	116	74	164	t
21	15	25		53	35	65	5	85	55	125	U	117	75	165	u
22	16	26		54	36	66	6	86	56	126	V	118	76	166	v
23	17	27		55	37	67	7	87	57	127	W	119	77	167	w
24	18	30		56	38	70	8	88	58	130	X	120	78	170	x
25	19	31		57	39	71	9	89	59	131	Y	121	79	171	y
26	1A	32		58	3A	72	:	90	5A	132	Z	122	7A	172	z
27	1B	33		59	3B	73	;	91	5B	133	[	123	7B	173	{
28	1C	34		60	3C	74	<	92	5C	134	\	124	7C	174	|
29	1D	35		61	3D	75	=	93	5D	135	]	125	7D	175	}
30	1E	36		62	3E	76	>	94	5E	136	^	126	7E	176	~
31	1F	37		63	3F	77	?	95	5F	137	_	127	7F	177	

The Morse Code

A ·−	N −·
B −···	O −−−
C −·−·	P ·−−·
D −··	Q −−·−
E ·	R ·−·
F ··−·	S ···
G −−·	T −
H ····	U ··−
I ··	V ···−
J ·−−−	W ·−−
K −·−	X −··−
L ·−··	Y −·−−
M −−	Z −−··
0 −−−−−	5 ·····
1 ·−−−−	6 −····
2 ··−−−	7 −−···
3 ···−−	8 −−−··
4 ····−	9 −−−−·
PERIOD ·−·−·−	
COMMA −−··−−	

Other Data Communication Codes

Baudot Code



Discrete Code

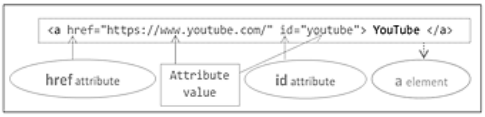
2D Code

Data Representation and Syntax in Web Pages

Tag	Description
<html> ... </html>	Declares the Web page to be written in HTML
<head> ... </head>	Delimits the page's head
<title> ... </title>	Defines the title (not displayed on the page)
<body> ... </body>	Delimits the page's body
<h*n*> ... </h*n*>	Delimits a level *n* heading
...	Set ... in boldface
...	Set ... in italics
...	Center ... on the page horizontally
...	Brackets an unordered (bulleted) list
...	Brackets a numbered list
...	Brackets an item in an ordered or numbered list
 	Forces a line break here
<p>	Starts a paragraph
<hr>	Inserts a horizontal rule
<img src="...">	Displays an image here
 ... 	Defines a hyperlink

```
<HTML>
<script type="text/javascript">
/**
 * This is a multiple-
 * line comment
 */
var index = 0;
var arr = [];

function push(elem) {
    // This comment may span only this line
    arr[index++] = elem;
}
</script>
</HTML>
```



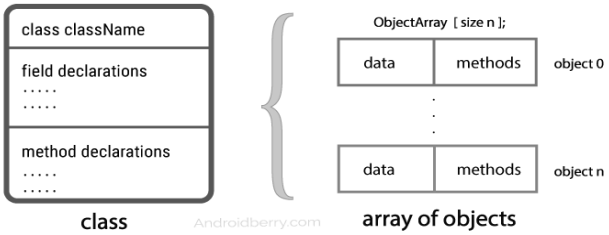
Data Type
byte
sbyte
short
ushort
int
uint
long
ulong
float
double
decimal
char
string
bool
object

XML

```
<empinfo>
   <employees>
      <employee>
         <name>James Kirk</name>
         <age>40></age>
      </employee>
      <employee>
         <name>Jean-Luc Picard</name>
         <age>45</age>
      </employee>
      <employee>
         <name>Wesley Crusher</name>
         <age>27</age>
      </employee>
   </employees>
</empinfo>
```

JSON

```
{  "empinfo" :
     {
          "employees" :  [
          {
               "name" : "James Kirk",
               "age" : 40,
          },
          {
               "name" : "Jean-Luc Picard",
               "age" : 45,
          },
          {
               "name" : "Wesley Crusher",
               "age" : 27,
          }
                         ]
     }
  }
```



Audio File Formats

Uncompressed Formats

- WAV (Waveform)
- AIFF (Audio Interchange File Format)

Compressed, Lossless Formats

- FLAC (Free Lossless Audio Codec)
- ALAC (Apple Lossless Audio Codec)

Compressed, Lossy Formats

- MP3 (MPEG Audio Layer III)
- AAC (Advanced Audio Coding)
- M4A (Audio Only MPEG-4 file)
- Vorbis (a.k.a. Ogg Vorbis)
- WMA (Windows Media Audio)

Image File Formats

Vector Formats

- AI (Adobe Illustration Program)
- EPS (Encapsulated Postscriped File)
- PDF (Portable Document Format)

Raster Formats

- PNG (Portable Network Graphics)
- JPG (Joint Photographic Experts Group)
- TIFF (Tagged Image File Format)
- GIF (Graphics Interchange Format)
- PSD (Adobe Photoshop Program)

Video File Formats

- ASF (Advanced System Format)
- AVI (Audio Video Interleave)
- FLV (Flash Video)
- M4V (iTunes Video)
- MKV (Matroska Video)
- MP4 (MPEG-4)
- MOV (Apple QuickTime)
- MPG (Moving Picture Experts Group)
- SWF (Shockwave Flash)
- VOB (DVD Video Object)
- WMV (Windows Media Video)

Presentation Layer Protocols

1. Secure Shell (SSH) – protocol for secure remote login between computers
2. Internet Message Access Protocol (IMAP) – used by clients to retrieve email messages from a mail server over a TCP/IP connection
3. X.25 Packet Assembler/Disassembler (PAD) – defines how DTEs communicate with the network and how packets are sent over that network using DCEs
4. Network Data Representation (NDR) – implementation of the presentation layer in the OSI model
5. eXternal Data Representation (XDR) **–** specification protocol for a standard representation of various data types
6. Lightweight Presentation Protocol (LPP) – describes an approach for providing "stream-lined" support of OSI application services on top of TCP/IP-based network for some constrained environments
7. Apple Filing Protocol (AFP)
8. Independent Computing Architecture (ICA)
9. NetWare Core Protocol (NCP)
10. Tox Protocol

The ***Application Layer*** is primarily intended for interacting with user and user applications. It specifies the shared communications protocols and interface methods used by hosts in a communications network. It contains the communications protocols and interface methods used in process-to-process communications across an Internet Protocol (IP) computer network

Services in the Application Layer

1. Directory Services – mapping between name and its variable or fixed value
2. File Services – include sharing and transferring files over the network
    - ***File Sharing*** – users can upload a file to a specific server or to its own computer and provide access to intended users
    - ***File Transfer*** – users can copy or move file from one computer to another or to multiple computers through the network that enables them to locate other users in the network and transfer files.
3. Communication Services
    - ***Email*** – the basis of today's internet features; all its users are provided with unique IDs and users can send an email through an email server
    - ***Social Networking*** –people can use it to find other known peoples or friends, can connect with them, and can share thoughts, pictures, and videos
    - ***Internet Chat*** – provides instant multimedia transfer services between two hosts
    - ***Discussion Boards*** – provide a mechanism to connect multiple peoples with same interests so that users can put queries, questions, suggestions etc. which can be seen by all other users and responded to
    - ***Remote Access*** – enables user to access the data residing on the remote computer; this feature is known as *Remote desktop*, which can be done via some remote device
4. Application Services – providing network based services to the users such as web services, database managing, and resource sharing
    - ***Resource Sharing*** – to use resources (servers, printers, and storage media , etc.) efficiently and economically, network provides a mean to share them
    - ***Databases*** – store data, processes it, and enables the users to retrieve it efficiently by using queries to help organizations make decisions based on statistics
    - ***Web Services*** (WWW) – used to connect to the internet, and access files and services from the internet servers

Common Application Layer Protocols

1. Hyper Text Transfer Protocol (HTTP) – works on client server model, being the foundation of WWW; hypertext is well organized documentation system which uses hyperlinks to link the pages in the text documents
2. Domain Name System (DNS) – works on Client Server model using UDP protocol for transport layer communication; the DNS server is configured with FQDN and email addresses mapped with their respective IP addresses
3. Simple Mail Transfer Protocol (SMTP) – used to transfer electronic mail from one user to another by means of email client software (User Agents) the user is using
4. Post Office Protocol version 3 (POP 3) – a simple mail retrieval protocol used by User Agents (client email software) to retrieve mails from mail server
5. File Transfer Protocol (FTP) – standard network protocol used for the transfer of computer files between a client and server on a computer network
6. Telnet – client-server protocol that can be used to open a command line on a remote computer, typically a server
7. Internet Relay Chat (IRC) – protocol that facilitates communication in text form
8. Internet Protocol Security (IPsec) – secure network protocol suite that authenticates and encrypts the packets of data for security purposes
9. Dynamic Host Configuration Protocol (DHCP) – used on IP networks to dynamically assign an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks

Port	Service name	Transport protocol
20, 21	File Transfer Protocol (FTP)	TCP
22	Secure Shell (SSH)	TCP and UDP
23	Telnet	TCP
25	Simple Mail Transfer Protocol (SMTP)	TCP
50, 51	IPSec	
53	Domain Name Server (DNS)	TCP and UDP
67, 68	Dynamic Host Configuration Protocol (DHCP)	UDP
69	Trivial File Transfer Protocol (TFTP)	UDP
80	HyperText Transfer Protocol (HTTP)	TCP
110	Post Office Protocol (POP3)	TCP
119	Network News Transport Protocol (NNTP)	TCP
123	Network Time Protocol (NTP)	UDP
135-139	NetBIOS	TCP and UDP
143	Internet Message Access Protocol (IMAP4)	TCP and UDP
161, 162	Simple Network Management Protocol (SNMP)	TCP and UDP
389	Lightweight Directory Access Protocol	TCP and UDP
443	HTTP with Secure Sockets Layer (SSL)	TCP and UDP

ASSESSMENT

Q&A

Answer what is asked in the following items. Each answer should be in a narrative form with at least 3 sentences and with normal formatting details.

1. Why is it important to understand how the presentation layer protocols work?
2. Discuss the main functions of the presentation layer in data communications.
3. Give at least 3 examples of application layer protocols with a brief description on each.
4. Explain, in your words, the importance of the four services of the application layer.

Research Activity

Watch the following YouTube tutorial about Cisco Packet Tracer:
Cisco Packet Tracer | Setup Application Layer Services

References and Suggested Readings

- Tomasi, Wayne, *Digital Communication Systems*
- Stallings, William, *Data and Computer Communication*
- Louis E. Frenzel Jr., *Principles of Electronic Communication Systems*
- **Various Online Resources**

Downloadable Course AVPs: https://bit.ly/3lp25qa

Downloadable Course PDFs: https://bit.ly/3FtitOt