ITI Presentation

Introduction to
Computer Networks & Cyber Security

Prepared By : Mohamed AboSehly

instructor : Ahmed Sayed

Computer Network Workshop

References:

o Essential Computer Science " Paul D. Crutcher,Neeraj Kumar Singh,Peter Tiegs"

o Cisco Student Guide ICND1

o CompTIA Network

o Data and Computer Communications " William Stallings 8th Edition"

o TCP/IP Protocol Suite "Behrouz A. Forouzan 4th Edition"

o Understanding IPv6 "Joseph Davies 2nd Edition"

o Distributed Systems "van Steen, Maarten, Tanenbaum, Andrew S."

Agenda

❖ **Session 1**
Network Essentials

❖ **Session 2**
Cyber Security Essentials

❖ **Session 3**
Virtualization & Cloud

Session 1 (Network Essentials)

- **Session Outlines**

  - **Computer Networks**

    - Definition and Basic Terminologies

  - **TCP/IP Protocol Suite**

    - Network Access Layer (Physical Layer /Datalink Layer)

    - Internet layer

    - Transport layer
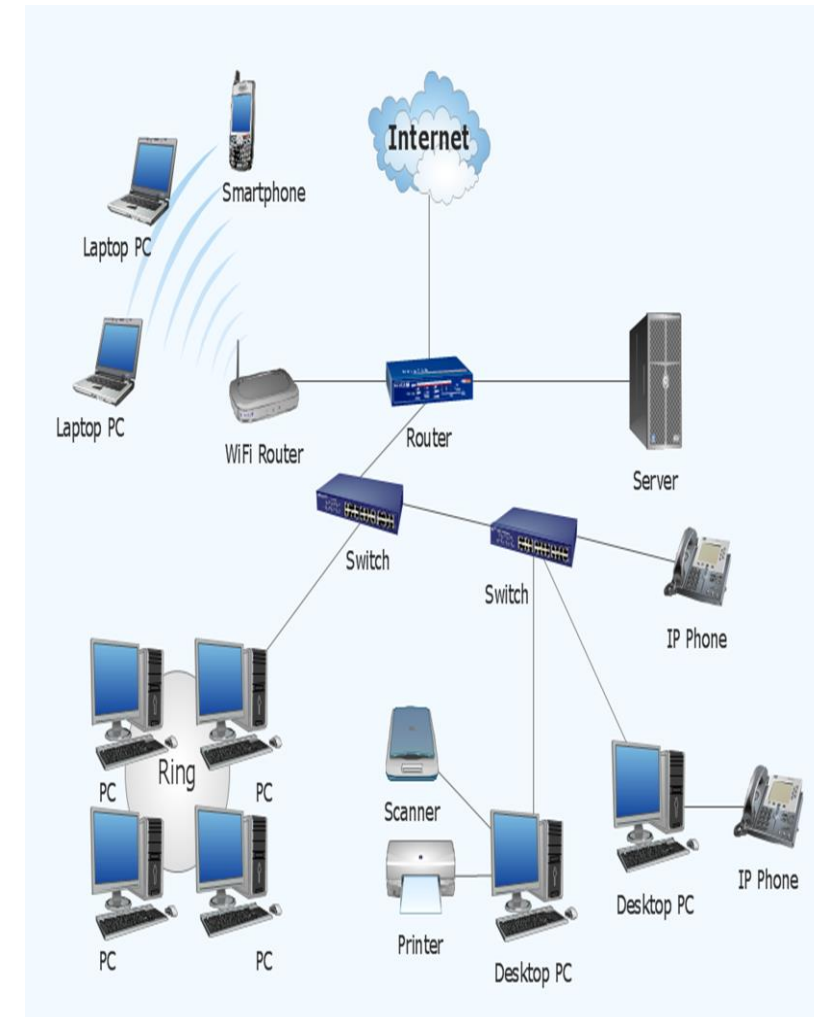
    - Application Layer

- **Computer Network :**

  - a collection of computers, and other devices, or peripherals connected together through connecting media to perform certain task such as :

  Share Resources

- **Resources can be :**

  - File Sharing

  - Devices Sharing

  - Software Sharing with multi-user licenses.

  - Voice and Video calls

  - Shared Internet Access

Session 1 (Network Elements)

- **Network Elements**
  Hardware
  - **Devices**
    - Computers – Printers –Phone – Routers - Switches
  - **Medium**
    - Wired -Wireless –<mark>Satellites</mark>
- **Software**
  - **Messages**
    - Information that travels over the medium such as Mails-WhatsApp….etc
  - **Protocols**
    - Governs how messages flow across network such as http –https-FTP-RDP

Session 1 (Network Basic Terminologies)

كارت الشبكه, لازم اي جهاز عشان يتصل بالشبكه يكون فيه كارت للشبكه تما م

- **NIC (Network Interface Card)/network adapter or LAN adapter.**

  - a hardware that enable the device to directly access the network

    كارت الشبكه ممكن يبقي الكارت الداخلي اللي ببيقي في الجهاز نفسه

    - Internal NIC (plugs into the motherboard directly)

    ممكن الكارت بتاع جهازك يبقي ضعيف او اي حاجه تانيه, لذلك فانت بحاجه لشئ خارجي لمساعدتك علي تحسين الاتصال بالشبكه ومن امثله زي جهاز الالفا المشهور في تقويه الشبكه

    - External NIC(Wireless and USB based)

- **Mac address:**

  - Physical Address, Unique address over the world burned on the

    NIC card

- **IP address :**   عنوان الجهاز داخل الشبكه فقط

  - logical address, identify each device on an IP network layer.

- **Protocols**

  - Communication rules that all entity must agree onhttp –https-FTP-RDP   can we define it as : is a set of rules that governs how the message travel across the network

Session 1 (Network Basic Terminologies)

- ## Hub
  is a device that connect more than one device with each other (create network with them)but here every time one of them send a message, that message will reach to all the devices in the messages adn that lead ot
  - Allow different nodes to communicate with each other at the same network(Slow the network)

- ## Repeater
  - Regenerate the signal over the same network before the signal becomes too weak or corrupted

- ## Access point (AP)
  - allows other Wi-Fi devices to connect to a wired network. An AP is a physical location where Wi-Fi access is available.

- ## Switch
  - Allow different nodes to communicate with each other at the same network and time without slowing each other

- ## Router
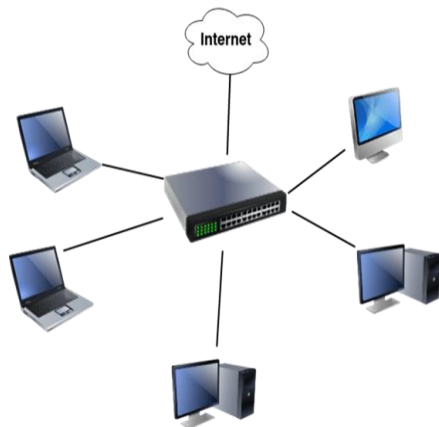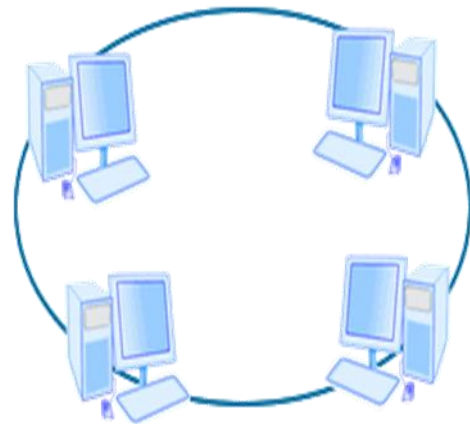 - Allow different networks to communicate with each other

- **Network Topology**
  - how devices are connected (shape) and how message flow from one device to another device, Each topology has its own advantages and disadvantages
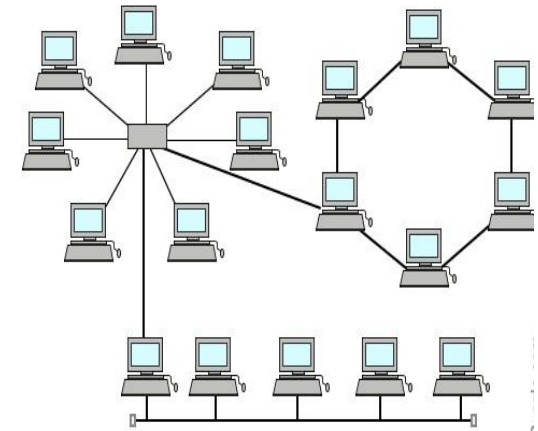

Star

Ring
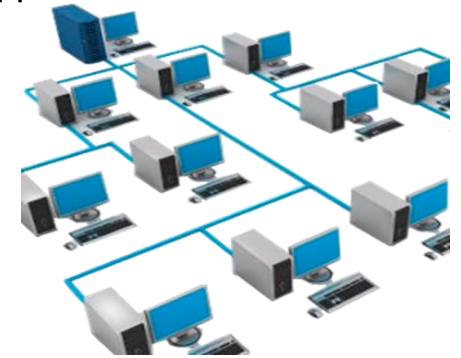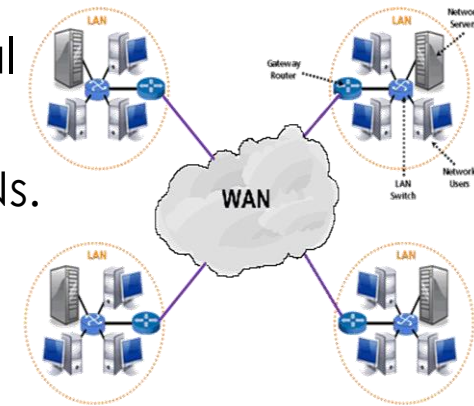

Mesh

Hybrid

- ## Local Area Networks (LAN)
  - a group of computers connected in small geographical area such as school, university campus or office building (100 -1000 M)
    - Allow users to share files and services
    - High speed of communications
    - Under administrative Control

- ## Wide Area Networks (WAN)
  - A WAN is a group of computers connected in Large geographical area such as country
    - WAN can contain multiple smaller networks, such as LANs or MANs.
    - Very low Speed
    - Under your ISP Administrative control example of WAN is Internet
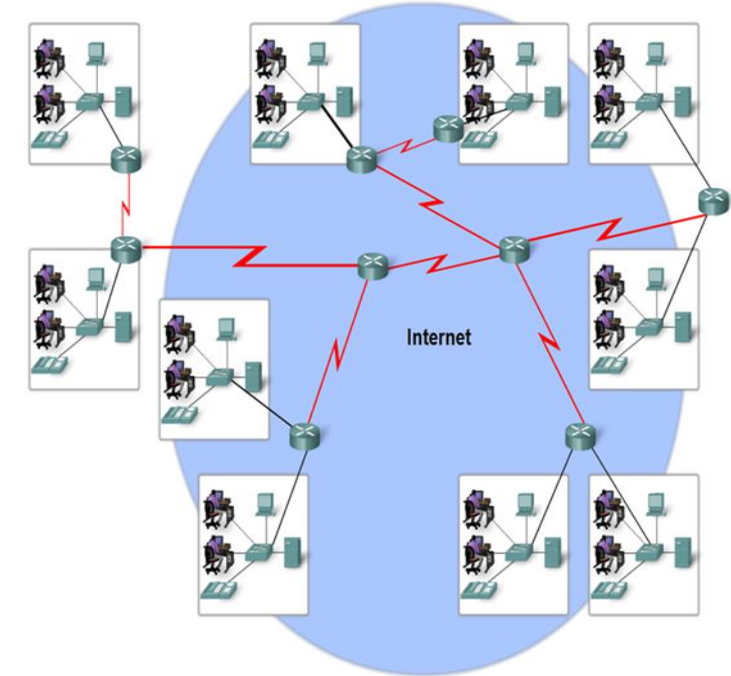
- **The internet**
  - is defined as a global mesh of interconnected networks
- **No one actually owns the Internet**
  - Many Orgs, ISPs, Companies, Govs own pieces of Internet Infrastructure.
    - ISOC: Internet Society
    - IETF: Internet Engineering Task Forum
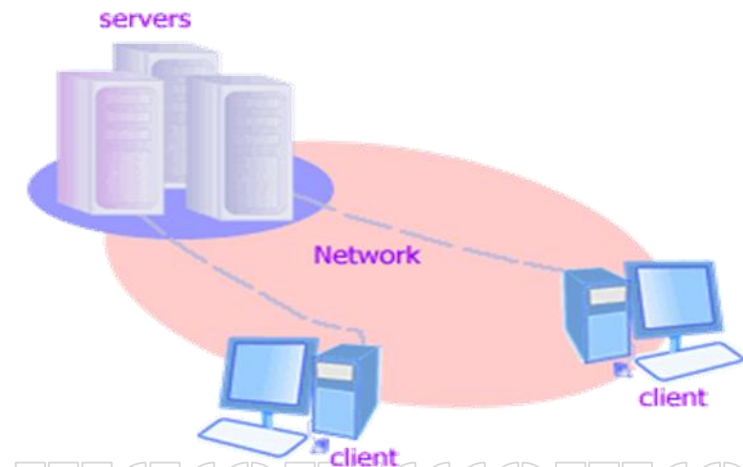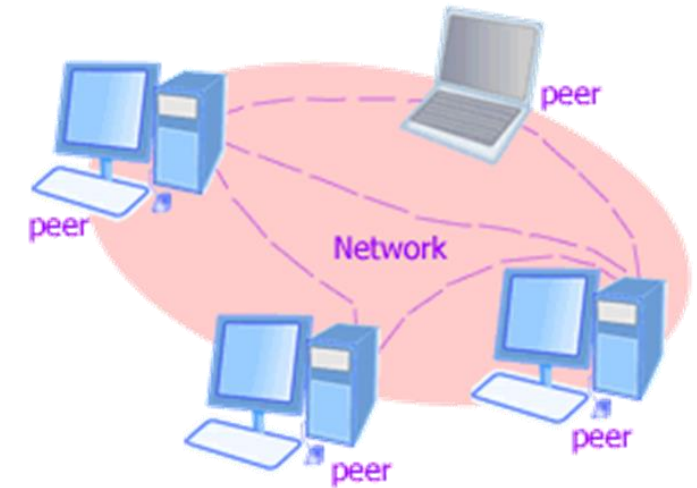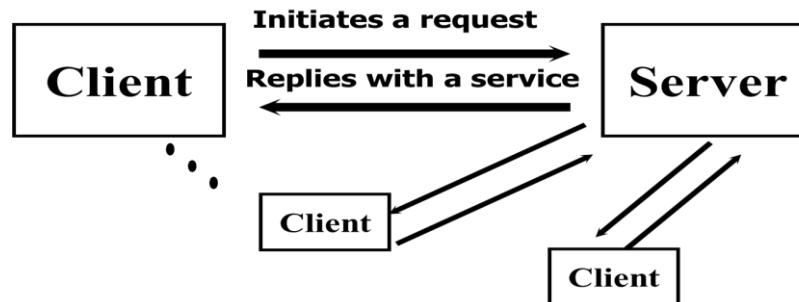   - **ICANN**: **Internet Corporation for Assigned Names and Numbers**
      https://www.submarinecablemap.com/

- **Peer to Peer Networks**
  - No dedicated resources to present specific service
  - Easy to work with
  - All nodes are the same (equal to use the resources)
- **Client/Server Networks**
  - Some nodes (SERVER) are dedicated to present services to other nodes (CLIENTS)
  - Server is more powerful
    - Mail Server
    - Web Server
    - File Server
    - Print Server

Client — Initiates a request → Server
Client ← Replies with a service — Server
Client
Client

Session 1 (TCP/IP Protocol Suite)

- **Why we need Protocols ?**
  - To communicate efficiently
  - Enable data to flow from one NIC to another
  - Control the messages and the messages quantity in the network.

- **OSI Reference Model**
  - **OSI**: Open Systems Interconnect
    - was defined by ISO in 1983
    - Give developers universal concepts so they can develop protocols
    - The OSI reference model breaks this approach into layers.

- **TCP/IP**
  - **Transmission Control Protocol/Internet Protocol.**
    - **Open standard protocol**
    - **Cross Platform** (default protocol for all modern operating systems)
      - Microsoft Operating Systems
      - LINUX Operating Systems
    - **Not tied to one vendor**
    - **Direct access to the Internet**(TCP/IP is the internet protocol)
      - Now internet use TCP/IP v4
      - Next version TCP/IP v6
    - **Routable**

- **TCP/IP VS. OSI Model**

OSI Model	TCP/IP Original	TCP/IP Updated
Application		
Presentation	Application	Application
Session		
Transport	Transport	Transport
Network	Internet	Network
Data Link	Link	Data Link
Physical		Physical

- **Some Protocols in TCP/IP Suite**

- **Network Access Layer**

  - **Physical Layer**
    - defines the electrical, mechanical, Transmission medium
    - movements of individual **Bits** from one node to next
  - **Datalink Layer**
    - Logical interface between <u>end system</u> and <u>network</u>
    - Error notification.
      (FRAMES, MEDIA ACCESS CONTROL)
    - Hop to Hop addressing
    - Error detection Mechanism (detects damaged or lost frames)

- **Physical Addresses (Mac)**
  - Physical Address burned on the card
  - Unique address over the world
  - 48-bit (6-byte) written as 12 hexadecimal digits;
  - every byte (2 hexadecimal digits) is separated by a colon
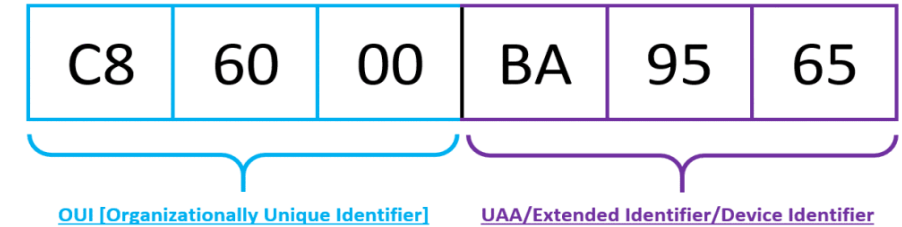
  - Physical addresses can be either
    - **Unicast**
    - **Multicast**
    - **Broadcast**

  - To check your physical address: -
    - **Ipconfig /all**
    - **GetMac**

| C8 | 60 | 00 | BA | 95 | 65 |

OUI [Organizationally Unique Identifier] UAA/Extended Identifier/Device Identifier

Unicast

Broadcast

Multicast

Client Group
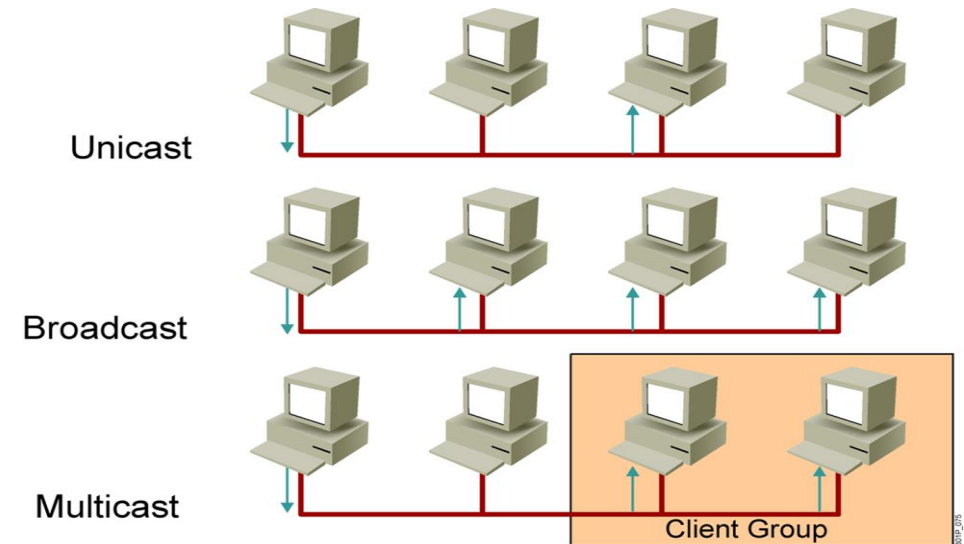
- **Internet / Network protocol Layer (IP Layer)**
  - Provides connectivity and path selection between two hosts (Source to Destination)
  - Routing of data (Provide mechanism to transmit data over independent networks that are linked together)
  - Logical addressing IPV4 , IPV6
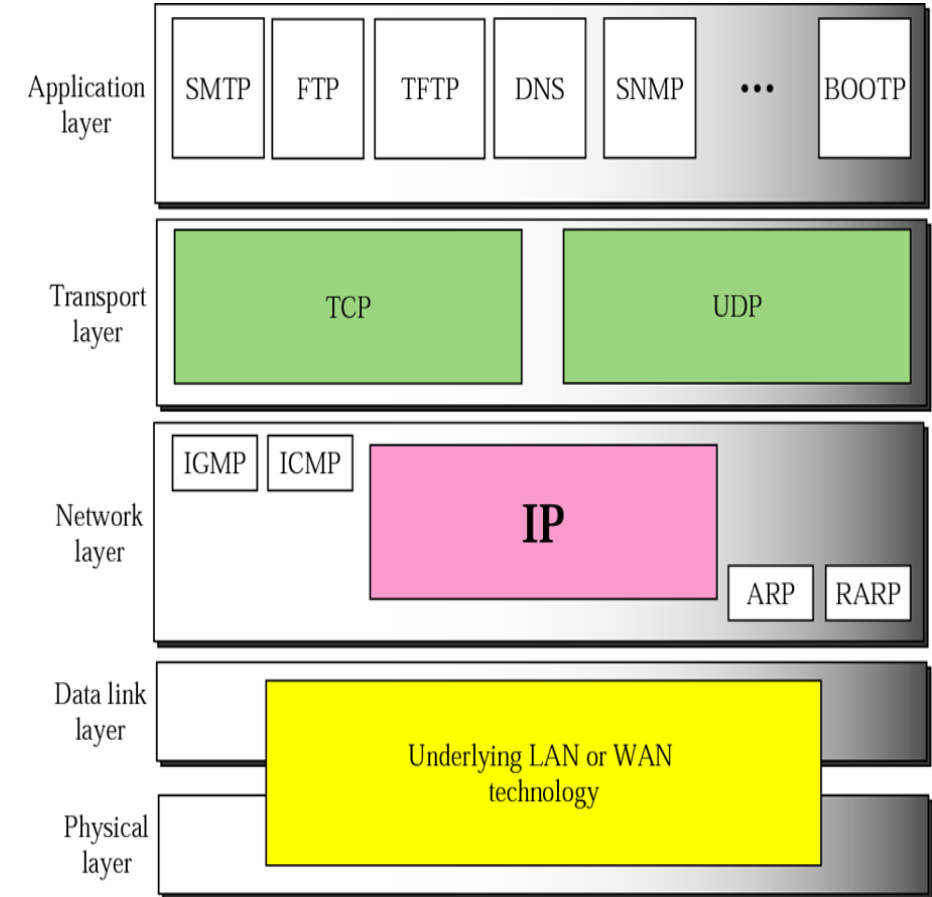
- **Internet Protocol (IP V4)**
  - Uniquely identify each device on an IP network layer.
  - Some times we called it the logical address
  - Every host (computer, networking device, peripheral) must have a unique address at the same network
  - The IP address 32 bit divided into 4 octets each octet 8 bit

1 octet = 8 bit each represents from 0 to 255 separated with dots

	Example			
An IP address is a 32-bit binary number	10101100 00010000 10000000 00010001			
For readability, the 32-bit binary number can be divided into four 8-bit octets	10101100	00010000	10000000	00010001
Each octet (or byte) can be converted to decimal	172	16	128	17
The address can be written in dotted decimal notation	172.	16.	128.	17

- **The address space of IPv4 is 232 or 4,294,967,296**

PUBLIC IP ADDRESSES (Real IP)

Class	Public IP Ranges
A	1.0.0.0 to 9.255.255.255 11.0.0.0 to 126.255.255.255
B	128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255
C	192.0.0.0 to 192.167.255.255 192.169.0.0 to 223.255.255.255

Private IP Addresses (Local IP)

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255 255

- **Nat** is used to Translate the private IP address to public IP addresses.

- **How to assign IP address to device**

  - Manually

  - Automatic (By DHCP)

  - APIPA (Random /Rang : 169.254.X.X)

- **To find your private IP**

  - **Ipconfig - Ipconfig /all   - Ipconfig /release - Ipconfig /renew**

- **ICMP (Ping) To test connectivity between Hosts**

  - **Ping IP**

  - **Ping URL**

  - **Ping IP -l   -n -t**

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 163 . 121 . 25 . 207
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 163 . 121 . 25 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 4 . 2 . 2 . 2
Alternate DNS server: 213 . 131 . 65 . 20

Advanced...

OK   Cancel

- **Internet Protocol (IP V6)**

  - 128-bit address, provides approximately (340,282,366,920,938,463,463,374,607,431, 768,211,456) = approximately 340 undecillion, or 340 billion billion billion billion, addresses)

  - Represented as eight groups, separated by colons, of four hexadecimal digits. The full representation may be simplified by several methods of notation;

2001:0db8:0000:0000:0000:8a2e:0370:7334

=

2001:db8::8a2e:370:7334
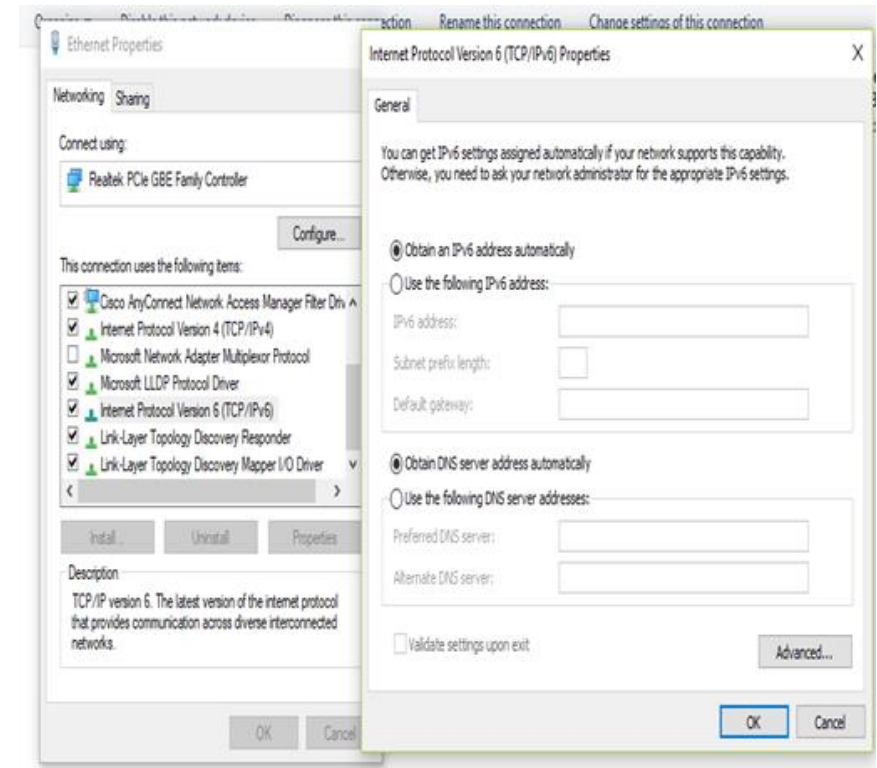
- **Internet Of Things (IOT)**
  - Aims connect all devices to the existing Internet infrastructure.
  - "things" that sense and collect data and send it to the internet.
  - (Eg:- coffee maker, A.C, Washing Machine, Ceiling Fan, lights , any thing) having sensors can be connected with internet.

- **PRACTICAL APPLICATIONS:-**
  - Smart Homes -Smart Cities-Energy - Environment monitoring- healthcare-Management

- **Transport Layer**

TCP Transmission Control Protocol)	UDP User Datagram Protocol
Reliable (Acknowledgement)	Unreliable (Best –Effort delivery)
Connection oriented (synchronization)	Connectionless (no notification)
Full duplex	Full duplex
Error control(Error checking(checksum)	Perform very limited error checking
Data-recovery features	Has no Data-recovery features
E-mail File sharing Downloading	Voice Streaming Video Streaming
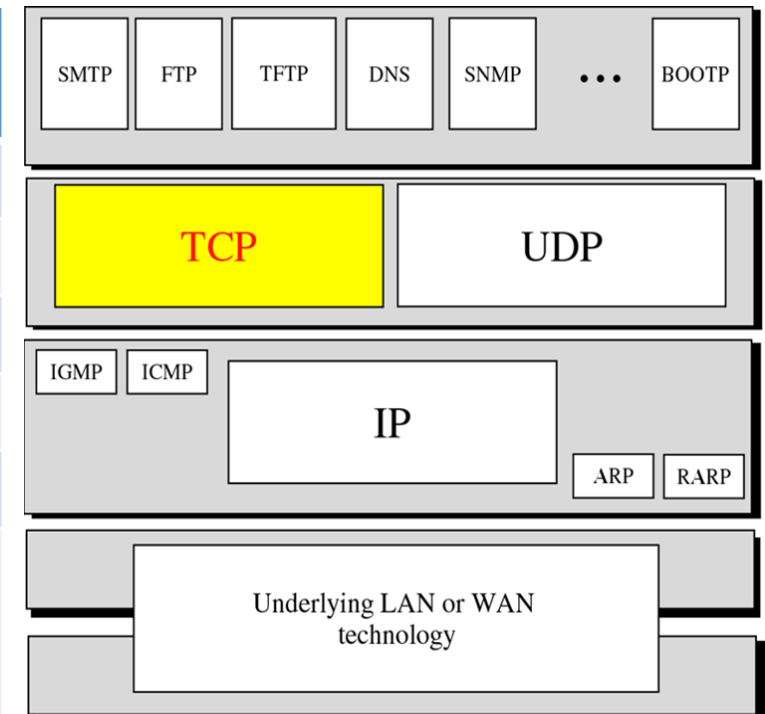
- **Transport Layer addressing (Port Numbers.)**
  - (ICANN) controls the port numbers.
  - **Well Known ports**
    - permanent used numbers.
      Range from 0 to 1,023 are assigned and controlled by ICANN
  - **Registered ports**
    - Range from 1,024 to 49,151 not assigned or controlled by ICANN
      but can be registered at ICANN to avoid duplication
  - **Dynamic ports**
    - Range from 49,152 to 65,535 are neither controlled nor registered
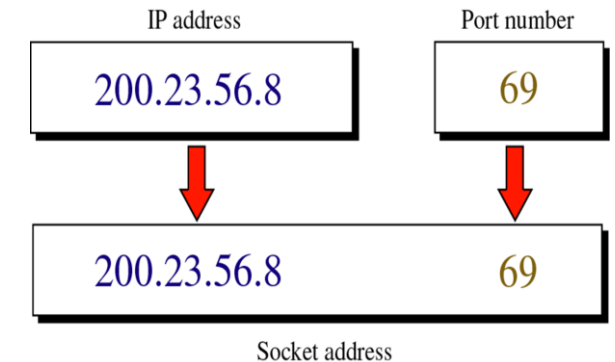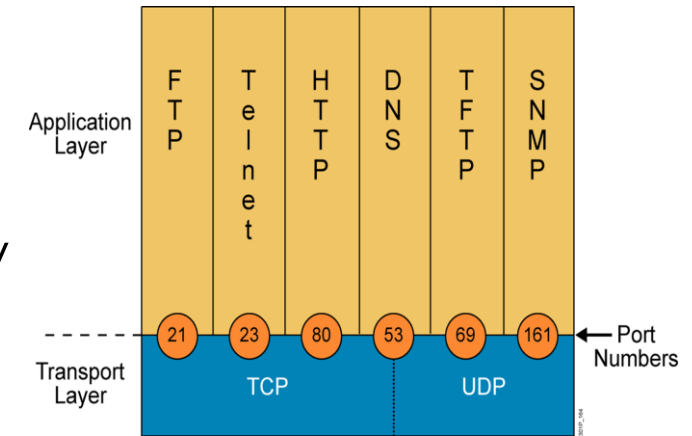
- **Application Layer**
  - Communication between processes or applications

  - Internet Services (Client/Web Server)
    - The World Wide Web: HTTP
    - Naming Service: DNS
    - File Transfer: FTP
    - Telnet Service
    - Electronic Mail service: IMAP, POP3, SMTP

| Application |
| Transport |
| Internet |
| Network Access |

- File transfer
  - FTP
  - TFTP
  - Network File System
- E-mail
  - Simple Mail Transfer Protocol
- Remote login
  - Telnet
  - rlogin
- Network management
  - Simple Network Management Protocol
- Name management
  - Domain Name System
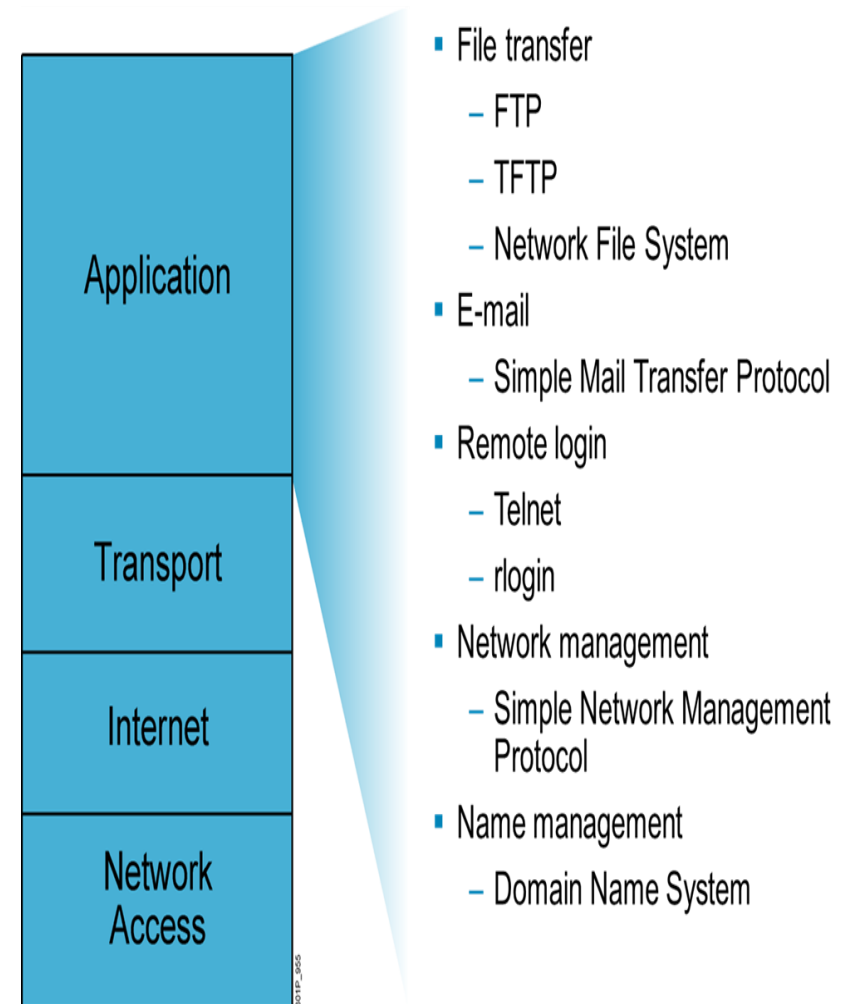
- **URL is Universal Resource Locator**

- **Protocol** : HTTP, HTTPS or FTP
- **Host** : is the domain name of the computer on which the information is located .
- **Port**: The URL can optionally contain the port number of the server
- **Path**: is the pathname of the file where the information is located.

- **HTTP (Hyper Text Transfer Protocol)**
  - Supports the delivery of web pages to the client
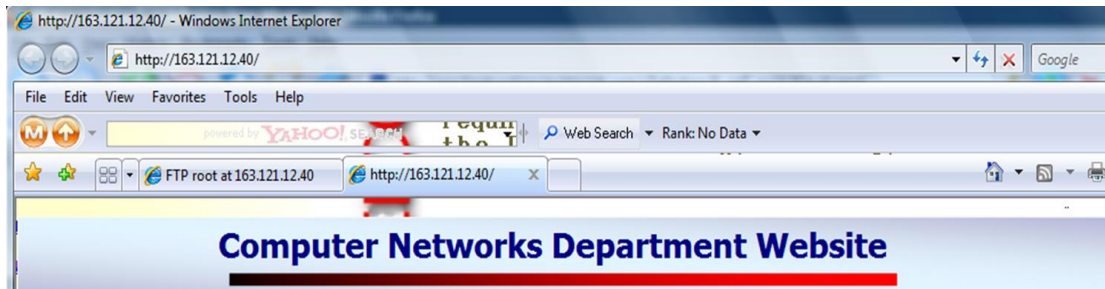
- ## **DNS** (Domain Name Servers)
  - A way to translate human-readable names into IP addresses
- ## How the client get the website
  - 1- check the cash
  - 2- check the hosts file
  - 3- Ask DNS server
- ## List of Top Level Domains (TLDs)

Resolving DNS Addresses
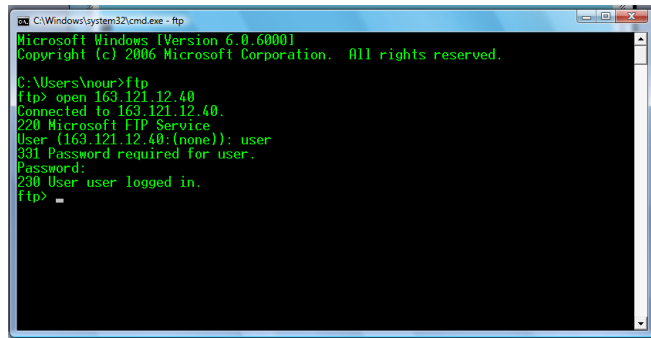
Domain Name	Assigned To
com	Commercial organization
edu	Educational institution
gov	Government organization
mil	Military group
net	Major network support center
org	Organization other than those above
country code	A country
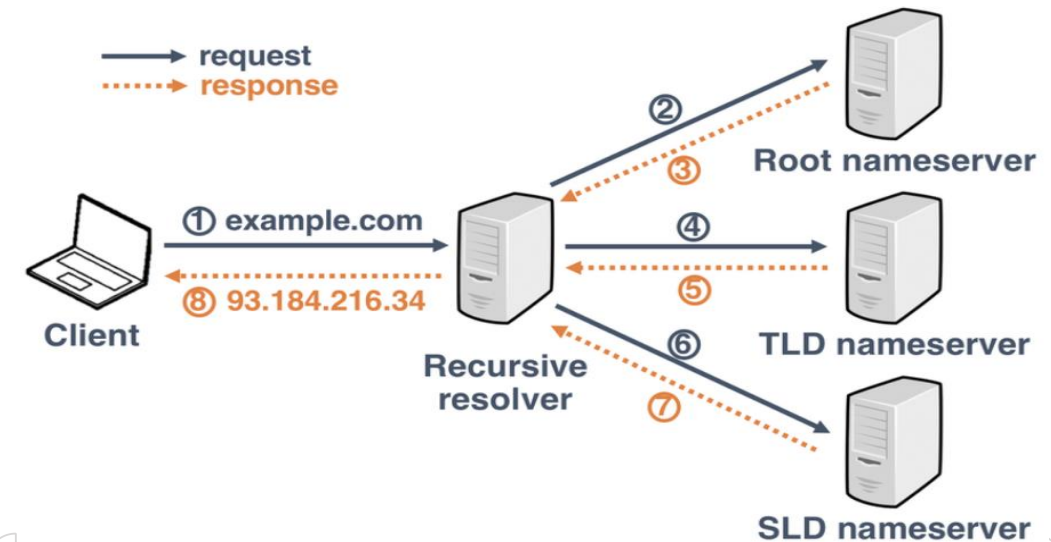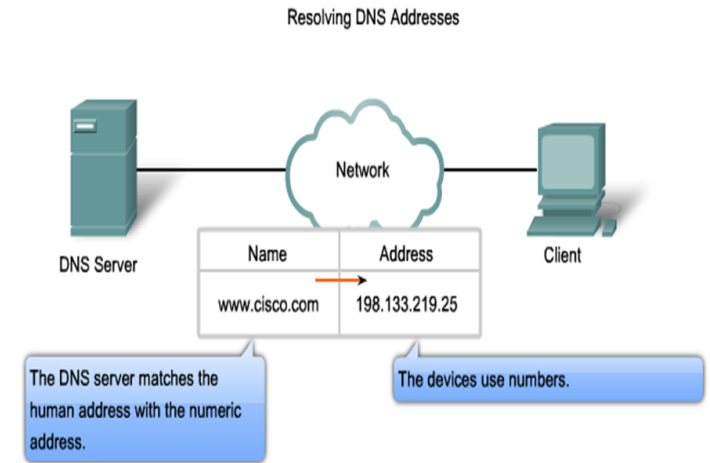
- ## **FTP** (File Transfer Protocol)
  - a transmission protocol that provides reliable data transfer between hosts
  - FTP Client
    - Use Internet Browser as FTP client.
    - Using MS Windows built-in FTP client
    - Third party programs "cute FTP"
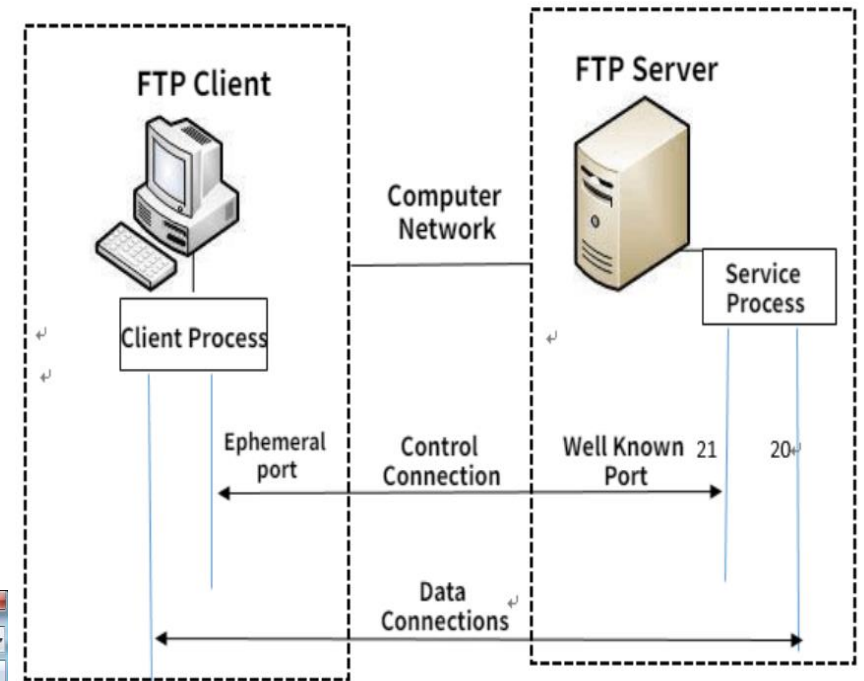
Working Principle of FTP

- ## Telnet /SSH or RDP

  - Telnet/SSH is a user command and an underlying TCP/IP protocol for accessing remote computers.

  - **Telnet/SSH**, an administrator can access someone else's computer remotely

  - **Remote Desktop Protocol (RDP**) is a Microsoft proprietary protocol that enables remote connections to other computers,

Telnet VS SSH

SSH(Secure Shell)	Telnet
Runs on port 22	Runs on port 23
Very Secure Protocol	Not Secure Protocol
Only major protocol to access	Joint abbreviation
Difficult to decrypt	No data encryption
All popular Operating System	Linux , Windows

- ## Mail Server and Clients

  - ### Mail Clients
    - **Web based** : Hotmail ,gmail
    - **Non web based :** Microsoft Outlook

- ## Mail Protocols

- **SMTP (send mail transfer Protocol)**
  - send messages back and forth to other Mail Servers or Email Clients

- **POP3 "Post Office Protocol version 3"**
  - the Email Client contacts the Mail Server to collect email messages
  - Download messages on the hard disk
  - can work Offline
  - Keep the user's quota on the server

- **IMAP4 "Internet Message Access Protocol version 4"**
  - Retrieve only message header
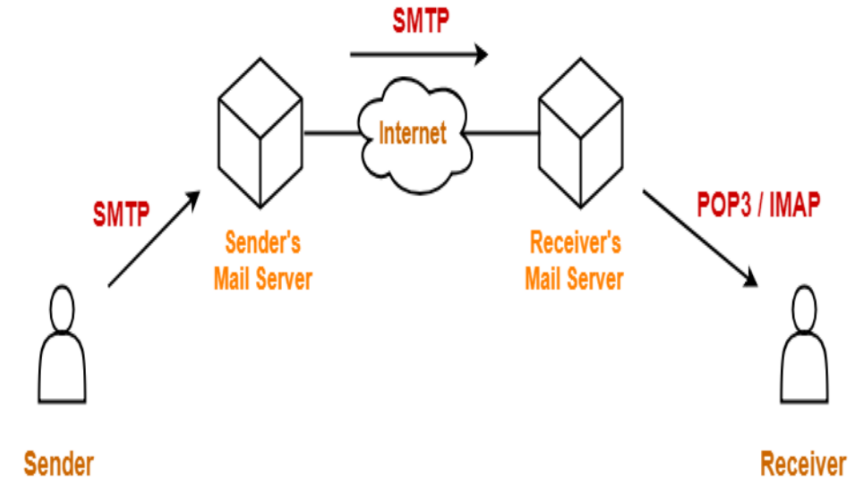
Session 1 Practices

- **Find your mac address**
  - Ipconfig /all
  - Get mac
- **Find your real IP addresses**
  - https://www.whatismyip.com/
- **Find your private IP addresses**
  - Ipconfig
  - Ipconfig /all
  - Ipconfig /release
  - Ipconfig /renew
- **Find current session and ports on your device**
  - Netstat -n
  - Netstat -a
- **Find The IP of the domain Yahoo.com**
  - Nslookup Yahoo.com

Session 2 (Cyber Security Essentials)

- **Session Outlines**
  - **Security Goals & Risks**
    - Confidentiality
    - Integrity
    - Availability
  - **Risks**
    - Threats & Vulnerabilities
    - Attackers methodology & Methods
    - Malware Types
  - **Security Defenses**
    - Firewalls (Static & Dynamic firewalls)
    - IDS /IPS
    - VPN
    - Proxy
    - Next generation Firewalls
  - **Encryption**
    - Symmetric & Asymmetric Key Cryptography
    - Digital Signatures /Digital Certificates

Session 2 (Security Goals)

- ## Cyber Security
  - protect systems, networks, programs, devices and data from cyber attacks
  - Security is a **shared responsibility** that each person must accept when they connect to the network.

- ## Security Goals Technically Defined
  - ### Confidentiality
    - Ensuring that information is not revealed to unauthorized persons
  - ### Integrity
    - Ensuring consistency of data and it should be possib to detect any modification of data
  - ### Availability
    - Ensuring that legitimate users are not denied access to information and resources

Session 2 (Risks & Threats)

- **Focus of Security is Risk**

  - **Risk = Threat x Vulnerabilities**

- **Vulnerability** is the degree of weakness which is found in every network and device.

- **Threats** is A person, thing, event or idea which poses danger to an **asset** in terms of that asset's confidentiality, integrity, availability or legitimate use

- **It's impossible** to totally eliminate risk & There is NO simple solution to securing information

- **Security 99.9 % Not found Why ?**
  - This can be seen through the different types of attacks that users face today.
  - New technologies / applications
  - New Vulnerabilities
  - the difficulties in defending against these attacks

- **Attack:** Any attempt to destroy, expose, alter, disable, steal or breaking into the information or breaking the systems or gain unauthorized access to or make unauthorized use of an asset

- **Passive Attack**
  - Difficult to detect, because the attacker isn't actively sending traffic (malicious or otherwise)
  - Example: An attacker capturing packets from the network and attempting to decrypt them

- **Active Attack**
  - Easier to detect, because the attacker is actively sending traffic that can be detected.
  - An attacker might launch an active attack in an attempt to access information or to modify data on a system.

- **What does a Malicious Hacker Do?**

  - **Reconnaissance**

    - where an attacker seeks to gather **as much information as possible** about a target to launching an attack.

  - **Scanning**

    - the hacker scans the network with specific information gathered during reconnaissance. Scanning for open ports, operating systems, applications,

  - **Gaining Access**

    - the true attack phase. The hacker exploits the system.

  - **Maintaining Access**

    - the hacker tries to retain his 'ownership' of the system.
    - Sometimes, hackers harden the system from other hackers.

  - **Covering Tracks**

    - activities undertaken by the hacker to extend his misuse of the system without being detected. Hackers can remain undetected for long periods.

Reconnaissance

Scanning

Covering tracks

Gaining access
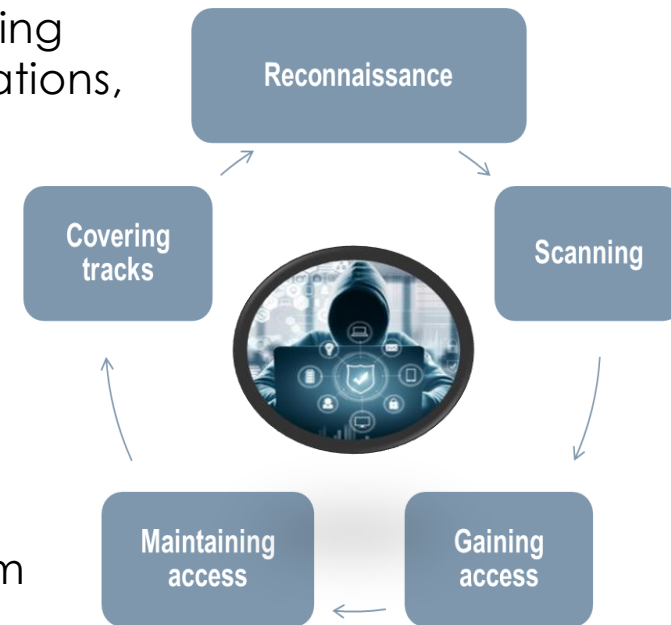
Maintaining access

- **Social engineering**
  - is a term that refers to the ability of something or someone to influence the behavior of a group of people.
- **PHISHING ATTACK:**
  - A fake web page which looks exactly like a popular website such (facebook, twitter, Gmail , paypal , bank page) to persuade you to enter information identity such as username , passwords and credit cards details
  - the hacker records the username and password and then tries that information on the real site.
- **HIJACK ATTACK**
  - a hacker takes over a session between you and another individual and disconnects the other individual from the communication. You still believe that you are talking to the original party and may send private information to the hacker by accident.
- **Insider Attack**
  - involves someone from the inside, such as a disgruntled employee, attacking the network.
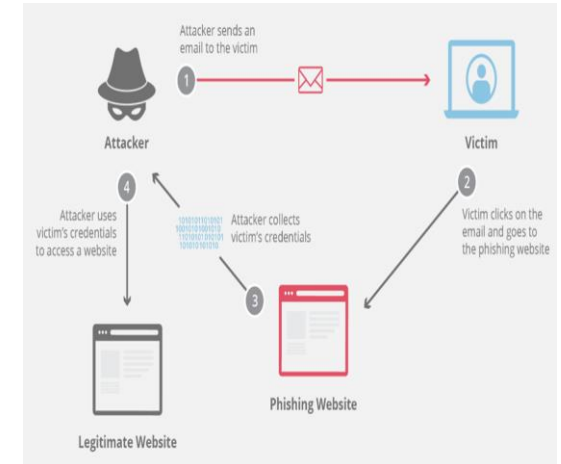
- **SPOOF ATTACK**
  - the hacker modifies the source address of the packets he or she is sending so that they appear to be coming from someone else. This may be an attempt to bypass your firewall rules.

- **BUFFER OVERFLOW ATTACK**
  - A buffer overflow attack is when the attacker sends more data to an application than is expected. usually results in the attacker gaining administrative access to the system in a command prompt or shell
  - **PASSWORD ATTACK**
  - An attacker tries to crack the passwords stored in a network account database or a password-protected file.
    - **Dictionary attack**
    - **Brute-force attack**
    - **Hybrid attack.**

Buffer Overflow Attack

| Function |
| Parameters |
| Return Function |
| Base Pointer |
| Buffer |

| Function |
| Parameters |
| Return Function |
| Base Pointer |
| Buffer |

Malicious Code

Before Attack   After Attack
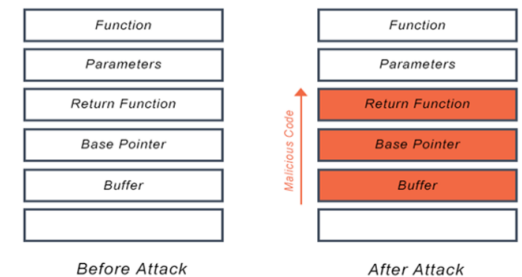
- ## Backdoor or Trapdoor
  - Secret entry point into a program ,Have been commonly used by developers
  - Can't be removed or scanned and the only way is to uninstall sw or format the system

- ## Trojan Horse
  - program with hidden side-effects which is usually superficially attractive eg game, software upgrade etc .
    - allows attacker to indirectly gain access they do not have directly
    - used to propagate a virus/worm or install a backdoor
    - Open some ports or pass some malicious files

- ## Viruses
  - A virus is malicious software that is attached to another program to execute a particular unwanted function on a user's workstation.
    - Both propagates itself & carries a payload
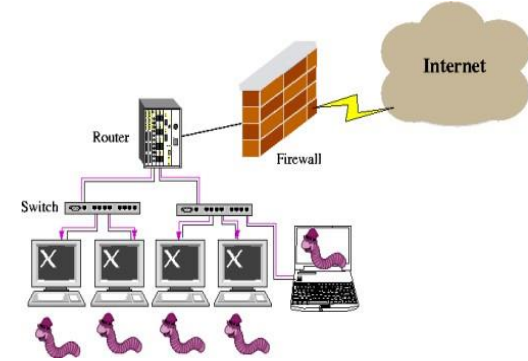   - Carries code to make copies of itself

- **Worms**
  - Replicating but not infecting program Typically spreads over a network Using users distributed privileges or by exploiting system vulnerabilities Widely used by hackers to create zombie pc's, subsequently used for further attacks, especially dos
  - Major issue is lack of security of permanently connected systems

- **Zombie**
  - Program which secretly takes over another networked computer then uses it to indirectly launch attacks
  - Often used to launch distributed denial of service (DDoS) attacks

- **Ransomware**
  - Malware that locks a computer or device or encrypts data (Crypto ransomware) on an infected endpoint with an encryption key ,only the attacker knows the key the data unusable until the victim pays a ransom (usually cryptocurrency, such as Bitcoin).

- ## **DoS Attack**
  - Denial of service is about without permission knocking off services, for example through crashing the whole system.
  - This kind of attacks are easy to launch and it is hard to protect a system against them.
  - Consume host resources
    - Memory
    - Processor cycles
  - Consume network resources
    - Bandwidth
      - Dos Attack (Ping of Death)
- ## **DDoS Attack**
- A distributed denial of service attack uses multiple machines to prevent the legitimate use of a service.
  - TCP SYN flood
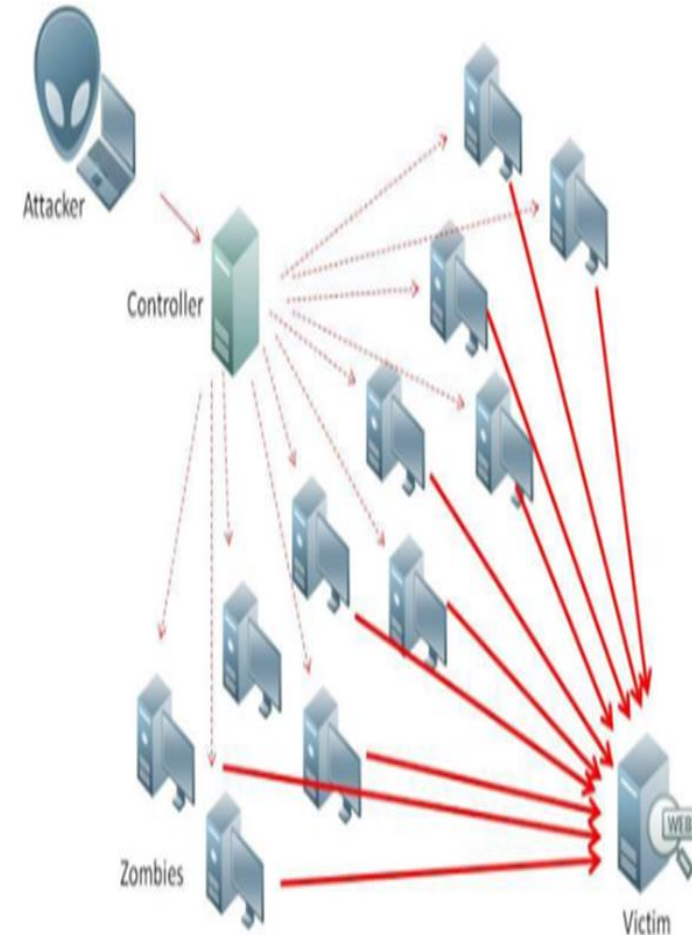
Session 2 (Malicious Software (Malware)types)

- ## Spam
 - Spam is a serious network threat that can overload ISPs, email servers and individual end-user systems. A person or organization responsible for sending spam is called a spammer. Spammers often make use of unsecured email servers to forward email. Spammers can use hacking techniques, such as viruses, worms and Trojan horses to take control of home computers.

- ## Spyware
  - Spyware is any program that gathers personal information from your computer without your permission or knowledge. This information is sent to advertisers or others on the Internet and can include passwords and account numbers.

- ## Tracking Cookies
  - Cookies are a form of spyware but are not always bad. They are used to record information about an Internet user when they visit websites
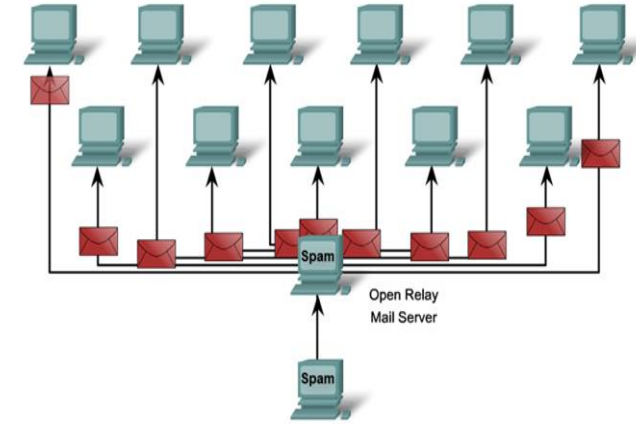
- **Firewall**
- A Firewall is one of the most effective security tools available for protecting internal network users from external threats.
- A firewall resides between two or more networks and controls the traffic between them as well as helps prevent unauthorized access
    - **Static Packet Filtering (stateless firewall)**
        - - Prevents or allows access based on IP or MAC addresses.
    - **Dynamic Packet Filtering (state full firewall)**
        - Incoming packets must be legitimate responses to requests from internal hosts. Unsolicited packets are blocked unless permitted specifically. SPI can also include the capability to recognize and filter out specific types of attacks such as DoS.
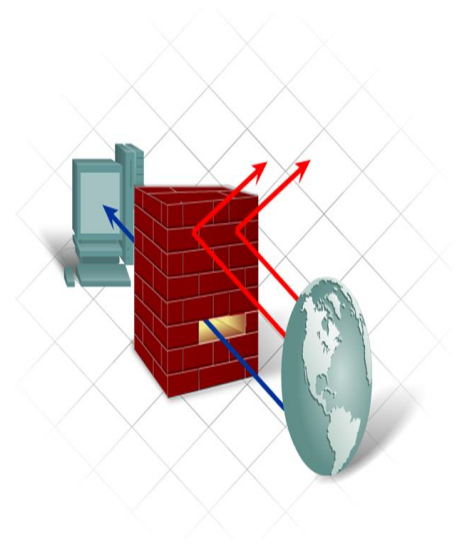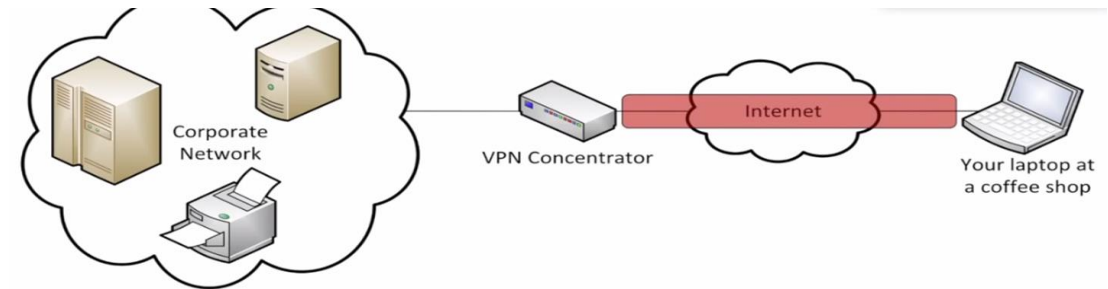
- **Proxy Server**
  - A computer system (or an application program) that intercepts internal user requests and then processes that request on behalf of the user
  - Goal is to hide the IP address of client systems inside the secure network

- **VPN**
  - **It Tunnel the traffic between the Two Sides of Network**
  - **Kinds:**
    - **Remote Access VPN**
    - **Site to Site VPN**

- **Intrusion Detection and Prevention Systems**
  - **NIDS:**
    - Watch the Network Traffic and if there is Intrusion it Detects that there is Bad traffic Flow.
    - it send alarms and logs
  - **NIPS:**
    - Stops the traffic if it detects that there is intrusion
  - **Signature-based:** look for the perfect match
  - **Anomaly-based:** Built a based line of what is normal
  - **Behavior-based:** observe and report
- **Next generation Firewall (NGFW)**
  - is,a "deep-packet inspection firewall that moves beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall."

NIDS and NIPS
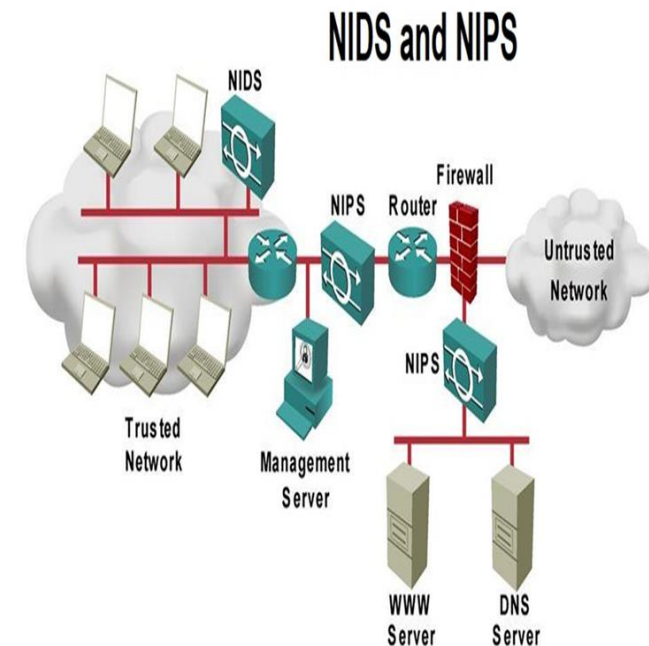
• **Encryption**

- encryption is the process of encoding information. This process converts the original representation of the information, known as **plaintext**, into an alternative form known as **ciphertext.**

- Unencrypted data, called plaintext, is sent through an encryption algorithm to generate a ciphertext. A key is used for encryption.

- in a symmetric encryption algorithm, the **same** key is also used for decryption. (Not secure) needs to be a secure way for the two sides to have the same key .like (At Rest Data (Bitlocker)

Symmetric Key Encryption

Asymmetric Key Encryption
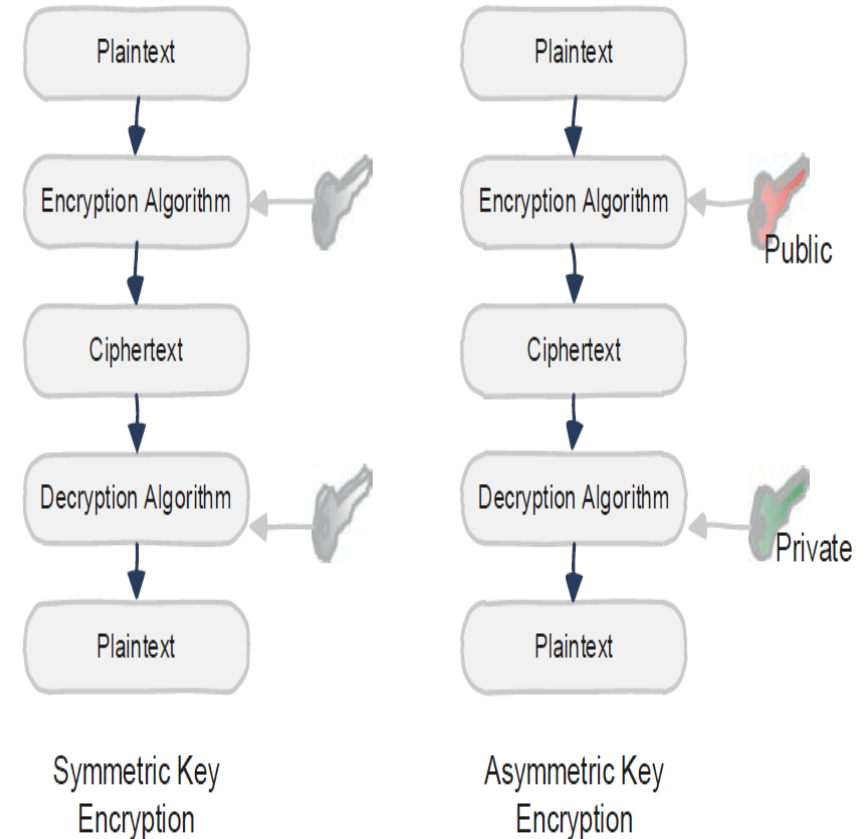
Session 2 (Digital Signatures & Certificates)

- **Digital Signatures**
  - A digital signature is done by hashing a document and then encrypting the hash with a private key.
  - Any entity (like a bank) that has the public key can verify that the document is signed by the owner of the private key.
  - digital signatures do not provide confidentiality but only provide nonrepudiation and integrity.

- **Digital Certificates** (public-key certificate)
  - electronic file that contains identification information about the holder, including the person's public key (used for encrypting and decrypting messages), along with the authority's digital signature,
  - the recipient can verify with the authority that the certificate is authentic.
  - Digital certificates are issued by certification authorities.
  - Websites usually also have digital certificates, to enable a person intending to buy its products to confirm that it is an authenticated site. Such certificates serve as the security basis for HTTPS

Session2 Practices

- How to use your local firewall to block a port and stop DOS attack from a zombie device

Session 3 (Distributed System)

- **Session Outlines**

  - Virtualization
    - Virtualization Benefits

  - Cloud computing
    - Cloud computing service models

Session 3 (Virtualization)

- **Virtualization**
  - Is a technology that run multiple same or different operating systems which is completely isolated from each other
  - Example: run both windows and Linux on the same machine

  - Virtualization is different from Dual Boot ?
  - Dual Boot run only one OS at the same time Virtualization run multiple OS at the same time
- **Virtualization Benefits**
  - Consolidation
  - Redundancy
  - Legacy hardware
  - Migration
  - Centralized management

- **Cloud computing**
  - A pool of resources that can be rapidly provisioned in an automated, on-demand manner.

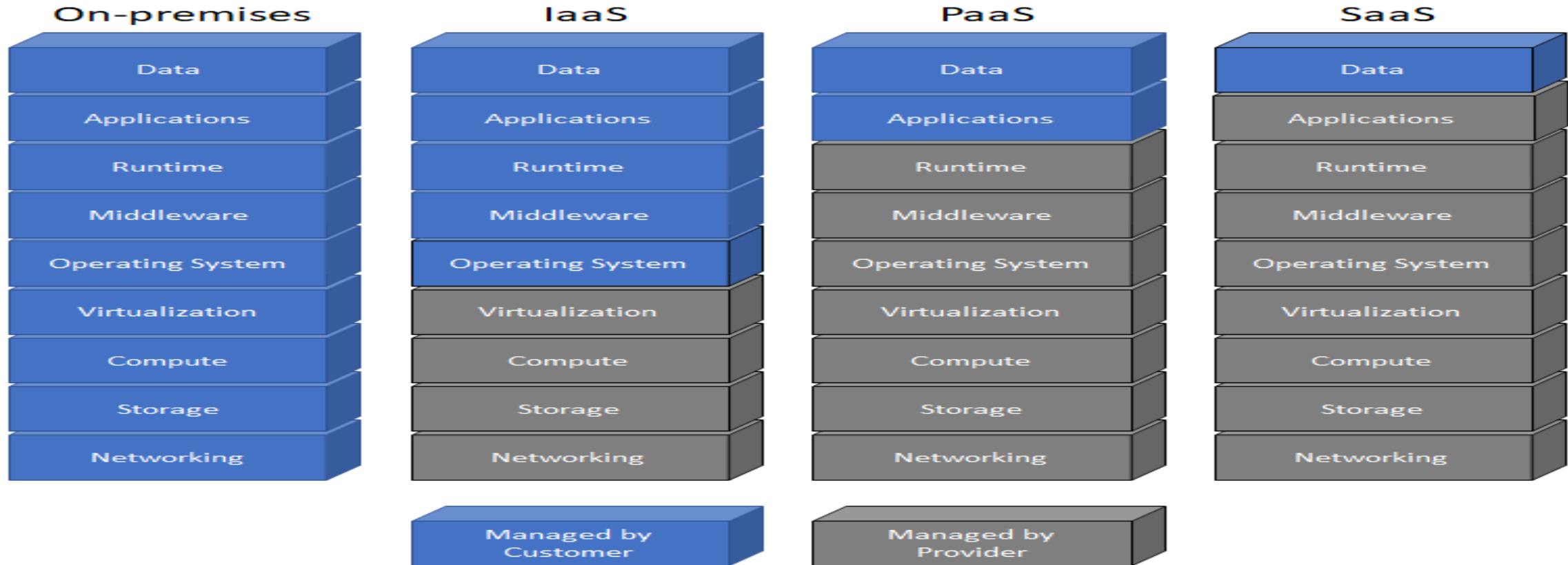- **Value of cloud computing is :**
  - Economies of scale
  - Elastic enough to scale with the needs of your organization.
  - Cost and operational benefits
  - Easily accessed by users no matter where they reside

- **Cloud computing service models**

Session 3 (Cloud computing service models)

- **Software as a service (SaaS).**
  - Customers are provided access to **an application** running on a cloud infrastructure.
  - but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure.

- **Platform as a service (PaaS).**
  - Customers can **deploy supported applications** onto the provider's cloud infrastructure,
  - but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure.
  - The company owns the deployed applications and data, and it is therefore responsible for the security of those applications and data.

- **Infrastructure as a service (IaaS).**
  - Customers can provision **processing, storage, networks, and other computing resources**, and **deploy and run operating systems and applications.**
  - the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer has control over operating systems, storage, and deployed applications, along with some networking components (for example, host firewalls).
  - The company owns the deployed applications and data, and it is therefore responsible for the security of those applications and data.

Session 3 (Cloud computing deployment model)

- **Public.**
  - A cloud infrastructure that is open to use by the general public. It's owned, managed, and operated by a third party (or parties), and it exists on the cloud provider's premises.

- **Community**.
  - A cloud infrastructure that is used exclusively by a specific group of organizations.

- **Private**.
  - A cloud infrastructure that is used exclusively by a single organization. It may be owned, managed, and operated by the organization or a third party (or a combination of both), and it may exist on premises or off premises.

- **Hybrid.**
  - A cloud infrastructure that comprises two or more of the aforementioned deployment models, bound by standardized or proprietary technology that enables data and application portability (for example, fail over to a secondary data center for disaster recovery or content delivery networks across multiple clouds).

Session 3 Practices

- Use the VMware Workstation tool to host the two different OS on your machine

Thank You