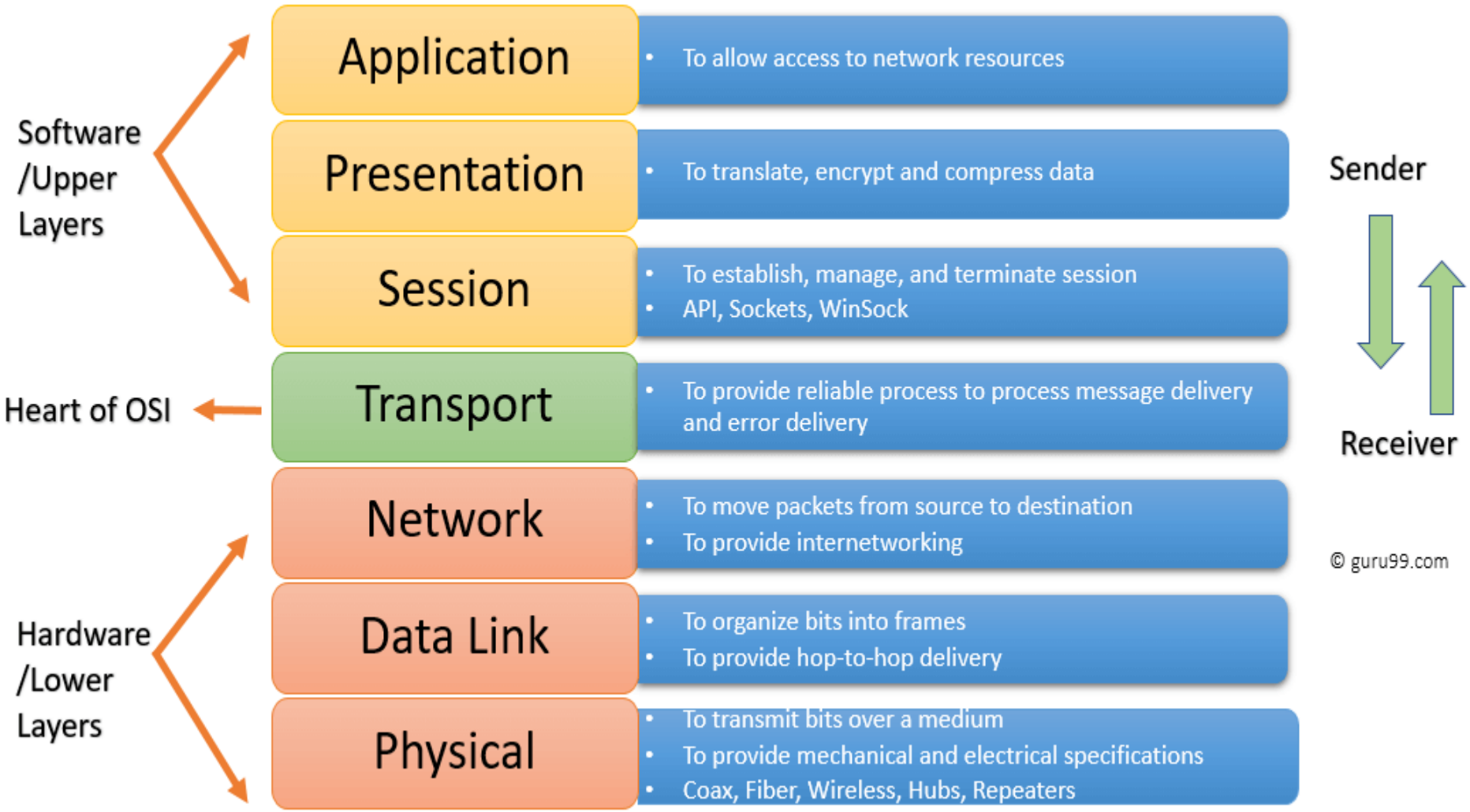
Unit-4 Telecommunications , Network and Internet Security and hours Application Development Security

The OSI Reference Model



- **Application Layer (Layer 7)**
- The Application Layer, the highest layer in the stack, is the one most directly related to the computer user. It provides several application services, such as file transfer, resource allocation, and the identification and verification of computer availability.
- **Presentation Layer (Layer 6)**
- As its name indicates, this layer translates or “presents” data to the Application Layer. Data encryption and decryption occur in this layer along with data translation. Whenever you view a photograph in JPEG (a compressed photo storage standard) format on the Internet, watch a video someone has sent you in MPEG format (a compressed movie storage format), or listen to an MP3 file (a compressed audio storage format), you are interacting with OSI Presentation Layer protocol services.
-

- **Session Layer (Layer 5)**
- The protocols at this level establish, maintain, and manage sessions between computers. When you request information about your checking account balance from your bank's web application, the Session Layer makes the initial contact with the host computer, formats the data you are sending for transmission, establishes the necessary communication links, and handles recovery and restart functions.
- **Transport Layer (Layer 4)**
- Protocols at this level provide the point-to-point integrity of data transmissions. They determine how to address the other computer, establish communication links, handle the networking of messages, and generally control the session. The Transmission Control Protocol (TCP) operates at this level. TCP allows two computers to connect with each other and exchange streams of data while guaranteeing delivery of the data and maintaining it in the same order.

- **Network Layer (Layer 3)**
- The Network Layer decides how small bundles, or packets, of data route between destination systems on the same network or interconnected networks. A packet (sometimes called a protocol data unit, or PDU) is a bundle of data organized for transmission that contains control information (destination, length, origin, and so forth), the data itself (payload), and error detection and correction bits.
- **Data Link Layer (Layer 2)**
- The Data Link Layer transfers units of information to the other end of the physical link. Protocols at this level establish communication links between devices over a physical link or channel, converting data into bit streams for delivery to the lowest layer, the Physical Layer

- **Physical Layer (Layer 1)**
- Finally, protocols at the Physical Layer transmit bit streams on a physical medium. They manage the interfaces of physical devices with physical transmission media, such as coax cable. This layer has the fewest tasks to perform. It sends bit streams across the network to another device and receives a bit stream response in return.

The OSI model and TCP/IP

- The primary protocols in TCP/IP are bundled in each layer and briefly described next:
- Transport Layer (host-to-host) protocols
- **Transmission Control Protocol:** TCP is a reliable service that maintains the proper sequence of incoming packets and acknowledges receipt to the user.
- • **User Datagram Protocol (UDP):** UDP is a less robust version of TCP. It does not acknowledge receipt of packets and is a connectionless and less reliable service. Its advantage over TCP is its faster speed and lower overhead.

- Network (Internet) Layer protocols:
- • **Internet Protocol:** The protocol of protocols, IP addresses are assigned by the Internet Assigned Numbers Authority to each host computer on the network.
- • **Address Resolution Protocol (ARP):** ARP matches an IP address to an Ethernet address.
- Thus, ARP and RARP (covered next) exist to help with network addressing tasks.
- • **Reverse Address Resolution Protocol (RARP):** If ARP translates an IP address to a MAC address, then RARP translates hardware interface (MAC) addresses to IP protocol addresses.
- • **Internet Control Message Protocol (ICMP):** The ICMP is tightly integrated with the IP protocol

- The following are the primary applications using TCP/IP:
- FTP
- TELNET
- SMTP

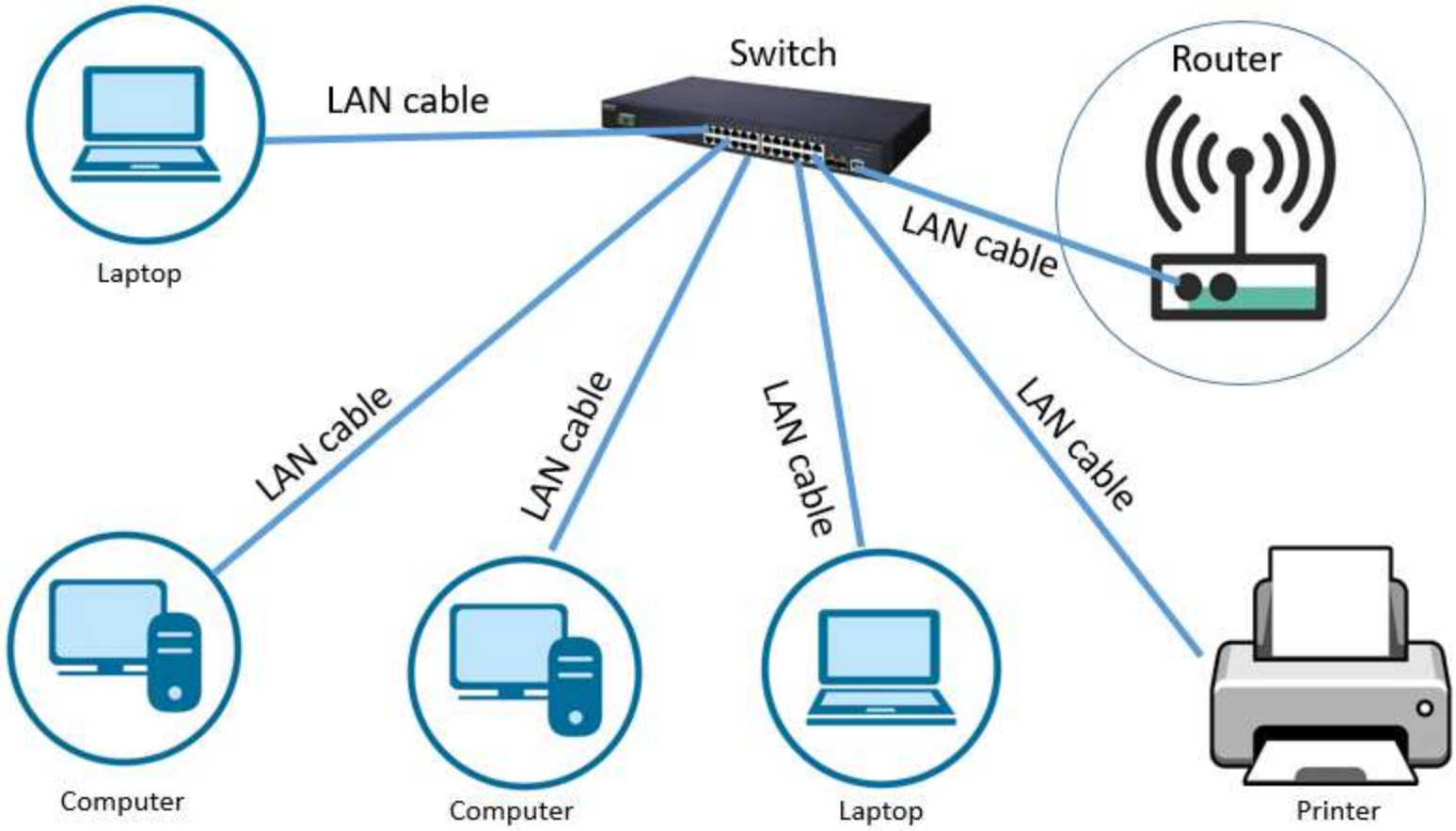
The OSI Model and Security

- **Authentication:** Access to documents can be restricted in one of two ways: by asking for a username and password or by using the hostname of the browser.
- **Access control:** Unlike authentication, which is security based on the user's identity, restricting access based on something other than identity is called access control.
- **Data confidentiality:** This service protects data against unauthorized disclosure and has two components: content confidentiality and message flow confidentiality.
- **Data integrity:** The goal is to protect data from accidental or malicious modification, whether during data transfer.
- **Nonrepudiation:** This service guarantees that the sender of a message cannot deny having sent the message and the receiver cannot deny having received the message.
- **Logging and monitoring:** These services allow IS specialists to observe system activity during and after the fact.

DATA NETWORK TYPES

- • Local area networks (LANs)
- • Wide area networks (WANs)
- • Internet, intranet, and extranets

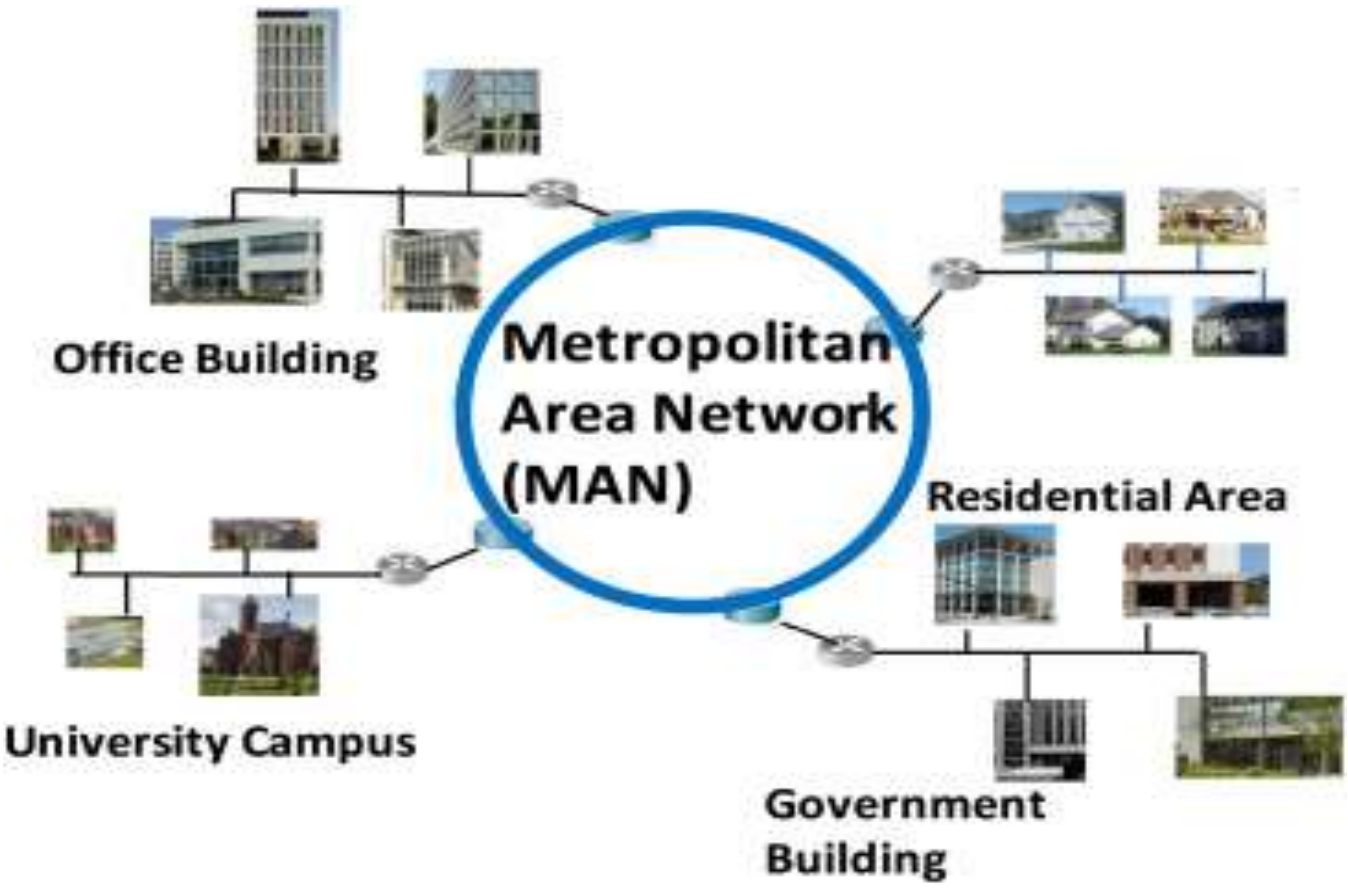
Local Area Networks



Local Area Network

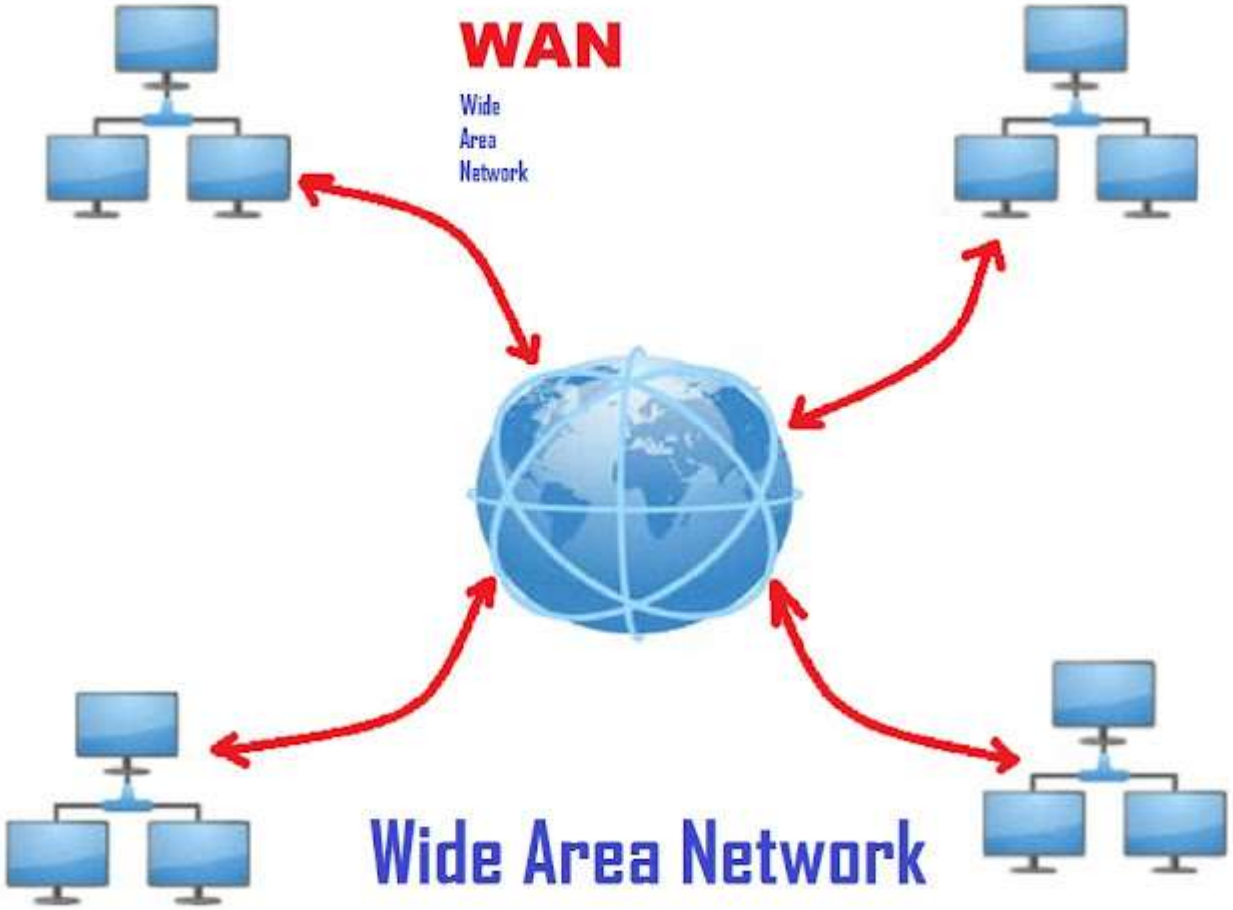
- A local area network, or LAN, is a network configuration designed for a limited space or geographic area, such as a series of offices in the same building (for example, a university administration building).
- LANs share network services such as databases, email, and application services by connecting workstations and servers through a set of LAN protocols and access methods.

Metropolitan Area Networks



- A Metropolitan Area Network (MAN) is a large computer network on the large geographical area that include several buildings or even the entire city (metropolis). The geographical area of the MAN is larger than LAN, but smaller than WAN. MAN includes many communicating devices and provides the Internet connectivity for the LANs in the metropolitan area.
- MAN is used to combine into a network group located in different buildings into a single network. The diameter of such a network can range from 5 to 50 kilometers.

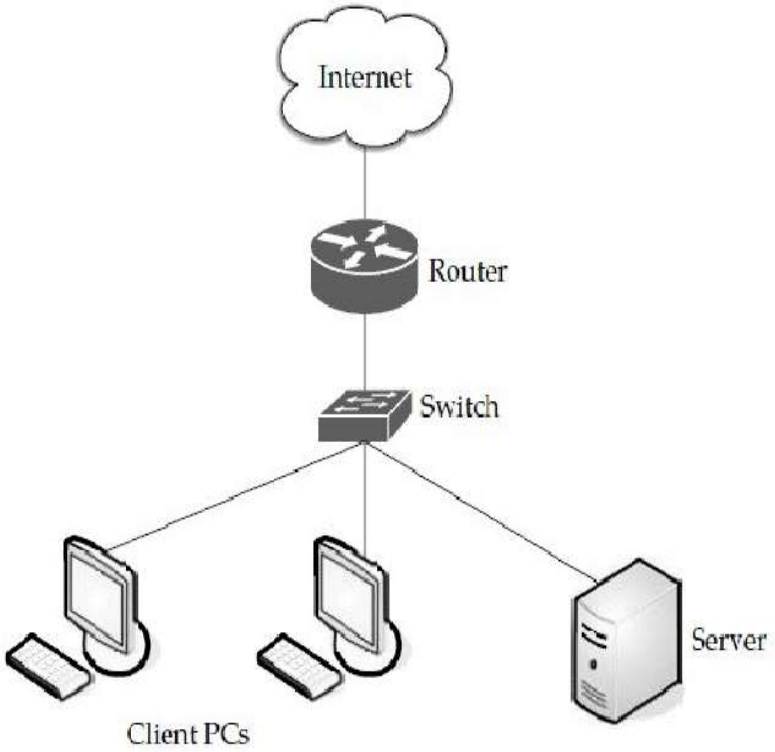
Wide Area Networks



- A group of smaller LANs connected logically or physically is referred to as a wide area network, or WAN.
- As you might suspect, the WAN covers a larger geographic area than a LAN (technically, a network that covers an area larger than a single building).
- A WAN can span an entire nation or even the globe using satellites.

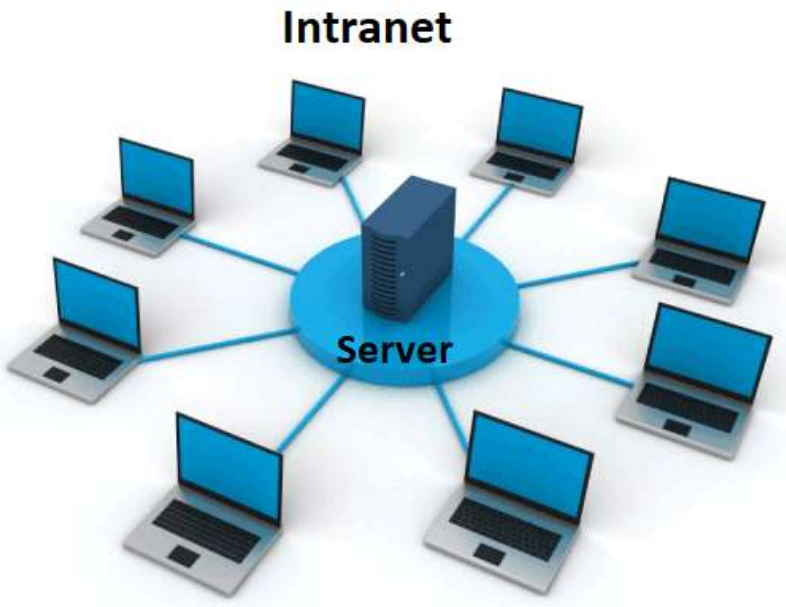
Internet

- Sometimes referred to as a network of networks, the Internet is an interconnection of different-sized networks (LANs) around the world. the Internet uses the TCP/IP protocols (covered shortly) in a scheme decentralized by design.
- Each host computer on the Internet is independent; its operators can choose the Internet services and local services they want to offer.



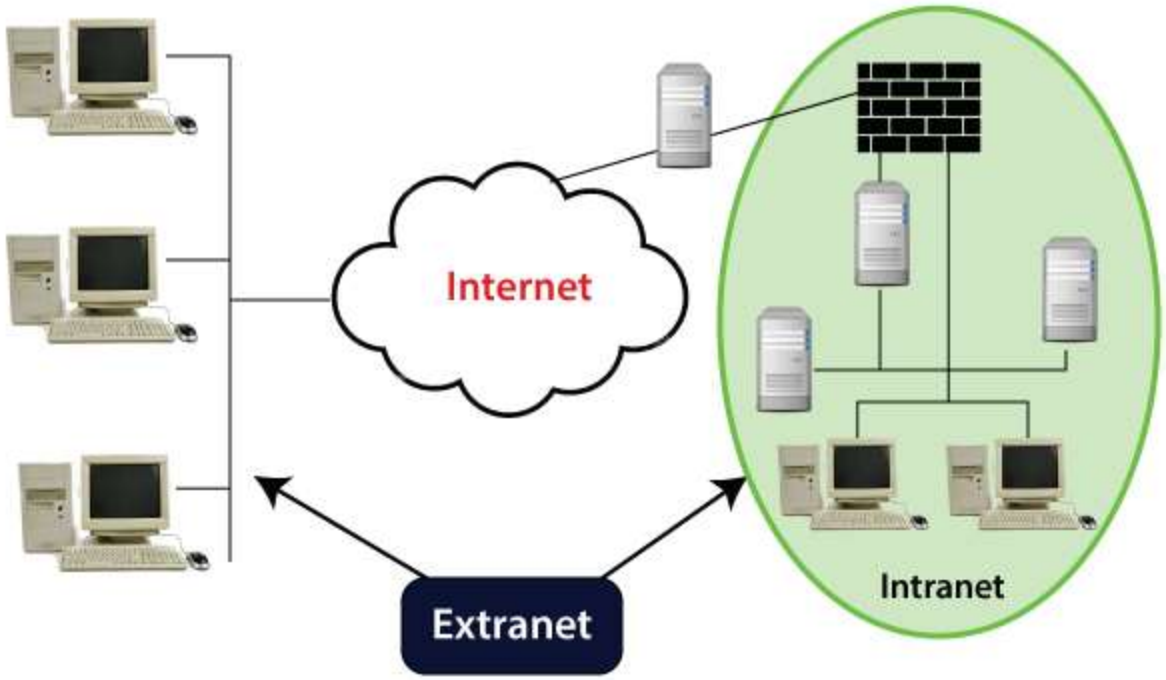
Intranet

- An intranet is a local or wide area network based on TCP/IP, but with fences (firewalls) that limit the network's access to the Internet. Intranets use the standard software and protocols you find on the Internet, but they are for private use and are not accessible to the public via the Internet. Companies can use low-cost Internet software such as browsers to build internal sites, such as human resources and internal job postings.
- An intranet is more secure than the Internet because it has a restricted user community and local control.

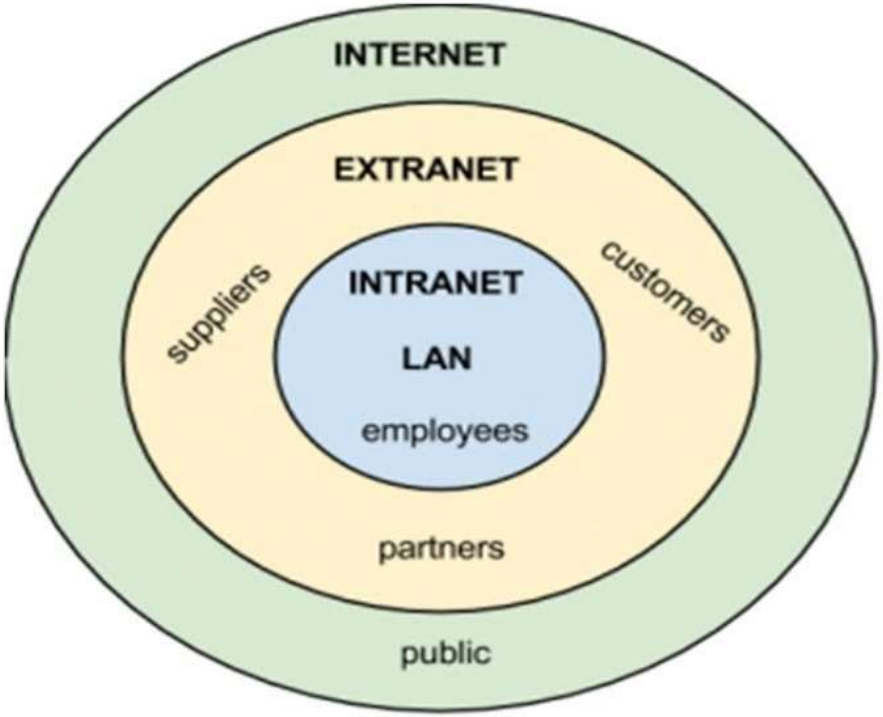


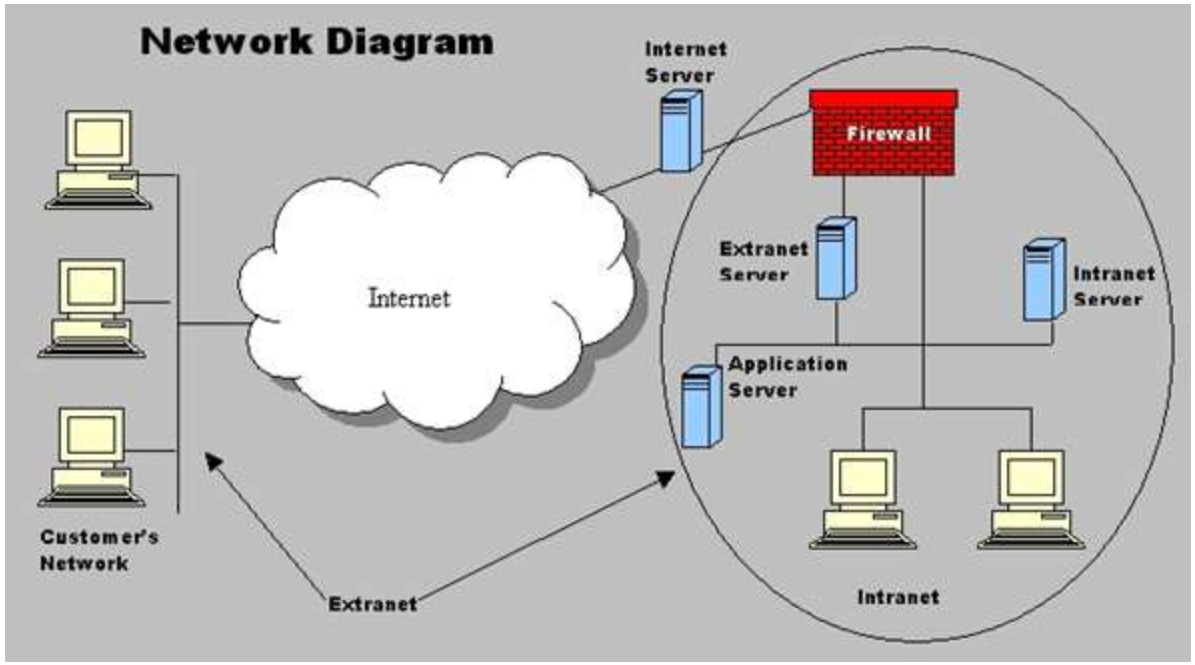
Extranet

- An extranet is an intranet that allows select users outside the firewalls to access the site. For example, a company might give vendors and suppliers limited access to the intranet while excluding the general public.



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	Information can be shared across the	Information can be shared securely within	Information can be shared between


INTERNET
EXTRANET
INTRANET
LAN
employees
suppliers
customers
partners
public

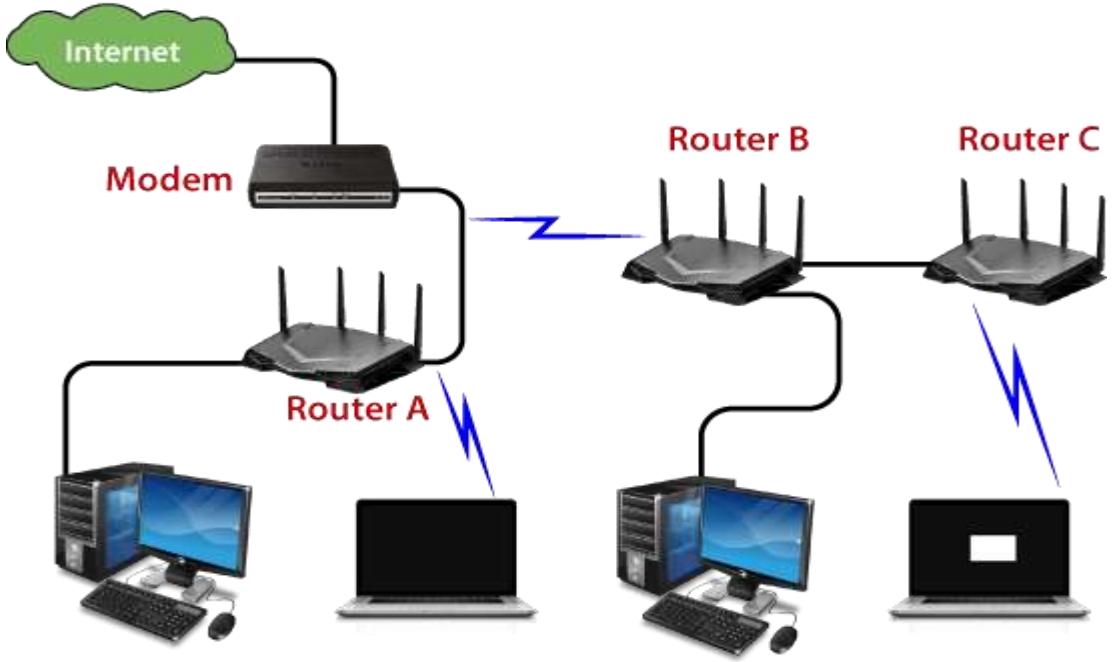

Network Diagram
Internet Server
Firewall
Extranet Server
Intranet Server
Application Server
Internet
Customer's Network
Extranet
Intranet

Protecting TCP/IP Networks

- Protecting computer networks is a challenging job and is best approached by applying the principle of defense in depth. These include the use of these components:
- • Routers
- • Firewalls
- • Intrusion detection systems (IDSs)
- • Intrusion prevention systems (IPSs)

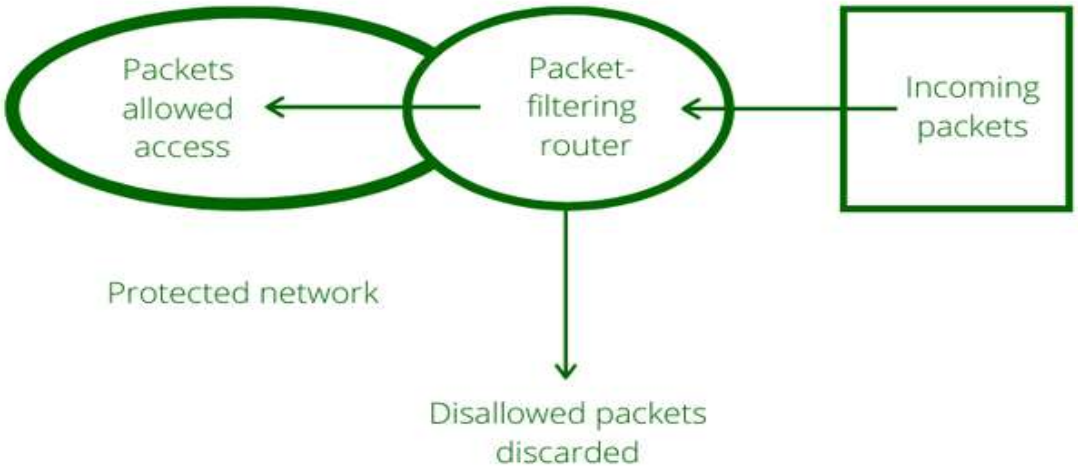
1. Routers

- A router is a network traffic management device that operates in between sub-networks (LANs) and routes traffic intended for or leaving the network segments to which it's attached.
- Network Address Translation (NAT) is often used on perimeter routers.
- Its purpose is to the hide the internal device IP addresses from Internet users, to help secure the network.



- **Packet Filtering**
- A packet filter is a simple and effective form of protection.
- It matches all packets against a series of rules.
- If the packet matches a rule, an action is performed; the packet is accepted, rejected, logged, and so forth.
- Because malicious network activity can harm network users, and because all network communications are packet based, packets can be inspected as they traverse the network; those that contain commands that are disallowed can be filtered out of the network and discarded before they cause harm or unauthorized activity.

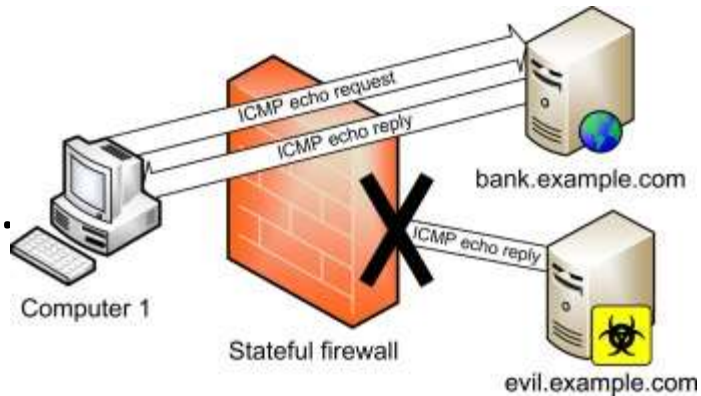
- ***Basic Packet Filtering***
- Basic or straight packet-filtering mechanisms allow communication originating from one side of the communication path.
- To enable two-way traffic, you must specify a rule for each direction.
- Packet-filtering firewalls identify and control traffic by examining the source, destination, port number, and protocol types (for example, UDP or TCP).



- ***Stateful Inspection Packet Filtering***
- Stateful inspection filtering is a more complex packet-filtering technology that filters traffic based on more than just source, destination, port number, and protocol type.
- Stateful inspection keeps track of the state of the current connection to help ensure that only desired traffic passes through.
- This allows the creation of one-way rules—for example, inside to outside.
- A packet-filtering router yields a permit or deny decision for each packet it receives.
- The router examines each IP

datagram to determine whether it

matches one of its packet-filtering rules.

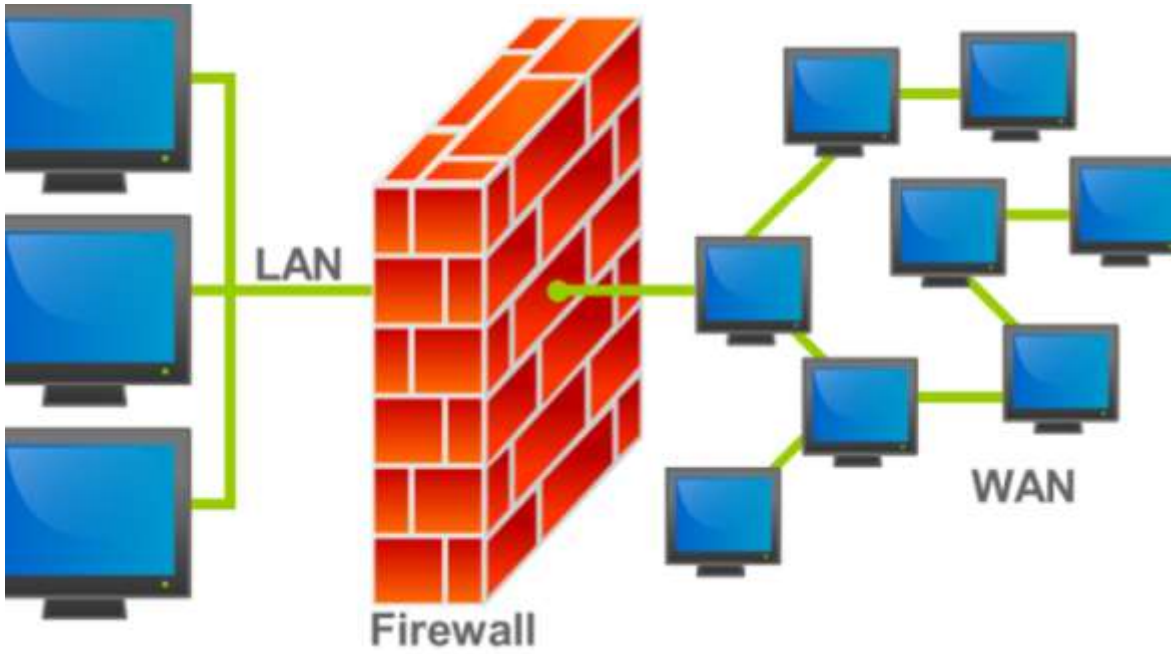


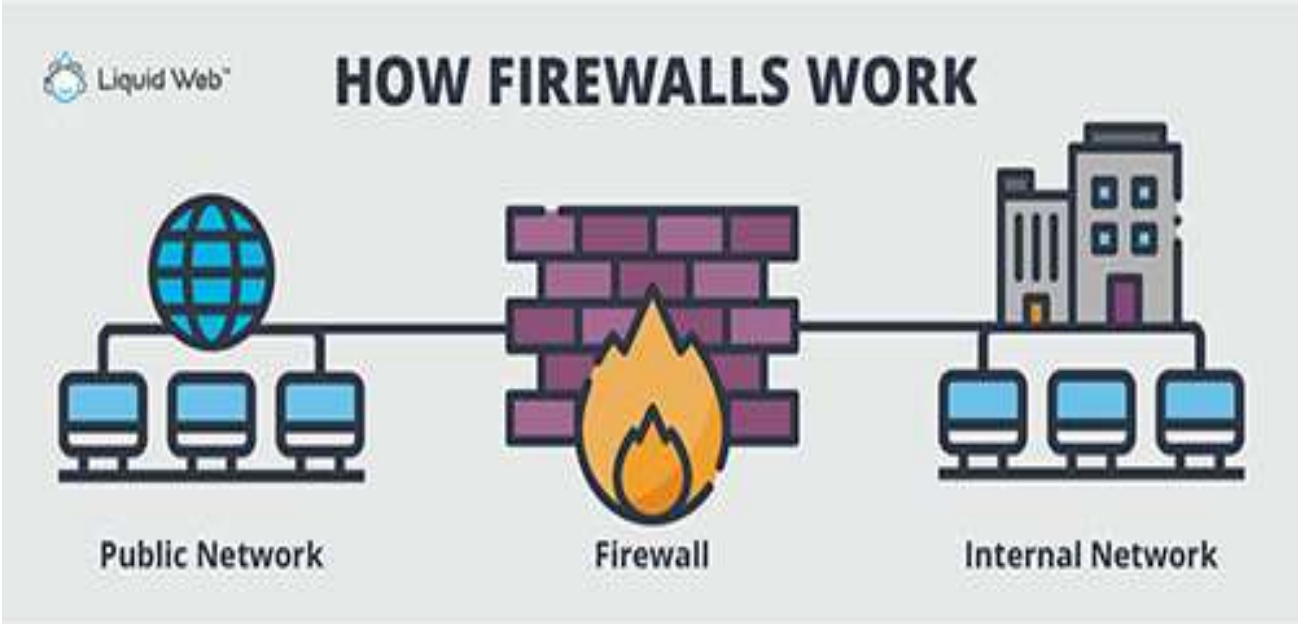
- ***Benefits of Packet-Filtering Routers***
- implementing packet filtering involves little or no cost because the feature is included as part of standard router software releases.
- Because a WAN interface usually provides Internet access, there is little impact on router performance if traffic loads are moderate and few filters are defined.
- Packet-filtering routers are generally transparent to users and applications, eliminating the need for specialized user training or specific software on each connected host system.

- ***Limitations of Packet-Filtering Routers***
- Defining packet filters can be a complex task because network administrators need to have a detailed understanding of the various Internet services, packet header formats (packets typically have header and trailer records marking the beginning and end of the data packet), and specific values they expect to find in each field
- Any packet that passes directly through a router could potentially be used to launch a data-driven attack. Data-driven attacks occur when the router forwards seemingly harmless data to an internal host.
- Generally, the packet throughput of a router decreases as the number of filters increase.
- IP packet filters might not be capable of providing enough control over traffic. A packet-filtering router can permit or deny a particular service, but it cannot understand the context/data of a particular service.

Firewalls

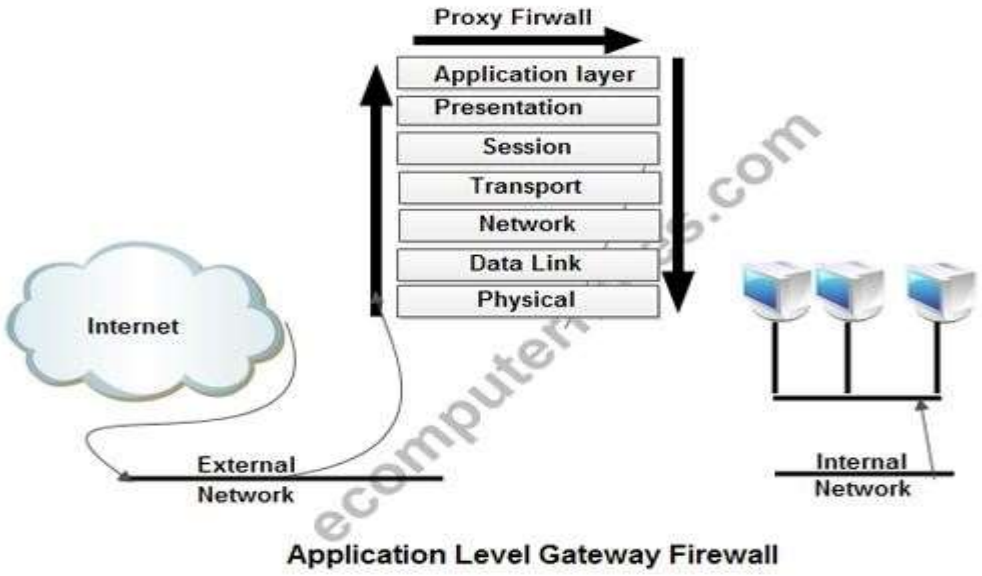
- Firewalls insulate a private network from a public network using carefully established controls on the type of requests they'll route to the private network for processing and fulfillment.
- Firewalls typically run monitoring software to detect external attacks on the site and protect the internal corporate network. When you install a firewall, you essentially break the network so that no communications can occur until the rules for permissible communications are established and implemented.
- Firewalls are an essential device for network security, and many of the architectures needed for security rely on one or more firewalls within an intelligent design.
- The following sections describe two of the most common firewall building block architectures: application-level gateways and bastion hosts.


LAN
WAN
Firewall


Liquid Web™
HOW FIREWALLS WORK
Public Network
Firewall
Internal Network

- **Application-Level Gateway Firewall**
- An application-level gateway enables the network administrator to implement stricter security policies than packet-filtering routers can manage.
- Instead of relying on a generic packet-filtering tool to manage the flow of Internet services through the firewall, special-purpose code (a proxy service) is installed on the gateway for each desired application.
- If the network administrator does not install the proxy code for a particular application, the service is not supported and cannot be forwarded across the firewall.
- In addition, the proxy code can be configured to support only the specific features of an application that

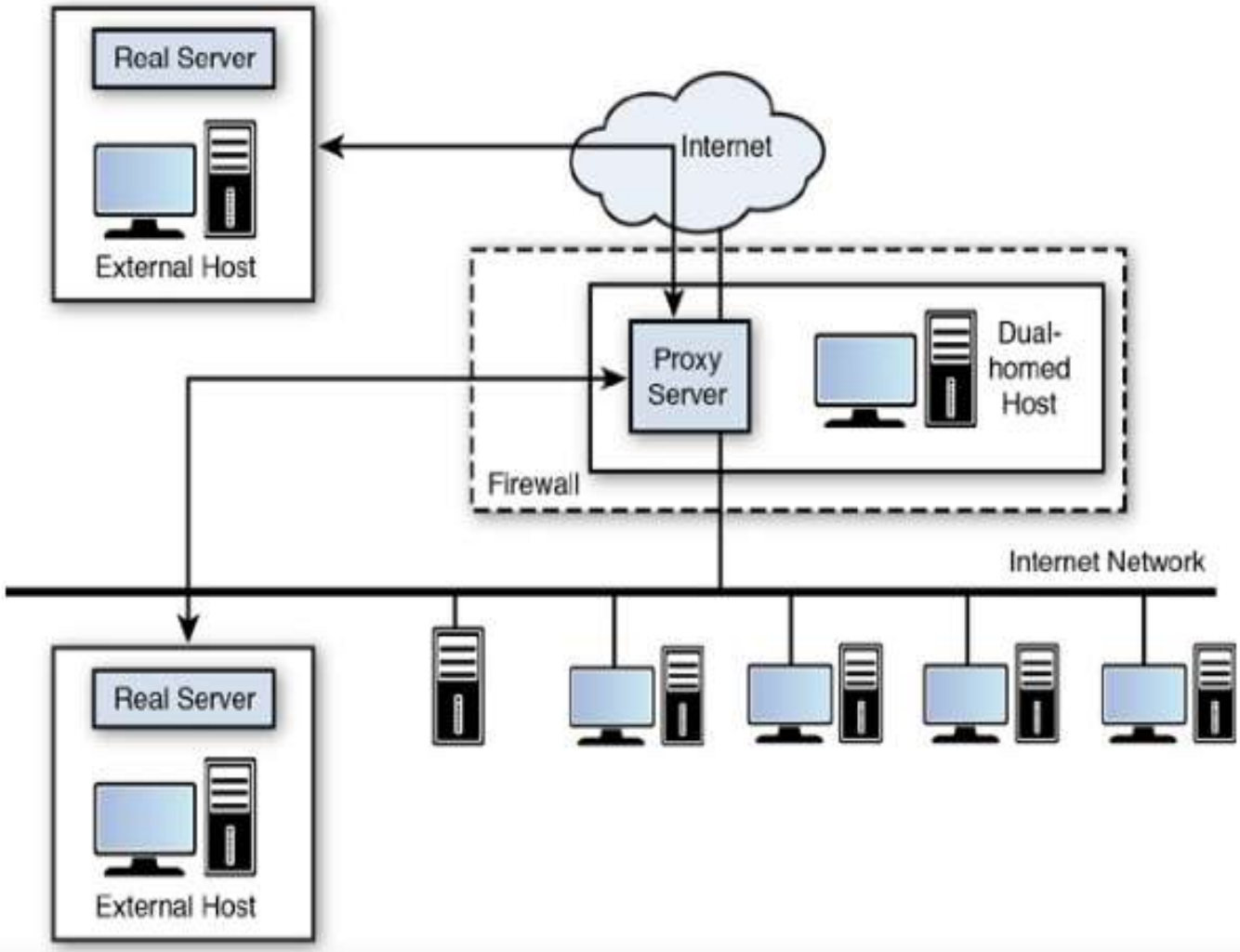
The network administrator considers acceptable, while denying all other features.



Application Level Gateway Firewall

- This enhanced security comes with increased costs in these areas:
  - Purchase of the dedicated gateway hardware
  - Configuration of the proxy service applications
  - Time, knowledge, and skills required to configure the gateway system
  - Degradation in the level of service provided to users because of the overhead of firewall operation
  - Lack of transparency for remote users, resulting in a less user-friendly system

Figure 12.4. Application-level gateway firewall configuration.



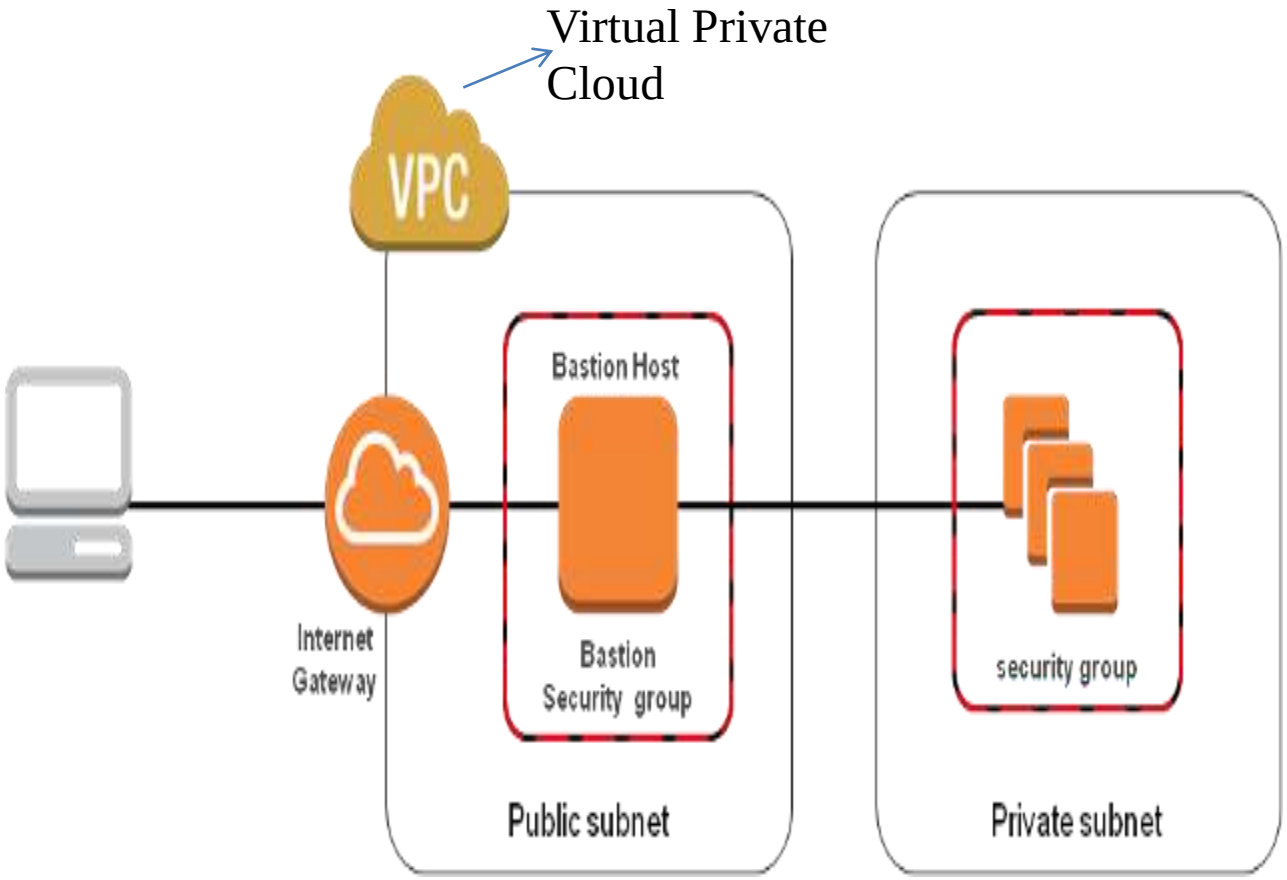
The following are characteristics of the proxy server:

- • Each proxy is configured to support only a subset of the standard application’s command set. If the proxy application does not support a standard command, it is simply not available to the authenticated user.
- • Each proxy is configured to allow access only to specific host systems. This means that the limited command/feature set can be applied only to a subset of systems on the protected network.
- • Each proxy maintains detailed audit information by logging all traffic, each connection, and the duration of each connection. Audit logs are essential tools for discovering and terminating intruder attacks. Each proxy is a small and uncomplicated program specifically designed for network security.
- • Each proxy is independent of all other proxies on the bastion host. If a problem occurs with the operation of any proxy or if a future vulnerability is discovered, it can be uninstalled without affecting the operation of the other proxy applications.
- • Each proxy runs as a non-privileged user in a private and secured directory on the bastion host.

Bastion Hosts

- An application-level gateway is often referred to as a bastion host because it is a designated system that is specifically armored and protected against attacks.
- application-level gateways allow information to flow between systems but do not allow the direct exchange of data.
- The primary risk of allowing packet exchange between inside systems and outside systems is that the host applications residing on the protected network's systems must be secured against any threat posed by the allowed services.
- The bastion host hardware platform operates a secure (hardened) version of its operating system.
- Network administrators install only services they consider essential on the bastion host.
- The bastion host might be configured to require additional authentication before a user is allowed access to the proxy services.

A bastion host is a server whose purpose is to provide access to a private network from an external/public network, such as the Internet.
This diagram shows connectivity flowing from an end user to resources on a private subnet through a bastion host:



- **Following the characteristics of a bastion host :**
  - The bastion host hardware platform executes a secure version of its operating system, making it a trusted system.
  - The network administrator installed services on the bastion host. These includes proxy application such as TELNET, DNS, FTP, SMTP.
  - The bastion host may requires authentication before a user is allowed access to the proxy services.
  - Each proxy maintains detailed audit information by monitoring all traffic, each connection, and the duration of each connection. The audit record is an essential tool for discovering and terminating intruder attacks.
  - Each proxy is independent of other proxies on the bastion host. If there is a problem with the operation of any proxy, or if a future vulnerability is discovered, it can be uninstalled without affecting the operation of the other proxy applications.
  - The portions of the file system containing executable code can be made read only (i.e. configuration file).

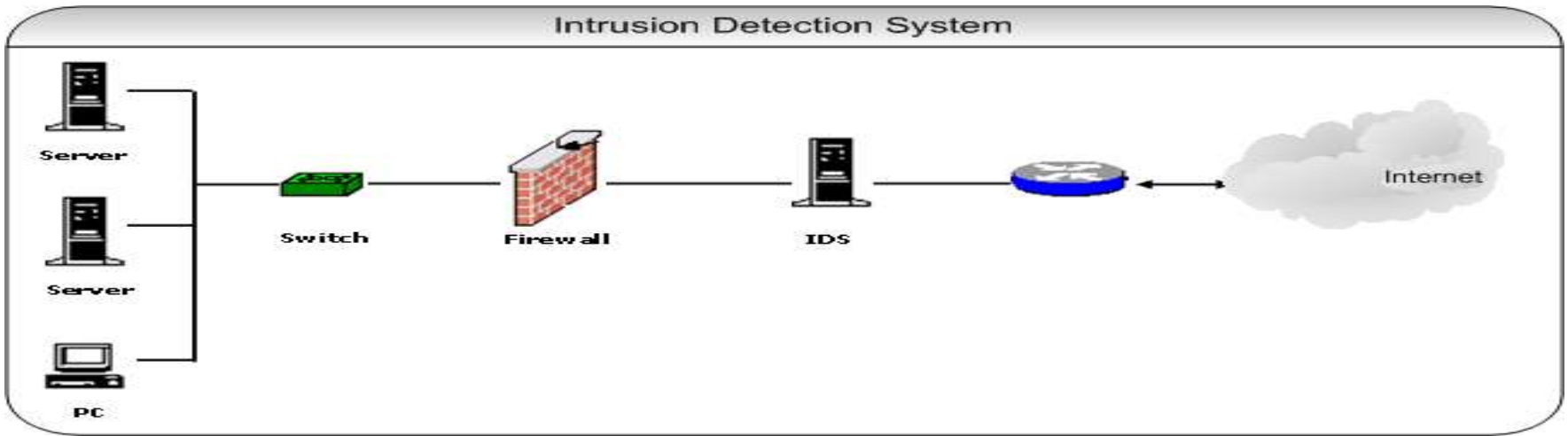
Benefits of Application-Level Gateways

- They give the network manager complete control over each service because the proxy application limits the command set and determines which internal hosts the service can access.
- the network manager has complete control over permitted services because the absence of a proxy for a particular service means that the service is completely blocked.
- Application-level gateways also have the capability to support strong user authentication and provide detailed logging information.
- the filtering rules for an application-level gateway are much easier to configure and test than for a packet-filtering router.

Intrusion Detection Systems

- An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered.

- It is a software application that scans a network or a system for harmful activity or policy breaching.
- The software applications are **Snort, SolarWinds, CrowdStrike Falcon, Suricata, Zeek, Security Onion etc.**



- One of the two most publicized risks to security is :
  1) Intruder / Opponent / Attacker / Hacker / Cracker
  2) Viruses
- **There are two classes of intruders :**
  - Outside Intruders
  - Inside Intruders

  - **Masquerader (Outsider Intruders) :** An individual who is unauthorized to use the computer and who penetrates (enters) in a system's access controls to use a legitimate user's account. **The masquerader is likely to be an outsider**.
  - **Misfeasor (Insider Intruders):** A legitimate user who accesses data or resources for which such access is not authorized, or they may be authorized for access but misuses his or her privileges. **The misfeasor generally is an insider**. Authorized / legitimate user performing in an unauthorized fashion.

What Kind of Intrusions?

- An intrusion is defined as any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource. Intrusions can be categorized into two main classes:
  - **Misuse intrusions** are well-defined attacks on known weak points within a system. (i.e. Based on patterns)

    As misuse intrusions follow well-defined patterns, they can be detected by doing pattern matching on audit information.

  - **Anomaly intrusions** are based on observations of deviations from normal system usage patterns. (i.e. Based on statistical / derivatives)

    Anomalous intrusions are detected by observing significant deviations from normal behavior.

Characteristics of Good Intrusion Detection Systems

- • It must run continually without human supervision. The system should be reliable enough to run autonomously in the background of the system being observed.
- • It must be fault tolerant. It must survive a system crash without requiring the rebuilding of the IDS's knowledge base each time the system is restarted.
- • It must resist subversion. The system should monitor itself to ensure that it has not been subverted.
- • It must impose minimal overhead on the attached network.
- • It must observe deviations from normal behavior.
- • It must be easily tailored to the network in question. Every system has different usage patterns, and the defense mechanisms should adapt easily to these patterns.
- • It must cope with changing system behavior over time as new applications are being added. The system profile will change over time, and the IDS must be capable of adapting.

False Positives, False Negatives, and Subversion Attacks

- IDS processing errors are categorized as false positives, false negatives, or subversion errors.
- A false positive occurs when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action. A **false positive** state is when the IDS identifies an activity as an attack but the activity is acceptable behavior. A false positive is a false alarm.
- A false negative occurs when an actual intrusive action has occurred, but the system allows it to pass as nonintrusive (legal user) behavior. A **false negative** state is the most serious and dangerous state. This is when the IDS identifies an activity as acceptable when the activity is actually an attack. That is, a false negative is when the IDS fails to catch an attack.
- A subversion error occurs when an intruder modifies the operation of the intrusion detector to force false negatives to occur.
  For eg. :The **error** message "Server sent unexpected return value (405 Method Not Allowed) means that the commit to the Subversion repository failed.
  The Error message : 404 (File Not Found)

- A false negative occurs when an actual intrusive action has occurred, but the system allows it to pass as nonintrusive behavior.
- A false negative error occurs when an action proceeds even though it is an intrusion.
- False negative errors are more serious than false positive errors because they give a misleading sense of security.
- If these actions are allowed to proceed, a suspicious action will not be brought to the attention of the operator.
- The intrusion detection system then is a liability because the security of the system is less than it was before the intrusion detector was installed.

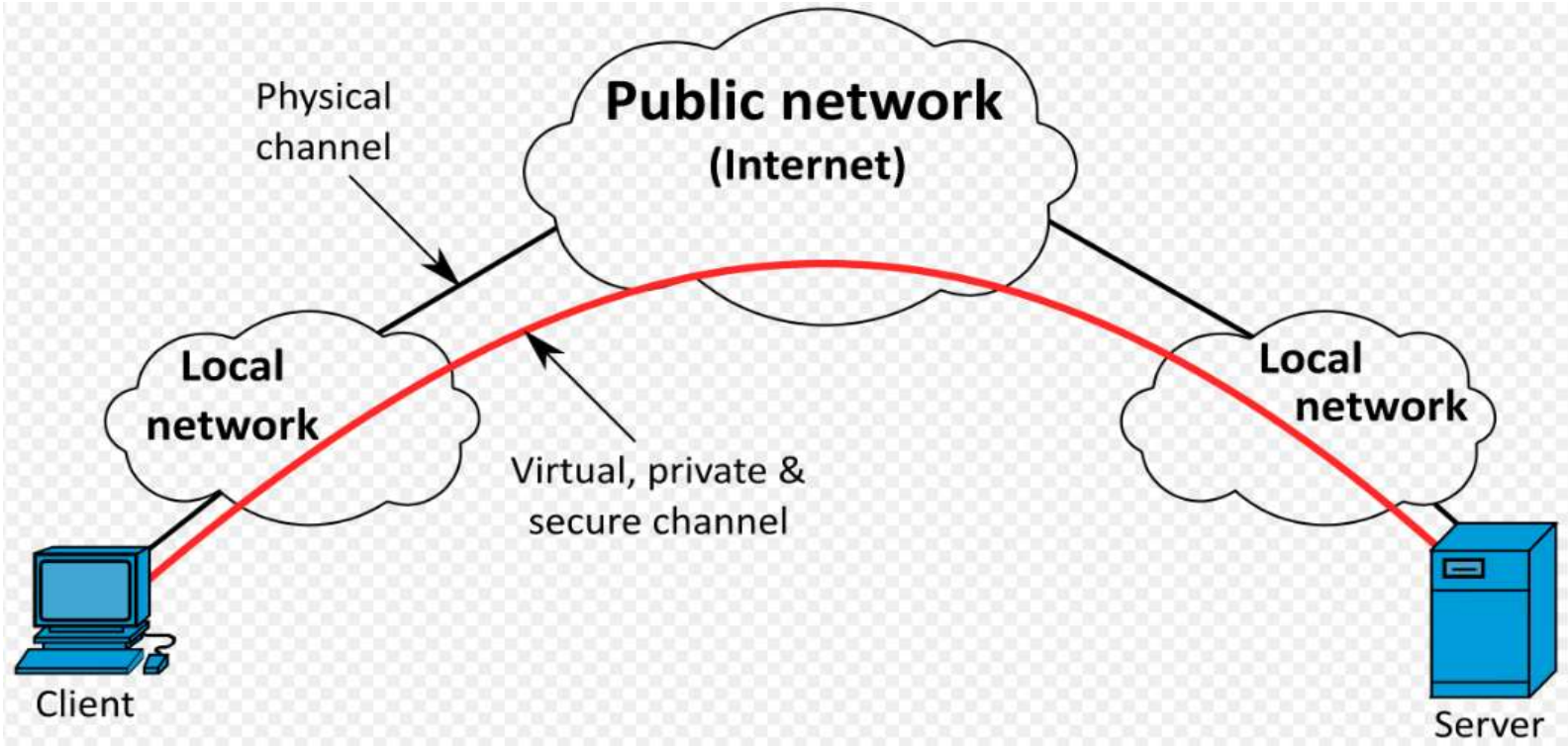
- A subversion error occurs when an intruder modifies the operation of the intrusion detector to force false negatives to occur.
- Subversion errors are more complex and tie in with false negative errors.
- An intruder could use knowledge about the internals of an intrusion detection system to alter its operation, possibly allowing anomalous behavior to proceed.
- The intruder could then violate the system's operational security constraints.

Intrusion Prevention Systems

- the IPS actively analyzes and performs actions on all traffic flows that enter the network, including these:
- • Sending an alarm to the administrator (such as an IDS)
- • Blocking traffic from the source address
- • Resetting the connection
- the IPS must detect and respond accurately, to eliminate threats and false positives (legitimate packets misread as threats).

VIRTUAL PRIVATE NETWORKS

- A virtual private network, or VPN, is a network technology that makes it possible to establish private “tunnels” over the public Internet. (For eg. : Cisco VPN – access remotely)
- A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. It makes use of tunneling protocols to establish a secure connection.
- The three primary uses for VPNs are for employee remote access to corporate networks(i.e. using FTP server), extranet connections with business partners and suppliers and branch office networks (intranet).
- All that is needed for a VPN is a specialized firewall, client, or server software (to initiate and maintain a connection) and an Internet service provider (ISP) connection for Internet connectivity.
- VPNs allow authorized users to pass through the firewalls.
- VPN uses encryption and authentication and to provide a secure connection through the internet.


Physical
channel
Public network
(Internet)
Local
network
Local
network
Virtual, private &
secure channel
Client
Server

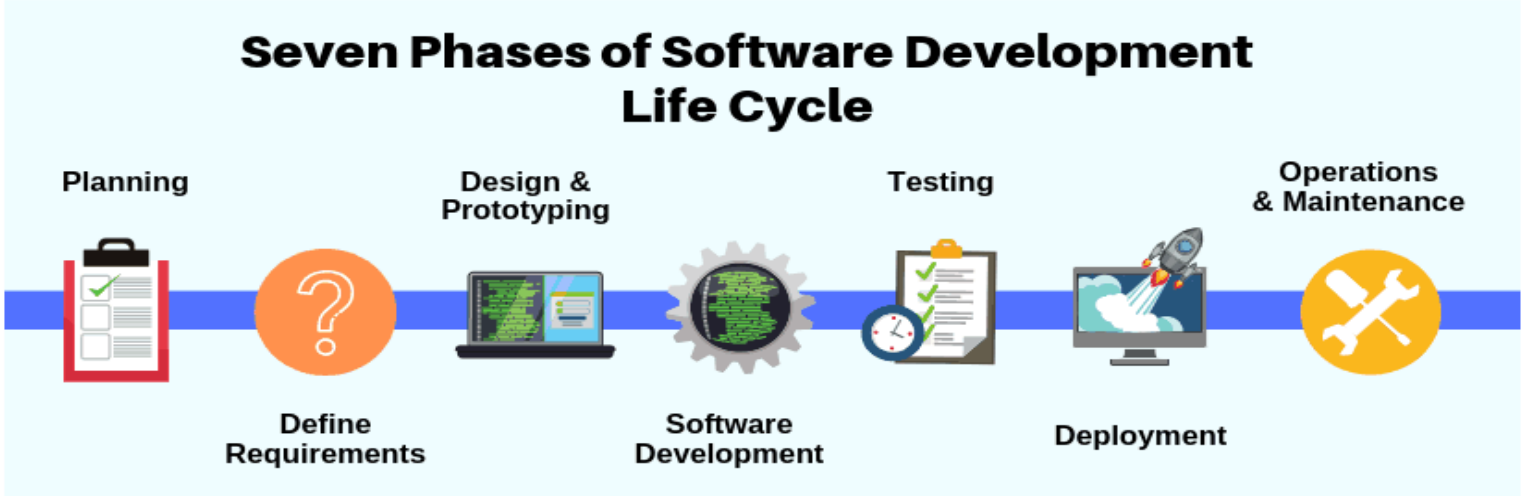
SOFTWARE DEVELOPMENT LIFE CYCLES

WHAT IS A SOFTWARE DEVELOPMENT LIFE CYCLE?

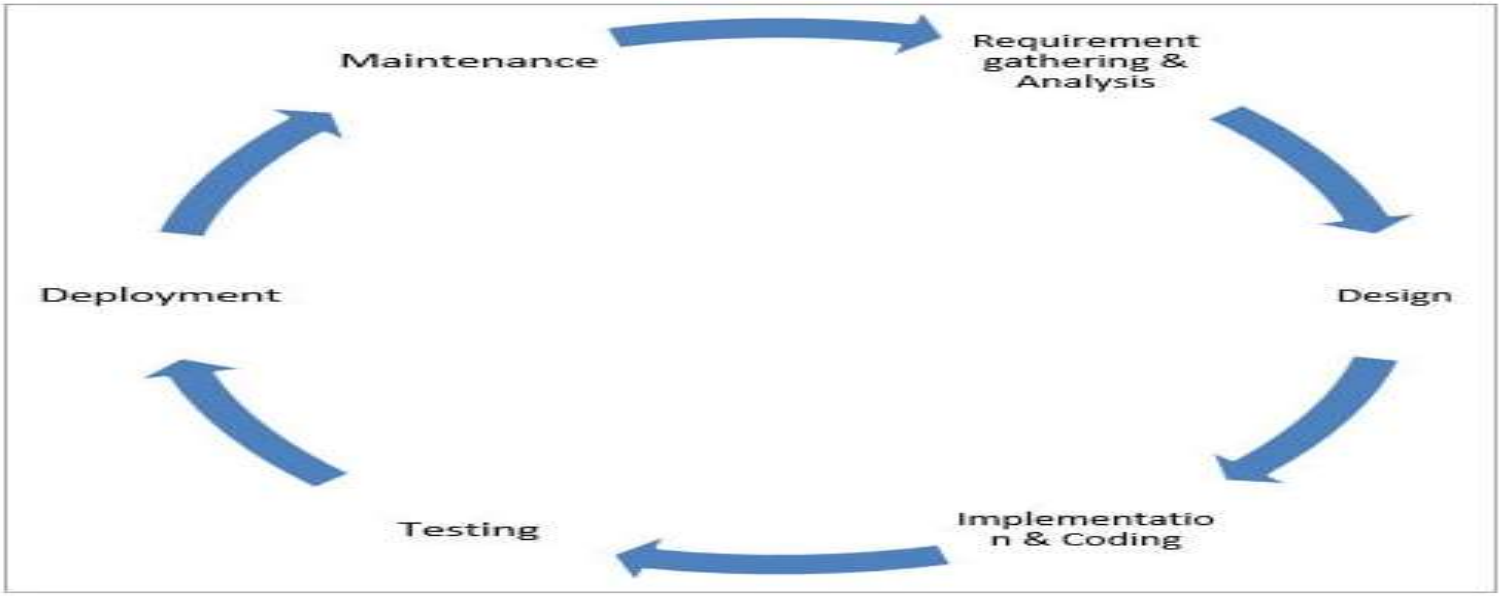
The software development life cycle (SDLC) is a framework defining tasks performed at each step in the software development process. The life cycle defines a methodology for improving the quality of software and the overall development process.

SDLC is the structure followed by a development team within the software organization. It aims to produce quality software that exceeds customer expectations, meets deadlines and cost estimates.

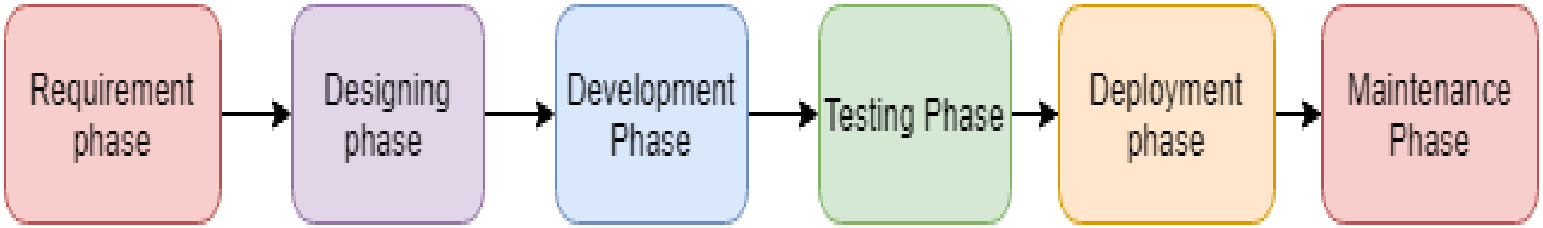
The Seven Phases of the SDLC



Below is the diagrammatic representation of the SDLC cycle:



Different phases of the software development cycle



- Requirement Phase
- Design Phase
- Build /Development Phase
- Testing Phase
- Deployment/ Deliver Phase
- Maintenance

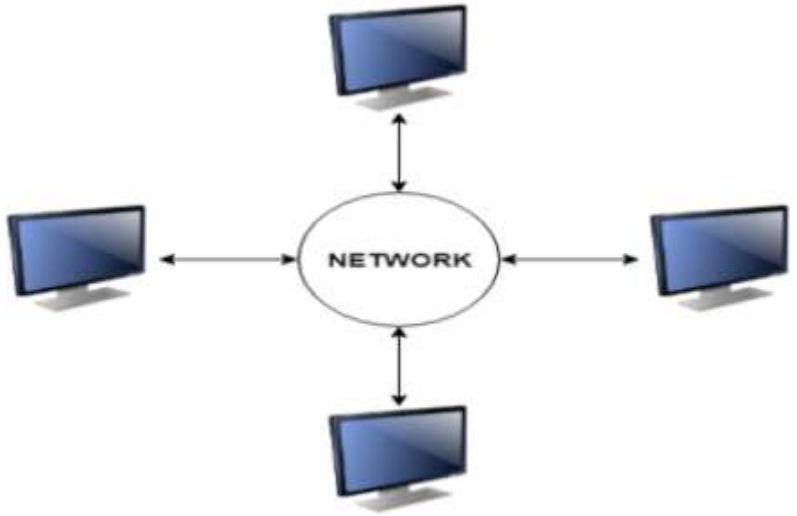
- **Requirement Phase :**
  - During this phase, the client states requirements, specifications, expectations, and any other special requirement related to the product or software. All these are gathered by the business manager or project manager or analyst of the service providing company.
  - The requirement includes how the product will be used and who will use the product to determine the load of operations. All information gathered from this phase is critical to developing the product as per the customer requirements.
- **Design Phase :**
  - In this stage, the requirements gathered in the SRS document is used as information to obtain the software architecture.
  - the developers then create either rough working models, or illustrates how the software will work, how it will look, how usage flows will move from screen to screen, and more.

- **Development / Implementation / Coding Phase :**
  - In this stage, the execution of design begins concerning script code.
  - In the coding phase, tasks are divided into units or modules and assigned to the various developers. It is the longest phase of the Software Development Life Cycle process.
  - Developers have to follow the coding guidelines defined by their management, and programming tools like compilers, interpreters, debuggers, etc. are used to generate and implement the code
- **Testing Phase :**
  - In this stage, Once the software is complete, and it is deployed in the testing environment.
  - The testing team starts testing the functionality of the entire system. This is done to verify that the entire application works according to the customer requirement.
  - During this phase, QA and testing team may find some bugs/defects which they communicate to developers.
  - The development team fixes the bug and send back to QA for a re-test. This process continues until the software is bug-free, stable, and working according to the business needs of that system.

- **Deployment / Installation Phase :**
  - Once the software testing phase is over and no bugs or errors left in the system then the final deployment process starts.
  - Based on the feedback given by the project manager, the final software is released and checked for deployment issues if any.
- **Maintenance:**
  - Once the system is deployed, and customers start using the developed system, following 3 activities occur.
  - **Bug fixing** - bugs are reported because of some scenarios which are not tested at all
  - **Upgrad**e - Upgrading the application to the newer versions of the Software
  - **Enhancement** - Adding some new features into the existing software

Distributed Systems

- A distributed system contains multiple nodes that are physically separate but linked together using the network.
- All the nodes in this system communicate with each other and handle processes in tandem.
- Each of these nodes contains a small part of the distributed operating system software.

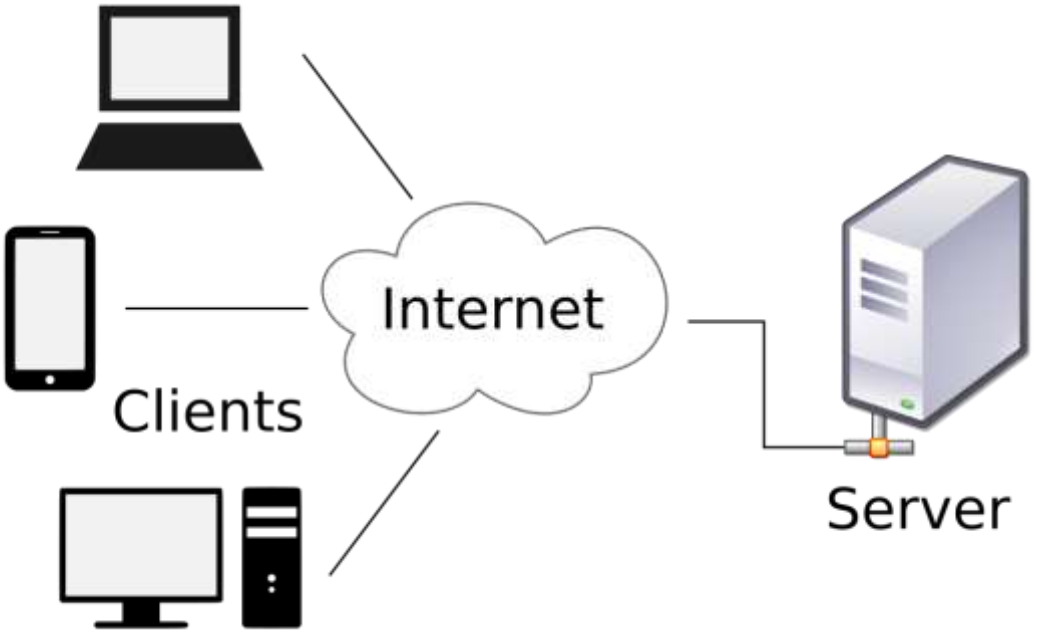


DISTRIBUTED OPERATING SYSTEM

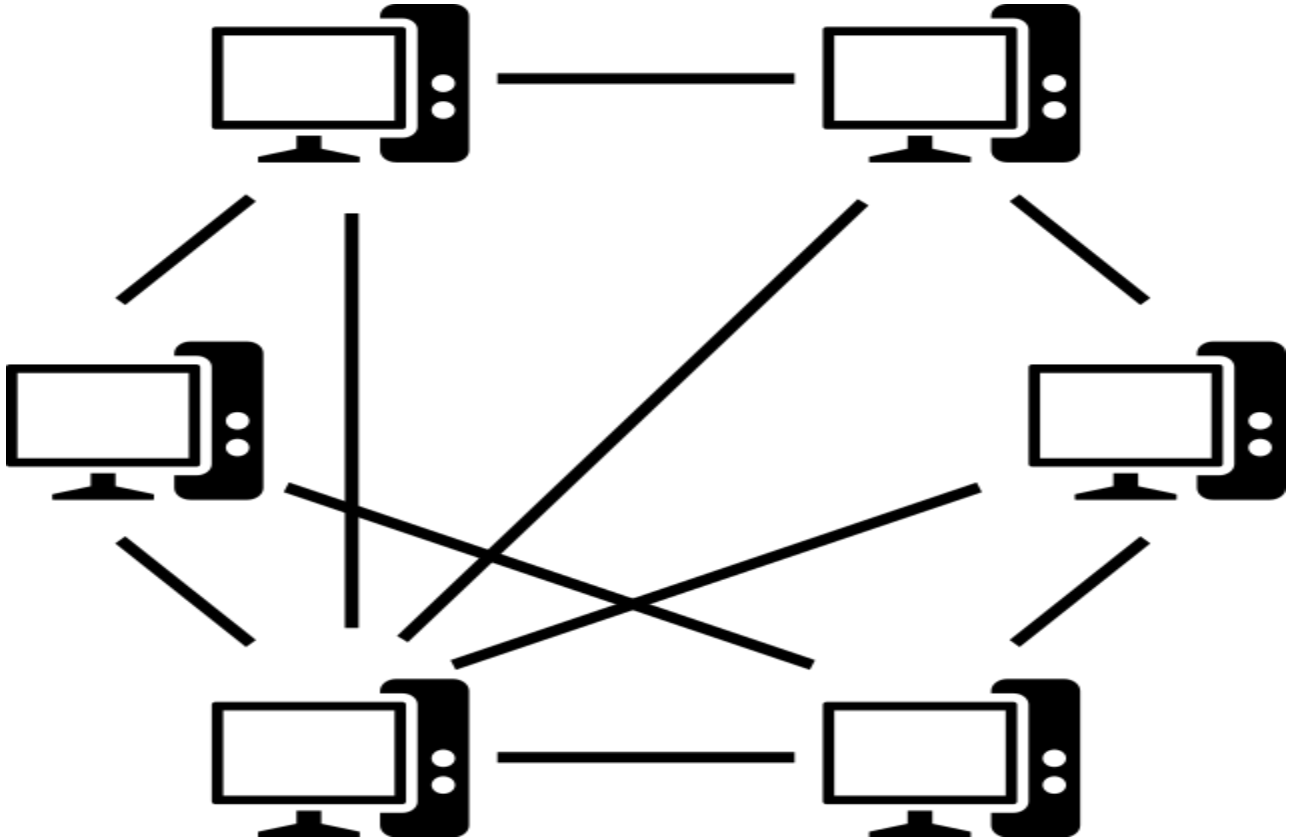
Types of Distributed Systems

The nodes in the distributed systems can be arranged in the form of client/server systems or peer to peer systems.

- **Client/Server Systems**
  - In client server systems, the client requests a resource and the server provides that resource. A server may serve multiple clients at the same time while a client is in contact with only one server. Both the client and server usually communicate via a computer network and so they are a part of distributed systems.



- **Peer to Peer Systems**
  - The peer to peer systems contains nodes that are equal participants in data sharing. All the tasks are equally divided between all the nodes. The nodes interact with each other as required as share resources. This is done with the help of a network.



Goals of Distributed Systems :

- Resource Sharing : allow many users to access to a common database.
- Openness : **Openness** is concerned with extensions and improvements of **distributed systems**. New components have to be integrated with existing components.
- Transparency : Location transparency and Fragmentation transparency.
- Scalability : It can operate correctly even as some aspect of the system is scaled to a larger size. (i.e. Add resource to a single node and to improve existing code to handle more work)

- The distributed software environment **introduces a number of risk factors for a centralized computing system.**
  - Software Agents
  - Java
  - Java Applets
  - ActiveX Controls
  - Distributed Objects

1) Software Agents :

Software Agents is a piece of software that functions acts as an agent for user or another program.

Working independent and continuously in a particular environment.

A **software agent** is autonomous (a person or entity that is **self-**controlling and not governed by outside forces) means it can perform tasks with no direct supervision or direct control , but can interact with another entity to obtain guidance or output results.

An autonomous system (AS) is a group of IP prefixes with a external routing policy.

In order for multiple autonomous systems to interact, each needs to have a unique identifier. **Autonomous system numbers can be public or private. Public ASNs** are required for systems to exchange information over the Internet. **A private ASN** can be used instead if a system is communicating solely with a single provider via Border Gateway Protocol (BGP).

2) Java :

Java is an object-oriented programming language used to create applets, servlets (small server-based programs) and JavaBeans.

Java is platform independent.

Java is a multi-threaded programming language.

Java is robust.

Java is very easy to learn and understand.

Security experts generally feel the security architecture of java is robust, its implementation is less.

3) Java Applets:

A java applet is a dynamic program module written in the java programming language in which java application embedded in a web page and downloaded to the user's machine for execution.

A **hostile applet** is any **applet** when downloaded, attempts to monopolize (exclusive ownership through legal privilege) or exploit your system's resources in an inappropriate manner.

For eg.: It can take control of your computer's operating system, corrupt or compromise data on your hard drive.

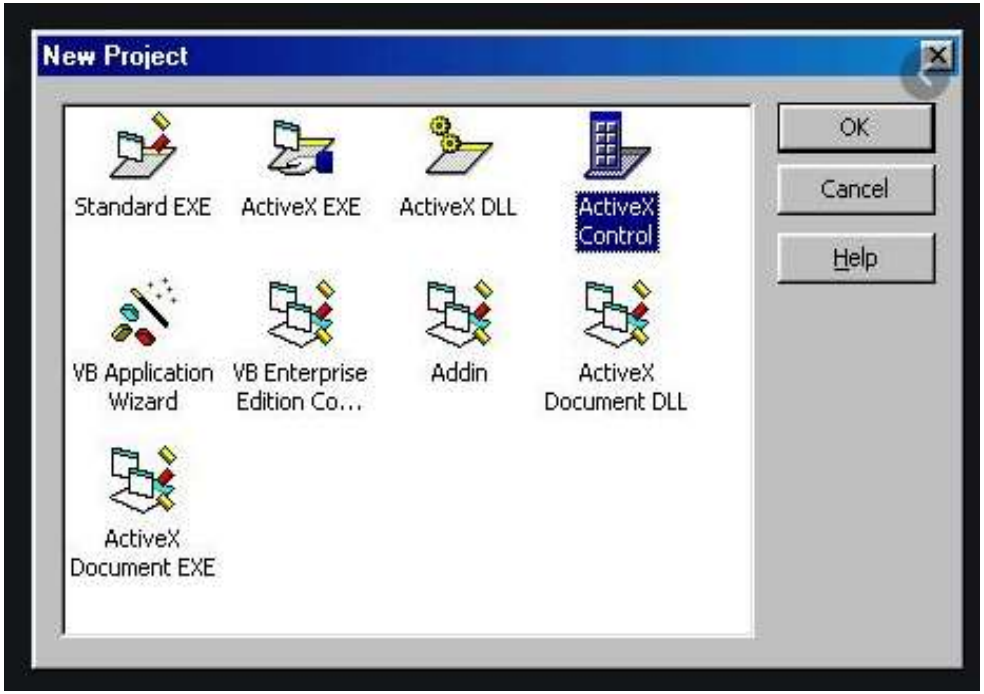
4) ActiveX Controls: - By Microsoft

ActiveX is a set of rules for how applications should store information and extends a browser's functionality. It works in Java and .net framework.

ActiveX controls officially run only in the Internet Explorer browser.

Software add-ons created with ActiveX are called ActiveX controls. These controls can be implemented in all types of programs, but they are most commonly distributed as small Web applications.

For example, a basic ActiveX control might display a clock on a webpage. (i.e. we an create our own ActiveX Controls.) Advanced ActiveX controls can be used for creating tickers and interactive presentations.



- ActiveX controls are similar to Java applets, but run through the ActiveX framework rather than the Java Runtime Environment (JRE). This means you must have ActiveX installed on your computer in order to view ActiveX controls in your Web browser. Additionally, when loading a custom ActiveX control within a webpage, you may be prompted to install it. If this happens, you should only accept the download if it is from a trusted source.

5) Distributed Objects

Distributed Object Model or DOM allows "objects" to interact across different operating platforms in a distributed processing environment.

A distributed object is one where methods can be invoked by remote process.

The Common Object Request Broker Architecture (CORBA) defines an architecture that allows client software to request a server process.

Distributed Systems – Distributed Objects

Using distributed objects, the client invokes a request for such a information- in a specified format – and the network determines the location, invokes the services and returns the results. The Object Request Broker (ORB) controls the messaging between objects on different platforms.

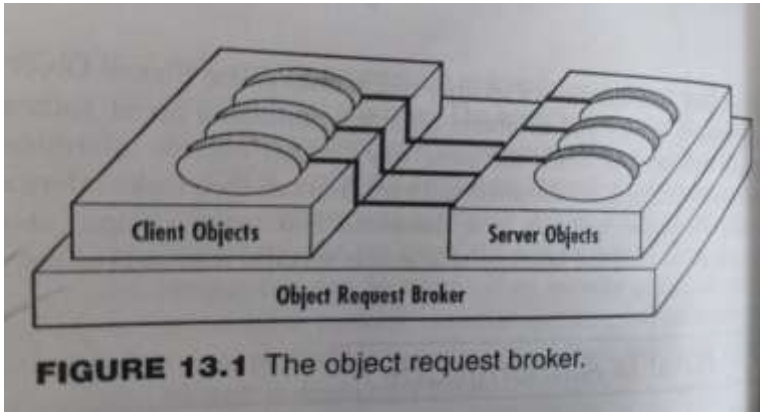


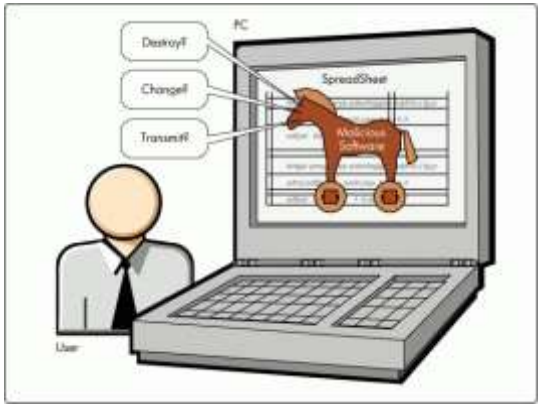
FIGURE 13.1 The object request broker.

In distributed computing, **distributed objects** are objects (in the sense of object-oriented programming) that are distributed across different IP address either in different processes on the same computer, or even in multiple computers connected via a network, but which work together by sharing data and invoking methods.

Malware

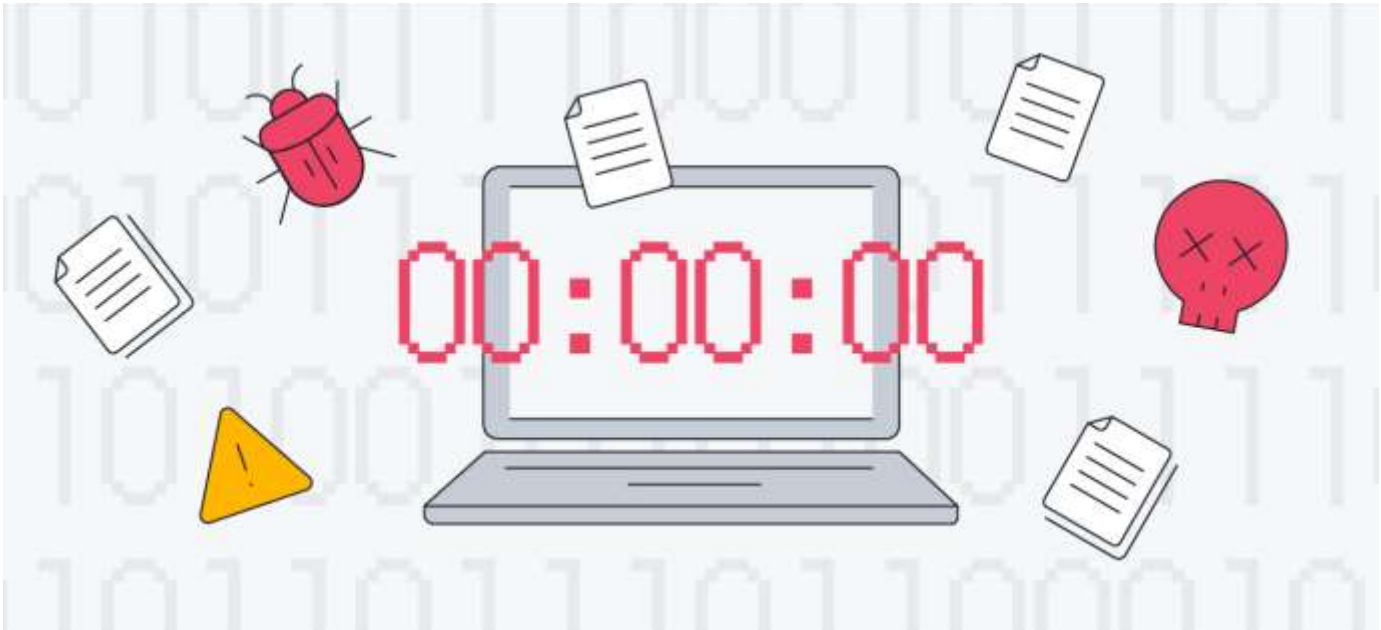
- Malware is malicious in that the code's intension is to wreak havoc (great damage) on the host computer.
- Malware is a program designed to gain access to computer systems, normally for the benefit of some third party, without the user's permission.
- Malware includes computer viruses, worms, Trojan horses, spyware, Botnets, Ransomware and other malicious programs.
- Types of malicious codes are:
  - Trojan horse
  - Virus
  - Logic bomb
  - Worm
  - Applet

- **Trojan horse :**
  - A Trojan horse, or “Trojan”, enters your system disguised as a normal, harmless file or program designed to trick you into downloading and installing malware.
  - As soon as you install a Trojan, you are giving cyber criminals access to your system.
  - Through the Trojan horse, the cyber criminal can steal data, install more malware, modify files, monitor user activity, destroy data, steal financial information, conduct denial of service (DoS) attacks on targeted web addresses, and more.
  - Trojan malware cannot replicate by itself; however, if combined with a worm, the damage Trojans can have on users and systems is endless.
  - **Remote Access Trojan** – This Trojan is designed to give the attacker full control over the computer.



- **Viruses :**
  - A Virus is a malicious executable code attached to another executable file.
  - The virus spreads when an infected file is passed from system to system.
  - Viruses can be harm or they can modify, delete or corrupt data.
  - Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.

- **Logic bomb :**
  - A **logic bomb** is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.
  - For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger), should they ever be terminated from the company.
  - Hidden code that is triggered by meeting or reaching a specific condition (date, time, event) much like a time bomb.



- **Worm :**
  - A computer worm is a type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage.
  - A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.
  - A program that propogates (the amount of time it takes for the head of the signal to travel from the sender to the receiver) itself by “worming” its way through communication protocols with no intervention from a user.
- **Applet :**
  - An applet (little application) is a small software program that supports a larger application program.
  - The java object that once downloaded can cause harm on the host computer. Because of Vulnerabilities found in the Java programming implementations on some browsers, it’s possible for an applet to gain privileges and then access local machine information or cause the browser to crash.

Antivirus Software

- Antivirus systems server different purposes. Some attempt to prevent infection in the first place by blocking the downloading of malicious code on the host computer.
- Others attempt to repair the damage once it is done.
- Many vendors have their software as the best antivirus tool on the market and there are plenty to choose from.
- Users should look for the following functionality and features when selecting antivirus software:
  - Software updates are automatically downloaded when the consumer is online.
  - Updates virus definitions are provided by the vendor when downloaded from the internet.
  - The software ptotects, but does not prevent.
  - Some of the better known tools include
  - Kaspersky, Symantec Norton AntiVirus,
  - Avast AntiVirus, Quick Heal,
  - Panda, F-Secure.
  - A vendor that provides timely information
  - about new viruses.

Improving Security Across the SDLC

- The Security Across the Software Development Life Cycle Task Force published the report *Improving Security Across the Software Development Life-cycle.*
- **The SDLC Task Force was composed of four subgroups.**
- The following guiding principles to increase software security throughout the SDLC:
  - **The Education Subgroup** called for the increased training and educating of software engineers to make software security.
  - **The Software Process Subgroup** called for the development and sharing of enhanced software security processes to make software systems safe from attacks.
  - **The Incentives Subgroup** recommended that software engineers be given incentive to develop an awareness of software security.
  - Finally, the **Patching Subgroup** wanted to make the process of applying software security patches "simple, easy and reliable."

- **Education Subgroup:**
  - The Education Subgroup's recommendation is a call for a change in the fundamental way people think about software, from the development of the simplest programs to the complex interdependencies of global systems.
  - It specifically recommend the following:
    - Begin a new effort to modernize educational and research programs to promote secure software development.
    - Create a software security certification program to promote increased security requirements in software design and development.

- **Software Process Subgroup:**
  - The Software Process Subgroup wants software engineers to follow standard processes and procedures to produce secure software.
  - The Software Process Subgroup's recommendations include a number of short, medium and long range steps to build more secure software systems.
  - **Short-term recommendations include:**
    - Software development processes that reduce defects in all phases of the SDLC (called "zero-defects").
    - Best practices for building secure software systems.
    - Software developers should measure the results of their efforts and publish them to promote across the industry.
  - **Mid-term recommendations include:**
    - Creating a security verification/validation program to review existing software development process.
    - Following all security measures (integrity, authentication, non-repudiation).
  - **Long-term recommendations include:**
    - Certifying processes with demo results in producing secure software.
    - Continuing to research and teach new techniques (New R&D).

- **Incentives Subgroup:**
  - Proper incentives can help to improve the security of the cyber space.
  - Some of the Incentives Subgroup recommendations include:
    - Job performance criteria on the quality and security of the software.
    - Creating industry awards for companies and individuals who promote software security practices.

- **Patch Management Subgroup:**
  - Software engineers must apply fixes or “patches” to the software to prevent the code from breaking or would be attackers.
  - The following recommendations of the Patch Management Subgroup include
    - Technology providers should include backup and risk mitigation/reduce plans for each patch.
    - It should encourage independent software vendors to stay current with the most advances secure software techniques and products.

Questions

- 1. Explain OSI model.
- 2. Write a short note on Malware.
- 3. Explain the subgroups of SDLC task force.
- 4. Explain SDLC in detail.
- 5. write a short note on firewall.
- 6. Explain distributed systems.
- 7. Explain IDS.