. Some of the main concepts of WAN that will be explained are as follows.

* A WAN is a data communications network that operates beyond a LAN’s geographic scope. One way that a WAN is different from a LAN is that, with a WAN, you must subscribe to an outside WAN service provider, such as ptcl, nayatel to use WAN carrier network services.
* Customer premises equipment (CPE): Devices physically located on the subscriber’s premises. Includes both devices owned by the subscriber and devices leased to the subscriber by the service provider.
* Demarcation (or demarc): The point at which the CPE ends and the local loop portion of the service begins. Often occurs at the POP of a building.
* Local loop (or “last-mile”): Cabling (usually copper wiring) that extends from the demarc into the WAN service provider’s central office.
* CO switch —A switching facility that provides the nearest point of presence for the provider’s WAN service.
* Toll network —The collective switches and facilities (called trunks) inside the WAN provider’s cloud.

WAN Virtual Circuits

* A virtual circuit is a logical circuit, as opposed to a point-to-point circuit, created to ensure reliable communication between two network devices. Two types of virtual circuits exist: switched virtual circuits (SVCs) and permanent virtual circuits (PVCs).

WAN Devices

WANs use numerous types of devices, including the following:

* Routers, which offer many services, including LAN and WAN interface ports.
* WAN switches, which connect to WAN bandwidth for voice, data, and video communication.
* Modems, which interface voice-grade services. Modems include CSUs/DSUs and TA/NT1 devices that interface ISDN services.
* Communication servers, which concentrate dial-in and dial-out user communication.

explanation of OSI Reference Model and its role in networking.

* WANs use the OSI reference model layered approach to encapsulation, just as LANs do, but they are mainly focused on the physical and data link layers.
* WAN standards typically describe both physical-layer delivery methods and data link layer requirements, including addressing, flow control and encapsulation.

WAN standards are defined and managed by a number of recognized agencies.

* International Telecommunication Union-Telecommunication Standardization Sector (ITU-T), formerly the Consultative Committee for International Telegraph and Telephone (CCITT)
* International Organization for Standardization (ISO)
* Internet Engineering Task Force (IETF)
* Electronic Industries Association (EIA)
* Telecommunications Industries Association (TIA)

The WAN Physical Layer

* WAN physical-layer protocols describe how to provide electrical, mechanical, operational, and functional connections for WAN services.

The WAN Data Link Layer

* The WAN data link layer defines how data is encapsulated for transmission to remote sites. WAN data-link protocols describe how frames are carried between systems on a single data path.
* Frame Relay —By using simplified encapsulation with no error correction mechanisms over high-quality digital facilities, Frame Relay can transmit data very rapidly compared to the other WAN protocols.
* Point-to-Point Protocol (PPP)—Described by RFC 1661, PPP was developed by the IETF. PPP contains a protocol field to identify the network layer protocol.
* ISDN—A set of digital services that transmits voice and data over existing phone lines.
* Link Access Procedure, Balanced (LAPB)—For packet-switched networks, LAPB is used to encapsulate packets at Layer 2 of the X.25 stack. It can also be used over a point-to-point link if the link is unreliable or there is an inherent delay associated with the link, such as in a satellite link. LAPB provides reliability and flow control on a point-to-point basis.
* Cisco/IETF—Used to encapsulate Frame Relay traffic. The Cisco option is proprietary and can be used only between Cisco routers.
* High-Level Data Link Control (HDLC)—An ISO standard, HDLC might not be compatible between different vendors because of the way each vendor has chosen to implement it. HDLC supports both point-to-point and multipoint configurations.

with explanation of different links used in WAN communication.

* Dedicated Lines: Dedicated lines, also called leased lines, provide full-time service. Dedicated lines typically are used to carry data, voice, and occasionally video. In data network design, dedicated lines generally provide core or backbone connectivity between major sites or campuses, as well as LAN-to-LAN connectivity.
* Packet-Switched Connections: Packet switching is a WAN switching method in which network devices share a permanent virtual circuit (PVC), which is like a point-to-point link that transports packets from a source to a destination across a carrier network.
* Circuit-Switched Connections: Circuit switching is a WAN switching method in which a dedicated physical circuit is established, maintained, and terminated through a carrier network for each communication session.
* ISDN Telephone companies developed ISDN with the intention of creating a totally digital network. ISDN devices include the following:
* Terminal Equipment 1 (TE1)—Designates a device that is compatible with the ISDN network. A TE1 connects to an NT of either Type 1 or Type 2.
* Terminal Equipment 2 (TE2)—Designates a device that is not compatible with ISDN and requires a TA.
* TA—Converts standard electrical signals into the form used by ISDN so that non-ISDN devices can connect to the ISDN network.
* NT Type 1 (NT1)—Connects four-wire ISDN subscriber wiring to the conventional two-wire local loop facility.
* NT Type 2 (NT2)—Directs traffic to and from different subscriber devices and the NT1. The NT2 is an intelligent device that performs switching and concentrating

An overview of Point to point Protocol.

* PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits (see Figure 11-1).
* PPP is the most widely used and most popular WAN protocol because it offers all the following features:
* Control of data link setup
* Provides for dynamic assignment of IP addresses

PPP Components: PPP addresses the problems of Internet connectivity by employing three main components:

* A method for encapsulating datagrams over serial links. PPP uses High- Level Data Link Control (HDLC) as a basis for encapsulating datagrams over point-to-point links.
* A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.
* A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

PPP Layer Functions: PPP uses a layered architecture, as shown in Figure 11-3. With its lower-level

functions, PPP can use

* Synchronous physical media, such as those that connect Integrated Services Digital Network (ISDN) networks.
* Asynchronous physical media, such as those that use basic telephone service for modem dialup connections.

PPP Frame Formats:

* Flag—Indicates the beginning or end of a frame and consists of the binary sequence 01111110.
* Address—Consists of the standard broadcast address, which is the binary sequence 11111111. PPP does not assign individual station addresses.
* Control—1 byte that consists of the binary sequence 00000011, which calls for transmission of user data in an unsequenced frame. A connectionless link service similar to that of Logical Link Control (LLC) Type 1 is provided.
* Protocol—2 bytes that identify the protocol encapsulated in the data field of the frame.
* Data—0 or more bytes that contain the datagram for the protocol specified in the protocol field. The end of the data field is found by locating the closing flag sequence and allowing 2 bytes for the frame check sequence (FCS) field. The default maximum length of the data field is 1500 bytes.
* FCS—Normally 16 bits (2 bytes). Refers to the extra characters added to a frame for error control purposes.

Overview of different components and frame format of PPP.

**PPP Components:** PPP addresses the problems of Internet connectivity by employing three main components:

* A method for encapsulating datagrams over serial links. PPP uses High- Level Data Link Control (HDLC) as a basis for encapsulating datagrams over point-to-point links.
* A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection.
* A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

PPP Layer Functions: PPP uses a layered architecture, as shown in Figure 11-3. With its lower-level

functions, PPP can use

* Synchronous physical media, such as those that connect Integrated Services Digital Network (ISDN) networks.
* Asynchronous physical media, such as those that use basic telephone service for modem dialup connections.

**PPP Frame Formats:**

* Flag—Indicates the beginning or end of a frame and consists of the binary sequence 01111110.
* Address—Consists of the standard broadcast address, which is the binary sequence 11111111. PPP does not assign individual station addresses.
* Control—1 byte that consists of the binary sequence 00000011, which calls for transmission of user data in an unsequenced frame. A connectionless link service similar to that of Logical Link Control (LLC) Type 1 is provided.
* Protocol—2 bytes that identify the protocol encapsulated in the data field of the frame.
* Data—0 or more bytes that contain the datagram for the protocol specified in the protocol field. The end of the data field is found by locating the closing flag sequence and allowing 2 bytes for the frame check sequence (FCS) field. The default maximum length of the data field is 1500 bytes.
* FCS—Normally 16 bits (2 bytes). Refers to the extra characters added to a frame for error control purposes.

**PPP Session Establishment:**

To establish communications over a point to-point link, PPP goes through four distinct phases:

**1.** Link establishment and configuration negotiation—An originating PPP

node sends LCP frames to configure and establish the data link.

**2.** Link-quality determination—The link is tested to determine whether the link quality is sufficient to bring up network-layer protocols. Note that this is an optional phase.

**3**. Network-layer protocol configuration negotiation—The originating PPP node sends NCP frames to choose and configure network-layer protocols. The chosen network-layer protocols—such as TCP/IP, Novell IPX, and AppleTalk—are configured, and packets from each network-layer protocol

can be sent.

**4.** Link termination—The link remains configured for communications until LCP or NCP frames close the link or until some external event occurs (for example, an inactivity timer expires or a user intervenes).

There are three classes of LCP frames:

* Link establishment frames—Used to establish and configure a link.
* Link termination frames—Used to terminate a link.
* Link maintenance frames—Used to manage and debug a link.

An overview of authentication involved in point to point protocol.

* The authentication phase of a PPP session is optional. After the link is established, and the authentication protocol chosen, the peer can be authenticated.
* When configuring PPP authentication, you can select PAP or CHAP.
* PAP—PAP provides a simple method for a remote node to establish its identity, using a two-way handshake. After the PPP link establishment phase is complete, a username/password pair is repeatedly sent by the remote node across the link until authentication is acknowledged or the connection is terminated.
* PAP is not a strong authentication protocol. Passwords are sent across the link in clear text
* CHAP—CHAP is used to periodically verify the identity of the remote node, using a three-way handshake. This is done upon initial link establishment and can be repeated any time after the link has been established. CHAP offers features such as periodic verification to improve security; this makes CHAP more effective than PAP.
* CHAP does not allow a caller to attempt authentication without a challenge.

Introduction to Frame Relay technology and its usage in the industry. Some definitions will be explained to the students about frame relay.

* Frame Relay is an industry-standard, switched data link layer protocol that handles multiple virtual circuits between connected devices.
* Frame Relay uses virtual circuits to make connections through a connection-oriented service.
* Frame Relay network can consist of computers, servers, and so on, on the user end; Frame Relay access equipment such as routers or modems; and Frame Relay network devices such as switches, routers, CSU/DSUs, or multiplexers.

**Frame Relay Terminology**

Following are some terms that are used to discuss Frame Relay:

**Access rate**—The clock speed (port speed) of the connection (local loop) to the Frame Relay cloud. It is the rate at which data travels into or out of the network.

**Data-link connection identifier (DLCI)—** a DLCI is a number that identifies the logical circuit between the source and destination device. The Frame Relay switch maps the DLCIs between each pair of routers to create a permanent virtual circuit (PVC).

**Local Management Interface (LMI)—**A signaling standard between the customer premises equipment (CPE) device and the Frame Relay switch that is responsible for managing the connection and maintaining status

between the devices. LMIs include support for a keepalive mechanism, which verifies that data is flowing; a multicast mechanism, which can provide the network server with its local DLCI.

**Committed information rate (CIR)—**The CIR is the guaranteed rate, in bits per second, that the service provider commits to providing.

**Committed burst—**The maximum number of bits that the switch agrees to transfer during a time interval. (It is noted as Bc.)

**Excess burst—**The maximum number of uncommitted bits that the Frame Relay switch attempts to transfer beyond the CIR. Excess burst is dependent on the service offerings available by the vendor, but is typically limited to the port speed of the local access loop.

**Forward explicit congestion notification (FECN)—**A bit set in a frame that notifies a DTE that congestion avoidance procedures should be initiated by the receiving device. When a Frame Relay switch recognizes congestion in the network, it sends a FECN packet to the destination device, indicating that congestion has occurred.

**Backward explicit congestion notification (BECN)—**A bit set in a frame that notifies a DTE that congestion avoidance procedures should be initiated by the sending device. when a Frame Relay switch recognizes congestion in the network, it sends a BECN packet to the source router, instructing the router to reduce the rate at which it is sending packets. If the router receives any BECNs during the current time interval,

it decreases the transmit rate by 25%.

**Discard eligibility (DE) indicator—**A set bit that indicates the frame may be discarded in preference to other frames if conjestion occurs. When the router detects network congestion, the Frame Relay switch will drop packets with the DE bit set first. The DE bit is set on the oversubscribed traffic (that is, the traffic that was received after the CIR was met).

overview of Frame relay operation.

* Frame Relay can be used as an interface to either a publicly available carrier provided service or to a network of privately owned equipment.
* The lines that connect user devices to the network equipment can operate at a speed selected from a broad range of data rates. Speeds between 56 kbps and 1.544 Mbps are typical, although Frame Relay can support lower and higher speeds.
* Frame Relay provides a means for multiplexing many logical data conversations, referred to as virtual circuits, through a shared physical medium by assigning DLCIs to each DTE/DCE pair of devices.
* Frame Relay standards address permanent virtual circuits (PVCs) that are administratively configured and managed in a Frame Relay network.

**Frame Relay Frame Format**

The Frame Relay frame format is shown in Figure. The flag fields indicate the beginning and end of the frame. Following the leading flag field are 2 bytes of address information.

**The following are the Frame Relay frame fields:**

**Flag**—Indicates the beginning and the end of the Frame Relay frame.

**Addres**s—Indicates the length of the address field. Although Frame Relay addresses are currently all 2 bytes long; the address bits allow for the possible extension of address lengths in the future. The eighth bit of each byte of the address field is used to indicate the address. The address contains the following information:

— DLCI Value—Indicates the DLCI value. Consists of the first 10 bits

of the Address field.

— Congestion Control—The last 3 bits in the address field, which control

the Frame Relay congestion notification mechanisms. These are

the FECN, BECN, and DE bits.

**Data**—Variable-length field that contains encapsulated upper-layer data.

**FCS**—Frame check sequence (FCS), used to ensure the integrity of

transmitted data.

## Introduction of Network security.

different security threats.

* Computer networks have grown in both size and importance in a very short time. This growth has pushed the requirement to secure networks.
* As the types of threats, attacks, and exploits have evolved, various terms have been coined to describe the individuals involved. Some of the most common terms are as follows:
* **White hat:** An individual who looks for vulnerabilities in systems or networks and then reports these vulnerabilities to the system’s owners so that they can be fixed.
* This person is ethically opposed to the abuse of computer systems. A white hat generally focuses on securing IT systems, whereas a black hat (the opposite) wants to break into them.
* **Hacker:** A general term that has historically been used to describe a computer programming expert. More recently, this term is often used in a negative way to describe an individual who attempts to gain unauthorized access to network resources with malicious intent.
* **Black hat:** Another term for individuals who use their knowledge of computer systems to break into systems or networks that they are not authorized to use, usually for personal or financial gain. A cracker is an example of a black hat.

**Security Policy:**

* The first step any organization should take to protect its data and itself from a liability challenge is to develop a security policy.
* A security policy is a set of principles that guides decision-making processes and enable leaders in an organization to distribute authority confidently.
* RFC 2196 states that a “security policy is a formal statement of the rules by which people who are given access to an organization’s technology and information assets must abide.”
* A security policy can be as simple as a brief “Acceptable Use Policy” for network resources, or it can be several hundred pages long and detail every element of connectivity and associated policies.
* The security policy also varies based on business type, company size, number of users, type of industry, threats, and vulnerabilities.

A security policy meets these goals:

* It informs users, staff, and managers of their obligations for protecting technology and information assets.
* It specifies the mechanisms through which these requirements can be met.
* It provides a baseline from which to acquire, configure, and audit computer systems and networks for compliance with the policy.

Common Security Threats

* When discussing network security, three common factors are vulnerabilities, threats, and attacks.

**Types of Network Attacks**

Various types of attacks can be launched against an organization. Understanding these attacks is the first step in being able to stop the attackers from disrupting your operations.

There are four primary classes of attacks:

* Reconnaissance
* Access
* Denial of service
* Malicious code (worms, viruses, and Trojan horses)

Reconnaissance Attacks

* Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities.
* It is also known as information gathering, and, in most cases, it precedes another type of attack.
* Reconnaissance is similar to a thief casing a neighborhood for vulnerable homes to break into, such as an unoccupied residence, or one with easy-to-open doors or open windows.

Reconnaissance attacks can consist of the following:

* Internet information queries
* Ping sweeps
* Port scans
* Packet sniffers
* External attackers can use Internet tools, such as the nslookup and whois utilities, to easily determine the IP address space assigned to a given corporation or entity. After the IP address space is determined, an attacker can ping the publicly available IP addresses to identify the addresses that are active.
* When the active IP addresses are identified, the intruder uses a port scanner to determine which network services or ports are active on the live IP addresses.
* A port scanner is software, such as Nmap or Superscan, that is designed to search a network host for open ports.
* The port scanner queries the ports to determine the application type and version, as well as the type and version of operating system (OS) running on the target host. Based on this information, the intruder can determine if a possible vulnerability that can be exploited exists.

Internal attackers may attempt to “eavesdrop” on network traffic. Network snooping and packet sniffing are common terms for eavesdropping. The information gathered by eavesdropping can be used to pose other attacks to the network.

Two common uses of eavesdropping are as follows:

* Information gathering: Network intruders can identify usernames, passwords, or information carried in a packet. The goal of this activity is to accumulate as much information as possible about the target.
* Information theft: The theft can occur as data is transmitted over the internal or external network.
* The network intruder can also steal data from networked computers by gaining unauthorized access. Examples include breaking into or eavesdropping on financial institutions and obtaining credit card numbers.
* The goal of this activity is to use the stolen information for personal gain or malicious reasons.

Three of the most effective methods for counteracting eavesdropping are as follows:

* Use switched networks instead of hubs. In this case, the use of a packet sniffer is essentially worthless, because traffic is not broadcast to all endpoints or network hosts.
* Using encryption that meets the organization’s data security needs without imposing an excessive burden on system resources or users.
* Implementing and enforcing a policy directive that forbids the use of protocols with known susceptibilities to eavesdropping. For example, the company policy may stipulate to use only SNMP version 3 and disallow other versions of SNMP.

**Access Attacks**

* Unauthorized system access is when an intruder gains access to a device for which he or she does not have an account or a password. Entering or accessing systems usually involve running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked.

Password Attacks

* Password attacks can be implemented using a packet sniffer to yield user accounts and passwords that are transmitted as clear text.
* Password attacks usually refer to repeated attempts to log in to a shared resource, such as a server or router, to identify a user account, password or both. These repeated attempts are called dictionary attacks or brute-force attacks.
* Dictionary attacks often succeed because users have a tendency to choose simple passwords that are short, single words or that are simple variations that are easy to predict, such as adding the number 1 to a word.
* A brute-force attack tool is more sophisticated because it searches exhaustively using combinations of character sets to compute every possible password made up of those characters.
* The downside is that more time is required to complete this type of attack. Brute-force attack tools have been known to solve simple passwords in less than a minute. Longer, more complex passwords may take days or weeks to resolve.

Trust Exploitation

* The goal of a trust exploitation attack is to compromise a trusted host, using it to stage attacks on other hosts in a network. If a host in a company’s network is protected by a firewall (inside host) but is accessible to a trusted host outside the firewall (outside host), the inside host can be attacked through the trusted outside host.

Man-in-the-Middle Attacks

* A man-in-the-middle (MITM) attack is carried out by attackers who manage to position themselves between two legitimate hosts. The attacker may allow the normal transactions between hosts to occur and only periodically manipulate the conversation between the two.
* An attacker can position himself between two hosts in many ways. The details of these methods are beyond the scope of this course, but a brief description of one popular method, the transparent proxy, will help illustrate the nature of MITM attacks.
* In a transparent proxy attack, an attacker may catch a victim by using a phishing e-mail or by defacing a website. Then the URL of a legitimate website has the attacker’s URL added to the front of it (prepended).

**DoS Attacks**

* Denial of service (DoS) is when an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users.
* DoS attacks involve rendering a system unavailable. This can be accomplished by physically disconnecting a system, crashing the system, or slowing it down to the point that it is unusable.
* DoS attacks are the most publicized form of attack and also are among the most difficult to eliminate.

Ping-of-Death Attacks

* The ping-of-death attack gained popularity back in the late 1990s. It took advantage of vulnerabilities in older operating systems.
* This attack modified the IP portion of a ping packet header to indicate that there was more data in the packet than there actually was.
* A ping normally is 64 to 84 bytes, whereas a ping of death could be up to 65,535 bytes. Sending a ping of this size may crash an older target computer. Most networks are no longer susceptible to this type of attack.

SYN Flood Attacks

* A SYN flood attack exploits the TCP three-way handshake. It involves sending multiple SYN requests (more than 1000) to a targeted server.
* The server replies with the usual SYNACK response, but the malicious host never responds with the final ACK to complete the handshake.
* This tie up the server until it eventually runs out of resources and cannot respond to a valid host request.

Other DoS Attacks

Other types of DoS attacks include the following:

* E-mail bombs: Programs send bulk e-mails to individuals, lists, or domains, monopolizing e-mail services.
* Malicious applets: These attacks are Java, JavaScript,

**DDoS Attacks**

* Distributed DoS (DDoS) attacks are designed to saturate network links with illegitimate data. This data can overwhelm an Internet link, causing legitimate traffic to be dropped.
* DDoS uses attack methods similar to standard DoS attacks but operates on a much larger scale. Typically, hundreds or thousands of attack points attempt to overwhelm a target.
* The client typically controls the handlers and agents that can be used to launch the attack.
* A handler is a compromised host that is running the attacker program. Each handler can control multiple agents.
* An agent is a compromised host that is running the attacker program. It is responsible for generating a stream of packets that is directed toward the intended victim.

Examples of DDoS attacks include the following:

* Smurf attack
* Tribe Flood Network (TFN)
* Stacheldraht
* MyDoom

**Mitigating DoS and DDoS Attacks**

* DoS and DDoS attacks can be mitigated by implementing special ant spoof and anti-DoS access control lists.
* ISPs can also implement a traffic rate policy, limiting the amount of nonessential traffic that crosses network segments.
* A common example is to limit the amount of ICMP traffic that is allowed into a network, because this traffic is used only for diagnostic purposes.

overview of the different mitigation techniques.

**Host- and Server-Based Security**

* Host- and server-based security must be applied to all network systems. Mitigation techniques for these devices include
* ■ Device hardening
* ■ Antivirus software
* ■ Personal firewalls
* ■ Operating system patches

Device Hardening

* When a new operating system is installed on a device, the security settings are set to the default values. In most cases, this level of security is inadequate. You should take some simple steps that apply to most operating systems:
* ■ Default usernames and passwords should be changed immediately.
* ■ Access to system resources should be restricted to individuals who are authorized to use those resources.
* ■ Any unnecessary services and applications should be turned off and uninstalled when possible.
* ■ Configure system logging and tracking.

Antivirus Software

* Install host antivirus software to protect against known viruses. Antivirus software can detect most viruses and many Trojan horse applications and prevent them from spreading in the network.
* Antivirus software does this in two ways:
* ■It scans files, comparing their contents to known virus signatures. Matches are flagged in a manner defined by the end user.
* ■It monitors suspicious processes running on a host that might indicate infection. This monitoring may include data captures, port monitoring, and other methods. Most commercial antivirus software uses both of these approaches.
* Keep in mind that antivirus software is good only if the definitions are up to date. Update antivirus software vigilantly.

Personal Firewalls

* PCs connected to the Internet through a dialup connection, DSL, or cable modem are as vulnerable as corporate networks.
* Personal firewalls reside on the user’s PC and attempt to prevent attacks.
* Personal firewalls are not designed for LAN implementations when compared to appliance-based or server-based firewalls, and they may prevent network access if installed with other networking clients, services, protocols, or adapters.

Operating System Patches

* The most effective way to mitigate a worm and its variants is to download security updates and patch all vulnerable systems.
* OS patches typically are downloaded from the operating system vendor, such as Microsoft or Apple. However, Linux is available in several distributions or flavors.
* It is critical to protect network hosts, such as workstation PCs and servers.
* These hosts need to be secured as they are added to the network, and they should be updated with security patches as these updates become available.

**Intrusion Detection and Prevention**

* Intrusion detection systems (IDS) detect attacks against a network and send logs to a management console.
* Intrusion prevention systems (IPS) prevent attacks against the network and should provide the following active defense mechanisms in addition to detection:
* ■ Prevention: Stops the detected attack from executing.
* ■ Reaction: Immunizes the system from future attacks from a malicious source.
* Either technology can be implemented at the network level or host level, or both for maximum protection.

Host-Based Intrusion Detection Systems

* Depending on the vendor, host-based intrusion typically is implemented as one of the following:
* ■ Passive technology, which was the first-generation technology, is called a host-based intrusion detection system (HIDS). HIDS sends logs to a management console after the attack has occurred and the damage is done.
* ■ Inline technology, called a host-based intrusion prevention system (HIPS), actually stops the attack, prevents damage, and blocks the propagation of worms and viruses.
* Active detection can be set to shut down t.he network connection or to stop impacted services automatically. Corrective action can be taken immediately. Cisco provides HIPS using the Cisco Security Agent software.
* HIPS software must be installed on each host, either the server or desktop, to monitor activity performed on and against the host.
* This software is called agent software. It performs intrusion detection analysis and prevention. Agent software also sends logs and alerts to a centralized management/policy server.
* The advantage of HIPS is that it can monitor operating system processes and protect critical system resources, including files that may exist only on that specific host.
* This means it can notify network managers when some external process tries to modify a system file in a way that may include a hidden back door program.

**The Network Security Wheel**

* The Network Security Wheel promotes retesting and reapplying updated security measures on a continuous basis. A security policy establishes the following:
* ■ Identifies the organization’s security objectives.
* ■ Documents the resources to be protected.
* ■ Identifies the network infrastructure with current maps and inventories.
* ■ Identifies the critical resources that need to be protected, such as research and development, finance, and human resources. This is called a risk analysis.
* The security policy is the hub upon which the four steps of the Security Wheel are based:

Step 1. Secure

Step 2. Monitor

Step 3. Test

Step 4. Improve

**The Enterprise Security Policy**

* “A security policy is a formal statement of the rules by which people who are given access to an organization’s technology and information assets must abide.”
* A security policy is a set of guidelines established to safeguard the network from attacks,from both inside and outside a company. Forming a policy starts with asking questions of the organization’s management:
* ■ How does the network help the organization achieve its vision, mission, and strategic plan?
* ■ What implications do business requirements have for network security?
* ■ How do those business requirements get translated into the purchase of specialized
* equipment and the configurations loaded onto devices?
* A security policy benefits an organization in the following ways:
* ■ It provides a means to audit existing network security and compare the requirements to what is in place.
* ■ It helps you plan security improvements, including equipment, software, and procedures.
* ■ It defines the roles and responsibilities of the company executives, administrators, andusers.
* ■ It defines which network and computer activities are and are not allowed.
* ■ It defines a process for handling network security incidents.
* ■ It enables global network security implementation and enforcement by acting as a standard between sites.
* ■ It creates a basis for legal action if necessary.

## Introduction to security features in cisco routers.

The Role of Routers in Network Security

* They advertise networks and filter who can use them.
* They provide access to network segments and subnetworks.

The following are examples of various security problems that can occur with a compromised

router:

* Compromising the access control can expose network configuration details, thereby facilitating attacks against other network components.
* Compromising the route tables can reduce performance, deny network communication services, and expose sensitive data by rerouting information to a compromised host.
* Misconfiguring a router traffic filter can expose internal network components to scans and attacks, making it easier for attackers to avoid detection.

Securing Your Network

Think about router security in terms of these categories:

**Physical security**: To provide physical security, locate the router in a locked room or locked cabinet that is accessible to only authorized personnel.

* It should also be free of any electrostatic or magnetic interference and should have controls for temperature and humidity.
* To reduce the possibility of DoS due to a power failure, install an uninterruptible power supply (UPS), and keep spare components available.
* Physical devices such as switches and CSUs/DSUs connected to the router should be stored in a locked facility, or they should remain in the possession of a trustworthy individual so that they are not compromised.
* A device that is left in the open could have Trojans or some other sort of executable file stored on it.

**Update the router whenever advisable**: Give the router the maximum amount of memory possible. Availability of memory can help protect against some DoS attacks while supporting the widest range of security services.

* The security features in an operating system evolve over time. However, the latest version of an operating system may not be the most stable version available.
* To get the best security performance from your operating system, use the latest stable release that meets your network’s feature requirements.

**Back up the router configuration and IOS**: Always have a backup copy of a configuration and IOS on hand in case a router fails. Keep a secure copy of the router operating system image and router configuration file on a CD or other storage device.

* Otherwise, a TFTP server is commonly used for backup purposes.

**Harden the router to eliminate the potential abuse of unused ports and services:**

* Harden the router to make it as secure as possible. A router has many services enabled by default.
* Many of these services are unnecessary and may be used by an attacker for information gathering or exploitation.
* You should harden your router configuration by disabling unnecessary services.

**Applying Cisco IOS Security Features to Routers**

* Before you configure security features on a router, you need a plan for all the Cisco IOS security configuration steps. The following are the steps to safeguard a router:

Step 1. Manage router security.

Step 2. Secure remote administrative access to routers.

Step 3. Log router activity.

Step 4. Secure vulnerable router services and interfaces.

Step 5. Secure routing protocols.

Step 6. Control and filter network traffic.

Securing Router Network Services

* Cisco routers support a large number of network services at Layers 2, 3, 4, and 7. Some of these services are application layer protocols that allow users and host processes to connect to the router.
* Others are automatic processes and settings intended to support legacy or specialized configurations that pose security risks.
* Some of these services can be restricted or disabled to improve security without degrading the operational use of the router.
* General security practice for routers should be used to support only the traffic and protocols a network needs.

The following list includes examples of commands that disable the associated service:

* ■ Small services such as echo, discard, and chargen: Use the no service tcp-smallservers and no service udp-small-servers commands.
* ■ BOOTP: Use the no ip bootp server command.
* ■ Finger: Use the no service finger and no ip finger commands.
* ■ HTTP: Use the no ip http server command.
* ■ SNMP: Use the no snmp-server command.
* ■ Cisco Discovery Protocol (CDP): Use the no cdp run command.
* ■ Remote configuration: Use the no service config command.
* ■ Source routing: Use the no ip source-route command.
* ■ Classless routing: Use the no ip classless command.

SNMP, NTP, and DNS Vulnerabilities

* SNMP, NTP, and DNS are three management services that should also be secured. The methods for disabling or tuning the configurations for these services are beyond the scope of this course.
* The following are descriptions and simple guidelines to secure these services:
* ■ SNMP: SNMP is the standard TCP/IP protocol for automated remote monitoring and administration. Several different versions of SNMP have different security properties. Versions of SNMP before version 3 shuttle information in clear text. Normally, SNMP version 3 should be used.
* ■ NTP: Cisco routers and other hosts use NTP to keep their time-of-day clocks accurate. If possible, network administrators should configure all routers as part of an NTP hierarchy, which makes one router the master timer and provides its time to other routers on the network. However, NTP leaves listening ports open and vulnerable. If an NTP hierarchy is not available on the network, you should disable NTP. Disabling NTP on an interface does not prevent NTP messages from traversing the router. To reject all NTP messages at a particular interface, use an access list.
* ■ DNS: Cisco IOS software supports looking up hostnames with the Domain Name System (DNS). DNS provides the mapping between names, such as central.mydomain. com, and IP addresses, such as 14.2.9.250—information that an attacker can exploit.

**Securing Routing Protocols**

* As a network administrator, you have to be aware that your routers are at risk of being attacked just as much as your end-user systems. Anyone with a packet sniffer such as Wireshark can read information propagating between routers. In general, routing systems can be attacked in two ways:
* ■ By disrupting peers
* ■ By falsifying routing information
* Disruption of peers is the less critical of the two attacks because routing protocols heal themselves, making the disruption last only slightly longer than the attack itself.
* A more subtle class of attack targets the information carried within the routing protocol. Falsified routing information generally may be used to cause systems to misinform (lie to) each other, to cause DoS, or to cause traffic to follow a path it would not normally follow.
* The effects of falsifying routing information are as follows:
* It redirects traffic to create routing loops.
* It redirects traffic so that it can be monitored on an insecure link that would potentially allow a hacker to gain access to confidential information.
* It redirects traffic to discard it.

## overview of cisco security device manager.

* The Cisco Router and Security Device Manager (SDM) is an easy-to-use, web-based device-management tool designed for configuring LAN, WAN, and security features on Cisco IOS software-based routers.
* SDM helps network administrators of small- to medium-sized businesses perform day-today operations. It provides easy-to-use smart wizards, automates router security management, and offers help through comprehensive online help and tutorials.

Cisco SDM Overview

* Cisco SDM is preinstalled by default on all new Cisco Integrated Services Routers (ISR). If it is not preinstalled, you must install it.
* The SDM files can be installed on the router, a PC, or both. An advantage of installing SDM on the PC is that it saves router memory and allows you to use SDM to manage other routers on the network.
* Cisco recommends using Cisco SDM to perform the initial configuration.
* Cisco SDM simplifies router and security configuration through the use of several intelligent wizards to enable efficient configuration of key router VPN and Cisco IOS firewall parameters.
* This capability permits administrators to quickly and easily deploy, configure, and monitor Cisco routers.
* Cisco SDM smart wizards can intelligently detect incorrect configurations and propose fixes, such as allowing DHCP traffic through a firewall if the WAN interface is DHCPaddressed.

**Secure Router Management**

* Periodically, the router requires updates to be loaded to either the operating system or the configuration file.
* These updates are necessary to fix known security vulnerabilities, support new features that allow more advanced security policies, or improve performance.
* You must follow certain guidelines when changing the Cisco IOS software on a router.
* Changes are classified as either updates or upgrades. An update replaces one release with another without upgrading the feature set. The software might be updated to fix a bug or to replace a release that is no longer supported. Updates are free.
* An upgrade replaces a release with one that has an upgraded feature set. The software might be upgraded to add new features or technologies or replace a release that is no longer supported. Upgrades are not free.
* Cisco.com offers guidelines to help you determine which method applies.
* Cisco recommends that you follow a four-phase migration process to simplify network operations and management. When you follow a repeatable process, you can also benefit from reduced costs in operations, management, and training. The four phases are as follows:
* ■ Plan: Set goals, identify resources, profile network hardware and software, and create a preliminary schedule for migrating to new releases.
* ■ Design: Choose new Cisco IOS releases and create a strategy for migrating to the releases.
* ■ Implement: Schedule and execute the migration.
* ■ Operate: Monitor the migration progress and make backup copies of images that are running on your network.
* A number of tools available on Cisco.com help you migrate Cisco IOS software. You can use the tools to get information about releases, feature sets, platforms, and images.
* The following tools do not require a Cisco.com login:
* ■ Cisco IOS Reference Guide: Covers the basics of the Cisco IOS software family.
* ■ Cisco IOS software technical documents: Documentation for each release of Cisco

IOS software.

* ■ Cisco Feature Navigator: Finds releases that support a set of software features and

hardware, and compares releases.

* The following tools require valid Cisco.com login accounts:
* ■ Download Software: Cisco IOS software downloads.
* ■ Bug Toolkit: Searches for known software fixes based on software version, feature set, and keywords.
* ■ Software Advisor: Compares releases, matches Cisco IOS software and Cisco Catalyst OS features to releases, and finds out which software release supports a given hardware device.
* ■ Cisco IOS Upgrade Planner: Finds releases by hardware, release, and feature set, and downloads images of Cisco IOS software.

## overview of Access control list.

* Network security is a huge subject. One of the most important skills a network administrator needs is mastery of access control lists (ACL).
* Administrators use ACLs to stop traffic or permit only specified traffic while stopping all other traffic on their networks.
* An access control list (ACL) is a sequential list of permit or deny statements that apply to addresses or upper-layer protocols.
* ACLs provide a powerful way to control traffic into and out of your network.
* ACLs enable you to control traffic into and out of your network. This control can be as simple as permitting or denying network hosts or addresses.
* ACLs can also be configured to control network traffic based on the TCP port being used.

**Packet Filtering**

* Packet filtering, sometimes called static packet filtering, controls access to a network by analyzing the incoming and outgoing packets and passing or halting them based on stated criteria.
* A router acts as a packet filter when it forwards or denies packets according to filtering rules. When a packet arrives at the packet-filtering router, the router extracts certain information from the packet header and makes decisions according to the filter rules about whether the packet can pass through or be discarded.
* Packet filtering works at the network layer of the Open Systems Interconnection (OSI) model or at the Internet layer of the TCP/IP model.
* As a Layer 3 device, a packet-filtering router uses rules to determine whether to permit or deny traffic based on source and destination IP addresses, source port and destination port, and the packet’s protocol.
* The ACL can extract the following information from the packet header, test it against its rules, and make “permit” or “deny” decisions based on
* ■ Source IP address
* ■ Destination IP address
* ■ ICMP message type
* The ACL can also extract upper-layer information and test it against its rules. Upper-layer information includes
* ■ TCP/UDP source port
* ■ TCP/UDP destination port
* An ACL is a router configuration script that controls whether a router permits or denies Packets.
* By default, a router does not have any ACLs configured and, therefore, does not filter traffic.
* Traffic that enters the router is routed according to the routing table.

Here are some guidelines for using ACLs:

* ■ Use ACLs in firewall routers positioned between your internal network and an external network such as the Internet.
* ■ Use ACLs on a router positioned between two parts of your network to control traffic entering or exiting a specific part of your internal network.
* ■ Configure ACLs on border routers—routers situated at the edges of your networks.

This provides a basic buffer from the outside network, or between a less controlled area of your own network and a more sensitive area of your network.

* ■ Configure ACLs for each network protocol configured on the border router interfaces. You can configure ACLs on an interface to filter inbound traffic, outbound traffic, or both.

**ACL Functions**

ACLs perform the following tasks:

* ■ Limit network traffic to increase network performance. For example, if corporate policy does not allow video traffic on the network, ACLs that block video traffic could be configured and applied. This would greatly reduce the network load and increase network performance.
* ■ Provide traffic flow control. ACLs can restrict the delivery of routing updates. If updates are not required because of network conditions, bandwidth is preserved.
* ■ Provide a basic level of security for network access. ACLs can allow one host to access part of the network and prevent another host from accessing the same area. For example, access to the Human Resources network can be restricted to select users.
* ■ Decide which types of traffic to forward or block at the router interfaces. For example, an ACL can permit e-mail traffic but block all Telnet traffic.
* ■ Control which areas a client can access on a network.
* ■ Screen hosts to permit or deny access to network.

**How ACLs Work**

ACLs are configured either to apply to inbound traffic or to apply to outbound traffic:

* ■ Inbound ACLs: Incoming packets are processed before they are routed to the outbound interface. An inbound ACL is efficient because it saves the overhead of routing lookups if the packet is discarded. If the packet is permitted by the tests, it is then processed for routing.
* ■ Outbound ACLs: Incoming packets are routed to the outbound interface, and then they

are processed through the outbound ACL.

* ACL statements operate in sequential order. They evaluate packets against the ACL, from the top down, one statement at a time.
* If a packet header and an ACL statement match, the rest of the statements in the list are skipped, and the packet is permitted or denied as determined by the matched statement.
* If a packet header does not match an ACL statement, the packet header is tested against the next statement in the list. This matching process continues until the end of the list is reached.
* At the end of every access list is an implied “deny all traffic” criteria statement. It is also sometimes called the “implicit deny any” statement. Therefore, if a packet does not match any of the ACL entries, it is automatically blocked. The implied “deny all traffic” is the default behavior of ACLs and cannot be changed.

## overview of different type of ACLs.

**Types of Cisco ACLs**

* The two types of Cisco ACLs are standard and extended:
* Standard ACLs filter packets based on source IP address only.
* Extended ACLs filter packets based on several attributes:
* ■ Source and destination IP addresses
* ■ Source and destination TCP and UDP ports
* ■ Protocol type (IP, ICMP, UDP, TCP, or protocol number)

**Standard ACLs**

* Standard ACLs allow you to permit or deny traffic from source IP addresses. The packet’s destination and the ports involved do not matter. For example, the following ACL statement allows all traffic from the network 192.168.30.0/24:
* Router(config)# access-list 10 permit 192.168.30.0 0.0.0.255
* Because of the implied “deny any” at the end, all other traffic is blocked with this ACL.
* Standard ACLs are created in global configuration mode.

**Extended ACLs**

* Extended ACLs filter IP packets based on several attributes, such as protocol type, source and IP address, destination IP address, source TCP or UDP ports, destination TCP or UDP ports, and optional protocol type information for finer granularity of control.
* Extended ACLs are created in global configuration mode.

**How a Standard ACL Works**

* A standard ACL is a sequential collection of permit and deny conditions that apply to source IP addresses.
* The packet’s destination and the ports involved are not examined.

**Two main tasks are involved in using ACLs:**

* Step 1. Create an access list by specifying an access list number or name and access conditions.
* Step 2. Apply the ACL to interfaces or terminal lines.

**Numbered ACL:**

* You assign a number based on whether your ACL is standard or extended:
* ■ 1 to 99 and 1300 to 1999: Standard IP ACL
* ■ 100 to 199 and 2000 to 2699: Extended IP ACL
* ■ You cannot add or delete entries within the ACL.

**Named ACL:**

* You assign a name by providing the name of the ACL:
* ■ Names can contain alphanumeric characters.
* ■ It is suggested that the name be written in CAPITAL LETTERS.
* ■ Names cannot contain spaces or punctuation and must begin with an alphabetic character.
* ■ You can add or delete entries within the ACL.
* ■ You can specify whether the ACL is standard or extended.

**Where to Place ACLs**

* The proper placement of an ACL to filter undesirable traffic makes the network operate more efficiently.
* Every ACL should be placed where it has the greatest impact on efficiency. The basic rules are as follows:
* ■ Like standard ACLs, extended ACLs can examine the source IP addresses, but they also

examine the destination IP address, protocols, and port numbers (or services).

* ■ Because standard ACLs do not specify destination addresses, place them as close to the destination as possible. This way, the ACL does not inadvertently block traffic to more destinations than intended.

overview of different IP addressing services such as DHCP, Nat and Pat.

* Every device that connects to a network needs an IP address. Network administrators manually assign static IP addresses to routers, servers, and other network devices whose locations (physical and logical) are not likely to change.
* However, desktop and laptop computers often change physical locations within an organization.
* Administrators attempting to provide manual IP address assignment for these hosts would be faced with the monumental task of readdressing the host every time an employee moves to a different office or cubicle.
* DHCP is a service that assigns IP addresses and other important network configuration information dynamically.
* DHCP makes the process of assigning new IP addresses almost transparent.

**DHCP Operation**

* Providing IP addresses to clients is the most fundamental task performed by a DHCP server.
* DHCP includes three different address allocation mechanisms to provide flexibility when assigning IP addresses:
* ■ Manual allocation: The administrator assigns a preallocated IP address to the client, and DHCP only communicates the IP address to the device.
* ■ Automatic allocation: DHCP automatically assigns a static IP address permanently to a device, selecting it from a pool of available addresses. There is no lease, and the address is permanently assigned to a device.
* ■ Dynamic allocation: DHCP automatically dynamically assigns, or leases, an IP

address from a pool of addresses for a limited period of time chosen by the server, or

until the client tells the DHCP server that it no longer needs the address.

**BOOTP and DHCP**

* The Bootstrap Protocol (BOOTP), defined in RFC 951, is the predecessor of DHCP and shares some of its operational characteristics.
* BOOTP gives a diskless workstation a way to acquire an IP address and boot configurations. A diskless workstation does not have a hard drive or operating system.
* Both DHCP and BOOTP are client/server-based and use UDP ports 67 and 68. Those ports are still known as BOOTP ports. Figure 7-3 shows the client/server relationship of DHCP and BOOTP**.**

There are three primary differences between DHCP and BOOTP:

* ■ The main difference is that BOOTP was designed for manual preconfiguration of the host information in a server database, whereas DHCP allows for dynamic allocation of network addresses and configurations to newly attached hosts.
* When a BOOTP client requests an IP address, the BOOTP server searches a predefined table for an entry that matches the MAC address for the client.
* If an entry exists, the corresponding IP address for that entry is returned to the client. This means that the binding between the MAC address and the IP address must have already been configured in the BOOTP server.
* ■ DHCP allows for recovery and reallocation of network addresses through a leasing mechanism. Specifically, DHCP defines mechanisms through which clients can be assigned an IP address for a finite lease period.
* This lease period allows for reassignment of the IP address to another client later, or for the client to get another assignment if the client moves to another subnet.
* Clients may also renew leases and keep the same IP address. BOOTP does not use leases. Its clients have reserved IP addresses that cannot be assigned to any other host.
* ■ BOOTP provides a limited amount of information to a host. DHCP provides additional IP configuration parameters, such as WINS and domain name.

## overview of Network Address translation service.

* Although private addresses are assigned to devices inside the network, NAT-enabled routers retain one or many valid Internet IP addresses outside the network.
* When the client sends packets out of the network, NAT translates the client’s internal IP address into an external address.
* To outside users, all traffic coming to and going from the network has the same IP address or is from the same pool of addresses.
* NAT has many uses, but its key use is to save IP addresses by allowing networks to use private IP addresses.
* NAT translates nonroutable, private, internal addresses into routable, public addresses.
* NAT has the added benefit of adding a degree of privacy and security to a network, because it hides internal IP addresses from outside networks.

**Dynamic Mapping and Static Mapping**

The two types of NAT translation are as follows:

* ■ Dynamic NAT uses a pool of public addresses and assigns them on a first-come, firstserved basis.
* When a host with a private IP address requests access to the Internet, dynamic NAT chooses an IP address from the pool that is not already in use by another host.
* ■ Static NAT uses a one-to-one mapping of local and global addresses, and these mappings remain constant.
* Static NAT is particularly useful for web servers or hosts that must have a consistent address that is accessible from the Internet. These internal hosts may be enterprise servers or networking devices.

**NAT Overload**

* NAT overloading (sometimes called Port Address Translation [PAT]) maps multiple private IP addresses to a single public IP address or a few addresses.
* This is what most home routers do. Your ISP assigns one address to your router, yet several members of your family can simultaneously surf the Internet.
* With NAT overloading, multiple addresses can be mapped to one or a few addresses because each private address is also tracked by a port number. When a client opens a TCP/IP session, the NAT router assigns a port number to its source address.

**Differences Between NAT and NAT Overload**

* NAT generally translates IP addresses only on a 1:1 correspondence between publicly exposed IP addresses and privately held IP addresses.
* NAT overload modifies both the private IP address and port number of the sender. NAT overload chooses the port numbers seen by hosts on the public network.
* NAT routes incoming packets to their inside destination by referring to the incoming source IP address given by the host on the public network.
* NAT overload generally has only one or very few publicly exposed IP addresses.
* Incoming packets from the public network are routed to their destinations on the private network by referring to a table in the NAT overload device that tracks public and private port pairs. This is called connection tracking.

## overview of the different components of network documentation.

* To efficiently diagnose and correct network problems, a network engineer needs to know how a network has been designed and what the network’s expected performance should be under normal operating conditions.
* This information is captured and contained in network documentation. Network documentation consists of various sources of information that provide a clear picture of the network’s design and characteristics.

**Documenting Your Network**

* Network configuration documentation provides a logical diagram of the network and detailed information about each component.
* Information such as the network’s physical and logical topologies, device configuration, end-system configurations, and various network baselines should be included.
* A hard copy of the documentation should be stored in a central location. The information could also be available on a protected intranet website.

**Network documentation should include these components:**

* ■ Network topology diagram
* ■ Network configuration table
* ■ End-system configuration table
* ■ Network baseline

**Network Documentation Process**

* The documentation process is a very time-consuming task.
* Having complete and accurate network information at your disposal makes it far easier to pinpoint an anomaly causing a network problem.
* The initial documentation could take a substantial amount of time to generate. However, after it is generated, the documentation becomes a maintenance task and is updated on a scheduled basis.
* In fact, maintaining up-to-date documentation is very important. Policies and procedures

must be in place to ensure accuracy.

* Any changes in the topology, devices, or end system must be revised and reflected in the documentation.
* Step 1. Log in to an undocumented device.
* Step 2. Discover relevant information about the device.
* Step 3. Record device information in the network configuration table.
* Step 4. Is this device important enough to add to the topology diagram?
* Step 5. Transfer relevant device information from the network configuration table to the topology diagram.
* Step 6. Is there any more information to discover for this device?
* Step 7. What neighboring devices are connected to this device?
* Step 8. Are any other neighbor devices undocumented?
* Step 9. If no undocumented devices exist, documentation is complete.
* Some commands that are useful to the network documentation process:
* ■ The ping command tests connectivity with neighboring devices before logging in to them. Pinging to other PCs in the network also initiates the MAC address autodiscovery process.
* ■ The telnet command logs in remotely to a device for accessing configuration information.
* ■ The ‘show ip interface’ brief command displays the up or down status and IP address of all interfaces on a Cisco router or switch.
* ■ The ‘show ip route’ command displays the routing table in a router to discover the directly connected neighbors, more remote devices (through learned routes), and the routing protocols that have been configured.
* ■ The ‘show cdp neighbor’ detail command displays detailed information about directly

connected Cisco neighbor devices.

**General Troubleshooting Procedures**

Stage 1: Gather Symptoms

* Troubleshooting begins with the process of gathering and documenting symptoms from the network, end systems, and users.
* In addition, the network administrator determines which network components have been affected and how the network’s functionality has changed compared to the baseline.
* Symptoms may appear in many different forms, including alerts from the network management system, console messages, and user complaints.
* While gathering symptoms, use questions as a method of localizing the problem to a smaller range of possibilities.

Stage 2: Isolate the Problem

* The problem is not truly isolated until a single problem, or a set of related problems, is identified.
* To do this, the network administrator examines the characteristics of the problems at the logical layers of the network so that the most likely cause can be selected.
* At this stage, the network administrator may gather and document more symptoms, depending on the problem characteristics that are identified.

Stage 3: Correct the Problem

* Having isolated and identified the cause of the problem, the network administrator works to correct the problem by implementing, testing, and documenting a solution.
* If the network administrator determines that the corrective action has created another problem, the attempted solution is documented, the changes are removed, and the network administrator returns to gathering symptoms and isolating the problem.

The three main methods of troubleshooting networks are

* ■ Bottom-up
* ■ Top-down
* ■ Divide-and-conquer
* Each approach has its advantages and disadvantages

**Bottom-Up Troubleshooting Method**

* In bottom-up troubleshooting you start with the physical components of the network and move up through the layers of the OSI model until the cause of the problem is identified.
* Bottom-up troubleshooting is a good approach to use when the problem is suspected to be a physical one.
* Most networking problems reside at the lower levels, so implementing the bottom-up approach often results in effective results.
* The disadvantage of bottom-up troubleshooting is that it requires you to check every device and interface on the network until you find the possible cause of the problem. Because each conclusion and possibility must be documented, this approach involves a lot of paperwork.
* A further challenge is determining which devices to start examining first.

**Top-Down Troubleshooting Method**

* In top-down troubleshooting you start with the end-user applications and move down through the layers of the OSI model until the cause of the problem has been identified.
* You test end-user applications of an end system before tackling the more specific networking pieces.
* Use this approach for simpler problems or when you think the problem is with a software application.
* The disadvantage of the top-down approach is that it requires you to check every network application until you find the possible cause of the problem.
* Each conclusion and possibility must be documented. The challenge is to determine which application to examine first.

**Divide-and-Conquer Troubleshooting Method**

* When you apply the divide-and-conquer troubleshooting approach toward troubleshooting a networking problem, you select a layer and test in both directions from the starting layer.
* In divide-and-conquer troubleshooting, you start by collecting users’ experiences with the problem and document the symptoms. Then, using that information, you decide at which OSI layer to start your investigation.
* After you verify that a layer is functioning properly, you assume that the layers below it is functioning, and you work up the OSI layers.
* If an OSI layer is not functioning properly, you work your way down the OSI layer model. For example, if users can’t access the web server and you can ping the server, you know that the problem is above Layer 3.
* If ICMP error messages are generated and you can’t ping the server, you know that the problem is likely at a lower OSI layer.

## overview of Network troubleshooting tools.

**Troubleshooting Tools**

* A wide variety of software and hardware tools are available to make troubleshooting easier.
* These tools may be used to gather and analyze symptoms of network problems. They often provide monitoring and reporting functions that you can use to establish the network baseline.

**Software Troubleshooting Tools**

* Software troubleshooting tools are constantly being produced and are evolving. The following are categories of tools available:
* ■ Network management systems (NMS)
* ■ Knowledge bases
* ■ Baselining tools
* ■ Protocol analyzers

**NMS Tools**

* Network management system (NMS) tools include device-level monitoring, configuration, and fault-management tools.
* These tools can be used to investigate and correct network problems. Network monitoring software graphically displays a physical view of network devices, allowing network managers to monitor remote devices without actually physically checking them.
* Device management software provides dynamic status, statistics, and configuration information for switched products.
* Commonly used network management tools are CiscoView, HP OpenView, SolarWinds, and WhatsUp Gold.

**Knowledge Bases**

* Online network device vendor knowledge bases have become indispensable sources of information.
* When vendor-based knowledge bases are combined with Internet search engines, a network administrator has access to a vast pool of experience-based information.
* Most vendors provide similar knowledge bases with varying levels of accessibility, usability, and usefulness.
* The Cisco Support page is comprehensive and useful. However, you must ensure that you are familiar with and accustomed to the resources and tools made available.
* Periodically revisit knowledge base sites, because the resources are constantly evolving.

**Baselining Tools**

* There are various approaches to baselining a network, and all of them involve using special

software.

* These software packages have features to automatically draw network diagrams, keep network software and hardware documentation up-to-date, and help measure network bandwidth use.

**Protocol Analyzers**

* A protocol analyzer captures network traffic as it traverses an identified interface.
* This captured traffic can then be displayed to reveal the field contents of frames, packets, and segments in a relatively easy-to-understand format.
* Most protocol analyzers can filter traffic that meets certain criteria so that, for example, all traffic to and from a particular device can be captured.
* Filtering is also very useful when you want to follow a specific packet stream.

**Hardware Troubleshooting Tools**

* Like software troubleshooting products, hardware troubleshooting products are also constantly being produced and evolving. The following are categories of tools available:
* ■ Network analysis module (NAM)
* ■ Digital multimeters
* ■ Cable testers
* ■ Cable analyzers
* ■ Portable network analyzers

**Network Troubleshooting**

* It is nearly impossible to troubleshoot any type of network connectivity issue without a network diagram that identifies IP addresses, network addresses, routing domains, and infrastructure devices such as routers, firewalls, switches, access points, servers, and so on.
* Generally, two types of network maps should be available:

■ Physical topology

■ Logical topology

* A physical network diagram shows the physical layout of the devices connected to the network.
* You must know how devices are physically connected to troubleshoot problems at the physical layer, such as cabling or hardware problems.
* Information recorded on the diagram typically includes

■ Device type

■ Model and manufacturer

■ Operating system version

■ Cable type and identifier

■ Cable specification

■ Connector type

■ Cabling endpoints

* This information is used primarily to troubleshoot physical problems with devices or cabling.
* It is also required when conducting network upgrades and future planning.
* In addition to the physical network diagram, some administrators also include actual photographs of their wiring closets as part of their network documentation.
* A logical network diagram shows how data is transferred on the network. Symbols are used to represent network elements such as routers, servers, hubs, hosts, VPN concentrators, and security devices. Information recorded on a logical network diagram may include

■ Device identifiers

■ IP address and subnet mask

■ Interface identifiers

■ Connection type

■ DLCI for virtual circuits

■ Site-to-site VPNs

■ Routing protocols

■ Static routes

■ Data-link protocols

■ WAN technologies used

**E-COMMERCE**

# Explain Concept and Terminologies

**What is E-commerce?**

Electronic commerce (ecommerce) refers to companies and individuals that buy and sell goods and services over the Internet. Ecommerce operates in different types of market segments and can be conducted over computers, tablets, smartphones, and other smart devices. Nearly every imaginable product and service is available through ecommerce transactions, including books, music, plane tickets, and [financial services](https://www.investopedia.com/ask/answers/030315/what-financial-services-sector.asp) such as stock investing and online banking.

**Type Of E-Commerce:**

Following are the most traditional types of e-commerce models and examples of what they mean:

1. Business to Consumer (B2C):

B2C e-commerce is the most popular e-commerce model. Business to consumer means that the sale is taking place between a business and a consumer, like when you buy something from an online retailer.

1. **Business to Business (B2B):**

B2B e-commerce refers to a business selling a good or service to another business, like a manufacturer and [wholesaler](https://www.the-future-of-commerce.com/2021/04/22/what-is-wholesale-distribution-definition-examples/), or a wholesaler and a retailer. Business to business e-commerce isn’t consumer-facing, and usually involves products like raw materials, software, or products that are combined. Manufacturers also sell directly to retailers via B2B ecommerce

1. **Consumer-to-business (C2B)**

is a type of e-commerce in which consumers make their products and services available online for companies to bid on and purchase. This is the opposite of the traditional commerce model of B2C.

A popular example of a C2B platform is a market that sells royalty-free photographs, images, media and design elements, such as iStock. Another example would be a job board.

1. **Mobile e-commerce**

([m-commerce](https://www.techtarget.com/searchmobilecomputing/definition/m-commerce)) refers to online sales transactions using mobile devices, such as smartphones and tablets. It includes mobile shopping, banking and payments. Mobile [chat bots](https://www.techtarget.com/searchcustomerexperience/definition/chatbot) facilitate m-commerce, letting consumers complete transactions via voice or text conversations.

# Technologies Involved in E-commerce

**Web server:**

Web servers are computers that deliver web content and hold a live copy of which ever webpage a user accesses, making it available to anyone who uses the internet

**Web authoring software:**

A web authoring software provides users with a set of tools which allows them to be able to create web pages of their choice, and simplifying the process which makes everything less technical.

**Browser:**

Software that allows users to access the internet and enables them to view web pages, images, and videos. The browser is able to run when the web server sends information to the browser and it displays the results back on-screen. There are different types of browsers that users can install and use, for example: Microsoft Internet explorer, Google Chrome, or Mozilla Firefox.

**Internet connection:**

Internet connection allows users to access internet services. It connects computer terminals and computers along with mobile phones and also computer networks all to the Internet, giving them admission to internet services.

**Domain name:**

People who use the internet will notice that they all have an IP address. This is based on which server hosts it. Although one user would have one IP address, as Google has many of web severs, Google would have plenty of other IP addresses. Because Domain named have been invented, it is easier to type the domain name rather than having to remember a certain IP address. Businesses benefit more with domain names as they would know that customers would find it hard to remember IP addresses. For example, typing www.ebay.co.uk is far more easier than remembering a 9 numbers referring to the website.

**Programming language:**

When it comes to web pages, they are regularly written in HTML or in a different type of HTML like XHTML. When using HTMLs other languages can be used within it for example: PHP, ASP, and JavaScript. As HTML can’t provide any capabilities for e-commerce, other languages would have to be used for example like ASP or PHP, which allow online payments to be made.

**Database:**

Websites that have an e-commerce system usually store customer records and other types of businesses information, and their catalogue of products. These things that are stored in the database are not usually seen by the customer as they are all stored somewhere else. Organisations that create these databases would use a language called MySQL in order to create them or an application like Oracle. When things on their websites need changing, for example a changing the price of an item, then the organisation can simply just change it in the database

**Web server software:**

Web server applications are ran on web servers that allow making web pages easier. For example, using FTP (file transfer protocol) would make uploading webpages onto websites much easier, whereas using programs like CuteFTP are more user friendly

# Impact Of Introducing E-commerce to the Society

**Global market place:**

Customers can buy products online due to e-commerce which allows global marketplace to develop. This enables customer to buy products online from all around the world right in their own homes without leaving their houses. For example if a customer were to run out of re-writable CDs and would like more, instead of going out to a shop and buying it from there, they can open up a websites like eBay, amazon or HMV and order them online and have them shipped to them wherever they are in the world.

**24/7 trading:**

As this is online shopping, one benefit is that e-commerce means twenty-four hour shopping at any time of the day and this benefits customers as they’re able to buy anything they wish when they want to without visiting any stores, for example a customer could even order a meal for them to eat on a website like hungryhouse.co.uk, and have it delivered directly to their door.

**Relatively low start-up and running costs:**

When it comes to setting up a store, finding a location is needed, purchasing stock and hiring staff and paying utility costs such as electricity and water. For businesses that are new all of the costs would have to be paid upfront and so this means the start-up costs are high. Online stores don’t have high initial costs as there are no premises to purchase and not much staff.

**Competitive edge:**

If there are two businesses that sell the same products and one is online based and the other is store based, the online store could be more successful as it allows customers to be more flexible with their choices of ordering what they please and so this reaches a global market. Online shops like Asos or New Look, have an e-commerce system that customers can scroll around on their website and select clothing’s to buy, whereas Primark, although it has an online presence giving customers an idea of what they sell, they do not have an e-commerce system, and so customers would have to go in store to buy their products. This gives businesses like Asos or New Look a benefit of attracting more customers because they do deliveries gaining that business some profit.

**Search facilities:**

When shopping in stores such as Sainsbury’s or Tesco’s, if a customer wants to find a specific item they want to purchase they would have to walk all over the shop down the aisles to find where their item can be found, or simply ask a member of staff to assist them to where that product would be, whereas e-commerce provides customers with a simple search tool where they can be able to search for their item without scrolling through pages and pages of the website. This also saves time and is more efficient

**Pricing opportunities:**

As bricks and clicks organisations have both a store and online website that customers can shop online from, when it comes to the online store, although they may have the same products as the normal store that customers go to, there may be some special online offers like discounts that customers and benefit from (this also happens in store based businesses when they reduce the price of specific items). For example, Amazon and eBay tend to send their registered customers emails giving them recommendations and offers from products that they have previously bought, or would simply have the offers on the front page of their website trying to attract customers to click it and buy them, whereas if It were in store they would keep those specific products that have offers on the online store the exact same price

**Gathering customer information:**

Organisations use the method of using loyalty cards to gather and track information about their customers. They use this method in order to increase their profit as they know what types of products interest their customers. When it comes to online shopping, customers would have to register in order to buy products from (for example) eBay, and by doing so when they purchase their products, eBay would keep this in their records for whenever customers go back to that website, they would have recommended products for them based on their previous purchases. Also by the customers previous purchases eBay would send emails sending their customers offers or recommendations attracting them back to their website.

**Alternative income:**

Businesses with e-commerce gain more profit by displaying pay-per-click advertising. Although it may not be fortunate for some customers, the customers that tend to click on them (even by accident) make that business gain some money for their business, as it has still been previewed by the customer.

**Pay Per Click:**

PPC stands for pay-per-click, a model of internet marketing in which advertisers pay a fee each time one of their ads is clicked. Essentially, it's a way of buying visits to your site, rather than attempting to “earn” those visits organically. **Search engine advertising** is one of the most popular forms of PPC.

**CPC (Cost per click):**

Cost per click (CPC) is a paid advertising term where an advertiser pays a cost to a publisher for every click on an ad. CPC is also called pay per click (PPC). CPC is used to determine costs of showing users ads on search engines, Google Display Network for [AdWords](https://sproutsocial.com/insights/adwords-quality-score/), social media platforms and other publishers. CPC is a significant factor in choosing bidding strategies and conversion bidding types to maximize clicks relative to budget size and target keywords.

# Potential risks to E-commerce System:

## Potential risks to an organisation of committing to an e-commerce system

**Consumer trust:**

Customers sometimes feel a bit wary of shopping online as it involves providing personal details. Some customers may feel worried that their personal details may be stolen and used as identity theft and that their card details could be used as fraud. This could be a risk on customers as it lowers the confidence customers have with shopping online, and also for the online business as it lowers their profit due to their customers being unconfident when it comes to shopping online.

**Lack of human contact:**

When it comes to online shopping, some customers would feel a little insecure about the fact that they aren’t able to speak or interact with any staff workers like they’d usually do in a normal walk-in store, and so they’d rather prefer to go and shop in the normal stores rather than online. When it comes to shopping online for clothes, customers become unsure over this decision as they aren’t able to try their clothes online as they would if they’d visit that shop.

**Delivery issues:**

Customers, who shop in traditional stores, select which products they wish to buy and purchase them, taking them home immediately, whereas online shopping a customer would have to wait a few days to receive their deliveries. For example if a customer were to use Sainsbury’s shopping online, the customer would even have to pay extra for their items to be delivered to their doors, and on top of that would still have to wait up to a certain amount of days for them to be ordered (or they could simply pay more for the next day delivery).

**International legislation:**

Businesses who sell products online have to not only follow legislations, but laws in which the countries of the customers that live there. For example, in the United States, people must be over the age of 21 to be able to buy alcohol, whereas in the UK the age limit to buy alcohol is 18. If an online business were to sell alcohol online and it was an American customer buying from an online UK shop where the age limit is 18, and they happen to be under 21 but over 18, then there would be a decision in which law to follow.

**Product description problems:**

As customers scroll around on e-commerce sites, they worry about the accuracy of the websites how the description based on the products that they sell aren’t completely right, for example when going on a website to look for and purchase a yellow coloured toaster, in the image it could be seen as yellow and would be described as yellow, but when they actually buy it and receive it, it suddenly turns out that it was in fact orange. This tends to put customers off from buying online from e-commerce websites

**Security issues:**

Shopping online requires customers’ personal details being used. This usually makes some customers feel uncomfortable as they think that their personal details aren’t safe, or even that the online organisation could use it in an unauthorised way and that they can’t possibly rely on the security of the website. They may have probably heard of phishing how criminals can access and steal their personal details, or how their money can be taken from their accounts, and so it that draws them away from online shopping and from returning to that website.

# Methods to promote an e-commerce system

**Use of effective search engines:**

Using search engines so that customers can find e-commerce sites to shop can be very useful. When a customer types in a search, that specific search engine (whether it is Google or Ask Jeeves) will provide that user with the best results, resulting in the best e-commerce websites

**Spider:**

In order for search engines to carry out web searches, and to find e-commerce sites, spiders are used to crawl over the web and fetch web pages, providing users with the best results relation to whatever they have searched.

**Meta Tags:**

Whenever a spider goes over and fetches these web pages, Meta tags are used along with HTML tags which provides information based on that page. These tags come in codes, and are not visible to the user.

Without the use of Meta tags, spider will carry out searches based on their guess on what the user has asked for, resulting in poor matches to the search.

What Treading Ahead can do in order to make sure their website is featured in searches for e-commerce sites, they can pay that search engine to feature their website as part of a sponsored link, therefore making customers view their website as a reliable site and top search.

**Newsgroups and forums:**

Treading Ahead can use newsgroups to set up bulletin boards via Usenet, and set up messages that they can send to internet users, such as trying to get them to visit and buy products from their website. This can attract large amounts of customers to their website. They can also create different topics based on their company, and send messages through there. They can even decide to set up a forum on their own website to communicate with customers online, and have discussions of what products they sell, or what products customers would like to see them sell, for example a new brad of trainers such as Adidas, and so they can take in this information and improve their organisation/website.

**Banners and pop-ups:**

Another way of advertising e-commerce websites is by using banners and pop-ups. Treading Ahead can benefit in using these as it means that they can place banners onto other popular websites for example like a social networking site called Facebook. They can be able to place a banner on Facebook and have their website advertised on their, and it would be clearly seen by Facebook users as they scroll on the page. They can also benefit in using pop-ups that pop-up onto of the web page that a user is already using. Although this can be annoying, company’s still chose to use this method.

**Site Name:**

If Treading Ahead would want customers to easily remember their website, they must choose/have a memorable domain name that can be remembered easily. Choosing a short domain name would be essential as it could be remembered well, whereas having a long one can also be quite forgetting, but if it were to be long and catchy, then it can still be memorable. As the organisation is called Treading Ahead, having the website’s domain name as [www.treadingahead.com](http://www.treadingahead.com/) would be fine, as it won’t really be forgotten as it resembles the company’s name.

**Direct marketing:**

Organisations use direct marketing so that they can advertise their products directly to customers through email. They send emails to people who have already registered and ordered products from their website. Once a customer has registered with Treading Ahead’s website in order to have their orders delivered to them, their email addresses would be kept in the company’s database, and would be used to send through promotions and recent products that are being sold within that company. Treading Ahead can use a customers’ recent purchase, such as a pair of simple Nike trainers, the company will record this down, and in return would send the customer an offer relating to that product, and for example something related to Nike such as a pair of Nike Air Jordans. These type of emails can sadly be considered as junk email if the customers aren’t bothered with them, whereas if they are interested in them, then it is still an effective method for the company.

**Effective user interface:**

Whilst having an e-commerce website, it is important that a useable and reliable interface is used. For example, Treading Ahead should use a simple and easy interface that a customer can use easily with no difficulties so that they can enjoy using the site, and would continue to go back to using it, whereas if the interface was to be difficulty and uneasy to use, then a customer wouldn’t find it simple to use and wouldn’t want to return to the website so that they can shop for their goods. Treading Ahead should use a simple interface so that they can attract customers, using a hard one could result in them losing customers.

**Establishing customer loyalty in a virtual environment:**

As some people tend to not trust using e-commerce websites, this means that Treading Ahead would still have to persuade customers to shop on their online shop. They can do this by personalising their website in a way that customers would see it to be trustable, when it comes to their products they can give clear descriptions and pictures to what is being sold, and can overall have great security on their website.

# How security measures in e commerce can be overcome

**Prevention of hacking:**

The issues that all e-commerce sites have to deal with is mainly hacking. If a hacker were to hack Treading Ahead and completely change information, the layout and design, and steal all information from the website, no consumer would want to use their website, and it would therefore be shutdown.

In this case, Treading Ahead would need to prevent hacking in order to have secure customer information, and not having them available for hackers to access. If a hacker were to be able to access customer information, many problems can occur such as fraud, identity theft, and stealing money from having access to bank information. To prevent hackers accessing Treading Ahead’s databases and information and data that are to be only seen by certain staff, specialist software would be required to be installed onto the system so that it can be able to check and look at ports that are on a computer and see if they are open or closed. If ports are found open, it’s gives hackers access to the computer system and allows them to view information. For example if Treading Ahead was to leave a port open, and a hacker has the same protocol as Treading Ahead, they can use it to send and transfer data across the network, stealing plenty of information. To prevent this Treading Ahead should make sure that they close all ports so that hackers cannot gain access into their e-commerce website, and not steal information.

**Viruses:**

Viruses occur as a problem for e-commerce websites as it can attach itself onto emails and programs, being able to replicate and cause problems for computer systems and web servers. If a virus were to be planted onto the website and a customer were to visit the website in order to purchase something online, customers would be warned by their search engines not to enter that website, an antivirus would too alert the customer not to enter the website, therefore making the site not trustable. If customers cannot trust the website they will not use it to purchase goods. For Treading Ahead to be able to prevent viruses, they would have to install antivirus software not only to all their business computers, but web servers too. Antivirus software is able to detect and prevent viruses from attacking a computers system, and with that Treading Ahead should update their antivirus every day, keeping out viruses. As new viruses are made and found every day, it is the antivirus’ job to prevent all virus attacks, keeping Treading Ahead’s computer system and web server safe from viruses.

**Identity theft:**

Using an e-commerce website means that a consumer is required to enter their personal details and bank details in order to order and receive their items purchased. Due to being required to enter personal information into these websites, Identity theft has been a problem that occurs when a criminal steals a customers’ details and claims it to be their own, resulting in this being a difficult issue to tackle. It is mainly detected after the victim notices that they have to pay for purchases made online or by card that they have not paid for, and the thief could also use their details to claim money that belongs to the victim. In order to prevent identity theft, it would be ensured that Treading Ahead are to increase the security on their website and make sure that customers change their passwords regularly.

**Firewall impact on performance:**

Firewalls are installed so that it can block out any unwanted access from accessing private networks. It controls exactly what goes in and out, and is to protect a computer and computer network, allowing only authorised accesses to access the data. Firewalls set up gateways which allows only authorised traffic to access the network, and any other traffic that are trying to access the network are to be inspected. If a customer were to go onto the Treading Ahead website and passes through the sites firewall, it will not allow the customer to see the scripts running on the page, preventing viruses and hackers attacking their system.

**Secure sockets layer:**

Websites having an SSL (Secure Sockets Layer) ensures customers that they have a secure communication whilst using the internet. The SSL is a protocol that is made specifically for being able to send information over the internet. Treading Ahead would need to use an SSL on their website as it secures customers when they access their account online or make online payments. Having an SSL provides endpoint authentication, which in this case means that the server and user are to identify who they are; the customer would do so by logging into their online account on Treading Ahead’s website. Treading Ahead would then need to use certificate-based authentication so that unauthorised accesses cannot read data entered into their site.

**HTTPs:**

HyperText Transport Protocol Secure (HTTPS) is the protocol used on many websites on the internet. If Treading Ahead were not to have an HTTPS, data entered into their website may not be protected as it is the HTTPS that protects data entered into websites. It would be best that Treading Ahead have a secure HTTPS so that when a customer enters their bank details into their website it would be protected, by the websites HTTPS. The way in which HTTPS protects data, is that the protocol uses encryption to protect the data, ad so it is ensured that Treading Ahead have an HTTPS to protect a customers’ bank details when entered into their website.

**RSA Certificates:**

RSA certificates are a way of using encryption for security, so that people accessing the website are all identified by a digital certificate, attached with a digital signature. Using an RSA certificate confirms the identity of a sender or recipient. The reason why Treading Ahead would need an RSA certificate in order to overcome security is because it provides security when it comes to customers using their bank cards to purchase products on their site.

**Strong passwords:**

E-commerce systems and web servers are both informed to use strong passwords so that no unauthorised accesses can access them; this is the same for all computer users. Strong passwords must contain both letters and numbers along with capital and lowercase letters, symbols included and should be more than eight characters long. As an e-commerce website draws in many hackers, it is ensured that Treading Ahead create a strong password for both e-commerce website and web server they use. The stronger the password, the less hackers can guess them, making them move on and away from the website.

**Alternative authentication methods:**

A common method of authentication is the use on digital signatures which verifies a user’s identity. It allows a user to be able to authenticate a document over the internet. For example, instead of a customer signing a document in the traditional way by using pen and paper, they can do it online using their digital signature to be able to sign documents. Another method could be the use of passwords. Using usernames and passwords identify a user signing onto a website, and if for instant signing into a banking site, extra security information are used to identify the user even more, and when entered correctly they are able to see their banking information, whereas if incorrect they can not access the website.

# Regulations governing e-commerce

**Data Protection Act 1998:**

Every organisation that stores personal information electronically on a computer is to follow the data protection act making sure that all information (Names, Addresses, telephone numbers etc.) stored is kept securely, and by following the eight principles. The effect that the data protection act has on e-commerce is that all online businesses must follow the principles when it comes to storing customers’ personal information that they use, whether it is to deliver products to them or use their contact addresses for emails, for example when a customer orders products from Treading Ahead’s e-commerce website, it is necessary for them to give that website their personal details like their name address and telephone number, along with their credit card details if they want their items ordered to their homes. When an e-commerce website receives these types of information from users signing up to their website t get deliveries, it’s a must for them to keep their information secure, as well as not sharing the details or using it for any other purposes.

**Computer Misuse Act 1990:**

This legislations are created in order to protect sensitive data that are stored on computers, preventing hackers and computer viruses’ from having access to the data. The offences that come with the computer misuse act are: Unauthorised access to computer programs or data, unauthorised access with the intent to commit further offences and unauthorised modification of computer material. Treading Ahead would have to make sure that their e-commerce site is not prone to hackers being able to access their website and databases, stealing customers’ details. They would have to make sure that their site is protected well enough for hackers not to gain access into their websites.

**Consumer Credit Act 1974:**

E-commerce websites require customers to pay for their products with the use of a credit/debit card. With the consumer credit act, it allows consumers to have rights to be able to pay off credit early, to be able to look at credit files, and a ‘cooling-off period’ of five days, if an order placed is to be cancelled. This may benefit the customer but can be a drawback for a company as even if the purchase is completed, the customer may still want a refund. The Consumer Credit Act protects payments that are made, but if the customer is not able to carry out this purchase, the e-commerce website will still receive the money from the bank and the customer will receive their item ordered.

**Trading Standards:**

Ensure that consumers and businesses maintain fair trading as well as having to follow legislations that are enforced such as: Trade descriptions act (1968), Prince marketing order (2004) and consumer protection act (1987). Trading standards have to handle problems like counterfeit goods, for example if an e-commerce website were to sell alcohol online they can only be able to sell it to a customer (in the UK) that is aged 18 and over, this goes the same for in a traditional store, alcohol cannot be purchased by someone under 18. It is ensured that Treading Ahead is to describe their products clearly, and to provide clear images of their products. This is important because customers who look to buy their products only see pictures available and base this on their judgement of buying the product, rather than just on the description

**Freedom of Information Act 2000:**

The freedom of information act ensures that the public have “the right to know” if they were to request information based on public bodies such as the government and legal entities like businesses. For example if someone would want to request information from Treading Ahead, the freedom of information act would allow a person to request a copy of any official information or communication, whether electronic, paper based or published by other means.

**Copyright Legislation:**

Whether it is software, music, books or videos (in this case its shoes & trainers in Treading Ahead’s store), all would be copyrighted by the law. It is forbidden to share these on a network, or even to a friend as well as making copies and selling them. The copyright legislation effects e-commerce as many people of the public are downloading music and videos, along with un-paid for software’s with the use of the internet providing them with these downloads. Even shoes and trainers can be copyrighted and sold as counterfeit goods online, dropping the sales of Treading Ahead’s as customers would see these items and buy them else where but cheaper. Having these items copyrighted would allow the owners to have control on how they are distributed

**E-Commerce Regulations:**

E-commerce regulations can be the same as an in-store regulation. For example if a customer were to purchase an item in a store, it could be an item of clothing, they would receive a receipt with the amount spent on that item, and would have a 30 day grantee if they wish to return or exchange this item, whereas on the e-commerce website when an order is placed they must send an invoice attached with the order and if a customer were to return the product, they would have the same rights as they do if they were doing the same for an in-store purchase

# Social implications of e-commerce on society

**Changing customer perspective:**

With e-commerce, some customers may be afraid of using e-commerce sites (because of issues such as fraud, and internet scams, identity theft etc.) to purchase products online. Issues like these effect e-commerce websites as they would have to change their customer’s perspectives on buying products online, as well as just their specific e-commerce website. In order to attract customers to e-commerce websites such as eBay, Amazon, or Play.com, the website should promise to **provide added value**

by provide added value:

products that the e-commerce website sells could have lower prices than in original stores, for example, a book can be £7.99 in an traditional store, but on the e-commerce website it can be sold for £4.99, but should also offer to sell products that cannot be bought in traditional stores, luring customers in to buy these products from their website.

By **providing good service** :

An e-commerce website should also change a customers’ perspective by **providing good service** as a traditional store would. The e-commerce website should offer a 24-hour delivery time along with a small additional cost

**ease and security:**

When it comes to ease and security, an e-commerce website is open 24/7 which benefits customers as this means 24/7 trading, a customer can shop using this website as any time of the day when they wish to. E-commerce websites make it easier to search for products customers want to buy as they offer a search tool, allowing customers to search and select which products they’d like to buy, whereas in a traditional store this process would be longer as customers would have to walk up and down the store searching for items, but e-commerce websites are easier to shop with.

**Economic and social impact due to speed of changes:**

As e-commerce becomes more popular, and is threatening traditional businesses, some e-commerce websites release products before they’re released in traditional stores, for example customers are able to pre-order items before they come out, and when they do come out they would get them on the day released. The speed of change impacts customers as prices can easily be changed on e-commerce websites as promotions are provided and sales take place, benefiting the customer.

**Bricks & Clicks – integrating high street and online presence:**

Before e-commerce was introduced, people were used to shopping at traditional stores in order to do their shopping. Nowadays as e-commerce if highly popular, people are able to go online on those specific shops and purchase their items online and have it delivered to their doors, for example Sainsbury’s have an online store for customers to process groceries as well as other products such as toiletries and other items and could pay for them to be delivered to their homes. As Sainsbury’s has both a traditional store and e-commerce site it is a brick and click organisation.

**Benefits for customers:**

As customers no longer have to leave their homes in order to do shopping because they have e-commerce websites to use in order to shop, this is called remote shopping, customers can purchase items online instead of going out to buy them in traditional stores. This is a benefit for a customer who (for example) lives in a distant place from their local stores and finds it difficult to travel to the stores to carry out their shopping, this could go by people who are housebound or simply do not have cars to travel to distant places.

Being able to purchase products online 24/7 benefits customers as this means they can shop at any time of the day, this could benefit those especially who have tight schedules at work and wouldn’t have time to visit traditional stores, and so instead they are able to purchase items online, even exactly where they are whether it is at home or if they are ordering it from their workplace.

Most e-commerce websites have plenty offers such as online discounts that wouldn’t usually be found in physical stores. For example in a clothes store such as New Look, if in a physical store a customer were to view clothes in that shop, some of the prices would be their original price, whereas if they were to look for that item online, they could see that that item has “50% off” or has been reduced from “£18.99 to £12.99”. This can be a massive benefit as customers tend to save money by these discounts.

## Drawbacks:

**payment security:**

When it comes to drawbacks of e-commerce, **payment security** can be an issue as some customers feel that the website is unsafe and that they cannot trust it. Customers may feel awry of inputting their personal details into e-commerce website as they may be afraid of issues such as identity theft or fraud and even their purchased items not being delivered to them

**accessing quality and fit without actual product:**

Moreover, when it comes to **accessing quality and fit without actual product**, customers may feel that not being able to try their purchased items such as clothing may be an issue as they would be unsure if the piece of clothing would fit them. This goes the same for products like food; some customers would prefer to view their products before buying them. Further drawbacks could be reliance on deliver services

**delivery service:**

As customers place their orders online and expect their goods to be delivered, they have to rely on the **delivery service**. At times deliveries could be delivered to customers late or their items could be damaged, making customers think twice about relying on e-commerce sites for shopping. As their items have to be delivered, some customers may want their deliveries posted at specific times such as for Christmas or a special event, and if their items are delivered late it disappoints the customers.

**Impact on employment:**

**Impact on employment** is a drawback as less staff is hired for the business, an ecommerce business would only need to hire staff to deal with the deliveries, therefore hiring big amounts of staff is unnecessary

**social divide**:

With **social divide**, although it may be a benefit as customers have access to 24/7 trading, some people don’t as they can’t afford to buy a computer or afford to access the internet therefore creating a social divide as not everyone can access and use ecommerce websites.

# Payment systems

**Electronic cheque:**

Using electronic cheques can be done in the same way as a paper cheque, instead of the person signing the check by pen and paper, the person can sign the cheque online. Electronic cheques are mostly used online for online orders and are handled in the same way a regular paper cheque is.

The way in which the customer has to sign an electronic cheque is by using their online digital signature. By using an electronic cheque, it offers great security like protective measures such as authentication and digital signatures. The use of electronic cheque makes transferring funds easy, as they are quickly processed online compared to sending paper cheques through the mail. Although electronic cheques are an efficient way of paying for orders online, there can also be some drawbacks like the fact that by signing electronic cheques online whilst purchasing goods is a slower process than debit or credit cards as they do not require digital signatures, and the goods are only sent off when the cheque is fully processed. When electronic cheques are received by from the payer to the payee, it would take some time for the business to receive the money, and would have to wait for it to come through before sending the payer their goods. Another drawback can also be that some businesses online may charge extra for the use on electronic cheques which may annoy customers.

**PayPal:**

When making payments online, some customers benefit from using PayPal as it ensures a safer way of transferring money online. It is safe and it is also a fast system

If a user were to register to PayPal and allow the website to store their bank details for late use, this would mean that purchasing goods online would be faster for users who register with PayPal, they would be able to make orders more speedy as it would only require a few clicks due to the fact that all their details are already registered with PayPal. After placing orders, PayPal carries out a customers’ payment quickly and directly from your bank account in a quick and safe way. Even if not registered to PayPal and a customer were to use PayPal to purchase goods online, PayPal would never share a customers’ information online or with anyone, they have a secure SSL and are a safe website that customers use daily when online shopping. If a customer is registered, all they need is their email address and password to carry out payments, and then they will quickly be done in just a few clicks. At any time, PayPal could decide to freeze a users account, making it inaccessible to the user, as they will not be able to use their account due to PayPal freezing their balance because they are protecting it from fraud, trying to investigate the account for any suspicious behaviour. When an account is frozen by PayPal, this may take up to some amount of weeks or even months. PayPal can also put your account on hold when they feel like doing so. This means that a user will not be able to access their account or make withdrawals. For a seller using PayPal, they may limit the amount of money you are able to spend within your account if they feel that you have broken the terms of service, or if they suspect general suspicious activity, they may hold your account.

**NoChex:**

NoChex is a way of being able to purchase products online. NoChex provides customers who use their online payment system with easy to use payment services, being able to handle online transactions for users who have debit cards. The benefits of using NoChex is that as a person opening an account it is an easy yet quick process and the fees are quite low. When transferring money from NoChex to your bank account it is a free process and only takes up to 2-4 days for the money to get into your bank account. Another benefit is that NoChex is very secure when it comes to accessing account, for example it provides high security by asking the user to enter different types of passwords or memorable questions. NoChex also carries out a speedy transaction process which is both fast, and free. There are only a few disadvantages of using NoChex which is the fact that people with NoChex accounts have to pay fees in order to receive money

**Credit cards:**

A credit card is a card that stores a good amount of money from a company, given to someone who wishes to use the money to purchase goods with it, although they would have to pay all the money back. The benefit of using a credit card is a quick payment method that it gives customers quick access to cash allowing the customer to spend cash on items that they wish to buy. When taking out transactions, credit cards are secure by the websites’ SSL. Also, if a credit card is lost then the card holder can cancel the credit card. Credit cards have more protection than a debit card, for example when purchasing items, if the company has an issue, such as processing the purchases, or a faulty in the system, the card holder will still be able to claim their money back. Also the credit card is secured if it gets lost and someone uses it as an act of fraud, if this happens the credit card provider will refund the money spent. Another advantage would be that some credit card companies allow costs to be paid interest-free, meaning that the holder has plenty of time to pay the money back. By using a credit card, the person would have to pay back all the money that they have spent in a certain amount of time, and if they were to go over, for example a month, interests are added making the customer pay more than they have spent, causing problems such as debt. Another drawback would be that card holders would have to keep track of all their transactions made whilst purchasing products with their card, so that they are able to know exactly how much they have spent in order to pay it back.

**Debit cards:**

A debit card is money stored in an account that has been earned, such as from a job, belonging to the holder which allows the them to transfer money which is in their bank accounts and take out transactions in order to pay for goods. Benefits of using a debit card to pay for purchased goods is that transactions are recorded by the bank provider, this allows customers that pay with debit cards to keep track of what they have spent with their cards. The money is theirs, as it is a debit card, this means that the customer buying with a debit card isn’t using borrowed money. Apart from providing personal details, whilst using a debit card to carry out online orders, the process only requires information that is on your card to be inputted into the website so they can carry out the purchase. Drawbacks of using a debit card is restricted spending. As it is money that someone has earns such as from a job, unlike a credit card where the holder can spent the amount of cash on anything they wish, a debit card holder has to carry out purchases restrictedly, based on the amount they have inside the account to spend. The process can be a bit slower than having to pay by cash, as it means typing in pin numbers, and waiting for the transaction to be processed. When online shopping, paying with a debit card comes with extra fees.

**Web Server:** Web servers are computers that deliver web content and hold a live copy of which ever webpage a user accesses, making it available to anyone who uses the internet.

**Web authoring software:** A web authoring software provides users with a set of tools which allows them to be able to create web pages of their choice, and simplifying the process which makes everything less technical.

**Browser:** Software that allows users to access the internet and enables them to view web pages, images, and videos. The browser is able to run when the web server sends information to the browser and it displays the results back on-screen. There are different types of browsers that users can install and use, for example: Microsoft Internet explorer, Google Chrome, or Mozilla Firefox.

**Internet connection:** Internet connection allows users to access internet services. It connects computer terminals and computers along with mobile phones and also computer networks all to the Internet, giving them admission to internet services.

**Domain name:** People who use the internet will notice that they all have an IP address. This is based on which server hosts it. Although one user would have one IP address, as Google has many of web servers, Google would have plenty of other IP addresses. Because Domain named have been invented, it is easier to type the domain name rather than having to remember a certain IP address. Businesses benefit more with domain names as they would know that customers would find it hard to remember IP addresses. For example, typing www.ebay.co.uk is far more easier than remembering a 9 numbers referring to the website

**Programming language:** When it comes to web pages, they are regularly written in HTML or in a different type of HTML like XHTML. When using HTMLs other languages can be used within it for example: PHP, ASP, and JavaScript. As HTML can’t provide any capabilities for e-commerce, other languages would have to be used for example like ASP or PHP, which allow online payments to be made

**Technologies:** hardware and software eg web servers, browsers, server software, web authoring tools, database system; networking eg TCP/IP addresses, ports and protocols; considerations eg domain names, multiple registration of domains (.com as well as.co.uk), programming requirements, download speeds, browser and platform compatibility

**Programming language:** When it comes to web pages, they are regularly written in HTML or in a different type of HTML like XHTML. When using HTMLs other languages can be used within it for example: PHP, ASP, and JavaScript. As HTML can’t provide any capabilities for e-commerce, other languages would have to be used for example like ASP or PHP, which allow online payments to be made

**Database:** Websites that have an e-commerce system usually store customer records and other types of businesses information, and their catalogue of products. These things that are stored in the database are not usually seen by the customer as they are all stored somewhere else. Organizations that create these databases would use a language called MySQL in order to create them or an application like Oracle. When things on their websites need changing, for example a changing the price of an item, then the organization can simply just change it in the database.

**Web server software:** Web server applications are ran on web servers that allow making web pages easier. For example, using FTP (file transfer protocol) would make uploading webpages onto websites much easier, whereas using programs like Cute FTP are more user friendly.

* **Global market place:** Customers can buy products online due to e-commerce which allows global marketplace to develop. This enables customer to buy products online from all around the world right in their own homes without leaving their houses.
* **24/7 trading:** As this is online shopping, one benefit is that e-commerce means twenty-four hour shopping at any time of the day and this benefits customers as they’re able to buy anything they wish when they want to without visiting any stores
* **Relatively low start-up and running costs**: When it comes to setting up a store, finding a location is needed, purchasing stock and hiring staff and paying utility costs such as electricity and water.
* **Competitive edge:** If there are two businesses that sell the same products and one is online based and the other is store based, the online store could be more successful as it allows customers to be more flexible with their choices of ordering
* **Search facilities:** When shopping in stores such as Sainsbury’s or Tesco’s, if a customer wants to find a specific item they want to purchase they would have to walk all over the shop down the aisles to find where their item can be found.
* **Pricing opportunities:** As bricks and clicks organisations have both a store and online website that customers can shop online from, when it comes to the online store, although they may have the same products as the normal store that customers go to, there may be some special online offers like discounts that customers and benefit from (this also happens in store based businesses when they reduce the price of specific items).
* **Gathering customer information:** Organizations use the method of using loyalty cards to gather and track information about their customers. They use this method in order to increase their profit as they know what types of products interest their customers. When it comes to online shopping, customers would have to register in order to buy products from (for example) eBay.
* **Alternative income:** Businesses with e-commerce gain more profit by displaying pay-per-click advertising. Although it may not be fortunate for some customers, the customers that tend to click on them (even by accident) make that business gain some money for their business, as it has still been previewed by the customer.
* **Consumer trust:** Customers sometimes feel a bit wary of shopping online as it involves providing personal details. Some customers may feel worried that their personal details may be stolen and used as identity theft and that their card details could be used as fraud. This could be a risk on customers as it lowers the confidence customers have with shopping online, and also for the online business as it lowers their profit due to their customers being unconfident when it comes to shopping online.
* **Lack of human contact:** When it comes to online shopping, some customers would feel a little insecure about the fact that they aren’t able to speak or interact with any staff workers like they’d usually do in a normal walk-in store, and so they’d rather prefer to go and shop in the normal stores rather than online. When it comes to shopping online for clothes, customers become unsure over this decision as they aren’t able to try their clothes online as they would if they’d visit that shop.
* **Delivery issues:** Customers, who shop in traditional stores, select which products they wish to buy and purchase them, taking them home immediately, whereas online shopping a customer would have to wait a few days to receive their deliveries. For example if a customer were to use Sainsbury’s shopping online, the customer would even have to pay extra for their items to be delivered to their doors, and on top of that would still have to wait up to a certain amount of days for them to be ordered (or they could simply pay more for the next day delivery).

**International legislation:** Businesses who sell products online have to not only follow legislations, but laws in which the countries of the customers that live there. For example, in the United States, people must be over the age of 21 to be able to buy alcohol, whereas in the UK the age limit to buy alcohol is 18. If an online business were to sell alcohol online and it was an American customer buying from an online UK shop where the age limit is 18, and they happen to be under 21 but over 18, then there would be a decision in which law to follow.

**Product description problems:** As customers scroll around on e-commerce sites, they worry about the accuracy of the websites how the description based on the products that they sell aren’t completely right, for example when going on a website to look for and purchase a yellow coloured toaster, in the image it could be seen as yellow and would be described as yellow, but when they actually buy it and receive it, it suddenly turns out that it was in fact orange. This tends to put customers off from buying online from e-commerce websites

**Security issues:** Shopping online requires customers’ personal details being used. This usually makes some customers feel uncomfortable as they think that their personal details aren’t safe, or even that the online organisation could use it in an unauthorised way and that they can’t possibly rely on the security of the website. They may have probably heard of phishing how criminals can access and steal their personal details, or how their money can be taken from their accounts, and so it that draws them away from online shopping and from returning to that website.

**Use of effective search engines:** Using search engines so that customers can find e-commerce sites to shop can be very useful. When a customer types in a search, that specific search engine (whether it is Google or Ask Jeeves) will provide that user with the best results, resulting in the best e-commerce websites. In order for search engines to carry out web searches, and to find e-commerce sites, spiders are used to crawl over the web and fetch web pages, providing users with the best results relation to whatever they have searched. Whenever a spider goes over and fetches these web pages, Meta tags are used along with HTML tags which provides information based on that page. These tags come in codes, and are not visible to the user. Without the use of Meta tags, spider will carry out searches based on their guess on what the user has asked for, resulting in poor matches to the search. What Treading Ahead can do in order to make sure their website is featured in searches for e-commerce sites, they can pay that search engine to feature their website as part of a sponsored link, therefore making customers view their website as a reliable site and top search.

**Newsgroups and forums:** Treading Ahead can use newsgroups to set up bulletin boards via Usenet, and set up messages that they can send to internet users, such as trying to get them to visit and buy products from their website. This can attract large amounts of customers to their website.

**Banners and pop-ups:** Another way of advertising e-commerce websites is by using banners and pop-ups. Treading Ahead can benefit in using these as it means that they can place banners onto other popular websites for example like a social networking site called Facebook.

**Spam:** is the internet equivalent of a direct mailshot. A business can use its own registered customer list (or buy a mailshot list) and then send an advert out in an email to all the people on the list.

**Site Name:** If Treading Ahead would want customers to easily remember their website, they must choose/have a memorable domain name that can be remembered easily.

* **Direct marketing:** Organisations use direct marketing so that they can advertise their products directly to customers through email. They send emails to people who have already registered and ordered products from their website. Once a customer has registered with Treading A head’s website in order to have their orders delivered to them
* **Effective user interface:** Whilst having an e-commerce website, it is important that a useable and reliable interface is used.
* **Establishing customer loyalty in a virtual environment:**

As some people tend to not trust using e-commerce websites, this means that Treading Ahead would still have to persuade customers to shop on their online shop. They can do this by personalising their website in a way that customers would see it to be trustable, when it comes to their products they can give clear descriptions and pictures to what is being sold, and can overall have great security on their website.

**Prevention of hacking**

The issues that all e-commerce sites have to deal with is mainly hacking. If a hacker were to hack Treading Ahead and completely change information, the layout and design, and steal all information from the website, no consumer would want to use their website, and it would therefore be shutdown. **Viruses**

Viruses occur as a problem for e-commerce websites as it can attach itself onto emails and programs, being able to replicate and cause problems for computer systems and web servers.

**Identity theft**

Using an e-commerce website means that a consumer is required to enter their personal details and bank details in order to order and receive their items purchased.

**Firewall impact on performance**

Firewalls are installed so that it can block out any unwanted access from accessing private networks. It controls exactly what goes in and out, and is to protect a computer and computer network, allowing only authorized accesses to access the data.

**Secure sockets layer**

Websites having an SSL (Secure Sockets Layer) ensures customers that they have a secure communication whilst using the internet. The SSL is a protocol that is made specifically for being able to send information over the internet.

**HTTPS**

Hypertext Transport Protocol Secure (HTTPS) is the protocol used on many websites on the internet. If Treading Ahead were not to have an HTTPS, data entered into their website may not be protected as it is the HTTPS that protects data entered into websites.

**RSA Certificates**

RSA certificates are a way of using encryption for security, so that people accessing the website are all identified by a digital certificate, attached with a digital signature

**Strong passwords**

E-commerce systems and web servers are both informed to use strong passwords so that no unauthorised accesses can access them; this is the same for all computer users.

**Alternative authentication methods**

A common method of authentication is the use on digital signatures which verifies a user’s identity. It allows a user to be able to authenticate a document over the internet.

**Data Protection Act 1998**

Every organisation that stores personal information electronically on a computer is to follow the data protection act making sure that all information (Names, Addresses, telephone numbers etc.) stored is kept securely, and by following the eight principles.

**Computer Misuse Act 1990**

This legislations are created in order to protect sensitive data that are stored on computers, preventing hackers and computer viruses’ from having access to the data.

**Consumer Credit Act 1974**

E-commerce websites require customers to pay for their products with the use of a credit/debit card. With the consumer credit act, it allows consumers to have rights to be able to pay off credit early, to be able to look at credit files, and a ‘cooling-off period’ of five days, if an order placed is to be cancelled. **Trading Standards**

Ensure that consumers and businesses maintain fair trading as well as having to follow legislations that are enforced such as: Trade descriptions act (1968), Prince marketing order (2004) and consumer protection act (1987).

**Freedom of Information Act 2000**

The freedom of information act ensures that the public have “the right to know” if they were to request information based on public bodies such as the government and legal entities like businesses.

**Copyright Legislation**

Whether it is software, music, books or videos (in this case its shoes & trainers in Treading Ahead’s store), all would be copyrighted by the law.

**E-Commerce Regulations**

E-commerce regulations can be the same as an in-store regulation.

Operating System

A program that acts as an intermediary between a user of a computer and the computer hardware. **Operating system goals:**

* Execute user programs and make solving user problems easier.
* Make the computer system convenient to use.

Use the computer hardware in an efficient manner.

Computer System Structure:

### Computer System Components:

Computers consist of hardware components such as the central processing unit (CPU), memory, storage devices, input/output devices, and peripherals, as well as software components such as the operating system and applications.

1. Hardware – provides basic computing resources (CPU, memory, I/O devices).

2. Operating system – controls and coordinates the use of the hardware among the various application programs for the various users.

3. Applications programs – define the ways in which the system resources are used to solve the computing problems of the users (compilers, database systems, video games, business programs).

4. Users (people, machines, other computers).

### Computer-system operation

• One or more CPUs, device controllers connect through common bus providing access to shared memory

• Concurrent execution of CPUs and devices competing for memory cycles.

* I/O devices and the CPU can execute concurrently
* Each device controller is in charge of a particular device type
* Each device controller has a local buffer
* Each device controller type has an operating system device driver to manage it
* CPU moves data from/to main memory to/from local buffers
* I/O is from the device to local buffer of controller
* Device controller informs CPU that it has finished its operation by causing an interrupt

**Common functions of interrupt:**

* Interrupt transfers control to the interrupt service routine generally, through the interrupt vector, which contains the addresses of all the service routines
* Interrupt architecture must save the address of the interrupted instruction
* A trap or exception is a software-generated interrupt caused either by an error or a user request
* An operating system is interrupt driven

**Interrupt handling:**

* The operating system preserves the state of the CPU by storing the registers and the program counter
* Determines which type of interrupt has occurred
* Separate segments of code determine what action should be taken for each type of interrupt

**I/O Structure:**

I/O Structure consists of Programmed I/O, Interrupt driven I/O, DMS, CPU, Memory, External devices, these are all connected with the help of Peripheral I/O Buses and General I/O Buses.

In the programmed I/O when we write the input then the device should be ready to take the data otherwise the program should wait for some time so that the device or buffer will be free then it can take the input.

Once the input is taken then it will be checked whether the output device or output buffer is free then it will be printed. This process is continued every time in transferring of the data.

I/O Interrupts

To initiate any I / O operation, the CPU first loads the registers to the device controller. Then the device controller checks the contents of the registers to determine what operation to perform.

There are two possibilities if I / O operations want to be executed. These are as follows

* Synchronous I / O − The control is returned to the user process after the I/O process is completed.
* Asynchronous I/O − The control is returned to the user process without waiting for the I/O process to finish.

Here, I/O process and the user process run simultaneously.

DMA Structure:

Direct Memory Access (DMA) is a method of handling I / O. Here the device controller directly communicates with memory without CPU involvement.

After setting the resources of I/O devices like buffers, pointers, and counters, the device controller transfers blocks of data directly to storage without CPU intervention.

DMA is generally used for high speed I / O devices.

**Storage Structure:**

Storage structure refers to the way in which data is stored and organized within a computer system. It involves the use of different storage media, such as hard disks and memory, to store and retrieve data. The storage hierarchy is a model that describes the different levels of storage used by a computer system. It ranging from the fastest and most expensive storage to the slowest and least expensive.

Storage Hierarchy :

* + Storage systems organized in hierarchy
    - Speed
    - Cost
    - Volatility
  + Caching – copying information into faster storage system; main memory can be viewed as a cache for secondary storage
  + Device Driver for each device controller to manage I/O

• Provides uniform interface between controller and kernel

The storage hierarchy is organized in such a way that each level provides a different balance between speed, cost and capacity. The fastest and most expensive storage is located at the top of the hierarchy, while the slowest and least expensive storage is located at the bottom.

The storage hierarchy typically consists of the following levels:

**Registers:**

Registers are the fastest type of storage in a computer system, but they are also the smallest. Registers are used to hold data that the CPU needs to access quickly, such as instructions and data being processed.

**Cache Memory:**

Cache memory is a small amount of high-speed memory that is used to temporarily store frequently accessed data. Cache memory is faster than main memory, but it is also more expensive.

**Main Memory (RAM):**

Main memory, also known as random access memory (RAM), is the primary storage used by a computer system. RAM is larger than cache memory, but it is also slower.

**Virtual Memory:**

Virtual memory is a technique used by computer systems to extend the amount of available memory by using hard disk space. Virtual memory allows programs to use more memory than is physically available in the computer.

**Secondary Storage:**

Secondary storage is used to store data and programs that are not currently being used by the computer system.

Examples of secondary storage include hard disks, solid-state drives, and optical disks.

**Tertiary Storage:**

Tertiary storage is used for long-term storage of data that is not frequently accessed. Examples of tertiary storage include tape drives and archival storage systems.

The storage hierarchy is organized in such a way that data is first stored in the fastest and most expensive storage, such as registers and cache memory, and then moved to slower and less expensive storage as needed. This allows the computer system to access data quickly when needed, while also providing a large amount of storage space for less frequently used data.

There are two types of storage devices:-

• Volatile Storage Device – It loses its contents when the power of the device is removed.

• Non-Volatile Storage device – It does not loses its contents when the power is removed. It holds all the data when the power is removed

**Storage Definitions and Notation Review**

The basic unit of computer storage is the bit . A bit can contain one of two values, 0 and 1. All other storage in a computer is based on collections of bits. Given enough bits, it is amazing how many things a computer can represent: numbers, letters, images, movies, sounds, documents, and programs, to name a few. A byte is 8 bits, and on most computers it is the smallest convenient chunk of storage. For example, most computers don’t have an instruction to move a bit but do have one to move a byte. A less common term is word, which is a given computer architecture’s native unit of data. A word is made up of one or more bytes. For example, a computer that has 64-bit registers and 64-bit memory addressing typically has 64-bit (8-byte) words. A computer Executes many operations in its native word size rather than a byte at a time.

Computer storage, along with most computer throughput, is generally

Measured and manipulated in bytes and collections of bytes. A kilobyte, or

KB, is 1,024 bytes; a megabyte, or MB, is 1,0242 bytes; a gigabyte , or GB , is

1,0243 bytes; a terabyte , or TB , is 1,0244 bytes; and a petabyte , or PB , is 1,0245 Bytes. Computer manufacturers often round off these numbers and say that a megabyte is 1 million bytes and a gigabyte is 1 billion bytes. Networking Measurements are an exception to this general rule; they are given in bits (Because networks move data a bit at a time).

Hardware protection and their protection:

Basically, hardware protection is divided into 3 categories: CPU protection, Memory Protection, and I/O protection. These are explained as follows:

1. **CPU Protection:**

CPU protection ensures that, a process does not monopolize the CPU indefinitely, as it would prevent other processes from being executed. Each process should get a limited time, so that every process gets time to execute it’s instructions. To address this, a timer is used to limit the amount of time, which a process can occupy from the CPU. After the timer expires, a signal is sent to the process for relinquishing the CPU. Hence one process cannot hold the CPU forever.

1. **Memory Protection:**

In memory protection, we are talking about that situation when two or more processes are in memory and one process may access the other process memory. To prevent this situation we use two registers which are known as: 1. Base register

1. **Limit register:**

So basically Base register store the starting address of program and limit register store the size of the process. This is done to ensure that whenver a process wants to access the memory, the OS can check that – Is the memory area which the process wants to access is previliged to be accessed by that process or not.

1. **I/O Protection:**

With I/O protection, an OS ensures that following can be never done by a processes:

Termination I/O of other process – This means one process should not be able to terminate I/O operation of othe processes.

View I/O of other process – One process should not be able to access the data being read/written by other processes from/to the Disk(s).

Giving priority to a particular process I/O – No process must be able to priorotize itself or other processes which are doing I/O operations, over other processes.

**Operating system structures**

Brief introduction of operating system

An operating system is the most important software that runs on a computer. It manages the computer's memory and processes, as well as all of its software and hardware. It also allows you to communicate with the computer without knowing how to speak the computer's language.

**Operating System handles the following responsibilities:**

* It controls all the computer resources.
* It provides valuable services to user programs.
* It coordinates the execution of user programs.
* It provides resources for user programs.
* It provides an interface (virtual machine) to the user.
* It hides the complexity of software.
* It supports multiple execution modes.
* It monitors the execution of user programs to prevent errors.

Types of Operating Systems



An Operating System performs all the basic tasks like managing files, processes, and memory. Thus operating system acts as the manager of all the resources, i.e. **resource manager**. Thus, the operating system becomes an interface between the user and the machine. It is one of the most required software that is present in the device.

Operating System is a type of software that works as an interface between the system program and the hardware. There are several types of Operating Systems in which many of which are mentioned below.

# Types of Operating Systems

**There are several types of Operating Systems which are mentioned below.**

* Batch operating system
* Multi programming system
* Multi-Processing System
* Multi-Tasking Operating System
* Time-sharing operating system
* Distributed Operating System
* Network operating system
* Real time operating system

# Batch Operating System

This type of operating system does not interact with the computer directly. There is an operator which takes similar jobs having the same requirement and groups them into batches. It is the responsibility of the operator to sort jobs with similar needs.

# Advantages of Batch Operating System

* It is very difficult to guess or know the time required for any job to complete. Processors of the batch systems know how long the job would be when it is in the queue.
* Multiple users can share the batch systems.
* The idle time for the batch system is very less.
* It is easy to manage large work repeatedly in batch systems.

# Disadvantages of Batch Operating System

* The computer operators should be well known with batch systems.
* Batch systems are hard to debug.
* It is sometimes costly.
* The other jobs will have to wait for an unknown time if any job fails.

**Examples of Batch Operating Systems:** Payroll Systems, Bank Statements, etc.

# Multi-Programming Operating System

Multiprogramming Operating Systems can be simply illustrated as more than one program is present in the main memory and any one of them can be kept in execution. This is basically used for better execution of resources.

# Advantages of Multi-Programming Operating System

* Multi Programming increases the Throughput of the System.
* It helps in reducing the response time.

**Disadvantages of Multi-Programming Operating System**

* There is not any facility for user interaction of system resources with the system.

# Multi-Processing Operating System

Multi-Processing Operating System is a type of Operating System in which more than one CPU is used for the execution of resources. It betters the throughput of the System.

**Advantages of Multi-Processing Operating System**  It increases the throughput of the system.

* As it has several processors, so, if one processor fails, we can proceed with another processor.

**Disadvantages of Multi-Processing Operating System**

* Due to the multiple CPU, it can be more complex and somehow difficult to understand.

# Multi-Tasking Operating System

Multitasking Operating System is simply a multiprogramming Operating System with having facility of a Round-Robin Scheduling Algorithm. It can run multiple programs simultaneously.

There are two types of Multi-Tasking Systems which are listed below.

* Preemptive Multi-Tasking
* Cooperative Multi-Tasking

# Advantages of Multi-Tasking Operating System

* Multiple Programs can be executed simultaneously in Multi-Tasking Operating System.  It comes with proper memory management.

**Disadvantages of Multi-Tasking Operating System**

* The system gets heated in case of heavy programs multiple times.

# Time-Sharing Operating Systems

Each task is given some time to execute so that all the tasks work smoothly. Each user gets the time of the CPU as they use a single system. These systems are also known as Multitasking Systems. The task can be from a single user or different users also. The time that each task gets to execute is called quantum. After this time interval is over OS switches over to the next task.

**Advantages of Time-Sharing OS**

Each task gets an equal opportunity.

* Fewer chances of duplication of software.
* CPU idle time can be reduced.
* Resource Sharing: Time-sharing systems allow multiple users to share hardware resources such as the CPU, memory, and peripherals, reducing the cost of hardware and increasing efficiency.
* Improved Productivity: Time-sharing allows users to work concurrently, thereby reducing the waiting time for their turn to use the computer. This increased productivity translates to more work getting done in less time.
* Improved User Experience: Time-sharing provides an interactive environment that allows users to communicate with the computer in real time, providing a better user experience than batch processing.

**Disadvantages of Time-Sharing OS**  Reliability problem.

* One must have to take care of the security and integrity of user programs and data.
* Data communication problem.
* High Overhead: Time-sharing systems have a higher overhead than other operating systems due to the need for scheduling, context switching, and other overheads that come with supporting multiple users.
* Complexity: Time-sharing systems are complex and require advanced software to manage multiple users simultaneously. This complexity increases the chance of bugs and errors.
* Security Risks: With multiple users sharing resources, the risk of security breaches increases. Timesharing systems require careful management of user access, authentication, and authorization to ensure the security of data and software.

# Examples of Time-Sharing OS with explanation

* **IBM VM/CMS**: IBM VM/CMS is a time-sharing operating system that was first introduced in 1972. It is still in use today, providing a virtual machine environment that allows multiple users to run their own instances of operating systems and applications.
* **TSO (Time Sharing Option)**: TSO is a time-sharing operating system that was first introduced in the 1960s by IBM for the IBM System/360 mainframe computer. It allowed multiple users to access the same computer simultaneously, running their own applications.
* **Windows Terminal Services**: Windows Terminal Services is a time-sharing operating system that allows multiple users to access a Windows server remotely. Users can run their own applications and access shared resources, such as printers and network storage, in real-time.

# Distributed Operating System

These types of operating system is a recent advancement in the world of computer technology and are being widely accepted all over the world and, that too, at a great pace. Various autonomous interconnected computers communicate with each other using a shared communication network. Independent systems possess their own memory unit and CPU. These are referred to as loosely coupled systems or distributed systems. These systems’ processors differ in size and function. The major benefit of working with these types of the operating system is that it is always possible that one user can access the files or software which are not actually present on his system but some other system connected within this network i.e., remote access is enabled within the devices connected in that network.

# Advantages of Distributed Operating System

* Failure of one will not affect the other network communication, as all systems are independent of each other.
* Electronic mail increases the data exchange speed.
* Since resources are being shared, computation is highly fast and durable.
* Load on host computer reduces.
* These systems are easily scalable as many systems can be easily added to the network.
* Delay in data processing reduces.

# Disadvantages of Distributed Operating System

* Failure of the main network will stop the entire communication.
* To establish distributed systems the language is used not well-defined yet.
* These types of systems are not readily available as they are very expensive. Not only that the underlying software is highly complex and not understood well yet.

**Examples of Distributed Operating Systems are** LOCUS, etc.

**The distributed os must tackle the following issues:**

* Networking causes delays in the transfer of data between nodes of a distributed system. Such delays may lead to an inconsistent view of data located in different nodes, and make it difficult to know the chronological order in which events occurred in the system.
* Control functions like scheduling, resource allocation, and deadlock detection have to be performed in several nodes to achieve computation speedup and provide reliable operation when computers or networking components fail.
* Messages exchanged by processes present in different nodes may travel over public networks and pass through computer systems that are not controlled by the distributed operating system. An intruder may exploit this feature to tamper with messages, or create fake messages to fool the authentication procedure and masquerade as a user of the system.

# Network Operating System

These systems run on a server and provide the capability to manage data, users, groups, security, applications, and other networking functions. These types of operating systems allow shared access to files, printers, security, applications, and other networking functions over a small private network. One more important aspect of Network Operating Systems is that all the users are well aware of the underlying configuration, of all other users within the network, their individual connections, etc. and that’s why these computers are popularly known as tightly coupled systems.

**Advantages of Network Operating System**  Highly stable centralized servers.

* Security concerns are handled through servers.
* New technologies and hardware up-gradation are easily integrated into the system.
* Server access is possible remotely from different locations and types of systems. **Disadvantages of Network Operating System**   Servers are costly.
* User has to depend on a central location for most operations.
* Maintenance and updates are required regularly.

**Examples of Network Operating Systems are** Microsoft Windows Server 2003, Microsoft Windows Server 2008, UNIX, Linux, Mac OS X, Novell NetWare, BSD, etc.

# Real-Time Operating System

These types of OSs serve real-time systems. The time interval required to process and respond to inputs is very small. This time interval is called **response time**. **Real-time systems** are used when there are time requirements that are very strict like missile systems, air traffic control systems, robots, etc.

# Types of Real-Time Operating Systems

* **Hard Real-Time Systems:**

Hard Real-Time OSs are meant for applications where time constraints are very strict and even the shortest possible delay is not acceptable. These systems are built for saving life like automatic parachutes or airbags which are required to be readily available in case of an accident. Virtual memory is rarely found in these systems.

* **Soft Real-Time Systems:**

These OSs are for applications where time-constraint is less strict.

# Advantages of RTOS

* **Maximum Consumption:** Maximum utilization of devices and systems, thus more output from all the resources.
* **Task Shifting:** The time assigned for shifting tasks in these systems is very less. For example, in older systems, it takes about 10 microseconds in shifting from one task to another, and in the latest systems, it takes 3 microseconds.
* **Focus on Application:** Focus on running applications and less importance on applications that are in the queue.
* Real-time **operating system in** the **embedded system:** Since the size of programs is small, RTOS can also be used in embedded systems like in transport and others.
* **Error Free:** These types of systems are error-free.
* **Memory Allocation:** Memory allocation is best managed in these types of systems.

# Disadvantages of RTOS

* **Limited Tasks:** Very few tasks run at the same time and their concentration is very less on a few applications to avoid errors.
* **Use heavy system resources:** Sometimes the system resources are not so good and they are expensive as well.
* **Complex Algorithms:** The algorithms are very complex and difficult for the designer to write on.
* **Device driver and interrupt signals:** It needs specific device drivers and interrupts signal to respond earliest to interrupts.
* **Thread Priority:** It is not good to set thread priority as these systems are very less prone to switching tasks.

**Examples of Real-Time Operating Systems are** Scientific experiments, medical imaging systems, industrial control systems, weapon systems, robots, air traffic control systems, etc. Commonly Used Operating System



There are various types of Operating Systems used throughout the world and this depends mainly on the type of operations performed. These Operating Systems are manufactured by large multinational companies like Microsoft, Apple, etc. the few most commonly used OS in the real world:

1. Windows
2. UNIX
3. LINUX
4. BOSS
5. SOLARIS

# Functions And Roles of operating system

An operating system (OS) plays a crucial role in a computer system. Its primary functions include:

1. Hardware Management: The OS manages and controls hardware resources such as the CPU, memory, storage devices, and input/output devices. It allocates these resources to different programs and ensures efficient utilization.
2. Process Management: The OS handles the execution of multiple processes (programs) simultaneously. It schedules processes, manages their execution, and provides mechanisms for inter-process communication.
3. Memory Management: It oversees the allocation and deallocation of memory to processes, ensuring efficient use of RAM and preventing conflicts between programs.
4. File System Management: The OS manages files and directories on storage devices, providing a hierarchical structure for data organization, and offering functions for file creation, deletion, and access control.
5. Device Management: It controls and coordinates input and output operations, including interactions with peripherals like printers, keyboards, and displays.
6. User Interface: The OS provides a user-friendly interface through which users can interact with the computer. This can be a command-line interface or a graphical user interface (GUI).
7. Security and Access Control: It enforces security policies, user authentication, and access control to protect the system from unauthorized access and malicious activities.
8. Error Handling: The OS detects and handles errors, preventing system crashes and providing error messages or logs for troubleshooting.
9. Networking: In modern computing, many OSes include networking capabilities to enable communication over local and wide-area networks.
10. Resource Monitoring: It monitors system performance and resource usage, providing tools and information for system administrators to optimize performance and troubleshoot issues.

Process Management

**Process:**

A process is a program in execution. For example, when we write a program in C or C++ and compile it, the compiler creates binary code. The original code and binary code are both programs. When we actually run the binary code, it becomes a process. A process is an ‘active’ entity instead of a program, which is considered a ‘passive’ entity. A single program can create many processes when run multiple times; for example, when we open a .exe or binary file multiple times, multiple instances begin (multiple processes are created).

**Process Management:**

Process management includes various tools and techniques such as process mapping, process analysis, process improvement, process automation, and process control. By applying these tools and techniques, organizations can streamline their processes, eliminate waste, and improve productivity. Overall, process management is a critical aspect of modern business operations and can help organizations achieve their goals and stay competitive in today’s rapidly changing marketplace.

**What is Process Management?**

If the operating system supports multiple users then services under this are very important. In this regard, operating systems have to keep track of all the completed processes, Schedule them, and dispatch them one after another. However, the user should feel that he has full control of the CPU. Process management refers to the techniques and strategies used by organizations to design, monitor, and control their business processes to achieve their goals efficiently and effectively. It involves identifying the steps involved in completing a task, assessing the resources required for each step, and determining the best way to execute the task.

Process management can help organizations improve their operational efficiency, reduce costs, increase customer satisfaction, and maintain compliance with regulatory requirements. It involves analyzing the performance of existing processes, identifying bottlenecks, and making changes to optimize the process flow.

Some of the systems call in this category are as follows.

* Create a child’s process identical to the parent’s.
* Terminate a process
* Wait for a child process to terminate
* Change the priority of the process
* Block the process
* Ready the process
* Dispatch a process
* Suspend a process
* Resume a process
* Delay a process
* Fork a process

# Key Components of Process Management

Below are some key component of process management.

* **Process mapping:** Creating visual representations of processes to understand how tasks flow, identify dependencies, and uncover improvement opportunities.
* **Process analysis:** Evaluating processes to identify bottlenecks, inefficiencies, and areas for improvement.
* **Process redesign:** Making changes to existing processes or creating new ones to optimize workflows and enhance performance.
* **Process implementation:** Introducing the redesigned processes into the organization and ensuring proper execution.
* **Process monitoring and control:** Tracking process performance, measuring key metrics, and implementing control mechanisms to maintain efficiency and effectiveness.

# States of Process

A process is in one of the following states:

* **New:** Newly Created Process (or) being-created process.
* **Ready:** After the creation process moves to the Ready state, i.e. the process is ready for execution.
* **Run:** Currently running process in CPU (only one process at a time can be under execution in a single processor)
* **Wait (or Block):** When a process requests I/O access.
* **Complete (or Terminated):** The process completed its execution.
* **Suspended Ready:** When the ready queue becomes full, some processes are moved to a suspended ready state
* **Suspended Block:** When the waiting queue becomes full.

Process Scheduling Algorithms

The operating system can use different scheduling algorithms to schedule processes. Here are some commonly used timing algorithms:

* **First-come, first-served (FCFS):** This is the simplest scheduling algorithm, where the process is executed on a first-come, first-served basis. FCFS is non-preemptive, which means that once a process starts executing, it continues until it is finished or waiting for I/O.
* **Shortest Job First (SJF):** SJF is a proactive scheduling algorithm that selects the process with the shortest burst time. The burst time is the time a process takes to complete its execution. SJF minimizes the average waiting time of processes.
* **Round Robin (RR):** Round Robin is a proactive scheduling algorithm that reserves a fixed amount of time in a round for each process. If a process does not complete its execution within the specified time, it is blocked and added to the end of the queue. RR ensures fair distribution of CPU time to all processes and avoids starvation.
* **Priority Scheduling:** This scheduling algorithm assigns priority to each process and the process with the highest priority is executed first. Priority can be set based on process type, importance, or resource requirements.
* **Multilevel queue:** This scheduling algorithm divides the ready queue into several separate queues, each queue having a different priority. Processes are queued based on their priority, and each queue uses its own scheduling algorithm. This scheduling algorithm is useful in scenarios where different types of processes have different priorities.

# Advantages of Process Management

* **Improved Efficiency:** Process management can help organizations identify bottlenecks and inefficiencies in their processes, allowing them to make changes to streamline workflows and increase productivity.
* **Cost Savings:** By identifying and eliminating waste and inefficiencies, process management can help organizations reduce costs associated with their business operations.
* **Improved Quality:** Process management can help organizations improve the quality of their products or services by standardizing processes and reducing errors.
* **Increased Customer Satisfaction:** By improving efficiency and quality, process management can enhance the customer experience and increase satisfaction.
* **Compliance with Regulations:** Process management can help organizations comply with regulatory requirements by ensuring that processes are properly documented, controlled, and monitored.

# Disadvantages of Process Management

* **Time and Resource Intensive:** Implementing and maintaining process management initiatives can be time-consuming and require significant resources.
* **Resistance to Change:** Some employees may resist changes to established processes, which can slow down or hinder the implementation of process management initiatives.
* **Overemphasis on Process:** Overemphasis on the process can lead to a lack of focus on customer needs and other important aspects of business operations.
* **Risk of Standardization:** Standardizing processes too much can limit flexibility and creativity, potentially stifling innovation.
* **Difficulty in Measuring Results:** Measuring the effectiveness of process management initiatives can be difficult, making it challenging to determine their impact on organizational performance.

**Memory Management in Operating System**

**Main Memory**

Main memory, commonly referred to as RAM (Random Access Memory), is the computer's primary temporary storage for actively processed data. Unlike permanent storage like hard drives, RAM is volatile, losing its contents when the computer powers down. It's organized into addressable cells, each holding data measured in bytes. Efficient memory management, involving allocation and deallocation, is essential for optimal performance. The amount of RAM directly impacts multitasking and program handling capabilities, making it a critical factor in overall system performance.

**Memory Management in an Operating System**

Memory management in OS is a technique of controlling and managing the functionality of Random access memory (primary memory). It is used for achieving better concurrency, system performance, and memory utilization.

Memory management moves processes from primary memory to secondary memory and vice versa. It also keeps track of available memory, memory allocation, and unallocated.

Why use Memory Management in OS?

Memory management keeps track of the status of each memory location, whether it is allocated or free.

Memory management enables computer systems to run programs that require more main memory than the amount of free main memory available on the system. This is achieved by moving data between primary and secondary memory.

Memory management addresses the system’s primary memory by providing abstractions such that the programs running on the system perceive a large memory is allocated to them.

It is the job of memory management to protect the memory allocated to all the processes from being corrupted by other processes. If this is not done, the computer may exhibit unexpected/faulty behavior.

Memory management enables sharing of memory spaces among processes, with the help of which, multiple programs can reside at the same memory location (although only one at a time). Storage Management



**Storage Management** is defined as it refers to the management of the data storage equipment’s that are used to store the user/computer generated data. Hence it is a tool or set of processes used by an administrator to keep your data and storage equipment’s safe. Storage management is a process for users to optimize the use of storage devices and to protect the integrity of data for any media on which it resides and the category of storage management generally contain the different type of subcategories covering aspects such as security, virtualization and more, as well as different types of provisioning or automation, which is generally made up the entire storage management software market.

**Storage management key attributes:** Storage management has some key attribute which is generally used to manage the storage capacity of the system.

These are given below:

1. Performance
2. Reliability
3. Recoverability
4. Capacity

**Feature of Storage management:** There is some feature of storage management which is provided for storage capacity. These are given below:

1. Storage management is a process that is used to optimize the use of storage devices.
2. Storage management must be allocated and managed as a resource in order to truly benefit a corporation.
3. Storage management is generally a basic system component of information systems.
4. It is used to improve the performance of their data storage resources.

**Advantage of storage management:** There are some advantage of storage management which are given below:

* It becomes very simple to manage a storage capacity.
* It generally reduces the time consumption.
* It improves the performance of system.
* In virtualization and automation technologies, it can help an organization improve its agility.

**Limitations of storage management:**

* Limited physical storage capacity: Operating systems can only manage the physical storage space that is available, and as such, there is a limit to how much data can be stored.
* Performance degradation with increased storage utilization: As more data is stored, the system’s performance can decrease due to increased disk access time, fragmentation, and other factors.
* Complexity of storage management: Storage management can be complex, especially as the size of the storage environment grows.
* Cost: Storing large amounts of data can be expensive, and the cost of additional storage capacity can add up quickly.
* Security issues: Storing sensitive data can also present security risks, and the operating system must have robust security features in place to prevent unauthorized access to this data.
* Backup and Recovery: Backup and recovery of data can also be challenging, especially if the data is stored on multiple systems or devices. File Systems in Operating System



A computer file is defined as a medium used for saving and managing data in the computer system. The data stored in the computer system is completely in digital format, although there can be various types of files that help us to store the data. What is a File System?

A file system is a method an operating system uses to store, organize, and manage files and directories on a storage device. Some common types of file systems include:

1. **FAT (File Allocation Table):** An older file system used by older versions of Windows and other operating systems.
2. **NTFS (New Technology File System):** A modern file system used by Windows. It supports features such as file and folder permissions, compression, and encryption.
3. **ext (Extended File System):** A file system commonly used on Linux and Unix-based operating systems.
4. **HFS (Hierarchical File System):** A file system used by macOS.
5. **APFS (Apple File System):** A new file system introduced by Apple for their Macs and iOS devices. A file is a collection of related information that is recorded on secondary storage. Or file is a collection of logically related entities. From the user’s perspective, a file is the smallest allotment of logical secondary storage.

**The name of the file is divided into two parts as shown below:**

* name
* Extension, separated by a period.

# Issues Handled By File System

We’ve seen a variety of data structures where the file could be kept. The file system’s job is to keep the files organized in the best way possible.

A free space is created on the hard drive whenever a file is deleted from it. To reallocate them to other files, many of these spaces may need to be recovered. Choosing where to store the files on the hard disc is the main issue with files one block may or may not be used to store a file. It may be kept in the disk’s non-contiguous blocks. We must keep track of all the blocks where the files are partially located.

# Advantages of File System

* **Organization:** A file system allows files to be organized into directories and subdirectories, making it easier to manage and locate files.
* **Data protection:** File systems often include features such as file and folder permissions, backup and restore, and error detection and correction, to protect data from loss or corruption.
* **Improved performance:** A well-designed file system can improve the performance of reading and writing data by organizing it efficiently on disk.

Disadvantages of File System

* **Compatibility issues:** Different file systems may not be compatible with each other, making it difficult to transfer data between different operating systems.
* **Disk space overhead:** File systems may use some disk space to store metadata and other overhead information, reducing the amount of space available for user data.
* **Vulnerability:** File systems can be vulnerable to data corruption, malware, and other security threats, which can compromise the stability and security of the system.

# File Directories

The collection of files is a file directory. The directory contains information about the files, including attributes, location, and ownership. Much of this information especially that is concerned with storage is managed by the operating system. The directory is itself a file, accessible by various file management routines.

# Advantages of Maintaining Directories

* **Efficiency:** A file can be located more quickly.
* **Naming:** It becomes convenient for users as two users can have same name for different files or may have different name for same file.
* **Grouping:** Logical grouping of files can be done by properties e.g. all java programs, all games etc.

**What is a file allocation table (FAT)?**

*The File Allocation Table (FAT) is a file system structure used by some operating systems, including older versions of Windows. It uses a table to keep track of the allocation status of each cluster (a fixed-size block of storage) on the disk. The FAT file system has evolved over time, with variations such as FAT12, FAT16, and FAT32, supporting different disk sizes and features.* **Operating system services:**

Operating systems provide an environment for execution of programs and services to programs and users One set of operating-system services provides functions that are helpful to the user:

User interface - Almost all operating systems have a user interface (UI).

Varies between Command-Line (CLI), Graphics User Interface (GUI), touch-screen, Batch

Program execution - The system must be able to load a program into memory and to run that program, end execution, either normally or abnormally (indicating error)

I/O operations - A running program may require I/O, which may involve a file or an I/O device

File-system manipulation - The file system is of particular interest. Programs need to read and write files and directories, create and delete them, search them, list file Information, permission management.

* One set of operating-system services provides functions that are helpful to the user (Cont.):
  + - **Communications** – Processes may exchange information, on the same computer or between computers over a network

 Communications may be via shared memory or through message passing (packets moved by the OS)

* + - **Error detection** – OS needs to be constantly aware of possible errors

 May occur in the CPU and memory hardware, in I/O devices, in user program

 For each type of error, OS should take the appropriate action to ensure correct and consistent computing

 Debugging facilities can greatly enhance the user’s and programmer’s abilities to efficiently use the system

* Another set of OS functions exists for ensuring the efficient operation of the system itself via resource sharing
  + - **Resource allocation -** When multiple users or multiple jobs running concurrently, resources must be allocated to each of them

 Many types of resources - CPU cycles, main memory, file storage, I/O devices.

* + - **Logging -** To keep track of which users use how much and what kinds of computer resources
    - **Protection and security -** The owners of information stored in a multiuser or networked computer system may want to control use of that information, concurrent processes should not interfere with each other

 **Protection** involves ensuring that all access to system resources is controlled

 **Security** of the system from outsiders requires user authentication, extends to defending external I/O devices from invalid access attempts

**System Call:**

* Programming interface to the services provided by the OS
* Typically written in a high-level language (C or C++)
* Mostly accessed by programs via a high-level Application Programming Interface (API) rather than direct system call use
* Three most common APIs are Win32 API for Windows, POSIX API for POSIX-based systems (including virtually all versions of UNIX, Linux, and Mac OS X), and Java API for the Java virtual machine (JVM)  **Example:**
* System call sequence to copy the contents of one file to another file



**System Call implementation**

* Typically, a number is associated with each system call

• **System-call interface** maintains a table indexed according to these numbers

* The system call interface invokes the intended system call in OS kernel and returns status of the system call and any return values
* The caller need know nothing about how the system call is implemented
  + - Just needs to obey API and understand what OS will do as a result call
    - Most details of OS interface hidden from programmer by API

 Managed by run-time support library (set of functions built into libraries included with compiler) **Types of system call:**

* Process control
  + create process, terminate process
  + end, abort
  + load, execute
  + get process attributes, set process attributes
  + wait for time
  + wait event, signal event
  + allocate and free memory
  + Dump memory if error
  + **Debugger** for determining **bugs, single step** execution
  + **Locks** for managing access to shared data between processes
* File management
  + create file, delete file
  + open, close file
  + read, write, reposition
  + get and set file attributes
* Device management
  + request device, release device
  + read, write, reposition
  + get device attributes, set device attributes
  + logically attach or detach devices
* Information maintenance
  + get time or date, set time or date
  + get system data, set system data
  + get and set process, file, or device attributes
* Communications
  + create, delete communication connection
  + send, receive messages if **message passing model** to **host name** or **process name**

 From **client** to **server**

* + **Shared-memory model** create and gain access to memory regions
  + transfer status information
  + attach and detach remote devices
* Protection
  + Control access to resources
  + Get and set permissions
  + Allow and deny user access

**System Services:**

* System programs provide a convenient environment for program development and execution. They can be divided into:
  + - File manipulation
    - Status information sometimes stored in a file
    - Programming language support
    - Program loading and execution
    - Communications
    - Background services
    - Application programs
* Most users’ view of the operation system is defined by system programs, not the actual system calls
* Provide a convenient environment for program development and execution
  + - Some of them are simply user interfaces to system calls; others are considerably more complex
    - **File management** - Create, delete, copy, rename, print, dump, list, and generally manipulate files and directories
* **Status information**
  + - * Some ask the system for info - date, time, amount of available memory, disk space, number of users
      * Others provide detailed performance, logging, and debugging information
      * Typically, these programs format and print the output to the terminal or other output devices
      * Some systems implement a **registry** - used to store and retrieve configuration information
* **File modification**
  + - * Text editors to create and modify files
      * Special commands to search contents of files or perform transformations of the text
* **Programming-language support** - Compilers, assemblers, debuggers and interpreters sometimes provided
* **Program loading and execution**- Absolute loaders, relocatable loaders, linkage editors, and overlay-loaders, debugging systems for higher-level and machine language
* **Communications** - Provide the mechanism for creating virtual connections among processes, users, and computer systems

• Allow users to send messages to one another’s screens, browse web pages, send electronic-mail messages, log in remotely, transfer files from one machine to another Introduction of System Call



In computing, a **system call** is a programmatic way in which a computer program requests a service from the kernel of the operating system it is executed on. A system call is a way for programs to **interact with the operating system**. A computer program makes a system call when it makes a request to the operating system’s kernel. System call **provides** the services of the operating system to the user programs via Application Program Interface (API). It provides an interface between a process and an operating system to allow user-level processes to request services of the operating system. System calls are the only entry points into the kernel system. All programs needing resources must use system calls.

A user program can interact with the operating system using a system call. A number of services are requested by the program, and the OS responds by launching a number of systems calls to fulfill the request. A system call can be written in high-level languages like C or Pascal or in assembly language. If a high-level language is used, the operating system may directly invoke system calls, which are predefined functions.

Services Provided by System Calls

* Process creation and management
* Main memory management
* File Access, Directory, and File system management
* Device handling(I/O)
* Protection
* Networking, etc.
* **Process control:** end, abort, create, terminate, allocate, and free memory.
* **File management:** create, open, close, delete, read files,s, etc.

#  Device management  Information maintenance  Communication

Features of System Calls

* **Interface:** System calls provide a well-defined interface between user programs and the operating system. Programs make requests by calling specific functions, and the operating system responds by executing the requested service and returning a result.
* **Protection:** System calls are used to access privileged operations that are not available to normal user programs. The operating system uses this privilege to protect the system from malicious or unauthorized access.
* **Kernel Mode:** When a system call is made, the program is temporarily switched from user mode to kernel mode. In kernel mode, the program has access to all system resources, including hardware, memory, and other processes.
* **Context Switching:** A system call requires a context switch, which involves saving the state of the current process and switching to the kernel mode to execute the requested service. This can introduce overhead, which can impact system performance.
* **Error Handling:** System calls can return error codes to indicate problems with the requested service. Programs must check for these errors and handle them appropriately.
* **Synchronization:** System calls can be used to synchronize access to shared resources, such as files or network connections. The operating system provides synchronization mechanisms, such as locks or semaphores, to ensure that multiple programs can access these resources safely.

System Calls Advantages

* **Access to hardware resources:** System calls allow programs to access hardware resources such as disk drives, printers, and network devices.
* **Memory management:** System calls provide a way for programs to allocate and deallocate memory, as well as access memory-mapped hardware devices.
* **Process management:** System calls allow programs to create and terminate processes, as well as manage inter-process communication.
* **Security:** System calls provide a way for programs to access privileged resources, such as the ability to modify system settings or perform operations that require administrative permissions.
* **Standardization:** System calls provide a standardized interface for programs to interact with the operating system, ensuring consistency and compatibility across different hardware platforms and operating system versions.

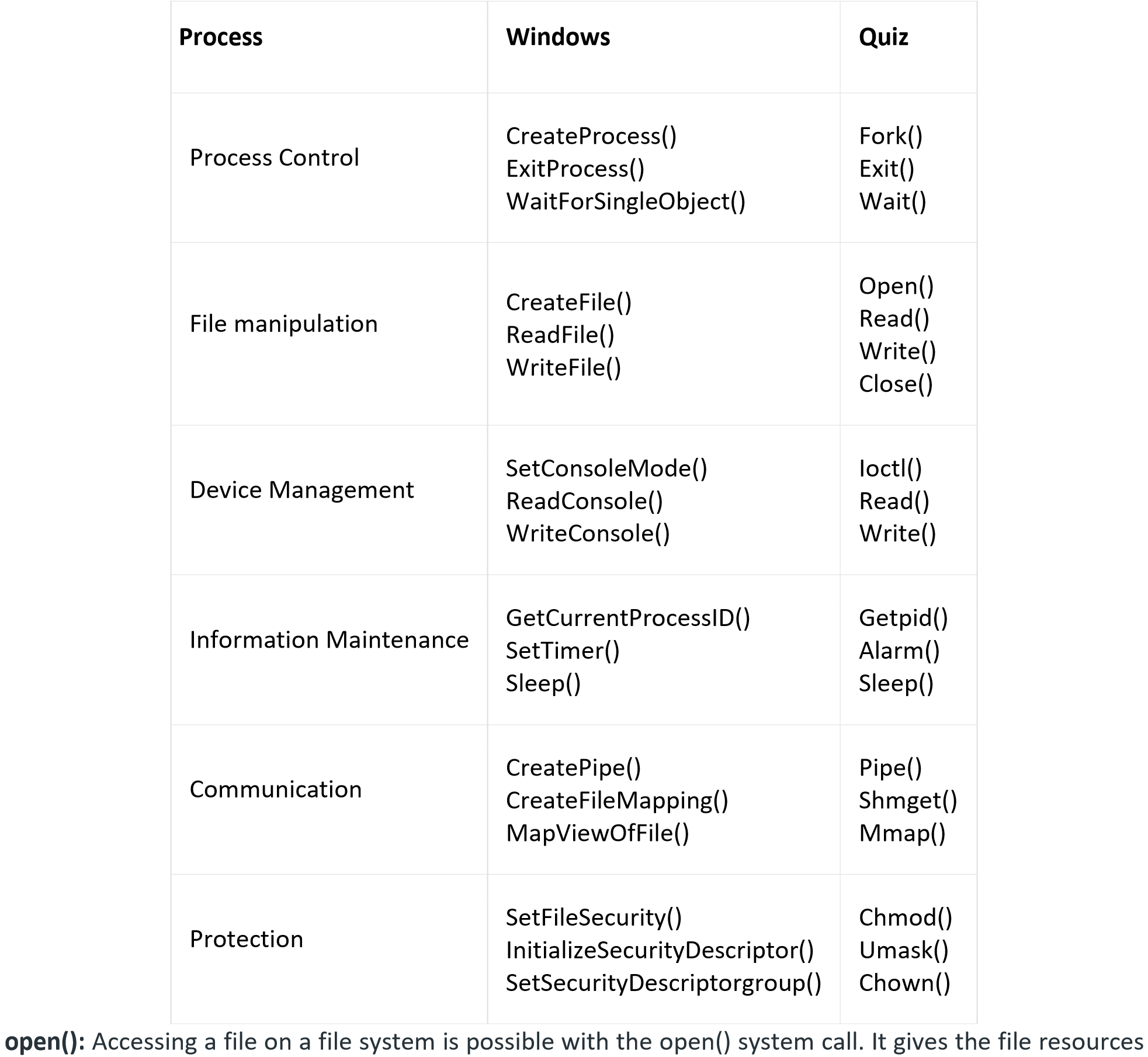
How does System Call Work?

Here is the detailed explanation step by step how system call work:

* **User need special resources :** Sometimes programs need to do some special things which can’t be done without the permission of OS like reading from a file, writing to a file , getting any information from the hardware or requesting a space in memory.
* **Program makes a system call request :** There are special predefined instruction to make a request to the operating system. These instruction are nothing but just a “system call”. The program uses these system calls in its code when needed.
* **Operating system sees the system call :** When the OS sees the system call then it recongnises that the program need help at this time so it temporarily stop the program execution and give all the control to special part of itself called ‘Kernel’ . Now ‘Kernel’ solve the need of program.
* **Operating system performs the operations :**Now the operating system perform the operation which is requested by program . Example : reading content from a file etc.
* **Operating system give control back to the program :** After performing the special operation, OS give control back to the program for further execution of program .

Examples of a System Call in Windows and Unix

System calls for Windows and Unix come in many different forms. These are listed in the table below as follows:



it needs and a handle the process can use. A file can be opened by multiple processes simultaneously or just one process. Everything is based on the structure and file system.

**read():** Data from a file on the file system is retrieved using it. In general, it accepts three arguments:

1. A description of a file.
2. A buffer for read data storage.
3. How many bytes should be read from the file Before reading, the file to be read could be identified by its file descriptor and opened using the open() function.

**wait():** In some systems, a process might need to hold off until another process has finished running before continuing. When a parent process creates a child process, the execution of the parent process is halted until the child process is complete. The parent process is stopped using the wait() system call. The parent process regains control once the child process has finished running.

**write():** Data from a user buffer is written using it to a device like a file. A program can produce data in one way by using this system call. generally, there are three arguments:

1. A description of a file.
2. A reference to the buffer where data is stored.
3. The amount of data that will be written from the buffer in bytes. **fork():** The fork() system call is used by processes to create copies of themselves. It is one of the methods used the most frequently in operating systems to create processes. When a parent process creates a child process, the parent process’s execution is suspended until the child process is finished. The parent process regains control once the child process has finished running. **exit():** A system call called exit() is used to terminate a program. In environments with multiple threads, this call indicates that the thread execution is finished. After using the exit() system function, the operating system recovers the resources used by the process.

Methods to pass parameters to OS

If a system call occur, we have to pass parameter to the Kernal part of the Operating system. For example look at the given **open()** system call:

So it is to be noted that :

* We can’t pass the parameters directly like in an ordinary function call.
* In Kernal mode there is a different way to perform a function call.

So we can’t run it in the normal address space that the process had already created and hence we cant place the parameters in the top of the stack because it is not available to the Kernal of the operating system for processing. so we have to adopt any other methods to pass the parameters to the Kernal of the OS.

# We can done it through, 1. Passing parameters in registers

1. **Address of the block is passed as a parameter in a register.**
2. **Parameters are pushed into a stack.**

Let us discuss about each points in detail:

**1. Passing parameters in registers.**

* It is the simplest method among the three
* Here we directly pass the parameters to registers.
* But it will it is limited when, number of parameters are greater than the number of registers.
* Here is the C program code:

|  |  |
| --- | --- |
| **2.Address of the block is passed as parameters** |  |

* It can be applied when the number of parameters are greater than the number of registers.
* Parameters are stored in blocks or table.
* The address of the block is passed to a register as a parameter.
* Most commonly used in Linux and Solaris.
* Here is the C program code:
* 3.Parameters are pushed in a stack
* In this method parameters can be pushed in using the program and popped out using the operating system
* So the Kernal can easily access the data by retrieving information from the top of the stack.  Here is the C program code

**Q.1: How does a system call work?**

**Answer:**

*When a program executes a system call, it transitions from user mode to kernel mode, which is a higher privileged mode. The transition is typically initiated by invoking a specific function or interrupting instruction provided by the programming language or the operating system.*

*Once in kernel mode, the system call is handled by the operating system. The kernel performs the requested operation on behalf of the program and returns the result. Afterward, control is returned to the user-level program, which continues its execution.* **Q.2: Why are system calls necessary? Answer:**

*System calls are necessary for several reasons:*

***Access to privileged operations:*** *Many operations, such as managing hardware devices or modifying system configurations, require higher privileges that are only accessible through system calls.*

***Resource management:*** *System calls provide a standardized interface for allocating and managing system resources like memory, files, and devices, ensuring fair and controlled access by different processes.* ***Abstraction:*** *System calls abstract the underlying complexities of the operating system, allowing application developers to interact with the system in a higher-level, platform-independent manner.* ***Security and protection:*** *System calls enforce access control and security policies, preventing unauthorized access to sensitive resources and protecting the integrity of the system.* **System Programs in Operating System**



**System Programming** can be defined as the act of building Systems Software using System

Programming Languages. According to Computer Hierarchy, Hardware comes first then is Operating System, System Programs, and finally Application Programs. Program Development and Execution can be done conveniently in System Programs. Some of the System Programs are simply user interfaces, others are complex. It traditionally sits between the user interface and system calls. In the context of an operating system, system programs are nothing but a special software which give us facility to manage and control the computer’s hardware and resources. As we have mentioned earlier these programs are more closely with the operating system so it executes the operation fast and helpful in performing essential opeartion which can’t be handled by application software .

Here are the examples of System Programs :

1. **File Management** &#x2013 A file is a collection of specific information stored in the memory of a computer system. File management is defined as the process of manipulating files in the computer system, its management includes the process of creating, modifying and deleting files.
2. **Command Line Interface(CLI’s) :** CLIs is the essential tool for user . It provide user facility to write commands directly to the system for performing any operation . It is a text-based way to interact with operating system. CLIs can perform many tasks like file manipulation,system configuration and etc.
3. **Device drivers :**Device drivers work as a simple translator for OS and devices . Basically it act as an intermediatry between the OS and devices and provide facility to both OS and devices to understand each other’s language so that they can work together efficiently without interrupt.
4. **Status Information** &#x2013 Information like date, time amount of available memory, or disk space is asked by some users. Others providing detailed performance, logging, and debugging information which is more complex. All this information is formatted and displayed on output devices or printed. Terminal or other output devices or files or a window of GUI is used for showing the output of programs.
5. **File Modification &#x2013** This is used for modifying the content of files. Files stored on disks or other storage devices, we use different types of editors. For searching contents of files or perform transformations of files we use special commands.
6. **Programming-Language support** &#x2013 For common programming languages, we use Compilers, Assemblers, Debuggers, and interpreters which are already provided to users. It provides all support to users. We can run any programming language. All important languages are provided.
7. **Program Loading and Execution** &#x2013 When the program is ready after Assembling and compilation, it must be loaded into memory for execution. A loader is part of an operating system that is responsible for loading programs and libraries. It is one of the essential stages for starting a program. Loaders, relocatable loaders, linkage editors, and Overlay loaders are provided by the system.
8. **Communications** &#x2013al connections among processes, users, and computer systems are provided by programs. Users can send messages to another user on their screen, User can send email, browsing on web pages, remote login, the transformation of files from one user to another.

Operating System Design and Implementation

An operating system is a construct that allows the user application programs to interact with the system hardware. Operating system by itself does not provide any function but it provides an atmosphere in which different applications and programs can do useful work.

There are many problems that can occur while designing and implementing an operating system. These are covered in operating system design and implementation.

**Operating System Design Goals**

It is quite complicated to define all the goals and specifications of the operating system while designing it.The design changes depending on the type of the operating system i.e if it is batch system, time shared system, single user system, multi user system, distributed system etc.

There are basically two types of goals while designing an operating system. These are −

User Goals

The operating system should be convenient, easy to use, reliable, safe and fast according to the users.

However, these specifications are not very useful as there is no set method to achieve these goals.

System Goals

The operating system should be easy to design, implement and maintain. These are specifications required by those who create, maintain and operate the operating system. But there is not specific method to achieve these goals as well.

**Operating System Mechanisms and Policies**

There is no specific way to design an operating system as it is a highly creative task. However, there are general software principles that are applicable to all operating systems.

A subtle difference between mechanism and policy is that mechanism shows how to do something and policy shows what to do. Policies may change over time and this would lead to changes in mechanism. So, it is better to have a general mechanism that would require few changes even when a policy change occurs.

For example - If the mechanism and policy are independent, then few changes are required in mechanism if policy changes. If a policy favours I/O intensive processes over CPU intensive processes, then a policy change to preference of CPU intensive processes will not change the mechanism.

**Operating System Implementation**

The operating system needs to be implemented after it is designed. Earlier they were written in assembly language but now higher level languages are used. The first system not written in assembly language was the Master Control Program (MCP) for Burroughs Computers.

Advantages of Higher Level Language

There are multiple advantages to implementing an operating system using a higher level language such as: the code is written more fast, it is compact and also easier to debug and understand. Also, the operating system can be easily moved from one hardware to another if it is written in a high level language.

Disadvantages of Higher Level Language

Using high level language for implementing an operating system leads to a loss in speed and increase in storage requirements. However in modern systems only a small amount of code is needed for high performance, such as the CPU scheduler and memory manager. Also, the bottleneck routines in the system can be replaced by assembly language equivalents if required

**Peer to peer network:**

In peer-to-peer (P2P) networking, a group of computers are linked together with equal permissions and responsibilities for processing data. Unlike traditional client-server networking, no devices in a P2P network are designated solely to serve or to receive data. Each connected machine has the same rights as its “peers”, and can be used for the same purposes.

**What are the Benefits of P2P Connections?**

P2P networking comes with a number of benefits. As an example, in a traditional client-server network model, if a server goes down, it can take the whole network with it. But in P2P, if a single device goes down, the others on the network can help pick up the slack. They also help ensure network traffic doesn’t get bottlenecked at one device, since traffic handling is distributed across many computers. **IP address:**

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.

Types of IP addresses

There are different categories of IP addresses, and within each category, different types.

Consumer IP addresses

Every individual or business with an internet service plan will have two types of IP addresses: their private IP addresses and their public IP address. The terms public and private relate to the network location — that is, a private IP address is used inside a network, while a public one is used outside a network.

Private IP addresses

Every device that connects to your internet network has a private IP address. This includes computers, smartphones, and tablets but also any Bluetooth-enabled devices like speakers, printers, or smart TVs. With the growing internet of things, the number of private IP addresses you have at home is probably growing. Your router needs a way to identify these items separately, and many items need a way to recognize each other. Therefore, your router generates private IP addresses that are unique identifiers for each device that differentiate them on the network.

Public IP addresses

A public IP address is the primary address associated with your whole network. While each connected device has its own IP address, they are also included within the main IP address for your network. As described above, your public IP address is provided to your router by your ISP. Typically, ISPs have a large pool of IP addresses that they distribute to their customers. Your public IP address is the address that all the devices outside your internet network will use to recognize your network.

Public IP addresses

Public IP addresses come in two forms – dynamic and static.

Dynamic IP addresses

Dynamic IP addresses change automatically and regularly. ISPs buy a large pool of IP addresses and assign them automatically to their customers. Periodically, they re-assign them and put the older IP addresses back into the pool to be used for other customers. The rationale for this approach is to generate cost savings for the ISP. Automating the regular movement of IP addresses means they don’t have to carry out specific actions to re-establish a customer's IP address if they move home, for example. There are security benefits, too, because a changing IP address makes it harder for criminals to hack into your network interface.

Static IP addresses

In contrast to dynamic IP addresses, static addresses remain consistent. Once the network assigns an IP address, it remains the same. Most individuals and businesses do not need a static IP address, but for businesses that plan to host their own server, it is crucial to have one. This is because a static IP address ensures that websites and email addresses tied to it will have a consistent IP address — vital if you want other devices to be able to find them consistently on the web. which is the two types of website IP addresses.

There are two types of website IP addresses

For website owners who don’t host their own server, and instead rely on a web hosting package – which is the case for most websites – there are two types of website IP addresses. These are shared and dedicated.

Shared IP addresses

Websites that rely on shared hosting plans from web hosting providers will typically be one of many websites hosted on the same server. This tends to be the case for individual websites or SME websites, where traffic volumes are manageable, and the sites themselves are limited in terms of the number of pages, etc. Websites hosted in this way will have shared IP addresses.

Dedicated IP addresses

Some web hosting plans have the option to purchase a dedicated IP address (or addresses). This can make obtaining an SSL certificate easier and allows you to run your own File Transfer Protocol (FTP) server. This makes it easier to share and transfer files with multiple people within an organization and allow anonymous FTP sharing options. A dedicated IP address also allows you to access your website using the IP address alone rather than the domain name — useful if you want to build and test it before registering your domain.

**The IPv4**

The most common type of IP address is known as IPv4, for “IP version 4.” Here’s an example of what an IPv4 address might look like:

24.156.99.202

An IPv4 address consists of four numbers, each of which contains 1-3 digits, with a single dot (.) separating each number. Each of the four numbers can range from 0 to 225. This group of numbers creates a unique address to let worldwide users send and retrieve data over internet connections.

IP Address Classes

Some IP addresses are reserved by the Internet Assigned Numbers Authority (IANA). These are typically reserved for networks that carry a specific purpose on the [Transmission Control Protocol/Internet Protocol (TCP/IP),](https://www.fortinet.com/resources/cyberglossary/tcp-ip) which is used to interconnect devices. Four of these IP address classes include:

1. **0.0.0.0**: This IP address in IPv4 is also known as the default network. It is the non-routeable meta address that designates an invalid, non-applicable, or unknown network target.
2. **127.0.0.1**: This IP address is known as the loopback address, which a computer uses to identify itself regardless of whether it has been assigned an IP address.
3. **169.254.0.1 to 169.254.254.254**: A range of addresses that are automatically assigned if a computer is unsuccessful in an attempt to receive an address from the DHCP.
4. **255.255.255.255**: An address dedicated to messages that need to be sent to every computer on a network or broadcasted across a network.

Further reserved IP addresses are for what is known as subnet classes. Subnetworks are small computer networks that connect to a bigger network via a router. The subnet can be assigned its own IP address system, so that all devices connecting to it can communicate with each other without having to send data via the wider network.

The router on a TCP/IP network can be configured to ensure it recognizes subnets, then route the traffic onto the appropriate network. IP addresses are reserved for the following subnets:

1. **Class A**: IP addresses between 10.0.0.0 and 10.255.255.255
2. **Class B**: IP addresses between 172.16.0.0 and 172.31.255.255
3. **Class C**: IP addresses between 192.186.0.0 and 192.168.255.255
4. **Class D or multicast**: IP addresses between 224.0.0.0 and 239.255.255.255
5. **Class E, which are reserved for experimental usage**: IP addresses between 240.0.0.0 and 254.255.255.254

IP addresses listed under Class A, Class B, and Class C are most commonly used in the creation of subnets. Addresses within the multicast or Class D have specific usage rules outlined in the Internet Engineering Task Force (IETF) guidelines, while the release of Class E addresses for public use was the cause of plenty of debate before the IPv6 standard was introduced.

IPv4 supports a maximum of approximately 4.3 billion unique IP addresses. IPv6 supports, in theory, a much higher maximum number: 340,282,366,920,938,463,463,374,607,431,768,211,456.

If your eyes glazed over when reading that number, rest assured there’s no chance of ever running out again.

An IPv6 address consists of eight groups of four hexadecimal digits. Here’s an example IPv6 address:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

**What is the use of an IP address?**

An IP address identifies every device connected to the internet. This enables computers and other internet-connected devices, such as mobile phones and Internet-of-Things (IoT) devices, to communicate over the internet and on local-area networks (LANs).

What happens if someone has your IP address?

The chances of being hacked through someone having your IP address is quite low. With an IP address, a user's location can be narrowed down to a specific area. A skilled cyber criminal could potentially work out who their ISP is and then use phishing attacks to find their personal details. A bigger concern might be IP addresses being sold on the dark web alongside other personal information.

An IP address is more likely to be used by content providers to target the user with content restrictions based on their geographical region. For example, services like Hulu and Netflix read IP addresses to prevent their U.S. content from being accessed by people outside the country.

What are the two types of IP addresses?

The two types of IP addresses are public IP addresses and private IP addresses. A public IP address is the main device people use to connect to the internet, which is typically their router. Private IP addresses are assigned to the devices that connect to the public IP address, such as desktop computers, mobile devices, laptops, printers, smart TVs, and tablets.

What is the 192.168 IP address?

The 192.168 IP address is where the private IP address range begins. This goes all the way through to 192.168.255.255. This IP address is not usually used on a network, and devices like computers and mobile phones will not be assigned it.

What is a loopback IP address?

The loopback IP address is 127.0.0.1. The loopback IP address is used by a computer to identify itself, regardless of whether or not it has been assigned an IP address.

**IPv6:**

Internet Protocol Version 6 (IPv6) is a network layer protocol that enables data communications over a packet switched network. Packet switching involves the sending and receiving of data in packets between two nodes in a network.

A main advantage of IPv6 is increased address space. The 128-bit length of IPv6 addresses is a significant gain over the 32-bit length of IPv4 addresses, allowing for an almost limitless number of unique IP addresses. The size of the IPv6 address space makes it less vulnerable to malicious activities such as IP scanning. IPv6 packets can support a larger payload than IPv4 packets resulting in increased throughput and transport efficiency.

What is TCP?

**Transmission Control Protocol (TCP)** is a communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send [packets](https://www.fortinet.com/resources/cyberglossary/what-is-packet-loss) across the internet and ensure the successful delivery of data and messages over networks.

TCP is one of the basic standards that define the rules of the internet and is included within the standards defined by the Internet Engineering Task Force (IETF). It is one of the most commonly used protocols within digital network communications and ensures end-to-end data delivery.

TCP vs. IP: What is the Difference?

TCP and IP are separate protocols that work together to ensure data is delivered to its intended destination within a network. IP obtains and defines the address—the IP address—of the application or device the data must be sent to. TCP is then responsible for transporting and routing data through the network architecture and ensuring it gets delivered to the destination application or device that IP has defined. Both technologies working together allow communication between devices over long distances, making it possible to transfer data where it needs to go in the most efficient way possible.

In other words, the IP address is akin to a phone number assigned to a smartphone. TCP is the computer networking version of the technology used to make the smartphone ring and enable its user to talk to the person who called them.

The four layers of the TCP/IP model are as follows:

Datalink layer: The datalink layer defines how data should be sent, handles the physical act of sending and receiving data, and is responsible for transmitting data between applications or devices on a network. This includes defining how data should be signaled by hardware and other transmission devices on a network, such as a computer’s device driver, an Ethernet cable, a network interface card (NIC), or a wireless network. It is also referred to as the link layer, network access layer, network interface layer, or physical layer and is the combination of the physical and data link layers of the Open Systems Interconnection (OSI) model, which standardizes communications functions on computing and telecommunications systems.

Internet layer: The internet layer is responsible for sending packets from a network and controlling their movement across a network to ensure they reach their destination. It provides the functions and procedures for transferring data sequences between applications and devices across networks.

Transport layer: The transport layer is responsible for providing a solid and reliable data connection between the original application or device and its intended destination. This is the level where data is divided into packets and numbered to create a sequence. The transport layer then determines how much data must be sent, where it should be sent to, and at what rate. It ensures that data packets are sent without errors and in sequence and obtains the acknowledgment that the destination device has received the data packets.

Application layer: The application layer refers to programs that need TCP/IP to help them communicate with each other. This is the level that users typically interact with, such as email systems and messaging platforms. It combines the session, presentation, and application layers of the OSI model.

**Backup:**

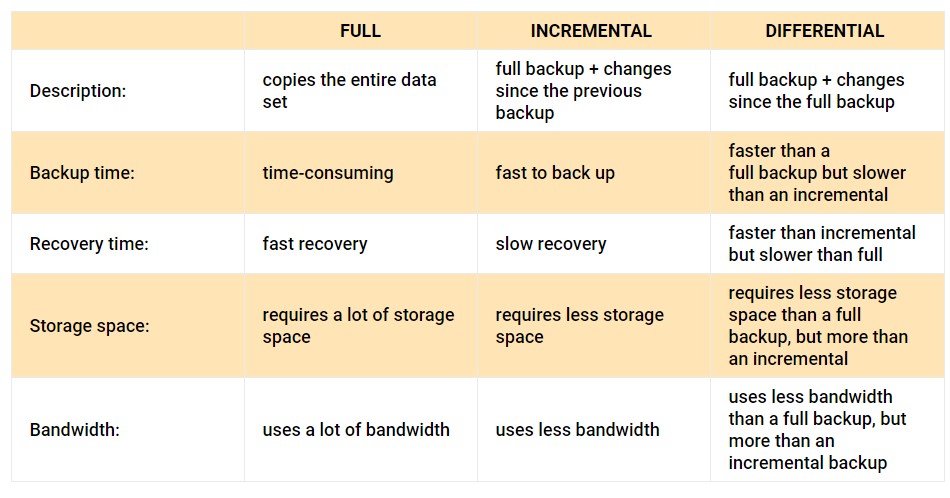
* Backup is an additional copy of data that can be used for restore and recovery purposes
* This Backup copy can be created by: – Simply copying data (there can be one or more copies) – • Mirroring data (the copy is always updated with whatever is written to the primary

Backup strategy:

* A backup is put in place to avoid permanent data loss
* To ensure the integrity of stored data
* Can get back to a previous version
* Build up the data correctly if current data found to be in error

Three basic types of backups

* Full backups
* Differential backups
* Incremental backups



**Full Backup:**

A full backup involves copying the entire data set of the system into a separate partition or onto an external disk.

It requires a lot of free disk space where the copy can be stored.

What’s more, doing a backup of the entire system takes up a lot of time

Schedule full backups on a daily, weekly, or biweekly basis, running incremental or differential backups in between.

For instance, a mid-sized company may set up daily backups of the entire data volume from Monday to Friday. In that case, their backup plan would appear as in the following image:

PROS:

* provides the best protection in terms of data recovery
* fast recovery of data in a single backup set

CONS:

* backup is time-consuming
* requires more storage space
* uses up a lot of bandwidth

**Incremental Backup:**

* An incremental backup is a resource-friendly alternative to full backup.
* Designed only to back up data that has changed since the previous backup. Therefore, it exclusively saves data that has been modified or added to the existing data volume.
* A smaller-sized company that doesn’t require full backups daily can set up incremental backups between two full backup occurrences.
* A full backup of the data set on Monday and then incremental backups between Tuesday and Friday. Therefore, on Tuesday, it creates copies of any changes that have been made since Monday. Next, on Wednesday, it will back up any changes made since Tuesday, and so on.
* As a result, the weekly backup will consist of one full backup along with several smaller backup sets. This method is efficient as it takes up less space on the system. Also, since the sets are smaller compared to the volume set, they take less time to back up.

* PROS:
* smaller backups that take up less storage space
* faster to backup • uses less bandwidth • CONS:
* time-consuming to recover
* risk of failed recovery if there is damage to a segment in the backup chain

**Differential Backup:**

A differential backup is similar to incremental as it relies on a full backup, followed by saving only the changes made on that source volume.

However, it differs in the way these changes are saved. While incremental backups save all changes made since the last backup, differential backups save changes made since the last full backup.

With such a setup, the backup sets do not rely on each other, but rather on the full backup they stem from. As they only consist of two backup sets, their recovery time is much better. This provides better data protection and a valid disaster recovery solution.

In the following example, you see a five-day incremental backup plan. It starts with a full backup on Monday. On Tuesday, it saves only the changes made on the data source. On Wednesday, the backup set consists of all the changes made from Monday to Wednesday. The same procedure is applied on Thursday and Friday.

* PROS:
* faster to restore as it only has two backup sets
* faster to back up compared to full backups
* takes up less space than full backups
* CONS:
* takes up more space than incremental backups
* slower to back up compared to incremental backups

**Groups in Operating System**

* A group is a collection of users who can share files and other system resources.
* For example, the set of users working on the same project could be formed into a group.
* A group is traditionally known as a UNIX group.
* Each group must have a name, a group identification (GID) number, and a list of user names that belong to the group.
* A GID identifies the group internally to the system.
* The two types of groups that a user can belong to are:
* Primary group – Specifies a group that the operating system assigns to files created by the user. Each user must belong to a primary group.
* Secondary groups – Specifies one or more groups to which a user also belongs. Users can belong to up to 15 secondary groups.
* Sometimes a user's secondary group is not important. For example, ownership of files reflect the primary group, not any secondary groups.
* Other applications, however, might rely on a user's secondary memberships. For example, a user has to be a member of the sysadmin group (group 14) to use the Admintool software, but it doesn't matter if group 14 is his or her current primary group.
* The groups command lists the groups that a user belongs to.
* A user can have only one primary group at a time.
* However, a user can temporarily change the user's primary group (with the newgrp command) to any other group in which the user is a member.

When adding a user account, you must assign a primary group for a user or accept the default group, staff (group 10). The primary group should already exist (if it doesn't exist, specify the group by a GID number).

* User names are not added to primary groups. If they were, the list might become too long. Before you can assign users to a new secondary group, you must create the group and assign it a GID number.
* Groups can be local to a system or can be managed through a name service.
* To simplify group administration, you should use a name service like NIS, which enables you to centrally manage group memberships.
* A number of built-in accounts are automatically created when you install Active Directory. This not only applies to user accounts, but group accounts as well.
* Many of these groups have preconfigured rights, which allow members to perform specific tasks.
* When users are added to these groups, they are given these rights in addition to any assigned permissions to access resources.
* The groups that are created when Active Directory is installed can be accessed through Active Directory Users and Computers, and are located in two containers: Builtin and Users.
* Although they are stored in these containers, they can be moved to other OUs (Organizational units) within the domain.
* An organizational unit (OU) is a container within a Microsoft Active Directory domain which can hold users, groups and computers.
* It is the smallest unit to which an administrator can assign Group Policy settings or account permissions.
* Those in the Built-in container have a domain local scope, while those in the Users container have either a domain local, global, or universal scope.
* **Default Groups in Builtin Container**
* Account Operators, which allows members to manage accounts
* Administrators, which gives members full control
* Backup Operators, which allows members to back up and restore files
* Guests, which gives members minimal access
* Incoming Forest Trust Builders, which is only available in forest root domains, and gives members permission to Create Inbound Forest Trusts
* Network Configuration Operators, which allows members to manage network settings
* Performance Monitor Users, which allows users to manage performance counters and use System Monitor
* Performance Log Users, which allows users to manage performance counters and use Performance Logs and Alerts
* Pre-Windows 2000 Compatible Access, which is used for backward compatibility
* Print Operators, which allows members to manage printers
* Remote Desktop Users, which allows members to connect to servers using Remote Desktop
* Replicator, which is used for replication purposes
* Server Operators, which allows members to manage servers
* Users, which contains every user account created in the domain

**Default Groups in Users Container**

* Cert Publishers, which gives members the ability to publish certificates
* DnsAdmins, which provides administrative access to the DNS Server service

DnsUpdateProxy, which provides members with the ability to perform dynamic updates for other clients

Domain Admins, which gives members full control of the domain

* Domain Computers, which includes computers that are part of the domain • Domain Controllers, which includes DCs

•

**User Group in Operating System**

* A User Group in Windows operating system can be defined as a Group or Collection of multiple User Accounts governed by the same or common set of privileges and security settings.
* For example, let us assume that you believe in providing Guests and Visitors to your house with access to your computer. In this case, you can create separate User Accounts for children, teens and adults with limited privileges.
* Now, instead of having to manage these accounts individually, you can Add these accounts to a User Group and manage these accounts at a Group Level.

Administrators: the users from this group have full control of the Windows computer and everything on it, including other user accounts.

Backup Operators: user accounts from this group can back up and restore files on the Windows computer, regardless of those files’ permissions.

Guests: users from this group have temporary profiles set when they log on, which are automatically deleted when they log out.

Power Users: can do almost everything administrators can, including creating other user accounts or even deleting them. However, they cannot change the settings for the Administrators group.

* Users: are the standard user accounts. They are the users who can do all the typical things people do on their computers, like browsing the internet, using the apps installed, accessing the files on the computer, or printing. However, standard users cannot do things like creating other user accounts, they cannot install applications on the computer, and they cannot install a printer on the computer.
* Third-party software and services can also create user groups used for various services. The most common example is virtualization software. For example, some VMWare products such as VMware Converter create user groups like \_\_vmware\_\_ and \_\_\_vmware\_conv\_sa\_\_\_, as well as \_\_\_VMware\_Conv\_SA\_\_\_ accounts, which are used to run virtual machines and standalone server jobs.
* **Shared Resources in Operating System**
* Shared resources, also known as network resources, refer to computer data, information, or hardware devices that can be easily accessed from a remote computer through a local area network (LAN) or enterprise intranet.
* Successful shared resource access allows users to operate as if the shared resource were on their own computer.
* The most frequently used shared network environment objects are files, data, multimedia and hardware resources like printers, fax machines and scanners.

Shared LAN points are used by a variety of system resources, such as hard drives, printers, scanners and network cards.

File and printer sharing occur via two network communication mechanisms: peer-to-peer (P2P) sharing and the client-server network model.

* Sharing network resources requires abiding by certain constraints, as follows:
* **Security:** Organizations present ongoing opportunities for unauthorized shared resources. Security mechanisms should be implemented to provide efficient parameters.
* **Compatibility:** Various client-server operating systems may be installed, but the client must have a compatible OS or application to access shared resources. Otherwise, the client may encounter issues that create communication delays and requires troubleshooting.
* **Mapping:** Any shared OS hardware drive, file or resource may be accessed via mapping, which requires a shared destination address and naming conventions.
* **File Transfer Protocol (FTP) and File Sharing:** FTP is not affected by shared resources because the Internet is FTP’s backbone. File sharing is an LAN concept.

**Shared Disk Storage in OS**

* Shared storage is a type of storage resource that is shared or accessed by multiple users.
* It is generally used in enterprise IT environments where a central storage infrastructure is shared between multiple users across the organization's network.
* Typically, shared storage is in the form of:
* Storage area network (SAN)
* Network attached storage (NAS)
* Storage server
* Cloud storage
* To access data within the shared storage, users are required to authenticate themselves on the shared storage medium, central storage server or a storage management application.
* Once authenticated, and based on their permission level, users can access, modify and create data to/from the shared storage.
* Shared storage can be accessed:
* Directly over the local network or through FTP
* Over the Internet through a storage management application
* Programmatic access using API
* Shared storage is a medium accessible by all of the subscribers in a network, intended for file storage and allowing simultaneous access by multiple subscribers without the need to duplicate files to their computers.
* Because only one file server exists containing all the data, backup and archiving processes are streamlined, and the risk of conflicting backups or archives is eliminated.
* A shared storage device differs from a storage area network (SAN). A shared storage device has multiple ports or a way to identify and track multiple sessions in a single port.
* In contrast, a SAN connects systems and storage for the purpose of transmitting data. Some SANs contain shared storage devices.
* While shared storage can reside on a physical drive, the associated hardware can get expensive. However, virtual storage can also be virtualized. For example, VMware offers a virtualized shared storage solution called vSphere.

**Shared Files in OS**

Files are used for all input and output (I/O) of information in the operating system, to standardize access to both software and hardware.

Input occurs when the contents of a file is modified or written to.

* Output occurs when the contents of one file is read or transferred to another file.
* For example, to create a printed copy of a file, the system reads the information from the text file and writes that information to the file representing the printer.
* File sharing, also known as file-swapping is the accessing or sharing of files by one or more users.
* It is performed on computer networks as a quick way to transmit data.
* Generally, a file-sharing system usually has more than one administrator, where the users may have the same or different access privileges.
* It also implies having an allocated amount of personal files in the common storage.
* File sharing has been used in mainframe and multi-user computer systems for many years, and now with widespread access to the internet, a file transfer system known as the File-Transfer Protocol or FTP is widely used.
* However, in the file-sharing system, the user can read and write in the files, and if the entire system is not available for access, at least the common file that is shared by the owner can be read and written onto.

**Shared Folder in OS**

* In computers, a folder is the virtual location for applications, documents, data or other subfolders.
* Folders help in storing and organizing files and data in the computer. The term is most commonly used with graphical user interface operating systems.
* A shared folder is a special type of workspace that enables you to share the contents of a folder in your Windows file system across all computers on which you have your account, and with other users by invitation.
* When we invite people to join a shared folder, they select a folder for sharing on their computers. All members of a shared folder have access to its contents (files and subfolders).
* A shared folder can contain applications, data, or a user's personal data, called a home folder.

Each type of data requires different shared folder permissions.

* The following are characteristics of shared folder permissions:
* Shared folder permissions apply to folders, not individual files. Because you can apply shared folder permissions only to the entire shared folder and not to individual files or subfolders in the shared folder, they provide less detailed security than NTFS permissions.
* Shared folder permissions don't restrict access to users who gain access to the folder at the computer where the folder is stored. They apply only to users who connect to the folder over the network.
* Shared folder permissions are the only way to secure network resources on a FAT volume. NTFS permissions aren't available on FAT volumes.
* The default shared folder permission is Full Control, and it is assigned to the Everyone group when you share the folder.

**Printer Sharing**

* Printer sharing is the process of sharing printers installed on one computer with other computers on the same network.

Printer sharing enables multiple users or clients to access a printer that they are not directly connected to.

Several computers with different operating systems, all connected to the same shared printer. This arrangement reduces the expense on a network, because fewer printers are required.

* In enterprise environments, you share printers when you set up your IT infrastructure to allow multiple computers in the network to use printers installed on other computers in your network.
* Windows facilitates printer sharing by handling communication between computers and devices on the network and printers.
* Each node or device on the network can print to any shared printer and, to some extent, make changes to the printer settings, depending on the permissions set by the administrator for each user.
* Printer sharing involves at least two computers:
* A server: the computer where you install your printer.
* A client: a computer that accesses your printer through the host.
* When you share a printer, your client installs the printer driver from your server. The print queue stays on the server.
* Shared printing can make it easier to share group access to printers you install on hosts when your users work on clients.
* If a printer is attached to a computer that supports printer sharing, the computer can share that printer with other computers on the same network.
* It does not matter whether the shared printer is old or new, as long as it is properly installed in one computer it can be shared by that computer.
* The sharing is facilitated by the OS, which handles the communication between computers and devices within the network and the printer itself.
* When a print request is sent from a networked computer, this is received by the computer where the shared printer is attached; this host computer initializes the printer and then sends the print job to it.
* Unfortunately, retrieval of the actual printouts still must be done manually by the initiator of the print job.

**Access Control in Operating System**

* A crucial element of operating systems is protection, controlling who is permitted to access various system resources and what they are allowed to do.
* Protection is the mechanism that enforces security policies.
* An operating system is responsible for giving programs access to the resources they need when they run.
* Different users will have different access privileges to files, devices, and other system resources.
* The operating system must enforce these access privileges.
* Users should not be able to read or modify data if a policy prohibits them from doing so. Processor time and system memory are also finite resources that need to be allocated across all process in a fair manner that conforms to established policies.
* Access control refers to the policies and mechanisms that control who is permitted access to resources and what they can do to those resources.
* To enforce security policies and protect resources, we need to know who they apply to. This requires authenticating the user.
* Authentication is the process of getting and validating a user’s identity. After that, the system can authorize the user’s access to a desired resource.

Authorization determines whether an authenticated user is permitted access to a resource and is based on the security policy.

A policy is the definition of what is or is not permissible in the organization. A protection mechanism enforces security policies.

* Processes are run by users. A protection mechanism enables different users to have varying levels of access to resources, an ability to run specific programs, and in some cases, run certain programs with privileges other than those of the user.
* At the operating system level, protection encompasses several components:
* User accounts: Users need to identify themselves and be authenticated so the system can have assurance of the integrity of the user and apply appropriate policies to the user’s requested actions.
* User privileges: Each process run by the system or by a user runs with specific privileges that define access rights – what resources the process can and cannot access. In most cases, these resources are files but they can be devices or communication interfaces.
* Scheduling: The operating system is responsible for scheduling processes and may give certain users a higher priority for the programs they run than others. Some processes may also need to run with a higher priority to service certain system events or real-time tasks effectively.
* Quotas: Many operating systems also support quotas: limits on how much file system space, memory, or CPU a process is allowed to use. These limits must also be enforced.

**Types of Access control**

* **Discretionary Access Control (DAC)**
* DAC provides access rights depending upon the rules already set by the administrators.
* In this type of access control model, each resource has an owner or admin that decides to whom to give access and at what level.
* DAC decentralizes security decisions, allowing administrators and resource owners to give access to users at specified levels.
* It uses ACLs (access control lists), which define at what level to give users permission to a particular resource.
* **Role-Based Access Control (RBAC)**
* System administrators use the RBAC (or non-discretionary) access control model to give access based on the organizational roles, rather than considering a single user account within a company.
* Only people with roles that need to do the particular work are given access to the resource.
* With RBAC, administrators define roles and determine the resources that a role needs access to.
* Each user is then assigned to a role that gives them the appropriate permissions to do their job.
* Users can join different groups but can only be given one role.
* **Attribute-Based Access Control (ABAC)**
* In contrast to the role-defined access control method of RBAC, ABAC is a complex strategy that applies a multitude of attributes to both users and resources.
* While it is more complicated than RBAC, it gives admins the flexibility to make decisions according to context and evolving levels of risk.
* Users are only able to access resources that have corresponding attributes.
* Attributes can include user demographics such as job title or security clearance; resource properties such as file type or creation date; and even environmental characteristics such as access location or time.

**Windows domain**

* A Windows domain is a form of a computer network in which all user accounts, computers, printers and other security principals, are registered with a central database located on one or more clusters of central computers known as domain controllers.
* Authentication takes place on domain controllers.
* Each person who uses computers within a domain receives a unique user account that can then be assigned access to resources within the domain.
* Starting with Windows Server 2000, Active Directory is the Windows component in charge of maintaining that central database.
* The concept of Windows domain is in contrast with that of a workgroup in which each computer maintains its own database of security principals.

**Configuration**

* Computers can connect to a domain via LAN, WAN or using a VPN connection.
* Users of a domain are able to use enhanced security for their VPN connection due to the support for a certification authority which is gained when a domain is added to a network, and as a result, smart cards and digital certificates can be used to confirm identities and protect stored information.
* **Domain controller**
* In a Windows domain, the directory resides on computers that are configured as domain controllers.
* A domain controller is a Windows or Samba server that manages all security-related aspects between user and domain interactions, centralizing security and administration.
* A domain controller is generally suitable for networks with more than 10 PCs.
* A domain is a logical grouping of computers.
* The computers in a domain can share physical proximity on a small LAN or they can be located in different parts of the world.
* As long as they can communicate, their physical location is irrelevant.
* Active Directory
* Computers inside an Active Directory domain can be assigned into organizational units according to location, organizational structure, or other factors.
* In the original Windows Server Domain system (shipped with Windows NT 3.x/4), machines could only be viewed in two states from the administration tools; computers detected (on the network), and computers that actually belonged to the domain.
* Active Directory makes it easier for administrators to manage and deploy network changes and policies to all of the machines connected to the domain.
* Workgroups
* Windows Workgroups, by contrast, is the other model for grouping computers running Windows in a networking environment which ships with Windows.
* Workgroup computers are considered to be 'standalone' - i.e. there is no formal membership or authentication process formed by the workgroup.
* A workgroup does not have servers and clients, and hence represents the peer-to-peer (or client-to-client) networking paradigm, rather than the centralized architecture constituted by Server-Client.
* Workgroups are considered difficult to manage beyond a dozen clients, and lack single sign on, scalability, resilience/disaster recovery functionality, and many security features.
* Windows Workgroups are more suitable for small or home-office networks.
* Using the domain controller, administrators can configure all sorts of security and use policies for all computers. For example, Group Policy makes all the following practices easy to apply:
* Removing items from the Start Menu
* Stop users from changing internet connection options
* Block the Command Prompt
* Redirect a certain folder to use one on the server instead
* Prevent the user from changing sounds
* Map a printer to new computers automatically
* This is just a small sampling of what Group Policy allows. Administrators can set these changes up once and have them apply to all computers, even new ones they set up later.

**Business Inquiry Letter**

A **Business inquiry letter** is a type of business letter written to communicate with a business organization to ask for information about specific jobs, products, or services. Usually, these letters are written in response to some kind of advertisement that you may have seen on television or the Internet. If you want to buy any product after seeing an advertisement but having trouble making up your mind, then you can write a product Inquiry letter to the organization to ask for more detailed information about the product.

There are many types of inquiry letters, but two major types are **product inquiry letters** and[**job inquiry letter**](https://www.doctemplates.net/job-inquiry-letter/). By writing an inquiry letter or email, you can ask the company to provide you a catalog or brochure with more details of their product. So, you can be sure about a certain thing before buying the product.

Business Inquiry Letter is written in a [**formal business letter format**](https://www.doctemplates.net/formal-business-letter-formats-with-examples/) and should be straightforward, compact and precise.

**Structure of a Business Inquiry Letter**

A letter can be divided into a few basic sections for better understanding;

1. A formal introduction needs to be used like “Dear Sir”, “Dear Ma’am” to start your letter. A formal introduction is required as you are not familiar with the recipient.
2. A description of your request is required; it includes the reference of the advertisement and name of the product or service. After writing down the reference, you have to ask for the details you require about the product. You can also ask for a catalog or brochure to help you with the details. If you have some additional details to ask for, except for the information on brochures or catalogs, you can specifically ask for that information.
3. A final summary can be written to explain your overall request.
4. A Signature of your agency or yours in a very formal way.

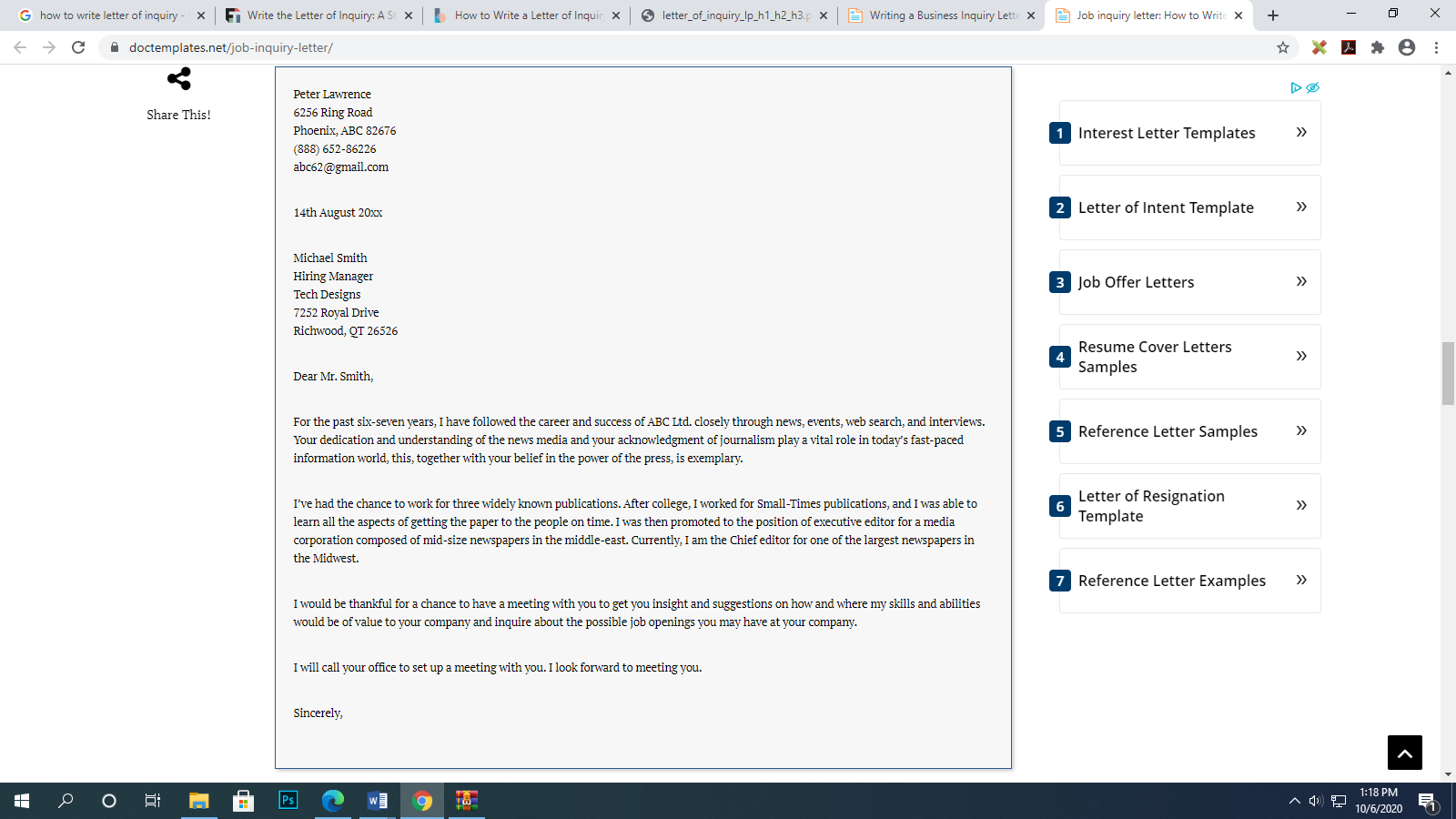
**Tips for writing a Business Inquiry Letter**

* Keep your letter short and precise. Don’t mention unnecessary information in such letters. Be very specific about the information you need. If you put only the necessary details, then your letter will look more readable, and you will still be able to convey your message.
* If you are [**inquiring about a job or work-related vacancy**](https://www.doctemplates.net/job-inquiry-letter/)**,** then you should try to properly start your letter with a professional but friendly tone. But always remember that rest of the letter should live up to the anticipation build by your impressive opening.
* You should know the exact source of your information. In an office, there are a number of people with dozens of different designations, and it is very important to know the appropriate recipient and direct your letter to him.
* You must research properly on the topic of your inquiry before you start writing the letter, to know as much as possible about your query.

## Elements of a Typical Letter of Inquiry

1. **Subject line**. Include a subject line so readers can immediately identify the contents of the letter—even before perusing the text.
2. **Introduction.** Explain why you’ve sent them the letter of inquiry to learn if you might be invited to submit a full proposal. Include the amount of funding you’re requesting in this section. Also provide a brief executive summary. The introduction should be a [short executive summary](https://www.thebalancesmb.com/how-to-write-the-executive-summary-of-your-grant-proposal-2501963). It includes the name of your organization, the amount of money requested, and a description of the project. You'll want to explain how the project fits with the funder's guidelines and funding interests.
3. **Organization overview.** Provide a brief overview of your organization with a clear focus on your ability to fulfill the stated need. Describe the staff and their relevant qualifications related to the project. (Save the mission statement for your full proposal.) Be concise and concentrate on your organization's ability to meet the need that you've stated. Give a brief history of your nonprofit and provide an overview of your programs. Make sure to connect directly what you currently do and what you want to accomplish with the requested funding.
4. **Need or problem statement.** Describe the need or problem clearly. Include relevant demographics, a few concrete examples of the problem, and supporting statistical data. Explain the [need that can be met by your project](https://www.thebalancesmb.com/how-to-write-a-need-statement-for-your-grant-proposal-2501959). Describe the target population and geographic area. Provide a few significant statistical facts and several examples.
5. **Project description.** Show that you have a viable solution appropriate to the need. Describe the project briefly and include supporting activities, direct staff involvement and titles, and desired objectives. How will you solve the need? Describe the project succinctly and include the major activities, names, and titles of key project staff, and your project's objectives.
6. **Other funding sources.**List other funding sources, including government agencies and private and public foundations, including those you currently are approaching for funding support. If you are approaching other agencies or nonprofits for [support of this project](https://www.thebalancesmb.com/what-is-a-letter-of-support-for-a-grant-proposal-2502223), mention them in a brief paragraph. Include whatever funding you've already gotten and explain how you expect to support the project after the start-up period.
7. **Fit with the funder’s focus.**Communicate clearly how your project relates to their funding guidelines and philanthropic philosophy.
8. **Clear closing.**Wrap up the letter with contact information. Assure your readers you are available to answer any additional questions that might not be covered in the letter. Show appreciation for their considering your request. Restate the intent of your project, invite additional questions and thank the funder for his or her time and consideration. Include any attachments asked for in the funder's guidelines.
9. **Attachments.** Include only those attachments clearly spelled out by potential funders’ guidelines. Attach a project budget clearly showing the relationship between financial support and project’s sustainability.

### **Job Inquiry Letter Sample**



### **Assignment:**

### Inquiry Letter for a Product

### Service Inquiry Letter

### Job Inquiry Letter

**Correspondence: Text Messages, Emails, Memos, and Letters**

Correspondence is the most important channel through which Business Communication and Official Communication takes place in any written or digital form between two or more parties. It may be in the form of letters, memos, e-mail messages, text messages, fax messages, voicemails, notes etc.

1. **Netiquette**

Text messaging, emailing, and posting on social media in a professional context requires that you be familiar with “netiquette,” or proper etiquette for using the internet. We have all heard the news stories about [people who have been fired](https://careers.workopolis.com/advice/14-canadians-who-were-fired-for-social-media-posts/) and [companies that have been boycotted for making offensive or inappropriate social media posts](https://www.entrepreneur.com/article/294925). People have even gone to prison for [illegal use of private messaging](https://en.wikipedia.org/wiki/Anthony_Weiner_sexting_scandals).  The digital world may seem like a free-for-all, “wild wild west” with no clear rules or regulations; however, this is clearly a dangerous perspective for a professional to take, as the consequences for breaking tacit rules, expectations, and guidelines for professional communications can be very costly.

The way that you represent yourself in writing carries significant weight. Writing in an online environment requires tact, skill, and an awareness that what you write may be there for a very long time and may be seen by people you never considered as your intended audience. From text messages to memos to letters, from business proposals to press releases, your written business communication represents you and your company:  your goal is to make it clear, concise, constructive, and professional.

We create personal pages, post messages, and interact via online technologies as a normal part of our careers, but how we conduct ourselves can leave a lasting image, literally. The photograph you posted on your Instagram page or Twitter feed may have been seen by your potential employer, or that insensitive remark in a Facebook post may come back to haunt you later.

**Guidelines for Communicating Online**

Following several guidelines for online postings, as detailed below, can help you avoid embarrassment later:

* **Know your context**
  + Introduce yourself
  + Avoid assumptions about your readers; remember that culture influences communication style and practices
  + Familiarize yourself with policies on Acceptable Use of IT Resources at your organization.
* **Remember the human**
  + Remember there is a person behind the words; ask for clarification before making judgment
  + Check your tone before you publish; avoid jokes, sarcasm, and irony as these can often be misinterpreted and get “lost in translation” in the online environment
  + Respond to people using their names
  + Remember that culture, age, and gender can play a part in how people communicate
  + Remain authentic and expect the same of others
  + Remember that people may not reply immediately. People participate in different ways, some just by reading the communication rather than jumping into it.
* **Recognize that text is permanent**
  + Be judicious and diplomatic; what you say online may be difficult or even impossible to retract later.
  + Consider your responsibility to the group and to the working environment
  + Agree on ground rules for text communication (formal or informal; seek clarification whenever needed) if you are working collaboratively
* **Avoid flaming:  research before you react**
  + Accept and forgive mistakes
  + Consider your responsibility to the group and to the working environment
  + Seek clarification before reacting; what you heard is not always what was said
  + Ask your supervisor for guidance. Sometimes, online behavior can appear so disrespectful and even hostile that it requires attention and follow up. In this case, let your supervisor know right away so that the right resources can be called upon to help.
* **Respect privacy and original ideas**
  + Quote the original author if you are responding with a specific point made by someone else
  + Ask the author of an email for permission before forwarding the communication.

1. **Texting**

Whatever digital device you use, written communication in the form of brief messages, or texting, has become a common way to connect. It is useful for short exchanges, and is a convenient way to stay connected with others when talking on the phone would be cumbersome. Texting is not useful for long or complicated messages, and careful consideration should be given to the audience.

When texting, always consider your audience and your company, and choose words, terms, or abbreviations that will deliver your message appropriately and effectively.

**Guidelines for Effective Business Texting**

If your work situation allows or requires you to communicate via text messages, keep the following tips in mind:

* **Know your recipient:**  “? % dsct” may be an understandable way to ask a close associate what the proper discount is to offer a certain customer, but if you are writing a text to your boss, it might be wiser to write, “what % discount does Murray get on $1K order?”
* **Anticipate unintentional misinterpretation:**  texting often uses symbols and codes to represent thoughts, ideas, and emotions. Given the complexity of communication, and the useful but limited tool of texting, be aware of its limitation and prevent misinterpretation with brief messages.
* **Use appropriately:**contacting someone too frequently can border on harassment. Texting is a tool. Use it when appropriate but don’t abuse it.
* **Don’t text and drive:**  research shows that the likelihood of an accident increases dramatically if the driver is texting behind the wheel.[[2]](https://pressbooks.bccampus.ca/technicalwriting/chapter/correspondence/#footnote-1081-2) Being in an accident while conducting company business would reflect poorly on your judgment as well as on your employer.

1. **Email**

Email is familiar to most students and workers. In business, it has largely replaced print hard copy letters for external (outside the company) correspondence, and in many cases, it has taken the place of memos for internal (within the company) communication.

Email can be very useful for messages that have slightly more content than a text message, but it is still best used for fairly brief messages. Many businesses use automated emails to acknowledge communications from the public, or to remind associates that periodic reports or payments are due. You may also be assigned to “populate” a form email in which standard paragraphs are used but you choose from a menu of sentences to make the wording suitable for a particular transaction.

Emails may be informal in personal contexts, but business communication requires attention to detail, awareness that your email reflects you and your company, and a professional tone so that it may be forwarded to any third party if needed. Email often serves to exchange information within organizations. Although email may have an informal feel, remember that when used for business, it needs to convey professionalism and respect. Never write or send anything that you wouldn’t want read in public or in front of your company president.

As with all writing, professional communications require attention to the specific writing context, and it may surprise you that even elements of form can indicate a writer’s strong understanding of audience and purpose. The principles explained here apply to the educational context as well; use them when communicating with your instructors and classroom peers.

**Guidelines for Effective Business Emails**

**Open with a proper salutation:** proper salutations demonstrate respect and avoid mix-ups in case a message is accidentally sent to the wrong recipient. For example, use a salutation like “Dear Ms. X” (external) or “Hi Barry” (internal).

**Include a clear, brief, and specific subject line:** this helps the recipient understand the essence of the message. For example, “Proposal attached” or “Electrical specs for project Y.”

**Close with a signature:** identify yourself by creating a signature block that automatically contains your name and business contact information.

**Avoid abbreviations:** an email is not a text message, and the audience may not find your wit cause to ROTFLOL (roll on the floor laughing out loud).

**Be brief:** omit unnecessary words.

**Use a good format:** divide your message into brief paragraphs for ease of reading. A good email should get to the point and conclude in three small paragraphs or less.

**Reread, revise, and review:** catch and correct spelling and grammar mistakes before you press “send.” It will take more time and effort to undo the problems caused by a hasty, poorly written email than to take the time to get it right the first time.

**Reply promptly:** watch out for an emotional response—never reply in anger—but make a habit of replying to all emails within twenty-four hours, even if only to say that you will provide the requested information in forty-eight or seventy-two hours.

**Use “Reply All” sparingly:** do not send your reply to everyone who received the initial email unless your message absolutely needs to be read by the entire group.

**Avoid using all caps:** capital letters are used on the Internet to communicate emphatic emotion or yelling and are considered rude.

**Test links:** if you include a link, test it to make sure it is working.

**Email ahead of time if you are going to attach large files:** audio and visual files are often quite large; be careful to avoid exceeding the recipient’s mailbox limit or triggering the spam filter.

**Give feedback or follow up:** if you don’t get a response in twenty-four hours, email or call. Spam filters may have intercepted your message, so your recipient may never have received it.

**Tip**:  add the address of the recipient last to avoid sending prematurely.  This will give you time to do a last review of what you’ve written, make sure links work, make sure you’ve added the attachment, etc., before adding the sender’s address and hitting send.

1. **Memos**

Memoranda, or **memos**, are one of the most versatile document forms used in professional settings.  Memos are “in house” documents (sent within an organization) to pass along or request information, outline policies, present short reports, and propose ideas.  While they are often used to inform, they can also be persuasive documents.  A company or institution typically has its own “in house” style or template that is used for documents such as letters and memos.

**Memo Format**

**Figure** shows a sample of our “in house” memo style (the style we will use for memo assignments written for this class), with annotations pointing out various relevant features. The main formatted portions of a memo are the Logo or Letterhead (optional), the Header Block, and the Message.  The attached [Memos PowerPoint](https://pressbooks.bccampus.ca/technicalwriting/wp-content/uploads/sites/296/2018/05/Memos-.ppt) reviews some of these features in detail.

**Design features of a 1-page memorandum.**

* The logo or letterhead is at the top of the page and centred or right-aligned (in this case, it is the University of Victoria letterhead).
* “Memorandum” appears at the top of the page left-aligned in large, bold font.
* The header block (which appears under the “Memorandum” heading) includes a “to,” “from,” “date,” and “subject” in a vertical list. Those values are aligned vertically for readability.
* A dividing line separates the header block from the message.
* The message begins by answering, “Why am I reading this?”
* The body of the message gives the details: (“What do I need to know?”)
* There is a table that is nicely formatted. (The table has a caption above the table in bold and italics, column headers are bold and centred, and text is left aligned.)
* A closing paragraph summarizes and indicates what (if any) action is expected of the reader (Answering, “What would you like me to do now?”)
* The text of this document uses an appropriate serif body font (Times New Roman)
* There is also a signature (optional)

**Memo Header Block**

The **Header Block** appears at the top left side of your memo, directly underneath the word **MEMO** or **MEMORANDUM** in large, bold, capitalized letters.  This section contains detailed information on the recipient, sender, and purpose.  It includes the following lines:

* **TO:**give the recipient’s full name, and position or title within the organization
* **FROM**:  include the sender’s (your) full name and position or title
* **DATE**:   include the full date on which you sent the memo
* **SUBJECT or RE**:  write a brief phrase that concisely describes the main content of your memo.

Place a horizontal line under your header block, and place your message below.

**Memo Message**

The length of a memo can range from a few short sentences to a multi-page report that includes figures, tables, and appendices.  Whatever the length, there is a straightforward organizational principal you should follow.  Organize the content of your memo so that it answers the following questions for the reader:

1. **Opening:** Do I have to read this?  Why do I have to read this?
2. **Details:** What do I need to know?
3. **Closing:** What am I expected to do now?

Memos are generally very direct and concise.  There is no need to start with general introductions before getting to your point. Your readers are colleagues within the same organization, and are likely familiar with the context in which you are writing.  The opening sentences of the memo’s message should make it clear to the reader whether they have to read this entire memo and why (if the memo is informing me about an elevator that’s out of service in a building I never enter, then I don’t really have to read any further).

The middle section of the message should give all of the information needed to adequately inform the readers and fulfill the purpose of the memo. Start with the most general information, and then add the more specific facts and details. Make sure there is enough detail to support your purpose, but don’t overwhelm your readers with unnecessary details or information that is already well known to them.

The final part of the message indicates what, if any, action is required or requested of the readers.  If you are asking your readers to do something, be as courteous as possible, and try to indicate how this action will also benefit them.

1. **Letters**

Letters are brief messages sent to recipients that are often outside the organization. They are often printed on letterhead paper that represents the business or organization, and are generally limited to one or two pages. While email and text messages may be used more frequently today, the business letter remains a common form of written communication. It can serve to introduce you to a potential employer, announce a product or service, or even serve to communicate feelings and emotions (compliant letters, for example).

There are many types of letters, and many adaptations in terms of form and content, but this chapter presents the fifteen elements of a traditional block-style letter. Letters may serve to introduce your skills and qualifications to prospective employers (cover letter), deliver important or specific information, provide documentation of an event or decision, or introduce an attached report or long document (letter of transmittal). **Figure** shows a letter of transmittal meant to introduce a technical report to its recipient.

A typical letter has 7 main parts:

1. **Letterhead/logo**:  Sender’s name and return address
2. **The heading:**  names the recipient, often including address and date
3. **Salutation**:  “Dear \_\_\_\_\_\_ ” use the recipient’s name, if known.
4. **The introduction**:  establishes the overall purpose of the letter
5. **The body**:  articulates the details of the message
6. **The conclusion:**  restates the main point and may include a call to action
7. **The signature line:**  sometimes includes the contact information

 Keep in mind that letters represent you and your company in your absence. In order to communicate effectively and project a positive image, remember that

* your language should be clear, concise, specific, and respectful
* each word should contribute to your purpose
* each paragraph should focus on one idea
* the parts of the letter should form a complete message
* the letter should be free of errors.

**Letters with Specific Purposes**

There are many possible reasons you might write a letter in a professional context.  Here is a list of the most common kinds of letters:

**Transmittal Letters:  w**hen you send a report or some other document, such as a resumé, to an external audience, send it with a cover letter that briefly explains the purpose of the enclosed document and a brief summary.  Click the link to download a [Letter of Transmittal Template (.docx)](https://pressbooks.bccampus.ca/technicalwriting/wp-content/uploads/sites/296/2018/05/Letter-of-Transmittal-Template.docx).

**Letters of Inquiry:** you may want to request information about a company or organization such as whether they anticipate job openings in the near future or whether they fund grant proposals from non-profit groups. In this case, you would send a letter of inquiry, asking for additional information. As with most business letters, keep your request brief, introducing yourself in the opening paragraph and then clearly stating your purpose and/or request in the second paragraph. If you need very specific information, consider placing your requests in list form for clarity. Conclude in a friendly way that shows appreciation for the help you will receive.

**Follow-up Letters:** any time you have made a request of someone, write a follow-up letter expressing your appreciation for the time your letter-recipient has taken to respond to your needs or consider your job application. If you have had a job interview, the follow-up letter thanking the interviewer for his/her time is especially important for demonstrating your professionalism and attention to detail.

Letters within the professional context may take on many other purposes, such as communicating with suppliers, contractors, partner organizations, clients, government agencies, and so on. For additional examples of professional letters, take a look at the sample letters provided by David McMurrey in his online textbook on technical writing: [Online Technical Writing: Examples, Cases & Models](https://www.prismnet.com/~hcexres/textbook/models.html).

# **Document Design**

Technical reports (including handbooks and guides) have various designs depending on the industry, profession, or organization. If you are taking a technical writing course, ask your instructor for any design specifications she has for your documents. The same is true if you are writing a technical report in a science, business, or government context. Organizations very often have their own “stylesheets” on which all organizational document designs are based, so make sure the design presented in this chapter is acceptable.

Technical reports have specifications as do any other kind of project. Specifications for reports involve layout, organization and content, format of headings and lists, the design of the graphics, and so on. The advantage of a required structure and format for reports is that you or anyone else can expect them to be designed in a familiar way—you know what to look for and where to look for it. Reports are usually read in a hurry—people are in a hurry to get to the information they need, the key facts, the conclusions, and other essentials. A standard report format is like a familiar neighborhood.

When you analyze the design of a technical report, notice how repetitive some sections are. This duplication has to do with how people read reports. They don’t read reports straight through: they may start with the executive summary, skip around, and probably not read every page. Your challenge is to design reports so that these readers encounter your key facts and conclusions, no matter how much of the report they read or in what order they read it.

* **Cover Letter**

The cover letter is either attached to the outside of the report with a paper clip or is bound within the report. It is a communication from you—the report writer—to the recipient, the person who requested the report and who may even be paying you for your expert consultation. Essentially, it says “Here is the report that we agreed I’d complete by such-and-such a date. Briefly, it contains this and that, but does not cover this or that. Let me know if it meets your needs.” The cover letter explains the context—the events that brought the report about. It contains information about the report that does not belong in the report.

In the example of the cover letter that follows, notice the standard business-letter format. If you write an internal report, use the memorandum format instead. In either case, the contents and organization are the same:

* **First paragraph.** Cites the name of the report, putting it in italics. It also mentions the date of the agreement to write the report.
* **Middle paragraph.** Focuses on the purpose of the report and gives a brief overview of the report’s contents.
* **Final paragraph.** Encourages the reader to get in touch if there are questions, comments, or concerns. It closes with a gesture of good will, expressing hope that the reader finds the report satisfactory.

As with any other element in a report, you may have to modify the contents of this letter (or memo) for specific situations. For example, you might want to add another paragraph, listing questions you’d like readers to consider as they review the report.

# **Cover page**

Be sure to create a cover page for your report. It’s a step that some report writers forget. Without a label, a report is anonymous; it gets ignored.

The best way to create a cover page is to use your word-processing software to design one on a standard page with a graphic box around the label information. Not much goes on the label: the report title, your name, your organization’s name, a report tracking number, and a date. There are no standard requirements for the label, although your company or organization should have its own requirements. (An example of a report label is shown below.)

Transmittal letter and report cover (with cover label).

* **Cover Sheet**

Many reports will contain a cover sheet that provides basic information.  The layout of the cover sheet may be dictated by whomever is to receive the report (i.e. the Graduate School has a pre-determined layout for thesis and dissertations).  The cover sheet will generally include the following information:

* Title of report
* Your name
* Names of group members (where appropriate)
* Date submitted

# **Abstract and Executive Summary**

Most technical reports contain at least one abstract—sometimes two, in which case the abstracts play different roles. Abstracts summarize the contents of a report, but the different types do so in different ways:

**Descriptive Abstract:** This type provides an overview of the purpose and contents of the report. In some report designs, the descriptive abstract is placed at the bottom of the title page (not the cover page), as shown in the following:

**Executive Summary:** Another common type is the executive summary, which also summarizes the key facts and conclusions contained in the report. Think of this as if you used a yellow highlighter to mark the key sentences in the report and then siphoned them all out onto a separate page and edited them for readability. Typically, executive summaries are one-tenth to one-twentieth the length of reports ten to fifty pages long. For longer reports, ones over fifty pages, the executive summary should not go over two pages. The point of the executive summary is to provide a summary of the report—something that can be read quickly.

If the executive summary, introduction, and transmittal letter strike you as repetitive, remember that readers don’t necessarily start at the beginning of a report and read page by page to the end. They skip around: they may scan the table of contents; they usually skim the executive summary for key facts and conclusions. They may read carefully only a section or two from the body of the report, and then skip the rest. For these reasons, reports are designed with some duplication so that readers will be sure to see the important information no matter where they dip into the report.

* **Table of Contents**

The TOC shows readers what topics are covered in the report, how those topics are discussed (the subtopics), and on which page numbers those sections and subsections start. In creating a TOC, you have a number of design decisions:

* Levels of headings to include. In longer reports, consider not including only the top two levels of headings. This keeps the TOC from becoming long and unwieldy. The TOC should provide an at-a-glance way of finding information in the report quickly.
* Indentation, spacing, and capitalization. Notice in the illustration below that items in each of the three levels of headings are aligned with each other. Although you can’t see it in the illustration, page numbers are right-aligned with each other. Notice also the capitalization: Main chapters or sections are all caps; first-level headings use initial caps on each main word; lower-level sections use initial caps on the first word only.
* Vertical spacing. Notice that the first-level sections have extra space above and below, which increases readability.

Using the automatic TOC creator in your word processor can help you produce a clean, professional document. If you prefer to make your own, learn to use dot leader tabs in order to line up the page numbers correctly. Make sure the words in the TOC are the same as they are in the text. As you write and revise, you might change some of the headings—don’t forget to change the TOC accordingly.

**List of Figures and Tables**

If your document has more than two figures or tables create a separate list of figures. The list of figures has many of the same design considerations as the table of contents. Readers use the list of figures to quickly find the illustrations, diagrams, tables, and charts in your report.

Complications arise when you have both tables and figures. Strictly speaking, figures are illustrations, drawings, photographs, graphs, and charts. Tables are rows and columns of words and numbers; they are not considered figures.

For longer reports that contain dozens of figures and tables each, create separate lists of figures and tables. Put them together on the same page if they fit. You can combine the two lists under the heading, “List of Figures and Tables,” and identify the items as figure or table.

* **Introduction**

The first part of the technical report is the introduction.  This sets the stage for the reader and provides needed background information.  As such, the introduction must cover the purpose of the design/experiment, scope of work, and any needed background knowledge.

* **Scope of Work**– The scope of work is a description of the design or laboratory. This section should include a brief description of the project and outline the calculation requirements.
* **Given Information**– This section should include information given in the problem statement. Typically, this section includes information that is provided by the professor or client and does not require interpretation.
* **Assumptions**– This section should briefly describe any assumptions that are made in addition to the project description and requirements. Typically, assumptions are made by the engineer, not the client, and can be modified or changed.
* **Background**– This section provides the needed technical background for the reader.  If the reader is not familiar with this area of study this section will need to be quite detailed so that the reader can fully understand the experiment and results.  Sometimes the background is its own separate chapter/section in a report.

List of figures and tables followed by the introduction. If there are no tables, make it “List of Figures.” In a technical writing course, ask your instructor if the decimal-numbering style for headings is required.

# **Body of the report**

The body of the report is of course the main text of the report, the sections between the introduction and conclusion. Illustrated below are sample pages.

# **Headings**

In all but the shortest reports (two pages or less), use headings to mark off the different topics and subtopics covered. Headings are the titles and subtitles you see within the actual text of much professional scientific, technical, and business writing. Headings are like the parts of an outline that have been pasted into the actual pages of the document.

Headings are an important feature of professional technical writing: they alert readers to upcoming topics and subtopics, help readers find their way around in long reports and skip what they are not interested in, and break up long stretches of straight text.

Headings are also useful for writers. They keep you organized and focused on the topic. When you begin using headings, your impulse may be to slap in the headings after you’ve written the rough draft. Instead, visualize the headings before you start the rough draft, and plug them in as you write.

Your task in this chapter is to learn how to use headings and to learn the style and format of a specific design of headings. Here are a number of helpful tips:

* Make the phrasing of headings self-explanatory: instead of “Background” or “Technical Information,” make it more specific, such as “Physics of Fiber Optics.”
* Make headings indicate the range of topic coverage in the section. For example, if the section covers the design and operation of a pressurized water reactor, the heading “Pressurized Water Reactor Design” would be incomplete and misleading.
* Avoid “stacked” headings—any two consecutive headings without intervening text.
* Avoid pronoun reference to headings. For example, if you have a heading “Torque,” don’t begin the sentence following it with something like this: “This is a physics principle…..”
* When possible, omit articles from the beginning of headings. For example, “The Pressurized Water Reactor” can easily be changed to “Pressurized Water Reactor” or, better yet, “Pressurized Water Reactors.”
* Don’t use headings as lead-ins to lists or as figure titles.
* Avoid “widowed” headings: that’s where a heading occurs at the bottom of a page and the text it introduces starts at the top of the next page. Keep at least two lines of body text with the heading, or force it to start the new page.

If you manually format each individual heading using the guidelines presented in the preceding list, you’ll find you’re doing quite a lot of repetitive work. The styles provided by Microsoft Word, OpenOffice Writer, and other software save you this work. You simply select Heading 1, Heading 2, Heading 3, and so on. You’ll notice the format and style are different from what is presented here. However, you can design your own styles for headings.

**What is a Feasibility Report?**

A feasibility report is an evidence that attempts to create some sort of action. Feasibility reports are created to persuade/help the decision makers to choose between available options. Remember that your option is not the only one, the decision makers will probably have many to choose from. A feasibility report also determines whether or not the investigated task can be done with the amount of resources available OR how many resources will be necessary in order to complete the task. A feasibility may be useful in a lot of different situations such as event planning, finances, or even remodeling your home.

**What is a feasibility study?**

A feasibility study is a way to evaluate the practicality and desirability of a project. Before a company invests time and money into a project, they need to know how successful the project will be before investing. Sometimes companies want to understand input costs, the amount of research that will need to be done, or even the marketability of a project. With input prices, it is essential that companies understand, (even before they put time and research into the project), how much it would cost to go through with their product. Companies also like to know if they put time into research and go through with their change or promotion of a product, how the public/people will react to the change. Will people be fighting over the new product or will it fall through? The purpose of feasibility studies is to provide companies information and analysis on whether or not you or your company should pursue this course of action.

Feasibility reports are usually used to sway decision makers towards one direction or the other. Many times there is only one course of action but, there needs to be a second course of action.

**Questions to Consider for Your Report:**

* **What to consider in creating feasibility studies/reports?**

It remains important to consider alternatives when you are creating a feasibility study. Decision makers in companies want to understand why they have to make a choice, and then why they should choose this certain option. Feasibility reports need to include detailed information on the problem that has presented itself to provide decision makers with a reason to consider further options.

* **Is your argument important and appropriate?**

When deciding on whether or not your feasibility study is important you must first recognize the target audience or reader. For professional organizations people want your argument or study to be based around needs or aims of the organization and their future. In professional settings, it is believed that those guiding points or criteria should be known by the people judging your study. In other words, make the study reasonable and have it relate to what you are looking at implementing or the change you want to see happen.

Facts can make your argument important. However, decision makers want to know that your sources are reliable. They want to be assured that the information they are receiving is from a credible source in the industry. This may turn out to be the most important aspect of any feasibility study and report. Due simply to the fact that any information you gather, no matter the presentation, can be ruined if you’re lacking information about your sources or in the worst case if your sources are not credible.

* **What to consider about your alternatives?**

It is important to understand how your alternatives compare to the criteria you set in place. In most cases your readers will want to understand how your results compared to others. This allows them to make an educated decision based simply around facts and results. Anderson considers this to be the heart of any feasibility report.

* **What have you found against your alternatives?**

Based on experiments and finding results about possible alternatives and how they fare, it is important to draw conclusions about the alternatives. This is not made to bash other options or products, but is made to set your product or idea apart. You should include general knowledge or conclusions about what each product does well. This remains an important part because once again decision makers need a basis for comparison, they need a reason to select your idea compared to the alternatives and may already be set in place, or in the near future.

* **What should you throw into a conclusion?**

Include in your conclusion how you’re going to go implement your ideas for the company and how it will enrich the company. Explain why the company should choose your course of action. Compare statistics and data and help the readers understand the logical choice and the course of action that would aid in selecting one option over the other. Explain your expertise on the subject matter and help them realize that your idea is the choice they are looking for. Based on your experiences they will most likely take your side if you present the argument efficiently. The company will select your course of action, based on the key points you outline in your feasibility study.

**Important Features of a Basic Feasibility Report**

Below are the seven elements of a feasibility report:

* **Introduction** – You need to persuade the decision maker to even consider any sort of alternative. You need to convince them to even read your report first. Tell them what they will gain personally or as an organization by considering your work.
* **Criteria/Constraints** – You must specifically map out the criteria of what the ideal outcomes are. This will allow you to make practical and logical decisions. You can present the criteria in your feasibility report in one of two ways. First, you can separate the criteria into its own section. This is best when you have a extensive report and you need to go in-depth with the explanation. Second, you can incorporate the criteria throughout your report as the criteria become relevant. However, it is important to realize that whichever strategy you chose make sure that the criteria is introduced early in the report. It is also very important to map out the constraints of your suggested solutions. This will show the audience that you understand and acknowledge the fact that no solution is perfect. This will also make sure that the audience makes the decision in their best interest.
* **Method** – It is very important to present facts that are accurate and relevant. You should state the reliable sources you used and what method they came from (internet, interview, book, etc.). Without a credible research method or credible sources your document itself will lack credibility.
* **Overview of Alternative Options** – You must underline the key features of each possible option. Make sure they are easy to understand and presented in a friendly layout. Keep in mind that the goal is to allow your audience to make the best decision.
* **Evaluation** – This should be the bulk of your report, you must evaluate the options using the criteria you created. Add graphs, charts, etc. to show that you have studied your options, and have come up with statistics that back up your reasons as to why your alternative beats the competition.
* **Conclusions** – You need to state the conclusion you have come up with. How did you evaluate the alternatives? And then from there, which alternative best fit your organization.
* **Recommendations** – You need to use your experience and knowledge in order to state which option you think should be adopted.
* Note: All seven element outlined do not need to be included in the feasibility report depending on audience, circumstance, mission, etc. Also the elements do not need to be in the exact order outlined above. Specifically the conclusion should be mentioned more than just at the end of the report. It should also be summarized in the beginning of the report and in the case the feasibility report is long, it can be mentioned in the middle as well.
* **Executive Summary**

An executive summary should be included at the beginning of the report. In 2-3 pages, the main points of the feasibility study are summarized for a quick review by busy administrators and school board members. The executive summary provides the reader with an overview of the feasibility study and will help them see the entire picture before they read the details. Some decision-makers may only read the executive summary. Thus, the executive summary should be concise and include the major findings of the study followed by a recommendation.

* **Introduction**

The purpose of the introduction of a feasibility report is two-fold:

* To answer the readers’ question: “Why do we need to look into these alternatives-do they matter?”

In order to answer this question, it is necessary to identify the problem that your report will help resolve or what your report is aimed at accomplishing.

* To talk about the other options that you have looked at and analyzed, as well as to tell how you went about researching and analyzing them.

**Note**: Usually, the introduction to a feasibility report briefly discloses some of the important conclusions and the most feasible options for change. Other elements of a report of this nature, such as the criteria, method, or any other kind of general background, may also be concisely noted and mentioned in this portion of the report.

* **Criteria/Constraints**

**What to consider in your feasibility study/report.** As you begin formulating what you would like to consider you should realize that usually criteria works around one or more of the following questions.

**Will your plan or course of action really do what is desired?**

This is often seen on the technical sides. What you have to ask yourself is whether or not your implementation or change really makes that much of a difference. Lets say you are looking to improve an aspect of your company. Will your change really improve the proficiency and speed of what their trying to do. Or will you find in your study that the change actually slows down production or the efficiency of the company’s workers. This is important to predict beforehand because sometimes an improvement in the workplace is not always an improvement in how a company works. But many of these factors you will not notice until after you complete your study. And in the worst case you may not see negative ailments until after the plan is implemented.

**What will it take to implement your course of action?**

Even though your plan of action may seem correct and efficient on paper, it may not be practical towards your line of work. You must take into account the circumstances that arise in every aspect of a professional setting. What you may find is that in one field your plan may be extremely successful, but in another may be a bust. This can also take place from company to company. As you work at different companies along the same field, you will begin to understand what can be successful in one workplace that may not work in another. Sometimes you have to take into account the amount of changes that will need to be implemented for your plan. Do you need to go through extensive changes in operations, or make upgrades to current equipment or materials that are currently in use or in stock? Sometimes the amount of money that needs to be put into a new project may be much more than the actual amount of benefit that would be received from the changes. You must consider your plan as a cost-benefit analysis.

**Cost of implementation.**

This may become the biggest factor in any business decision. How much will it cost? In not only business, but any professional field, the benefits must outweigh the costs in any decision. This is even the case when deciding to work on one aspect of a project compared to the other. When forming criteria for a feasibility report, you must understand the costs if all went as planned. Then you might even want to find out what the cost would be if you had minor or major setbacks. It is important to understand the costs because unless the benefits outweigh the costs, a company will most likely not go through with your proposed plan of action. Also it is important to look into the future of the company. Maybe your plan of action will not be beneficial for the first year in existence, but what about the years following that? This must be considered because like any other decision in business, the original fixed cost may be high but the marginal gains may be high. In that case it may be a good decision for the company to make a change if it is beneficial for the future. Think about health care companies. Would it be beneficial for a company to invest in new equipment even though the upright payment is very high?

**Is your idea/product desirable?**

This is as simple as is your plan going to sell. Will people want to overextend themselves for change, or will they reject what you are trying to do? Sometimes a change or solution must be more than just effective and affordable. You must consider the consumers and people that will be changing. Sometimes many feasible courses of action do not succeed simply because they create effects that drive the consumers away. Because of this, the product or plan does not sell. These undesirable side effects can be as simple as tearing away employee morale. Sometimes even though a plan is promoting and expected to increase productivity, how will the employees react? Many times companies overlook how their employees are going to react to change. But the fact of the matter is that the only way to increase production is to keep employees happy. If they are not pushed to improve the company and their own status then they simply will not find change necessary.

* **Method**

This section of your feasibility report is one of substantial magnitude and importance. This part of your paper demonstrates to the reader what you discovered, through your research, actually matters and has reliability. By telling your audience how you came to know what you have found out and know now, you are demonstrating to them that your results are trustworthy and that they truly hold significance in meaning. With strong methods for finding out your facts, your readers will then feel comfortable and confident to make the necessary changes.

**It’s all about the source**

The question of what sources to use completely varies from study to study. There are several different types of sources that you could use to find your facts-it all just depends on what you are trying to find answers to. Sources can include (but are not limited to):

* Academic journals or reports
* Library research
* Phone calls
* Face-to-face interviews
* Meetings with those who are knowledgeable about the topic or are in your company/organization
* Surveys (Survey Monkey!)
* Usability Testing
* Lab testings

**How much is enough?**

The length and density of content will vary from each report to the next. You should take into consideration your audience as well as the context and purpose, for which your paper is written. The main goal is to purely get the point across to the readers that what you are reporting has validity, by describing how the means of attaining your information are sound and secure. Make sure that your writing is reader-centered and that they would be satisfied. Doing thus will ensure that your method is long and descriptive enough.

**Where does it fit?**

The placement of this section of your report will also depend on the type of report that you are writing. If there are only a couple of different methods used throughout your research, it might be a good idea to fit them into the beginning of your report, writing a paragraph for each technique. If you have several, unrelated methods, however, it would be good to place those paragraphs throughout the report, where they would best accompany your analysis or data.

**Important note**

Sometimes, if it is really obvious how you went about your research, then there might not even be a need to talk about your methods. It is key, though, that your readers always have a clear understanding of the way you obtained your facts and that they are worth trusting.

* **Revision Checklist**

Once your feasibility study is complete, analyze the checklist to ensure every topic has been addressed.

**Introduction**

1. Does it tell your readers why you conducted this study?
2. Does it provide background information the readers will need or want?
3. Does it identify the action or alternatives you investigated?
4. Does it persuade readers to use this study as a valid document?

**Criteria**

1. Does it identify the standards by which the action or alternatives were evaluated?

**Method**

1. Does it explain the way you obtained the facts and ideas presented in the report?
2. Does it persuade the readers that this method would produce reliable results?

**Overview of Alternatives**

1. Does it present a general description of each alternative?

**Evaluation**

1. Does it evaluate the action or alternative in terms of criteria?
2. Does it present the facts and evidence that supports each evaluative statement?

**Conclusions**

1. Does it explain the significance from the reader’s viewpoint of your facts?
2. Does it state the conclusion plain and simple?

**Recommendations**

1. Does it advise which course of action or alternative you recommend?
2. Does it present recommendations which stand out?
3. Does it suggest specific steps your readers may take to act on each of your recommendations?

# **Academic Writing Vs Technical Writing**

# Academic writing is any writing done to fulfill a requirement of a college or university. Academic writing is also used for publications that are read by teacher and researchers or presented at conferences. Academic writing could include any writing assignment given in an academic setting.  Academic writing involves a teacher and a writing assignment. The teacher reads and evaluates the work.

The substance of technical/business/workplace writing, also known as professional writing, is different from academic writing—no longer is there a teacher who mustread the work. It becomes the responsibility of the writer to entice the reader successfully.

Technical writing is closely related to the description of a product. The main strategy followed in technical writing is to clearly explain the steps to accomplish the task in such a way that any person will be able to do it. Technical writing mainly consists of user manual preparation that contains detailed working and properties of an equipment or product. Other types of technical writings include business letters, memos, product descriptions, warning labels and, to some extent, editorial letters.

Technical writing is linked to the processes. It involves a step by step explanation of a procedure so that anyone can understand it. From business letters to the product descriptions and editorial letters, it conveys the technical information such as engineering and scientific studies in the easiest way possible. Academic writing is more specific in nature as it is linked to a particular discipline. It is a complex form of writing which can more commonly be seen in the form of scholarly articles and textbooks.

**Difference Between Academic and Technical Writing**

There is a huge difference between the technical and academic writing. A skilled academic writer may not have the proficiency in technical writing and vice versa.

* In academic writing, a person intends to prove a theory or viewpoint in one way or the other, whereas technical writing is entirely goal-oriented and it talks about different ways by which the desired goal can be achieved. An academic writing is used in the form of theses, essays or book reports.
* Writing at work focuses on problem solving. Unlike academic writing where you write to persuade your professor how much you know, at work you write to help you perform your job. Primarily, you are trying to achieve a specific goal and to complete a job task.
* Work-related writing targets multiple audiences with different perspectives. In college our primary and, typically, only audience is our professor. Professors approach student writing similarly. They want to read what you've written and they're trying to determine if you've mastered the course content. The professor is also an expert or authority on the subject matter. But, as an employee you may write to many readers with varied backgrounds--some highly educated experts and some less knowledgeable than you are. You will also write to people within and outside your department and organization. These readers won't necessarily read what you've written unless you persuade them your message is relevant and will help them perform their jobs. You have to make your message relevant, clear, and easy to read.
* Writing at work may be read by unknown readers. At school, professors rarely share students' writing with others, and students rarely target multiple audiences. But, on the job, you not only target a primary reader but also secondary and tertiary readers who may or may not be known to you. For example, your boss (the primary reader) may decide to give your report to her boss (secondary reader) who decides to pass it along to one of her employees (tertiary reader). You always need to assume that others will read your documents, that photocopies could be mailed, and that copies of your documents could be filed for further use.
* Writing produced at work can be used indefinitely and can be used in legal proceedings. While college papers have a limited life span (typically for 1 class), work documents can be filed and used indefinitely. Moreover, parts or all of documents can be used out of context in situations unrelated to the original scenario. Thus, work documents could be used in legal proceedings. You should word your documents carefully to prevent them from being misused. Ultimately, you are responsible for the document, and others can use parts or all of it to support their claims in litigation.
* The format for work documents varies greatly from the format for academic documents. In school, you primarily write essays, research papers, lab reports, etc. But you rarely write memos, letters, procedures, policies, or employee evaluations—all common work documents. You need to become very comfortable with different organizational patterns and different formats for your writing.
* Technical writing intends to explain the working of a product or service in a step-by-step process. While the academic writing revolves around the results of the academic research. However, sometimes it is also based on one’s viewpoint on a particular topic.
* The target audience in both the types of writing is very different. In academic writing, the target audience is research scholars or professionals who have an expertise in a specialization. Technical writing targets any person who needs to know the task followed by a particular organization.

**Key Elements of Technical Writing**

Technical writing, just as any other form of writing, has certain characteristics which distinguish it from other types of writing. It is very different from writing opinion pieces, essays, prose, non-fiction, or fiction. Technical documents are written in a [business writing](https://grammar.yourdictionary.com/style-and-usage/types-of-business-communication-writing.html) style rather than one that is academic or creative in nature.

1. Audience - Understand the target audience so that your document or technical content may connect them quickly, and they can proceed with the understanding and fulfill their requirements. A technical writer must consider the following questions about his audience:
   1. How familiar are readers with the subject and with the specialized terms and abbreviations you need to use?
   2. What is the best way to explain those terms or shortened forms - footnotes, endnotes, glossary, table of abbreviations, appendix, links?
   3. Do you need to accommodate secondary readers (e.g. the manager or financier who will make the decision about the proposal), and how will you do that?
2. Clarity - The logical flow of the document will help readers understand the content. It can be useful to ask someone who is not familiar with the topic to review your writing before you finalize it. Using headings, illustrations, graphs or tables can be useful - your aim is to make it as easy as possible for your readers to understand what you've written. Consider how the way the text sits on the page or screen - another clue to maximizing clarity for your readers. Technical writing presents information clearly, leaving little to no room for misunderstanding. It requires the use of [clear, concise sentences](https://grammar.yourdictionary.com/grammar/writing/10-tips-for-writing-clear-concise-sentences.html).
3. Accuracy - The information and the interpretation of data that you present must be accurate. If it's not, your readers will question the credibility of the content. Be careful to clearly differentiate between fact and opinion, and to accurately cite references to other works.
4. Brevity - Strive to find the balance between the amount of information presented and the time needed to read the document. Remember that you can use an appendix or link to provide supplementary or background information. Consider using an illustration, table or graph rather than words to explain a concept - but remember, if you use a 'visual', don't give a long-written explanation.
5. Sentence length - Generally, complex or unfamiliar concepts are best presented in shorter sentences. This will give readers time to digest small pieces of information before moving on to the next. While this can be difficult to achieve, try to aim for approximately 25 words per sentence. If you find you've written a series of long sentences, look for 'and', 'but', 'however' and similar words where you can break the sentence.
6. Paragraphs - The age-old rule about one topic per paragraph is a useful guide. That doesn't mean that you can have only one paragraph for each topic, but it does mean that having only one topic in each paragraph makes for clear, logical writing.
7. Reader-centricity - You are writing for your readers. Make it as easy as possible for them to understand your work.
8. Straightforward - This type of writing is straightforward; it requires relaying information in a way that is direct and straight to the point, without the use of [literary devices](https://examples.yourdictionary.com/basic-types-of-literary-devices.html).
9. Precise - The language used in technical writing should be very precise, describing objects and procedures in an exact manner.
10. Easily understood - Effective technical writers avoid words that people may not understand and will avoid an eloquent writing style.
11. Denotative meanings - This type of writing relies on the [denotative meanings](https://examples.yourdictionary.com/examples-of-denotation.html) of words to ensure that misunderstandings don’t occur due to differing interpretations based on connotation.
12. Detailed - Technical writing is very detailed and informative, leaving nothing to the imagination. The perfect example of technical writing is a textbook. Most textbooks describe the subject matter as fully as possible.
13. Very structured - Technical writing is very structured. This type of writing needs to have an obvious composition that makes it easy for readers to follow along. The audience needs to be able to rely on technical writing for step-by-step instructions.
14. Skimmable - Technical documentation should be designed with skimmability in mind, so it’s easy for readers to scan through the full document and easily find information they need. Technical writers should incorporate meaningful, descriptive headings and include a thorough table of contents and/or index.
15. Problem-solving focus - Technical documents should be created with problem solving in mind. Readers use these documents to learn how to perform certain tasks or gain technical information, so they should be easy to follow and organized in a way that’s easy to refer back to ask questions come up.

## Rhetorical Nature of Technical and Professional Writing

Communication in the workplace is practiced and accomplished for many practical purposes. The goal is to effectively convey information to an audience. Workplace writing differs from written communication in other contexts, such as educational or social arenas.

In the workplace, writing is considered a legal document and is frequently archived or retained for several years at a time. These writings can be referenced to in the future if legal complications arise.

Workplace writing also varies from typical writing due to the fact that the audience is generally reading documents not for entertaining nor teaching themselves; it should contain important, relevant and needed information only, with no redundancy.

## Reader-Centric Writing

Workplace writing should always focus on the audience; what does the reader need to know? Writing should effectively convey the precise information that the reader is seeking. If the writing is an attempt to persuade the reader, then the writer must consider what will persuade the reader most. For example, a work team may be writing a proposal to install new production machinery in a factory. Different readers in the company will want different information from this proposal. A well-written document will consider every potential reader and give the information that each reader is seeking.

Throughout all of your work, constantly think about your readers. As you make each writing decision, consider your readers’ characteristics, goals, expectations, situation, and other factors that will shape their response to what you say. Concentrate on crafting a communication that will be persuasive and usable in your readers’ eyes. These are two important qualities of successful work-related communications. Focus specifically on the ways your readers will respond, moment by moment, while they are reading your communication. This will be the only opportunity to influence your readers directly.

## Effective Workplace Writing

Workplace writing must be persuasive and usable to all potential readers. For a document to be efficient, it must be easily understood by the intended audience. It is important to use simple sentences, words, and structure so that all that view the document can comprehend it. A document that is hard to understand is not usable or effective, since the audience will be unable to properly understand the document. Highly usable writing should help readers quickly locate, understand, and use the information to complete their task(s). It can be used as a reference, a how-to, or a means for them to see your progress on your own tasks and what still needs to be done.

Persuasive writing should convince readers that the information is accurate and should be followed. For example, a reader may be considering several different proposals. The chosen proposal is most likely to be the one that is most persuasive; however, if writing is not persuasive, then it is not likely to be followed. Thus, the entire writing effort will have been wasted. It is pertinent to understand, though, that being persuasive does **NOT**mean conducting unethical behaviour. Do not write a document to simply to have yours preferred or chosen over others.

**Always be sure to use ethical practices.**

Some ethical practice questions to ask yourself: Did I cite my sources? Did I use credible information? Did I “twist” any information? Am I using the correct language? Am I only telling the truth, no “bluffing”? Am I being realistic? Am I being timely? Am I being accurate? Am I giving a correct assessment and perception of what will be done?

## How Writers and Readers Interact?

Writers and readers interact in unique ways. In all cases, writing is a one-way flow of information.

Therefore, writers must consider and include all of their readers’ needs. Every reader is different, but an effective writer must anticipate what will be most useful to the audience. Additionally, the world is extremely diverse. Some readers may be more relaxed or open-minded than others. For this reason, writers must learn to be careful in their writing to ensure they won’t discourage or offend any of their readers. If a reader is offended, any decision made will likely not be made in the writer’s favour. Effective writing eliminates unnecessary pieces of information and ensures a concise document.

Different readers may construe different meanings from the same words. The meaning may be shaped by a user’s previous experience, culture, or even a user’s state of mind. Each reader will construct a meaning based on the context of the writing and their previous experiences. This is why when writing a document you must start with who your audience is and what they need to know.

Readers react moment by moment when reading a document. Important information will usually have a greater impact if it is placed at the beginning of a document. This ensures that it will be read right away. Many readers will not finish a document, and so this “inverted pyramid” writing style is very effective. In addition, the average business professional says that they do not spend more than 30 seconds reading a resume, and no more than 5 minutes on a business proposal. It is prudent to place the most important information at the beginning of the document and least important at the end. The writer should ensure stylistic continuity as well. A writer attempting humour in a long technical document may confuse the reader; while the same humour, if used while writing about a personal anecdote, may more easily amuse the reader. To reiterate, every reader will have a different reaction to a piece of writing, and these reactions will depend on everything from the context of the writing to the reader’s cultural upbringing.

**Role of Communication**

Effective communication is a building block of successful organizations, In other words, communication acts as organizational blood. All managers and employees need to be aware of how people behave in order to provide the best working environment. Organizational behavior is about how people may be motivated to work together in more effective ways. The interaction required to direct a group toward a set of common goals is called organizational communication.

**The importance of communication in an organization can be summarized as follows:**

1. Communication promotes motivation by informing and clarifying the employees about the task to be done, the manner they are performing the task, and how to improve their performance if it is not up to the mark.
2. Communication is a source of information to the organizational members for decision-making process as it helps identifying and assessing alternative course of actions.
3. Communication also plays a crucial role in altering individual’s attitudes, i.e., a well-informed individual will have better attitude than a less-informed individual. Organizational magazines, journals, meetings and various other forms of oral and written communication help in molding employee’s attitudes.
4. Communication also helps in socializing. One cannot survive without communication.
5. Communication also assists in controlling process. It helps controlling organizational member’s behavior in various ways. There are various levels of hierarchy and certain principles and guidelines that employees must follow in an organization. They must comply with organizational policies, perform their job role efficiently and communicate any work problem and grievance to their superiors. Thus, communication helps in controlling function of management.

**Importance of Good Communication Skills at Workplace**

Good communication is an essential tool in achieving productivity and maintaining strong working relationships at all levels of an organization. Employers who invest time and energy into delivering clear lines of communication will rapidly build trust among employees, leading to increases in productivity, output and morale in general. Meanwhile, employees who communicate effectively with colleagues, managers and customers are always valuable assets to an organization and it is a skill which can often set people apart from their competition when applying for jobs. Poor communication in the workplace will inevitably lead to unmotivated staff that may begin to question their own confidence in their abilities and inevitably in the organization. The importance of strong communication runs deep within a business. Here are five key reasons you should be paying attention:

1. **Team building** – Building effective teams is really all about how those team members communicate and collaborate together. By implementing effective strategies to boost communication will go a long way toward building effective teams. This, in turn, will improve morale and employee satisfaction.
2. **Gives everyone a voice** – An employee satisfaction can rely a lot on their having a voice and being listened to, whether it be in regards to an idea they have had or about a complaint they need to make. Well established lines of communication should afford everyone, no matter their level, the ability to freely communicate with their peers, colleagues and superiors.
3. **Innovation** – Where employees are enabled to openly communicate ideas without fear of ridicule or retribution they are far more likely to bring their idea to the table. Innovation relies heavily on this and an organization which encourages communication is far more likely to be an innovative one.
4. **Growth** – Communication can be viewed both internally and externally. By being joined up internally and having strong lines of communication you are ensuring that the message you are delivering externally is consistent. Any growth project relies on strong communication and on all stakeholders, whether internal or external, being on the same wavelength.
5. **Strong management** – When managers are strong communicators, they are better able to manage their teams. The delegation of tasks, conflict management, motivation and relationship building (all key responsibilities of any manager) are all much easier when you are a strong communicator. Strong communication is not just the ability to speak to people but to empower them to speak to each other – facilitating strong communication channels is key.

**Written Communication Skills at Workplace**

In today’s workplace, effective communication makes all the difference in the world. Big and small companies are dedicating entire departments to making sure the inflow and outflow of communication is both accurate and representative of their company. Without being able to effectively communicate your business offerings, even though you might have the best product in the world, your business won’t survive.

Nearly every job will require some degree of written communication skills, whether it’s sending emails, writing memos or providing briefs and reports. The ability to communicate clearly, concisely and concretely in writing ensures that everyone you work with understands what you’re telling them. Because written communication skills are so important in business, it’s worth taking the time to improve yours.

### **Think first, write second**

Considering the purpose, and key message, of your communication prior to actually putting pen to paper is incredibly fruitful. Make note of exactly what you want your audience to take away from your email, memo, or proposal, and keep that in the back of your mind the whole time you’re writing.

### **Be straightforward**

There is a time and a place for long-winded, creative language – but the workplace isn’t it. Most of the people that will be reading your communication are time-poor, and need to know the key information right off the bat. Therefore, write your key point at the very top of the document – don’t hide it somewhere in the middle. Include the key information succinctly in the email subject line if you can. Everything the audience reads after this will have more context, considering they already know the key message.

### **Trim it down**

Don’t use five words to explain something that could be said in two. Re-read your writing back to yourself through the lens of a time-pressed manager to ensure each word is useful. As soon as a reader hits a sentence full of unnecessary words, they tune out. MIT Sloan School Managerial Communication lecturer Kara Blackburn recommends using contractions, removing prepositions, and replacing -ion words with actions verbs.

### **Keep it simple**

Buzzwords, acronyms and other industry-specific jargon are rampant in business writing. Occasionally their use is inevitable, sometimes even helpful, but they certainly shouldn’t be relied upon. O’Hara explains that if you’re using too many buzzwords, your writing looks generated, in genuine, and even uninformed. In addition, don’t use overly lavish language to look intelligent – generally, it stands out like a sore thumb.

### **Read everything**

Everything you write, you should read back to yourself. Be critical of your own writing. Is it clear? Does it follow a neat structure? Are your sentences too long or short? Put yourself in the shoes of your reader, and honestly determine if your argument is presented well. Reading out loud can be really helpful here. Every time you need to take a breath, there needs to be a comma or a full stop. Print it out, and read the hard copy – studies show we process information better when it’s printed. Welcome feedback from colleagues on your work. After all, how else will you learn!

Read everything to yourself–even out loud–before sending, posting, or even letting your co-workers read it. This is one of the easiest ways to improve your written skills, because it’ll help you catch mistakes. The goal of reading everything you write will help you catch small grammatical or spelling errors, as well as ensuring that you are writing a clear message. Reading everything over a few times will also allow you to catch things you might’ve missed, or things you may simply decide don’t make sense.

### **Practice makes perfect**

No one became an expert at anything overnight. Just like all skills, Blackburn explains that writing improves with practice. Reading well-written material as often as possible is a great way to improve. Pay attention to all written communication that you compose, taking note of sentence structure, flow, and word selection. Blackburn suggests readying The Wall Street Journal for a great example of written style. It’s worthwhile creating a style and grammar guide for your workplace, so every employee can improve their skills. Ensure you have time in your day to edit and revise all your written communication – the edits you make yourself on a regular basis are the ones that will really stick in your brain.

It might not seem to be the most common thing, but a lot of people do better with hands-on learning, and taking notes from your boss or senior-level co-workers might do the trick for you. Review letters, memos, and emails prepared by others in the company. Look for patterns in business communication, like short, to-the-point paragraphs and requests for further action. Pay special attention to the letters and other documents created by your boss and other members of the management team.

## Be Clear and Concise

Work on being clear and concise when it comes to any form of written communication. You need to be able to impart information and instructions so that your employees will understand. If this isn’t done properly, your entire communications strategy might be misinterpreted, which can lead to things like brand confusion, marketing disasters, and public relations nightmares. You may understand how to do a task perfectly, but if you’re not able to list out the steps in a clear and concise way, your meaning might get lost in translation.

* **Keep It Confidential**

Confidentiality is important for a lot of reasons. The data pertaining to recruitment, compensation, and management of employees is naturally sensitive. If information is misconstrued, interpreted incorrectly, or written incorrectly, big problems could eventually arise. The smallest of errors, like switching “and” for “or,” could mean all the difference in the world. When you’re writing pertinent, sensitive, or confidential information, it’s important to read everything, have it looked at by other teammates, and just double-check everything. You can’t be too safe.

* **Avoid Stirring Up Trouble**

The list of words to avoid when mitigating conflict in the workplace is nearly infinite. As Generation Y starts entering the workforce, employers must be on the lookout for terms associated with their generation that could potentially worsen a conflict situation. One of the most commonly used words of this generation is “whatever.” It’s used quite frequently, and it’s pretty irritating. When someone is using this phrase they are saying, “I’m not interested in what you have to say.” That’s a hot button in the workplace and can take conflict to an entirely new level.

Another big word to watch out for is “you.” It doesn’t sound bad, but when you’re using the word during a heated interaction, it tends to point blame on the individual instead of working out the present conflict. When writing reviews or individual developmental plans, you’ll want to avoid words like this because they may come across in an entirely new way that will not help the situation.

* **Watch Your Verticals and Horizontals**

There has been a lot of discussion surrounding how to address a boss vs. a co-worker in an email. In a formal business environment, an email to your boss (vertical communication) should be simple and direct, following this format: give a formal greeting, address your concern, and close. If someone is in a position of power, their inbox is usually flooded with tons of emails, so keeping it simple and direct is the way to go. As far as addressing a co-worker who is on the same level as you (horizontal), you’ll want to keep it professional, but you can be more careless in how you actually address them and the message being delivered.

While mastering written communication is essential in the workplace, it is not the only thing to focus on. Good communication in the workplace requires strengths in all areas, including verbal, non-verbal, and written. With time and practice, these skills will develop over time and will boost your career in the best ways. Make sure that you aren’t focusing 100% on one type of communication style, because to be successful, you’ll need to master two, if not all three.

#### **The Foundations of Effective Technical Writing**

* [**Purpose**](https://www.thoughtco.com/purpose-rhetoric-and-composition-1691706)**:** Getting something done within an organization (completing a project, persuading a customer, pleasing your boss, etc.)
* **Your knowledge of the topic:** Usually greater than that of the reader
* [**Audience**](https://www.thoughtco.com/audience-rhetoric-and-composition-1689147)**:** Often several people, with differing technical backgrounds
* **Criteria for evaluation:** Clear and simple organization of ideas, in a format that meets the needs of busy readers
* **Statistical and graphic support:** Frequently used to explain existing conditions and to present alternative courses of action

**Characteristics of Good Technical Writer**

**Who are Technical writers?** A Technical writer who understands topics clearly and makes a blog, documentation, online user help, user guide, and so on. With the assistance of users, the way to use products or services. In short Professional writers who take complicated technical issues and transform them into a version that’s more understandable for the commoner are referred to as technical writers.

**What skills does a Technical writer Require to have:**

A Technical writer requires a robust foundation generally, including knowledge of common grammar and punctuation conventions. The process involves multiple reviews and revisions before the publication of labour.

* **Understanding the Topic:** A Technical writer possesses to be extremely attentive and alert in putting down the words. Content should be highly explicit and informative. content chosen by a Technical writer isn’t for entertainment purposes, therefore one has got to make content in such how that the reader doesn’t have any problem in understanding and gets to understand the content during a pretty simple and transparent language. A Technical writer has got to keep this in mind because this is often one among the talents and qualities of a Technical writer.
* **Knowledge required:** Accurately like all other jobs, you’ll need certain things to shine at your job. Technical Writers should be quite knowledgeable in writing.
  + ability to analyse, evaluate, simplify and communicate technical information
  + knowledge of the professional area they’re writing on.
  + ability to edit, design and plan technical documentation
  + skills in information science, web publishing, and graphic design.
* **Appropriate Language Usage:** A Technical writer uses formal English, straight language, and straightforward terms. confirm to pick the accurate term. Employ correct scientific terms and conventions for engineers. Replace words that are a drag for the foreign reader, like the verb “do” and words with multiple meanings.
* **Direct Language:** In technical writing, every word must have an area within the sentence and meaning. Use direct statements and a lively voice, avoiding past the maximum amount as possible, except within the executive summary, where past is usually used. Use the future to project into the longer-term Avoid saying an equivalent thing twice and repeating an equivalent word during a sentence. When a sentence contains an equivalent word twice, try rewriting the sentence. Reword negative language to the positive. Provide certainty by eliminating auxiliaries like would, should, could, may, and might. Avoid ambiguous words and phrases by selecting a clearer alternative.
* **Don’t take yourself too seriously:** Most of the technical writers cover serious matters, but that doesn’t mean everything has got to be taken seriously to the purpose where there’s no room for satire or humor. Sometimes a technical writer content must recheck to interact with the audience, and stepping back and having a touch of fun with the content is superb thanks to doing this. Remember, you’re writing your technical content so people will read it, and while in a perfect world, the knowledge should be enough, it’s often not the case. Connect the reader to interact at every opportunity for max impact on your content.
* **Critical thinking:** Critical thinking may be a broad term. And also, it seems to be one among the foremost skills for a technical writer. Critical thinking is often explained because of the ability to form reasoned and clear judgments. This idea includes gathering information, analyzing, and systematizing given or selected content. Just being systematic is merely a little piece of critical thinking. Effective technical writing all depends upon the author having excellent critical thinking skills.

While the definition of critical thinking skills differs depending on who’s arranging the defining, a panel of experts defined them as “process of purposeful self-regulatory judgment that drives problem-solving and decision-making”. Hence, a number of us may question how critical thinking and writing are related; what do problem-solving and decision-making need to do with effective Technical writing? and therefore the answer is “Everything!” Critical thinking skills are intimately connected to how glorious we address. Writing may be a big puzzle and it’s up to you as writers to work out the way to put the puzzle together.

The straightforward elements of the puzzle are the audience and purpose. However, beyond these aspects, the weather that structure the particular document which determine whether the reader will understand or not.

These include word choice, paragraph and syntax , logic, and reason, both of which are integral parts of critical thinking. In short, writers needn’t only to develop their critical thinking skills, but to know and use them when writing, whether they’re writing workplace documents, blogging, or journaling. These critical thinking skills will go an extended way toward helping writers write usable, logical, and well-reasoned documents.

* **Analytical Skills:** Analytical skills are important because it allows you to seek out solutions to common problems while you write and make decisions about what actions to require next. Understanding problems and analyzing things for solutions may be a fundamental skill in every position at each level. Developing this ability can improve your being as a Technical writer, assist you achieve company goals, and eventually support your personal career goals.
* **Know the Content:** Correct content should be chosen or known, but you would like to know what you’re writing about better than the audience that you’re writing. That doesn’t mean you need to be a full-blown expert, but you would like to understand the positive writing and negative writing on content. So, you simply are going to be tolerable to clearly explain it to somebody else and anticipate any questions which may arise. Do research, take some time , take notes, and if you’re not an expert, consult someone who is. in order that you’ll be an honest technical writer.
* **Build a transparent Structure:** It’s not almost what you say about the content but it’s how you present the content. Your writing needs a transparent structure. Don’t just dump a bunch of knowledge and expect your reader to form a sense of what you’ve got written. believe your order of presentation. What must be explained first? How does the knowledge get to be sequenced and determined? What needs more explanation, and what can do with less? Your writing should present a transparent path of development, smoothly transitioning from one point to a different and it should clearly emphasize the foremost crucial ideas.
* **Research on your skills:** These research skills may involve you as an efficient technical writer, but it probably affects outsourcers foremost. Working in an outsourcing company means you’ve got a spread of client companies you’ve never heard of and are unaware of their products and services. Writing documentation under such circumstances may be a tough note. Only after hours of thorough research, you’ll gather enough information on the given field to start out with the writing process. Besides, performing some research is usually great even for the world you are feeling pretty confident about. Remember that we sleep in a constantly changing world.

**Qualities of Good Technical Writing**

* It has an effective design, which makes a good impression
* It is designed so that it can be read selectively
* It has a rational and distinct plan
* Reads coherently and cumulatively throughout
* Answers readers’ questions as they arise in the readers’ minds
* It has the necessary front matter to characterize the report and disclose its purpose and scope
* It has a body that provides essential information and that is written clearly without jargon or padding
* When appropriate, uses tables and graphs to present and clarify its content
* It has, when needed, a summary or set of conclusions to reveal the results obtained
* It conveys an impression of authority, thoroughness, soundness, and honest work
* It can stand alone and be understood by readers who are not part of the initial audience
* Makes a positive statement about the writer and the organization

It should be free from typographical errors, grammatical slips, and misspelled words

**The Basic Parts of the Composing Process**

Writing effectively begins with your understanding that writing well requires a process. If you understand the process, why it’s important, then you can see the value of using it. The more frequently you use it, the more efficient you will become in using the composing process. The result: a better percentage of the documents you write will achieve their intended goal.

This composing process has several parts:

* **analyzing** the situation which requires a written response,
* **choosing** content, arranging content,
* **drafting** and **revising**, and then
* **editing** the finished draft.

Writing requires each activity, but most of the time the activities are recursive: that is, you begin with an analysis of a situation which requires you to write; but as you choose and then arrange content, you are probably drafting and doing some revising. Once you are satisfied with your content and your arrangement, you may decide to focus on revision to improve articulation of the content you are presenting. Editing, the final stage, is usually an important “quality check” to ensure that what you have written is correct in content, usage, punctuation, spelling, and sentence structure. Editing allows you to look at your document as a whole, to assess its quality.

Writing becomes extremely difficult if you try to do all the parts at once! Or (equally difficult) you may try to prepare an outline about the subject or topic first and then try to follow the outline in collecting information. Neither method will produce an effective document. Research has shown that good writers usually follow a basic process. What you produce will make your writing tasks easier and the results more effective than if you focused on collecting and outlining information.

1. **Analyzing the Writing Situation**

The first step in composing is the most critical to the success of what you write. In this step, you need to know why you are writing, what you are attempting to achieve with your document, what situation or problem has led to the necessity of your writing this document. Then, you need to consider your readers—those who will/may read your document.

Every technical or workplace document is written to respond to a specific situation. Each document has a targeted audience. Writing responds to both--the situation and the readers in that situation. Writing is NOT simply compiling information about a subject.

1. **Choosing/Discovering Content**

Sources for content may include previous reports prepared by the organization, research material from databases, indexes, and the World Wide Web; interviews, surveys, statistics, technical periodicals, and books. What you need to include should always be guided by why you are writing, what your reader needs, and how your reader perceives the subject.

As you search for information, remember your purpose as what you want your reader to know and do with what you write. In the workplace, writing solves problems and enables the organization to operate.

After you have considered your purpose and begun to research your topic, begin to list ideas that you can use to develop your topic. If you wish to do this activity on your computer, simply list ideas. Then, move/insert/delete ideas. Based on these ideas, ask yourself what additional information will you need to locate. Computers are great for allowing you to list and then turn lists of ideas into larger units. Don’t like what you wrote? Delete it. You may want to begin your document by writing your purpose at the beginning--to help you stay on track.

1. **Arranging Content**

As you collect and begin summarizing information and data, you will begin to consider how to arrange the material. In what order should you present your content? Most reports begin with an introduction, followed by a summary of the report. Or, the introduction may be combined with a summary of the report. The discussion section, in which you present the supporting information, follows. Most reports follow some version of this plan. You may be able to choose your arrangement, or you may be told how to organize your document. Proposals, for example, often have specific, required sections. Many business organizations have rules on how reports distributed to clients outside the firm should be written. In Part III, you will see various ways to arrange and present material in a variety of technical documents. As we say repeatedly, these are suggested approaches and guidelines that can and should be modified depending on the needs of the topic, readers, and the purpose of the document. Effective writing responds to all three.

A useful way to arrange content is to place material in “stacks” which can be used as a resource when you begin writing. If you know what arrangement you want/are required to use, sort material so that you can easily find it when you begin drafting specific segments of your document. You can also sort material electronically: create folders of information on each segment of your report. Then, arrange material within each folder before you begin drafting. This method allows you to track material you use and insert appropriate citations when you use material from a specific source.

If you use electronic articles from your library’s database, you can insert these articles into files that can be accessed later, when you begin to draft your document.

1. **Drafting and Revising**

Drafting is a highly individual activity. Few writers do it exactly alike, but many writers now draft on their computers. Most writers work on a document in a start/stop fashion. When you begin your draft, open your file and save it with the name of your report. Then, begin keyboarding ideas or sections. (You may wish to move/paste material you listed, arranged, and then developed in Step 2.) You may wish to type the names of your main segments, boldface those, and insert information beneath the appropriate segment. This method helps you keep track of the information that you are using to develop your draft. Note that some of the ideas in the list of ideas become headings in Figure 2-1. Some are combined with other ideas. Note that you can arrange, delete, and add ideas as you need to.

When you prepare a research report or project, as you insert information, indicate the source of all your material. Use parentheses ( ) or brackets [ ] to remind you of the source of the information. This method will help you develop your list of references for your List of Sources or Bibliography and to ensure that you “give credit where credit is due.”

As you continue to draft, you will revise. But during the drafting stage you should revise only for meaning. Try to avoid worrying about sentences that don’t sound “quite right.” If the sentence you write captures what you want to say, even clumsily, don’t stop to revise. You can “clean up” these sentences later. Word processing programs, like Word, will alert you to problems in sentence structure and spelling. Don’t attempt to correct these mechanical problems, unless you feel you can do so without slowing your ability to transfer your ideas from your mind to the screen. Focus on presenting your material to your reader(s): then you can begin a formal revision process once you believe you have your basic ideas on the screen or page.

1. **Revision**

During the formal revision process, you will want to revise from different perspectives. You may want to revise several times and focus on different issues:

**Logic.** Does your presentation make sense? Try reading paragraphs aloud that seem to you to be “scrambled.” Hearing what you have written often tells you if/where problems in logic are occurring. Is the order in which your material is written appropriate for the purpose and for your reader(s)?

**Completeness.** Is your presentation complete, in terms of the purpose of your document and your readers’ needs and requirements? Is your information correct? Does your document contain all requested information?

**Style.** Examine each paragraph and each sentence. Are your paragraphs really paragraphs? Do they have topic sentences? Do all the sentences in the paragraph pertain to the meaning you are building in the paragraph? Try to open each paragraph with a topic sentence. Eliminate or recast sentences that provide little support for the topic sentence. Sentences should be concise. Achieving a Readable Style, clear, concise, precise sentences encourage your reader(s) to follow your ideas. Today’s readers usually dislike wordy, dense, opaque sentences. Watch the length of paragraphs. Paragraphs that are too long discourage readers and tend to become incoherent.

**Visuals.** Do you need visuals—photos, graphs, drawings, pictorial illustrations—to help your reader “see” and remember key ideas? Creating Tables and Figures, will provide you guidelines on developing visuals that will be effective. Visuals combined with text often provide the best means of communicating with your reader(s).

1. **Document Design**

When you began drafting, if you used headings or names of report segments to help you organize your draft, you began at that point to design your document. Document design refers to the way information is arranged and displayed on the page. With word processing, you have many choices of font, typeface, and even color. Your choices in these areas, and then your placement of visuals, can encourage or discourage your reader(s) from attempting to skim and then begin digesting what you have to say. The importance of how information looks on the page, cannot be stressed enough. If you want what you have written to be read, then you have the responsibility of designing the page so that information is inviting and accessible. Examine the final draft of Bob’s memo, located at the end of this unit: note how the message looks after Bob’s initial revision of his draft:

1. **Editing**

Editing is a critical writing requirement. In complex reports, you will want to perform several “edits”: one for mechanics—spelling, usage, punctuation, sentence structure. When your word processing program, usually a green line under a sentence or phrase—suggests that there’s a problem with your sentence, stop and check the sentence carefully. Another edit focuses on citing sources: Check your documentation to be sure that you give credit or sources of all information you have used. Be sure that when you use graphics and ideas from other sources you give credit to the source. A third edit focuses on the document as a whole: How does it look? How does it sound? Is the important information easy to locate? Is the document complete?

In short, don’t try to check for every error at once, in one reading. Editing requires care, objective reading, and diligence.

A technical report is a formal report designed to convey technical information in a clear and easily accessible format. It is divided into sections which allow different readers to access different levels of information.

**Structure**

A technical report should contain the following sections:

|  |  |
| --- | --- |
| **Section** | **Details** |
| Title page | Must include the title of the report. Reports for assessment, where the word length has been specified, will often also require the summary word count and the main text word count |
| Summary | A summary of the whole report including important features, results and conclusions |
| Contents | Numbers and lists all section and subsection headings with page numbers |
| Introduction | States the objectives of the report and comments on the way the topic of the report is to be treated. Leads straight into the report itself. Must not be a copy of the introduction in a lab handout. |
| The sections which make up the body of the report | Divided into numbered and headed sections. These sections separate the different main ideas in a logical order |
| Conclusions | A short, logical summing up of the theme(s) developed in the main text |
| References | Details of published sources of material referred to or quoted in the text (including any lecture notes and URL addresses of any websites used. |
| Bibliography | Other published sources of material, including websites, not referred to in the text but useful for background or further reading. |
| Acknowledgements | List of people who helped you research or prepare the report, including your proofreaders |
| Appendices (if appropriate) | Any further material which is essential for full understanding of your report (e.g. large scale diagrams, computer code, raw data, specifications) but not required by a casual reader |

**Presentation**

For technical reports required as part of an assessment, the following presentation guidelines are recommended;

|  |  |
| --- | --- |
| Script | The report must be printed single sided on white A4 paper. Hand written or dot-matrix printer reports are not acceptable. |
| Margins | All four margins must be at least 2.54 cm |
| Page numbers | Do not number the title, summary or contents pages. Number all other pages consecutively starting at 1 |
| Binding | A single staple in the top left corner or 3 staples spaced down the left hand margin. For longer reports (e.g. year 3 project report) binders may be used. |

**Technical Writing Process**

No matter what type of writing you are doing, academic writing, professional writing, or personal writing, it can be made easier by using the writing process.  The writing process consists of the different stages that a writer follows to produce a good piece of writing.  Although different sources may label and group the stages in various ways, the stages of the writing process are essentially as follows:

1. **Preparation**

Writing, like most professional tasks, requires solid preparation. In fact, adequate preparation is as important as writing a draft. In preparation for writing, your goal is to accomplish the following four major tasks:

* Identify the topic and establish your primary purpose.
* Assess your audience (or readers) and the context.
* Determine the scope of your coverage.
* Select the appropriate medium.

**Identify the topic:** In addition to understanding that writing is a process, writers should understand that choosing a good topic for technical writing is an essential step. A good topic not only covers what technical writing will be about but also fits the assignment’s purpose and its audience.

When selecting a topic, you may also want to consider something that interests you or something based on your own life and personal experiences. Even everyday observations can lead to interesting topics. After writers think about their experiences and observations, they often take notes on paper to better develop their thoughts. These notes help writers discover what they have to say about their topic.

Reading plays a vital role in all the stages of the writing process, but it first figures in the development of ideas and topics. Different kinds of documents can help you choose a topic and also develop that topic.

**Establishing Your Purpose:** To establish your primary purpose simply ask yourself what you want your readers to know, to believe, or to be able to do after they have finished reading what you have written. Be precise. Often a writer states a purpose so broadly that it is almost useless. A purpose such as “to report on possible locations for a new research facility” is too general. However, “to compare the relative advantages of Paris, Singapore, and San Francisco as possible locations for a new research facility so that top management can choose the best location” is a purpose statement that can guide you throughout the writing process. In addition to your primary purpose, consider possible secondary purposes for your document. For example, a secondary purpose of the research-facilities report might be to make corporate executive readers aware of the staffing needs of the new facility so that they can ensure its smooth operation regardless of the location selected.

**Identify the audience:** The main point of writing is to clearly relay information to a targeted reader. Understanding what your readers know (and do not) and their potential biases, among other things, will help you plan the project such that it has meaning for readers.

Again, be precise and ask key questions. Who exactly is your reader? Do you have multiple readers? Who needs to see or to use the document? What are your readers’ needs in relation to your subject? What are their attitudes about the subject? (Skeptical? Supportive? Anxious? Bored?) What do your readers already know about the subject? Should you define basic terminology, or will such definitions merely bore, or even impede, your readers? Are you communicating with international readers and therefore dealing with issues inherent in global communication?

In addition to knowing the needs and interests of your readers, learn as much as you can about the context. Simply put, context is the environment or circumstances in which writers produce documents and within which readers interpret their meanings.

**Determining the Scope:** Determining your purpose and assessing your readers and context will help you decide what to include and what not to include in your writing. Those decisions establish the scope of your writing project. If you do not clearly define the scope, you will spend needless hours on research because you will not be sure what kind of information you need or even how much. Given the purpose and audience established for the report on facility locations, the scope would include such information as land and building costs, available labor force, cultural issues, transportation options, and proximity to suppliers. However, it probably would not include the early history of the cities being considered or their climate and geological features, unless those aspects were directly related to your particular business.

**Selecting the Medium:** Finally, you need to determine the most appropriate medium for communicating your message. Professionals on the job face a wide array of options—from e-mail, fax, voice mail, videoconferencing, and Web sites to more traditional means like letters, memos, reports, telephone calls, and face-to-face meetings. The most important considerations in selecting the appropriate medium are the audience and the purpose of the communication. For example, if you need to collaborate with someone to solve a problem or if you need to establish rapport with someone, written exchanges could be far less efficient than a phone call or a face-to-face meeting. However, if you need precise wording or you need to provide a record of a complex message, communicate in writing.

1. **Research**

The only way to be sure that you can write about a complex subject is to thoroughly understand it. To do that, you must conduct adequate research, whether that means conducting an extensive investigation for a major proposal—through interviewing, library and Internet research, and careful note-taking—or simply checking a company Web site and jotting down points before you send an e-mail to a colleague.

**Methods of Research:** Researchers frequently distinguish between primary and secondary research, depending on the types of sources consulted and the method of gathering information. Primary research refers to the gathering of raw data compiled from interviews, direct observation, surveys, experiments, questionnaires, and audio and video recordings, for example. In fact, direct observation and hands-on experience are the only ways to obtain certain kinds of information, such as the behavior of people and animals, certain natural phenomena, mechanical processes, and the operation of systems and equipment. Secondary research refers to gathering information that has been analyzed, assessed, evaluated, compiled, or otherwise organized into accessible form. Such forms or sources include books, articles, reports, Web documents, e-mail discussions, and brochures. Use the methods most appropriate to your needs, recognizing that some projects will require several types of research and that collaborative projects may require those research tasks to be distributed among team members.

**Sources of Information:** As you conduct research, numerous sources of information are available to you, including the following:

* Your own knowledge and that of your colleagues
* The knowledge of people outside your workplace, gathered through interviewing for information
* Internet sources, including Web sites, directories, archives, and discussion groups
* Library resources, including databases and indexes of articles as well as books and reference works
* Printed and electronic sources in the workplace, such as various correspondence, reports, and Web intranet documents Consider all sources of information when you begin your research and use those that are appropriate and useful. The amount of research you will need to do depends on the scope of your project. See also documenting sources.

1. **Organization**

Without organization, the material gathered during your research will be incoherent to your readers. To organize information effectively, you need to determine the best way to structure your ideas; that is, you must choose a primary method of development.

**Methods of Development:** An appropriate method of development is the writer’s tool for keeping information under control and the readers’ means of following the writer’s presentation. As you analyze the information you have gathered, choose the method that best suits your subject, your readers’ needs, and your purpose. For example, if you were writing instructions for assembling office equipment, you would naturally present the steps of the process in the order readers should perform them: the sequential method of development.

If you were writing about the history of an organization, your account would most naturally go from the beginning to the present: the chronological method of development. If your subject naturally lends itself to a certain method of development, use it—do not attempt to impose another method on it.

Often you will need to combine methods of development. For example, a persuasive brochure for a charitable organization might combine a specific-to-general method of development with a cause-and-effect method of development. That is, you could begin with persuasive case histories of individual people in need and then move to general information about the positive effects of donations on recipients.

**Outlining:** Once you have chosen a method of development, you are ready to prepare an outline. Outlining breaks large or complex subjects into manageable parts. It also enables you to emphasize key points by placing them in the positions of greatest importance. By structuring your thinking at an early stage, a well-developed outline ensures that your document will be complete and logically organized, allowing you to focus exclusively on writing when you begin the rough draft. An outline can be especially helpful for maintaining a collaborative-writing team’s focus throughout a large project. However, even a short letter or memo needs the logic and structure that an outline provides, whether the outline exists in your mind or on-screen or on paper.

At this point, you must begin to consider layout and design elements that will be helpful to your readers and appropriate to your subject and purpose. For example, if visuals such as photographs or tables will be useful, this is a good time to think about where they may be positioned to be most effective and if they need to be prepared by someone else while you are writing and revising the draft. The outline can also suggest where headings, lists, and other special design features may be useful.

1. **Writing**

When you have established your purpose, your readers’ needs, and your scope and have completed your research and your outline, you will be well prepared to write a first draft. Expand your outline into paragraphs, without worrying about grammar, refinements of language usage, or punctuation. Writing and revising are different activities; refinements come with revision.

Write the rough draft, concentrating entirely on converting your outline into sentences and paragraphs. You might try writing as though you were explaining your subject to a reader sitting across from you. Do not worry about a good opening. Just start. Do not be concerned in the rough draft about exact word choice unless it comes quickly and easily—concentrate instead on ideas.

Even with good preparation, writing the draft remains a chore for many writers. The most effective way to get started and keep going is to use your outline as a map for your first draft. Do not wait for inspiration—you need to treat writing a draft as you would any on-the-job task. The entry writing a draft describes tactics used by experienced writers—discover which ones are best suited to you and your task.

Consider writing an introduction last because then you will know more precisely what is in the body of the draft. Your opening should announce the subject and give readers essential background information, such as the document’s primary purpose. For longer documents, an introduction should serve as a frame into which readers can fit the detailed information that follows.

Finally, you will need to write a conclusion that ties the main ideas together and emphatically makes a final significant point. The final point may be to recommend a course of action, make a prediction or a judgment, or merely summarize your main points—the way you conclude depends on the purpose of your writing and your readers’ needs.

1. **Revision**

The clearer finished writing seems to the reader, the more effort the writer has likely put into its revision. If you have followed the steps of the writing process to this point, you will have a rough draft that needs to be revised. Revising, however, requires a different frame of mind than does writing the draft. During revision, be eager to find and correct faults and be honest. Be hard on yourself for the benefit of your readers. Read and evaluate the draft as if you were a reader seeing it for the first time.

Check your draft for accuracy, completeness, and effectiveness in achieving your purpose and meeting your readers’ needs and expectations. Trim extraneous information: Your writing should give readers exactly what they need, but it should not burden them with unnecessary information or sidetrack them into loosely related subjects.

### **Diagrams, graphs, tables and mathematics**

It is often the case that technical information is most concisely and clearly conveyed by means other than words. Imagine how you would describe an electrical circuit layout using words rather than a circuit diagram. Here are some simple guidelines;

|  |  |
| --- | --- |
| Diagrams | Keep them simple. Draw them specifically for the report. Put small diagrams after the text reference and as close as possible to it. Think about where to place large diagrams. |
| Graphs | Clearly marked visuals that show statistical trends or provide examples of how to perform a specific task, when balanced with well-developed writing, can make for extremely useful documents. Some things are just too difficult to explain without a visual example. |
| Tables | Is a table the best way to present your information? Consider graphs, bar charts or pie charts. Dependent tables (small) can be placed within the text, even as part of a sentence. Independent tables (larger) are separated from the text with table numbers and captions. Position them as close as possible to the text reference. Complicated tables should go in an appendix. |
| Mathematics | Only use mathematics where it is the most efficient way to convey the information. Longer mathematical arguments, if they are really necessary, should go into an appendix. You will be provided with lecture handouts on the correct layout for mathematics. |

**The report layout**: The appearance of a report is no less important than its content. An attractive, clearly organized report stands a better chance of being read. Use a standard, 12pt, font, such as Times New Roman, for the main text. Use different font sizes, bold, italic and underline where appropriate but not to excess. Too many changes of type style can look very fussy.

Do not try to revise for everything at once. Read your rough draft several times, each time looking for and correcting a different set of problems or errors. Concentrate first on larger issues, such as unity and coherence; save mechanical corrections, like spelling and punctuation, for later proofreading.

### **Proofreading:** This refers to the checking of every aspect of a piece of written work from the content to the layout and is an absolutely necessary part of the writing process. You should acquire the habit of never sending or submitting any piece of written work, from email to course work, without at least one and preferably several processes of proofreading. In addition, it is not possible for you, as the author of a long piece of writing, to proofread accurately yourself; you are too familiar with what you have written and will not spot all the mistakes.

**Completing a Peer Review:** Do not work in a vacuum. Find a trusted colleague who will read the document with an objective eye and will provide honest feedback. In addition, including others early in the process can reduce the possibility of major edits and revisions later.

After working so closely with a piece of writing, writers often need to step back and ask for a more objective reader. What writers most need is feedback from readers who can respond only to the words on the page. When they are ready, writers show their drafts to someone they respect and who can give an honest response about its strengths and weaknesses.

You, too, can ask a peer to read your draft when it is ready. After evaluating the feedback and assessing what is most helpful, the reader’s feedback will help you when you revise your draft. This process is called peer review.

The purpose of peer feedback is to receive constructive criticism of your writing. Your peer reviewer is your first real audience, and you have the opportunity to learn what confuses and delights a reader so that you can improve your work before sharing the final draft with a wider audience (or your intended audience).

It may not be necessary to incorporate every recommendation your peer reviewer makes. However, if you start to observe a pattern in the responses you receive from peer reviewers, you might want to take that feedback into consideration in future assignments. For example, if you read consistent comments about a need for more research, then you may want to consider including more research in future assignments.

**Informal and Formal Oral Reports**

An oral report may be delivered around a small table with just a few listeners or in a large auditorium to hundreds of people.

* **Informal oral reports** are generally characterized by small-group settings with a high degree of [audience interaction](http://web.mit.edu/course/21/21.guide/audience.htm) and a relaxed manner of [delivery](http://web.mit.edu/course/21/21.guide/delivery.htm) and dress. An informal oral report might be an impromptu presentation. Informal oral presentations can foster the free exchange of ideas and be important for producing action items.
* **A formal oral report** is distinguished by its adherence to an agreed-upon format or [outline](http://web.mit.edu/course/21/21.guide/outline.htm). Formal oral reports are usually prepared well in advance of presentation and are therefore well [rehearsed](http://web.mit.edu/course/21/21.guide/delivery.htm#ora-rehr). Your [manner of delivery](http://web.mit.edu/course/21/21.guide/delivery.htm) is extremely important in a formal oral report situation. Audience interaction is generally limited to the [question and answer period](http://web.mit.edu/course/21/21.guide/ora-out.htm#q-and-a) at the conclusion of your report. Formal oral reports may follow an outline similar to the parts of any formal [written report](http://web.mit.edu/course/21/21.guide/reports.htm) and may be presented to an audience of one's peers or to an interested general or mixed audience in a setting such as a large auditorium or hall. However, the size of a room or an audience does not solely define a formal situation. Formal oral reports may also include presentations to small in-house groups of [managers](http://web.mit.edu/course/21/21.guide/managers.htm) or academic committees, for example. Presenting effective formal oral reports is an important means of establishing and maintaining your credentials and authority within a field or within an organization.

## Topic and Situation for the Oral Presentation

For the oral report in a technical writing course, imagine that you are formally handing over your final written report to the people with whom you set up the hypothetical contract or agreement. For example, imagine that you had contracted with a software company to write its user guide. Once you had completed it, you'd have a meeting with chief officers to formally deliver the guide. You'd spend some time orienting them to the guide, showing them how it is organized and written, and discussing some of its highlights. Your goal is to get them acquainted with the guide and to prompt them for any concerns or questions.

As you can see, you shouldn't have to do any research to prepare for this assignment—just plan the details of your talk and get at least one visual ready. If you have a report topic that you'd prefer not to present orally, discuss other possibilities with your instructor. Here are some brainstorming possibilities in case you want to present something else:

* **Purpose:** One way to find a topic is to think about the purpose of your talk. Is it to instruct (for example, to explain how to run a text editing program on a computer), to persuade (to vote for or against a certain technically oriented bond issue), or simply to inform (to report on citizen participation in the new recycling program).
  + Informative purpose: An oral report can be primarily informative. For example, as a member of a committee involved in a project to relocate the plant, your job might be to give an oral report on the condition of the building and grounds at one of the sites proposed for purchase. Or, you might be required to go before the city council and report on the success of the new city-sponsored recycling project.
  + Instructional purpose: An oral report can be primarily instructional. Your task might be to train new employees to use certain equipment or to perform certain routine tasks.
  + Persuasive purpose: An oral report can be primarily persuasive. You might want to convince members of local civic organizations to support a city-wide recycling program. You might appear before city council to persuade its members to reserve certain city-owned lands for park areas, softball and baseball parks, or community gardens.
* **Topics:** You can start by thinking of a technical subject, for example, solar panels, microprocessors, drip irrigation, or laser surgery. For your oral report, think of a subject you'd be interested in talking about, but find a reason why an audience would want to hear your oral report.
* **Place or situation:** You can find topics for oral reports or make more detailed plans for them by thinking about the place or the situation in which your oral report might naturally be given: at a neighborhood association? at the parent–teachers' association meeting? at a church meeting? at the gardening club? at a city council meeting? at a meeting of the board of directors or high-level executives of a company? Thinking about an oral report this way makes you focus on the audience, their reasons for listening to you, and their interests and background.

**Contents and Requirements for the Oral Presentation**

The focus for your oral presentation is clear, understandable presentation; well-organized, well-planned, well-timed discussion. You don't need to be Mr. or Ms. Slick-Operator—just present the essentials of what you have to say in a calm, organized, well-planned manner.

When you give your oral presentation, we'll all be listening for the same things. Use the following as a requirements list, as a way of focusing your preparations:

* Plan to explain to the class what the situation of your oral report is, who you are, and who they should imagine they are. Make sure that there is a clean break between this brief explanation and the beginning of your actual oral report.
* Make sure your oral report lasts no longer than the maximum stipulated by the event organizers or your instructor. If you are in a technical-writing class, ask your instructor to use signals to indicate when the maximum is approaching, has arrived, or has past.
* Pay special attention to the introduction to your talk:
  + Indicate the purpose of your oral report
  + Give an overview of its contents
  + Find some way to interest the audience.
* Use at least one visual—preferably slides using presentation software (such as PowerPoint) or transparencies for the overhead projector. Flip charts and objects for display are okay. But avoid scribbling stuff on the chalkboard or whiteboard or relying strictly on handouts.
* Make sure you discuss key elements of your visuals. Don't just throw them up there and ignore them. Point out things about them; explain them to the audience.
* Plan to explain any technical aspect of your topic clearly and understandably. Don't race through complex, technical stuff—slow down and explain it carefully so that we understand it.
* Use "spoken headings"—by now, you've gotten used to using headings in your written work. There is a corollary in oral reports. With these, you give your audience a very clear signal you are moving from one topic or part of your talk to the next.
* Plan your report in advance and practice it so that it is organized. Make sure that listeners know what you are talking about and why, which part of the talk you are in, and what's coming next. Overviews and spoken headings greatly contribute to this sense of organization.
* End with a real conclusion. People sometimes forget to plan how to end an oral report and end by just trailing off into a mumble. Remember that in conclusions, you can:
  + summarize (go back over high points of what you've discussed)
  + conclude (state some logical conclusion based on what you have presented)
  + provide some last thought (end with some final interesting point but general enough not to require elaboration)
  + or some combination of these three
* And certainly, you'll want to prompt the audience for questions and concerns.
* As mentioned above, be sure your oral report is carefully timed according to the maximum allowed.

**Preparing for the Oral Presentation**

Pick the method of preparing for the talk that best suits your comfort level with public speaking and with your topic. However, do some sort of preparation or rehearsal—some people assume that they can just jump up there and ad lib for the expected time frame and be relaxed, informal. It doesn't often work that way—drawing a mental blank is the more common experience.

Here are the obvious possibilities for preparation and delivery:

* Write a script, practice it; keep it around for quick-reference during your talk.
* Set up an outline of your talk; practice with it, bring it for reference.
* Set up cue cards, practice with them, and use them during your talk.
* Write a script and read from it (preferably, occasionally glance at it).

Of course, the extemporaneous or impromptu methods are also out there for the brave and the adventurous. However, please bear in mind that up to 25 people will be listening to you—you owe them a good presentation, one that is clear, understandable, well-planned, organized, and on target with your purpose and audience. It doesn't matter which method you use to prepare for the talk. Of course the head-down style of reading your report directly from a script has its problems. There is little or no eye contact or interaction with the audience. The delivery tends toward a dull monotone that either puts listeners off or is hard to understand.

For some reason, people tend to get nervous if they are new to oral presentations. Try to remember that your classmates and instructor are a very forgiving, supportive group. You don't have to be a slick entertainer—just be clear, organized, and understandable. The nerves will wear off someday, the more oral presenting you do.

**Getting the Presentation Started: the Introduction**

To get your presentation off to a good start, plan on doing the following:

1. Introduce yourself and say a bit about yourself.
2. Indicate the topic and purpose of your presentation.
3. Find some brief way to indicate the importance of your topic—spark some interest.
4. Provide a brief in-sentence list of what your presentation will cover; provide a roadmap.

**Delivering an Oral Presentation**

When you give an oral report, focus on common problem areas such as these:

* **Timing**—Make sure you keep within the expected time limit. Anything way under is also a problem. Do some rehearsal, write a script, or find some other way to get the timing just right.
* **Volume**—Obviously, you must be sure to speak loud enough so that all of your audience can hear you. You might find some way to practice speaking a little louder in the days before the oral presentation.
* **Pacing, speed**—Sometimes, oral presentators who are a bit nervous talk too fast. All that adrenaline causes them to speed through their talk. That makes it hard for the audience to follow. In general, it helps listeners to understand you better if you speak a bit more slowly and deliberately than you do in normal conversation. Slow down, take it easy, be clear.
* **Gestures and posture**—Watch out for nervous hands flying all over the place. This too can be distracting—and a bit comical. At the same time, don't turn yourself into a mannikin. Plan to keep your hands clasped together or holding onto the podium and only occasionally making some gesture. As for posture, avoid slouching at the podium and leaning against the wall.
* **Verbal crutches**—Watch out for too much "uh," "you know," "okay" and other kinds of nervous verbal habits. Instead of saying "uh" or "you know" every three seconds, just don't say anything at all. In the days before your oral presentation, practice speaking without these verbal crutches. The silence that replaces them is not a bad thing—it gives listeners time to process what you are saying.

**Planning and Preparing Visuals for Oral Presentations**

Prepare at least one visual for this report. Here are some ideas for the "medium" to use for your visuals:

* **Presentation software slides**—Projecting images ("slides") using software such as Powerpoint has become the standard, even though maligned by some. One common problem with the construction of these slides is cramming too much information on individual slides. A quick search on terms like Powerpoint presentation will enable you to read about creating these slides and designing them intelligently. Of course, the room in which you use these slides has to have a computer projector.
* **Transparencies for overhead projector**—The overhead projector used with transparencies seems to have been relegated to antiquity—but not entirely. In this method, you design your visual on a sheet of blank paper, then photocopy it, and then get a transparency of it.
* **Posterboard-size charts**—Another possibility is to get some posterboard and draw and letter what you want your audience to see. Of course, it's not easy making charts look neat and professional.
* **Handouts**—You can run off copies of what you want your listeners to see and hand them out before or during your talk. This option is even less effective than the first two because you can't point to what you want your listeners to see and because handouts take listeners' attention away from you. Still, for certain visual needs, handouts are the only choice.
* **Objects**—If you need to demonstrate certain procedures, you may need to bring in actual physical objects. Rehearse what you are going to do with these objects; sometimes they can take up a lot more time than you expect.

Avoid just scribbling your visual on the chalkboard or whiteboard. Whatever you scribble can be neatly prepared and made into a presentation slide, transparency, or posterboard-size chart. Take some time to make your visuals look sharp and professional—do your best to ensure that they are legible to the entire audience. As for the content of your visuals, consider these ideas:

* **Drawing or diagram of key objects**—If you describe or refer to any objects during your talk, try to get visuals of them so that you can point to different components or features.
* **Tables, charts, graphs**—If you discuss statistical data, present it in some form or table, chart, or graph. Many members of your audience may be less comfortable "hearing" such data as opposed to seeing it.
* **Outline of your talk, report, or both**—If you are at a loss for visuals to use in your oral presentation, or if your presentation is complex, have an outline of it that you can show at various points during your talk.
* **Key terms and definitions**—A good idea for visuals (especially when you can't think of any others) is to set up a two-column list of key terms you use during your oral presentation with their definitions in the second column.
* **Key concepts or points**—Similarly, you can list your key points and show them in visuals. (Outlines, key terms, and main points are all good, legitimate ways of incorporating visuals into oral presentations when you can't think of any others.)

During your actual oral report, make sure to discuss your visuals, refer to them, guide your listeners through the key points in your visuals. It's a big problem just to throw a visual up on the screen and never even refer to it.

**Technical Memo Organization**

Technical memos are essentially short technical reports geared to answer specific client questions.  Generally, memos are much shorter than reports (only 1 to 2 pages) and have less introductory and background information.  Often the memos are in the form of a letter or an email.  Results are often given in a supplementary section (enclosure in a letter or attachment to an email).

* Subject line – regardless of whether the form is a letter or email, there needs to be a short subject line for the memo
* Addressee – Memos are written for someone. You should address the memo to a person or a committee or group.
* Introductory paragraph – Although the introduction is not a long as in a report, the memo still needs to state the purpose of the memo and any assumptions or given information that was used in the experiment or design.
* Discussion paragraphs – These paragraphs answer the specific questions of the client. They are similar to a report discussion, but more targeted to the audience and the questions asked.  All discussions should be quantitative.
* Conclusion – This optional paragraph may sum up some important points or recommendation. It can also provide encouragement for the client to contact you for more information.

**Technical Writing Format**

The format or flow of information is important in helping the reader easily understand and process the information.  Learn more about the common format used in technical reports and how to use citations and references.

* **General Format**

The format or flow of information is important in helping the reader easily understand and process the information.  The format builds the scaffold upon which the communication is based.  A strong consistent and recognizable format aids the reader in processing the information

In general, there is an orderly explanation that explains the logic of the work.  The paragraphs are also arranged in a consistent format usually starting with a topic sentence and then other sentences related to the topic of the paragraph.

The format of the technical writing depends on the audience and purpose.  A short memo may simply describe the purpose of the memo in the first paragraph and answer a few key questions in the subsequent paragraphs.  A comprehensive lab or design report will be longer and typically divided into many sections.  There is not one “correct” format.  The main importance is that the writing is structured so that the reader can easily and quickly recognize important information. This section provides some format examples for technical reports and memos.  The formatting requirements for citations, references, cross-references, and cover sheets are the same for all written communications.

## Citations

Most technical reports reference other sources of information.  As such, the use of citations and cross-references is important.   If you are discussing the ideas in a source at length (for example, in a summary), you do not need to cite every consecutive sentence. Cite the first time you mention the source, as long the following sentences clearly indicate that the ideas come from the same source.

There are two common conventions in Engineering: 1) the author-date format and 2) the numerical format.  You will use the author date format for all assignments in Engineering, however the numerical format is required by some journals (such as the American Concrete Institute journals).

### **Author-date format**

The author-date format is the default format used by the ASCE style guide (https://ascelibrary.org/doi/pdf/10.1061/9780784479018.ch05) and will be the default format you will use in reports for the Civil Engineering program.  The in-text citations consist of the names of individuals and corporate authors and the year of publication of the cited work in parentheses immediately following the information cited.  All citations must appear in the list of references.

#### **Examples**

* **Basic format:**
* **Paraphrased information** – you have gathered information from the source(s) but you are not directly copying what they have written.
  + Reinforced concrete (RC) flat-plate structures, as compared with other RC structural systems, generally cost less and are faster to construct (Gilsanz et al. 2015).
* **Quoted information** – you want to maintain the way the original text wrote the information.  Try not to use quotations unless it is important to maintain the text.  In the following example, the code language may be under discussion so the exact language of the code is quoted.
  + “Buildings and other structures shall be designed to sustain local damage with the structural system as a whole remaining stable and not being damaged to an extent disproportionate to the original local damage.” (ASCE 2002, p. 2)
* **If the author is mentioned in sentence** – Indicate year of publication only in parentheses following the author’s name.
  + Qian and Li (2014) performed static and dynamic loading tests of multi-panel flat-plate subassemblies with reduced scales to examine the collapse resistance of flat plates.
* **Two individual authors** – Include the last name of each author.
  + Construction failure is avoidable (Feld and Carper 1977).
* **Three or more individual authors** – The first author’s name is given, followed by “et al.” (no italics) and the year.
  + Innovative technologies can be used to determine the longevity of key infrastructure features (McCullough et al. 2004).
* **Multiple works produced by the same author(s) in the same year** – Designate works with sequential lower-case letters appended to the year.
  + Previous cases of progressive collapse of buildings have been investigated by Sasani et al. (2007a, 2007b).

### **Numerical format**

The numerical format is preferred by some journals and other publications.  In this format, all the references are arranged numerically by the order in which they appear in the text.  The citation simply consists of the number related to that reference either as a superscript or in brackets.  This uses less room for the citation, but also does not provide information on who wrote the report or when the report was written.

* Construction failure is avoidable1.  -Or- Construction failure is avoidable [1].

If the author is mentioned in the sentence, the number is still used.

* According to Wynham2, no additional support is necessary.  -Or- According to Wynham [2], no additional support is necessary.

## References

References give the reader the information they need to know so that they can find the reference for more information. Depending on where the report is published, the required format for the references may be slightly different.  In Civil Engineering, the default format is the ASCE style.  The excerpt below is directly from the ASCE style guide at https://ascelibrary.org/doi/pdf/10.1061/9780784479018.ch05.

### **Books**

If a whole book is used (or pages here and there throughout the book), page numbers need not be given. If no author is listed, titles should be alphabetized. If a specific chapter is being used, the chapter title and inclusive page numbers should be included. Reports must include the full institution name and location.

* Evans, G. M., and Furlong, J. C. (2003). Environmental biotechnology: Theory and applications, Wiley, Chichester, U.K.
* Moody’s municipal and government manual. (1988). Moody’s Investors Service, New York.

### **Building Codes and Provisions**

Building codes, provisions, and standards should be listed alphabetically by the name of the promulgating institution. If a title and code number are given, the title should be in quotes, and the code number in italics; if only a title is given, the title should be in italics.

* ACI (American Concrete Institute).(1989). “Building code requirement for reinforced concrete.” ACI 318-89,Farmington Hills, MI.
* Building Officials and Code Administrators International (BOCA). (1993). The BOCA national building code, Country Club Hills, IL.
* CEN (European Committee for Standardization). (1992). “Design of steel structures, part 1.1.”Eurocode 3, Brussels.

### **Electronic Materials**

CD-ROM—The section, chapter, and page numbers should be provided if available:

* Liggett, J. A., and Caughey, D. A. (1998). “Fluid statistics.” Fluid mechanics(CD-ROM), ASCE, Reston, VA, Section …, Chapter …, pp. …

### **Website**

The following elements should be included: author’s name (if known); year of publication or last revision (if available); full title of the document, in quotation marks; title of the complete work (if applicable), in italics; full web address, enclosed within angle brackets; and date of the visit (if applicable), in parentheses. If the Web page shows no year of publication, the year of the visit may be used in its place.

* Arizona Dept. of Commerce. (2005). “Community profile: Hualapai Indian Reservation.” 〈[http://www](http://www/).azcommerce/com/doclib/commune/ualapai.pdf〉(Mar. 17, 2014).
* “Acquisition reform network.” (1998). Arnet, 〈[http://www](http://www/).arnet.gov〉(Jan. 21, 2010)

### **Journal Articles**

The standard format for a paper published in a U.S. journal is as follows:

* Beskos, D. E. (1987). “Boundary element methods in dynamic analysis.” Appl. Mech. Rev.,40(1), 1–23.

#### **ASCE Journals**

ASCE no longer uses page numbers and has adopted a new format for its references (including those older papers that still contain page numbers). Use the following style for citation to an ASCE journal:

* Authors. (Year of initial publication). “Title of paper.” Journal abbr., DOI, CID/page range.
* Irish, J. L., and Resio, D. T. (2013). “Method for estimating future hurricane flood probabilities and associated uncertainty.” J. Waterway, Port, Coastal, Ocean Eng., 10.1061/(ASCE)WW.1943-5460.0000157, 04013015.

#### **ASCE Committee/Technical Reports**

ASCE committees, task forces, etc. publish reports, proposed codes and standards, commentaries on codes and standards, and so on. The committee is the author.

* ASCE Task Force on Friction Factors in Open Channels. (1963). “Friction factors in open channels.” J. Hydraul. Div., 89(2), 97–143.
* **Cross-References**

In addition to referencing other sources of information, cross-references are also used to refer to figure, tables, and equations within the report.  You must refer to every table, figure, equation used in the text.  For documents in Engineering use the full reference (i.e. Figure #, Table #, Equation #) instead of an abbreviation (i.e. Fig., Eq.).  If the item (figure, table, or equation) is a noun in the sentence then use it as a proper noun and capitalize the first letter.

* Figure 1 shows the stress-strain curve of aluminum.
* The stress-strain curve of aluminum is shown in Figure 1.

If the item (figure, table, equation) serves as a reference (where to go for more information), then include it in parentheses.

* The stress-strain curve of aluminum is non-linear (Figure 1).

All exhibits (Figures, Tables, Equations) should be sequentially numbered throughout the report (don’t skip numbers) and the cross-reference in the text should occur before the figure.  If you change the order of your figures you have to renumber them.  If the report is in several chapters, then the number may contain a chapter and/or sub-chapter number (i.e. Figure 3-4).  The use of automatic features in Word makes keeping track of these things easier.

You can also use cross-references to refer to different sections in the report.  This is common in technical reports in which the chapters and sub-sections are numbered.

**Method/Techniques of Oral Report/Oral Presentation**

1. **Impromptu Speaking**

Impromptu speaking is the presentation of a short message without advance preparation. Impromptu speeches often occur when someone is asked to “say a few words” or give a toast on a special occasion. You have probably done impromptu speaking many times in informal, conversational settings. Self-introductions in group settings are examples of impromptu speaking: “Hi, my name is Steve, and I’m a volunteer with the Homes for the Brave program.” Another example of impromptu speaking occurs when you answer a question such as, “What did you think of the documentary?”

The advantage of this kind of speaking is that it’s spontaneous and responsive in an animated group context. The disadvantage is that the speaker is given little or no time to contemplate the central theme of his or her message. As a result, the message may be disorganized and difficult for listeners to follow.

Here is a step-by-step guide that may be useful if you are called upon to give an impromptu speech in public.

* Take a moment to collect your thoughts and plan the main point you want to make.
* Thank the person for inviting you to speak.
* Deliver your message, making your main point as briefly as you can while still covering it adequately and at a pace your listeners can follow.
* Thank the person again for the opportunity to speak.
* Stop talking.

As you can see, impromptu speeches are generally most successful when they are brief and focus on a single point.

1. **Extemporaneous Speaking**

Extemporaneous speaking is the presentation of a carefully planned and rehearsed speech, spoken in a conversational manner using brief notes. By using notes rather than a full manuscript, the extemporaneous speaker can establish and maintain eye contact with the audience and assess how well they are understanding the speech as it progresses. The opportunity to assess is also an opportunity to restate more clearly any idea or concept that the audience seems to have trouble grasping.

For instance, suppose you are speaking about workplace safety and you use the term “sleep deprivation.” If you notice your audience’s eyes glazing over, this might not be a result of their own sleep deprivation, but rather an indication of their uncertainty about what you mean. If this happens, you can add a short explanation; for example, “sleep deprivation is sleep loss serious enough to threaten one’s cognition, hand-to-eye coordination, judgment, and emotional health.” You might also (or instead) provide a concrete example to illustrate the idea. Then you can resume your message, having clarified an important concept.

Speaking extemporaneously has some advantages. It promotes the likelihood that you, the speaker, will be perceived as knowledgeable and credible. In addition, your audience is likely to pay better attention to the message because it is engaging both verbally and nonverbally. The disadvantage of extemporaneous speaking is that it requires a great deal of preparation for both the verbal and the nonverbal components of the speech. Adequate preparation cannot be achieved the day before you’re scheduled to speak.

Because extemporaneous speaking is the style used in the great majority of public speaking situations, most of the information in this chapter is targeted to this kind of speaking.

1. **Speaking from a Manuscript**

Manuscript speaking is the word-for-word iteration of a written message. In a manuscript speech, the speaker maintains his or her attention on the printed page except when using visual aids.

The advantage to reading from a manuscript is the exact repetition of original words. As we mentioned at the beginning of this chapter, in some circumstances this can be extremely important. For example, reading a statement about your organization’s legal responsibilities to customers may require that the original words be exact. In reading one word at a time, in order, the only errors would typically be mispronunciation of a word or stumbling over complex sentence structure.

However, there are costs involved in manuscript speaking. First, it’s typically an uninteresting way to present. Unless the speaker has rehearsed the reading as a complete performance animated with vocal expression and gestures (as poets do in a poetry slam and actors do in a reader’s theater), the presentation tends to be dull. Keeping one’s eyes glued to the script precludes eye contact with the audience. For this kind of “straight” manuscript speech to hold audience attention, the audience must be already interested in the message before the delivery begins.

It is worth noting that professional speakers, actors, news reporters, and politicians often read from an autocue device, such as a TelePrompTer, especially when appearing on television, where eye contact with the camera is crucial. With practice, a speaker can achieve a conversational tone and give the impression of speaking extemporaneously while using an autocue device. However, success in this medium depends on two factors: (1) the speaker is already an accomplished public speaker who has learned to use a conversational tone while delivering a prepared script, and (2) the speech is written in a style that sounds conversational.

1. **Speaking from Memory**

Memorized speaking is the rote recitation of a written message that the speaker has committed to memory. Actors, of course, recite from memory whenever they perform from a script in a stage play, television program, or movie scene. When it comes to speeches, memorization can be useful when the message needs to be exact and the speaker doesn’t want to be confined by notes.

The advantage to memorization is that it enables the speaker to maintain eye contact with the audience throughout the speech. Being free of notes means that you can move freely around the stage and use your hands to make gestures. If your speech uses visual aids, this freedom is even more of an advantage. However, there are some real and potential costs. First, unless you also plan and memorize every vocal cue (the subtle but meaningful variations in speech delivery, which can include the use of pitch, tone, volume, and pace), gesture, and facial expression, your presentation will be flat and uninteresting, and even the most fascinating topic will suffer. You might end up speaking in a monotone or a sing-song repetitive delivery pattern. You might also present your speech in a rapid “machine-gun” style that fails to emphasize the most important points. Second, if you lose your place and start trying to ad lib, the contrast in your style of delivery will alert your audience that something is wrong. More frighteningly, if you go completely blank during the presentation, it will be extremely difficult to find your place and keep going.

1. **Reading**

In case of long speeches, it may be necessary to read some parts of your speech text. There are occasions when you have to convey some critical and complex or technical information, or some official statement. In that case, you do not want to make mistakes or look absurd by ad-libbing. There you must read it verbatim—word for word. The good thing with reading method is that there are minimum chances of any mistake—technical, grammatical, or that of pronunciation. But this method oral delivery is that there is very little eye contact, which results in the loss of your audience’s attention.

**The 7 Most Effective Oral Presentation Techniques:**

1. **Explore the Venue**
2. **Know the Audience**
3. **Engage the Audience**
4. **Have Passion**
5. **Master the Content**
6. **Keep to the Time**
7. **Practice, Practice and Practice Again**

## Effective Presentation Techniques

An effective presentation will be one where the audience leaves you with the information that you want them to. They will then, hopefully, act on that information in the desired way.

To get an audience to absorb information, you will need to deliver it in the way most appropriate to that specific situation. You will need to have a good understanding of both your content and the audience to make this happen.

There are of course a variety of different techniques that we won’t talk about today. Instead, we will focus on just a few of the most important presentation techniques, mastering them will make things go much easier down the line.

Once you have read through this guide there is a checklist at the bottom you can use during your presentation preparation.

### **Explore the Venue**

Before you give any sort of a presentation, you should know exactly where you will give it. Even if you are delivering the same speech to a similar crowd, the venue can make all the difference. Make sure you explore the venue before you give the speech. This will give you all sorts of benefits.

Firstly, you will likely feel more comfortable giving the speech if you have been in the venue beforehand. This will help to eliminate any of those pesky pre-presentation nerves. If you feel like you will get nervous, do whatever you can to relax.

Also, there may be important logistical information that you will only find out about when you explore the venue. The audio-visual equipment might be unfamiliar to you, or it might not even be working. By going in first and familiarizing yourself with it, you can save time later on.

You can set up any equipment or presentation aids you like in the time before you speak. This will help you take ownership of the space you will speak in and make you more comfortable.

Exploring the venue beforehand will also simply help you to visualize what your presentation will be like later on. Making sure that you have enough seats and know where everyone will be can make things go smoother.

### **Know the Audience**

Another vital, and often overlooked, aspect of any presentation is the audience themselves. You need to know who you are speaking to and will then have to tailor your presentation to their needs.

Let’s use the example of a local water authority. Their representatives will often have to speak in front of many different groups, all of which need different approaches. Our job here will be to discuss how our organization impacts each of these groups. This means we will tailor our presentation to each individually.

#### **Speaking at a School:** Here, you will need to really simplify your message and talk about what your organization does in its most basic terms. The focus should be on how the actions of the local water authority impact the community at large.

I would focus my efforts on discussing the nature of the work done by the local water authority and how vitally important it is. With a younger crowd interactive games and maybe even small science experiments can often work really well, helping engagement.

#### **Speaking to a Resident’s Association:** When speaking to the representatives of a local community, you will need to go into more detail about practicalities. With groups like this, the focus should be on how your services will impact daily life. This is especially true if there are going to be any disruptions.

Even though this group should have a better understanding of your organisation’s actions, you shouldn’t assume everyone knows everything about what you do. There will always be some people who have less of an understanding, so you should be prepared for that.

### **Engage with the Audience**

Once you know who you will be speaking to, you need to find out how to best engage them with the content of your presentation. This can be difficult, depending on the group. But getting this right can often mean the difference between success and failure.

We have all listened to presentations where we have been less than engaged. Most of us have had to suffer through what felt like an eternity for the speaker to get on with their point. When this happens, the audience will leave the room and everyone’s time was wasted!

In order for an audience to feel engaged, they will have to be interested, feel invested and understand what the speaker is talking about. Let’s go over these points.

#### **Understanding:** The audience will need to understand the information you are giving them. Make sure that you are clearly heard and your information is easily seen. Using tools like microphones, slides and charts can be really helpful here.

Most importantly however is your voice. In an oral presentation, you will need to make sure that you are speaking clearly and making an effort to talk directly to the audience. Practice this if need be.

#### **Interested and Invested:** You will need to make the audience interested in what you have to say. The best way to do this is to make them invested in your topic. Try to relate what you are talking about back to their lives as much as possible.

### **Have Passion**

Arguably the best way of getting the audience invested in your presentation is for you to be invested in it first. While this may be a little difficult, depending on the topic, you really should make an effort to be passionate about your presentation.

Let’s go back to our earlier example of a local water authority. It can be difficult to get passionate about a local water supply, but try to find a certain angle on it. By talking about how fundamentally necessary this service is, you can get a sense of how important getting it right will be.

Think about your presentation and try to find an aspect of it that makes you feel some sort of genuine emotion. This can really be any aspect at all, provided it is in some way related to your presentation topic.

This is important because its almost impossible to fake passion. When you are truly invested in something it will show in other ways and if you are talking about something you are passionate over, it will shine through in your talk. People will notice.

### **Master the Content**

This is your presentation and you should take ownership of all aspects of it. The most fundamental aspect of your presentation is its content.

Make sure you know exactly what you are going to say to your audience before your talk and know as much information relating to your topic as possible before you step into the room. This way you will be prepared if there are any surprise questions.

A great way to get ready for any surprise questions is to prepare far more of a speech than you will actually wind up saying. By taking parts of your presentation out before you give it, you will have extra things to say if asked on them. I love this tactic and use it all the time!

### **Keep to the Time**

By mastering the content and taking parts of your speech out when necessary, you will be better able to stick to your allotted time. For most presentations, you will be given a time limit. Stick to this limit as much as possible.

If you go too much over the limit you will start to impact all of the other things we have spoken about so far. People will become less engaged and the effectiveness of everything you have done so far will be diminished.

This can be a major factor if you are one of a number of speakers. If everyone starts to go over their time, then the impact on all the presentations is just going to be compounded. Have some courtesy to your fellow speakers and keep to your time limits!

### **Practice, Practice and Practice Again**

### The most effective technique when preparing any oral presentation is to practice it as much as possible. This advice is something of a cliché for a reason.

If you practice your presentation constantly, then you will be able to keep track of all the things we have spoken about in this guide and more.

When practicing your presentation, try it by yourself at first. Then record it, without keeping track of the time at first. Then, you will have to make sure you stick to the time limit by adding content or, more likely, taking some out.

If you are still a little unsure about your presentation at this point, try it out in front of friends and family. I find that this will be the hardest part of any presentation and will seem far more daunting than going in front of strangers. Once you have done it in front of loved-ones, you can do it in front of anyone!!

1. **Internal Correspondence**

Internal correspondence is a written communication between the employees, units, departments, and branches of the same organization. Internal correspondence can either be formal or less formal. Routine internal correspondence are usually less formal, such as quick instructions between a supervisor and a staff, and these are normally in the form of email.

There are other more formal types of internal correspondence which include promotion letter, written reprimand, notice to explain, memorandum, formal requests for approval, and letter of approval or dismissal. These types of communication are ideally printed on paper, signed by the sender, and physically received by the recipient.

1. **External Correspondence**

External correspondence takes place between different organizations, or between an organization and their individual clients. This is a form of written communication made by a company to those who do not belong to their organization.

External correspondence is commonly made to vendors, creditors, suppliers, existing customers, prospective clients, financial institutions, government offices, law and accounting firms, business affiliates, sponsors or donors, and other offices that have either direct or indirect business relationship with the company.

1. **Sales Correspondence**

Sales correspondence refers to sales-related communications. It is not limited to just selling a product or service, but it also includes other activities relating to sales. Sales correspondence include marketing letters, offer and discount letters, sales proposals, invoices, statement of accounts, sales reports, order confirmation, purchase orders, letters of authorization, collection letters, and such.

For the purpose of selling, it is important to know how to [write quality sales letters](http://www.letters.org/sales-letter/sample-sales-letter-2.html) to be able to communicate effectively. Also, marketing and offer letters should reflect truthful and non-misleading information. Other kinds of sales correspondence — such as invoice, purchase orders, and collection letters — must contain accurate information.

1. **Personalized Correspondence**

Personalized correspondence involved personal and emotional factors. Despite being labeled as “personalized”, this type of correspondence can also be used for business purposes. Examples of personalized correspondence include letters of gratitude, letters of favours or requests, appreciation notes, letters of congratulations of commendation, and such.

This particular type of correspondence doesn’t need to have a very formal tone. Though this can be done via email, writing an actual, physical letter is more preferable because it has a sense of personal touch. You may use a regular office paper for this, or perhaps a personalized yet [cheap note pads](https://www.banana-print.co.uk/notepads/), or a greeting card for a certain purpose (e.g. Thank You card, Congratulations card, etc).

1. **Circulars**

Circulars are notices that are communicated to a large number of people within the organization. It is also referred to as office instructions or announcements. Often, general announcements (such as changes in contact information, details about meetings with shareholders, instructions about certain protocols, etc.) are being communicated via circulars.

1. **Routine Correspondence**:

Routine correspondence refers to correspondence on routine matters like inquiries, acknowledgements, replies, orders, invitations and appointment letters.

1. **Technical Feasibility Study**

The engineering feasibility of the project in viewed in the technical feasibility. Certain important engineering aspects are covered which are necessary for the designing of the project like civil, structural and other relevant aspects. The technical capability of the projected technologies and the capabilities of the personnel to be employed in the project are considered.

In certain examples especially when projects are in third world countries, technology transfer between cultures and geographical areas should be analyzed. By doing so productivity gain (or loss) and other implications are understood due to the differences in fuel availability, geography, topography, infrastructure support and other problems.

1. **Managerial Feasibility Study**

Managerial feasibility is ascertained by certain key elements like employee involvement, demonstrated management availability & capability and commitment. The managerial and organizational structure of the project is addressed by this feasibility which ensures that the proponent’s structure mentioned in the submittal is feasible to the kind of operation undertaken.

1. **Economic Feasibility Study**

Economic feasibility refers to the feasibility of the considered project to produce economic benefits. A benefit-cost analysis is needed. Furthermore, the economic feasibility of a project can also be evaluated by breakeven analysis. In order to facilitate the consistent basis for the evaluation, the tangible and intangible facet of a project must be translated into the economic terms. Economic feasibility is critical even when the project is non-profit in nature.

1. **Financial Feasibility**

Financial feasibility must be differentiated from economic feasibility. The ability of the project management to raise sufficient funds required to implement the proposed project is included in the financial feasibility. Additional investors and other sources of funds are considered by the project proponents for their projects in many cases.

In such situations feasibility, sources, soundness and applications of these project funds may be a hindrance. Other aspects of financial feasibility should also be viewed, if appropriate, like creditworthiness, loan availability, equity, and loan schedule. The implications of land purchase, leases and other estates inland are also reviewed in the financial feasibility analysis.

1. **Cultural Feasibility Study**

The compatibility of the proposed project with the cultural environment of the project is included in the cultural feasibility. Planned operations should be integrated with the local cultural beliefs and practices in labor-intensive projects. For example, what a person is willing to perform or not perform is influenced by his religious beliefs.

1. **Social Feasibility Study**

The effect that a proposed project may have on the social system in the project environment is addressed in the social feasibility. It may happen that a particular category of employees may be short or not available as a result of ambient social structure.

The influence on the social status of the participants by the project should be evaluated in order to guarantee compatibility. It must be identified that employees in particular industries may have specific status symbols within the society.

1. **Safety Feasibility Study**

Another important aspect that must be considered in project planning is safety feasibility. Safety feasibility involves the analysis of the project in order to ascertain its capacity to implement & operate safely with the least unfavorable effects on the environment. Mostly in complex projects, environmental impact assessment is not properly addressed.

1. **Political Feasibility Study**

The directions for the proposed project are mostly dictated by political considerations. This is certainly correct for large projects with potential visibility that may have important political implications and government inputs. For example, regardless of the merit of the project, the political necessity may be a source of assistance for a project.

1. **Market Feasibility Study**

Market feasibility must not be mixed up with economic feasibility. The potential influence of market demand, competitive activities and available market share should be considered in the market feasibility analysis. During the start-up, ramp-up and commercial start-up phases of the project, possible competitive activities (local, regional, national and international) should be analyzed for early contingency funding and impacts on the operating costs.

1. **Schedule Feasibility**

In Schedule Feasibility Study mainly timelines/deadlines is analyzed for proposed project which includes how many times teams will take to complete final project which has a great impact on the organization as purpose of project may fail if it can’t be completed on time.

1. **Operational Feasibility**

In Operational Feasibility degree of providing service to requirements is analyzed along with how much easy product will be to operate and maintenance after deployment. Along with this other operational scopes are determining usability of product, Determining suggested solution by software development team is acceptable or not etc.

1. **Legal Feasibility**

In Legal Feasibility study project is analyzed in legality point of view. This includes analyzing barriers of legal implementation of project, data protection acts or social media laws, project certificate, license, copyright etc. Overall it can be said that Legal Feasibility Study is study to know if proposed project conform legal and ethical requirements.

**Types of Technical Reports**

* **Technical-background report.** The background report is the hardest to define but the most commonly written. This type of technical report provides background on a topic--for example, solar energy, global warming, CD-ROM technology, a medical problem, or U.S. recycling activity. However, the information on the topic is not just for anybody who might be interested in the topic, but for some individual or group that has specific needs for it and is even willing to pay for that information. For example, imagine an engineering firm bidding on a portion of the work to build a hemodialysis clinic. The engineers need to know general knowledge about renal disease and the technologies used to treat it, but they don't want to have to go digging in the library to find it. What they need is a technical background report on the subject.
* **Instructions.** These are probably the most familiar of all the types of reports. Students often write backup procedures for the jobs they do at their work. Others write short user manuals for an appliance, equipment, or program. If there is too much to write about, they write about some smaller segment--for example, instead of instructions on using all of WordPerfect, just a guide on writing macros in WordPerfect.
* **Feasibility, recommendation, and evaluation reports.** Another useful type of report is one that studies a problem or opportunity and then makes a recommendation. A feasibility report tells whether a project is "feasible"--that is, whether it is practical and technologically possible. A recommendation report compares two or more alternatives and recommends one (or, if necessary, none). An evaluation or assessment report studies something in terms of its worth or value For example, a college might investigate the feasibility of giving every student an e-mail address and putting many of the college functions online. The same college might also seek recommendations on the best hardware and software to use (after the feasibility report had determined it was a good idea). In practice, however, it's hard to keep these two kinds of reports distinct. Elements of the feasibility and recommendation report intermingle in specific reports--but the main thing is to get the job done!
* **Primary research report.** Primary research refers to the actual work someone does in a laboratory or in the field--in other words, experiments and surveys. You may have written a "lab report," as they are commonly called, for one of your previous courses. This is a perfectly good possibility for the technical report as well. In this type of report, you not only present your data and draw conclusions about it, but also explain your methodology, describe the equipment and facilities you used, and give some background on the problem. You can modify this type by summarizing other primary research reports. For example, you could report on the research that has been done on saccharine.
* **Technical specifications**. In this report type, you discuss some new product design in terms of its construction, materials, functions, features, operation, and market potential. True specifications are not much on writing--the text is dense, fragmented; tables, lists, and graphics replace regular sentences and paragraphs whenever possible. Thus, specifications are not a good exercise of your writing abilities. However, you can write a more high-level version--one that might be read by marketing and planning executives.
* **Report-length proposal.**A proposal is an offer or bid to do a certain project for someone. Proposals may contain other elements--technical background, recommendations, results of surveys, information about feasibility, and so on. But what makes a proposal a proposal is that it asks the audience to approve, fund, or grant permission to do the proposed project. If you plan to be a consultant or run your own business, written proposals may be one of your most important tools for bringing in business. And, if you work for a government agency, nonprofit organization, or a large corporation, the proposal can be a valuable tool for initiating projects that benefit the organization or you the employee-proposer (and usually both). A proposal should contain information that would enable the audience of that proposal to decide whether to approve the project, to approve or hire you to do the work, or both. To write a successful proposal, put yourself in the place of your audience--the recipient of the proposal--and think about what sorts of information that person would need to feel confident having you do the project.
* **Business prospectus.** If you are ambitious to run your own business, you can write a business prospectus, which is a plan or proposal to start a new business or to expand an existing one. It is aimed primarily at potential investors. Therefore, it describes the proposed business, explores the marketplace and the competition, projects revenues, and describes the operation and output of the proposed business.
* **Progress Report.** A progress report is exactly what it sounds like – a document that explains in detail how you far you've gone towards the completion of a project. It outlines the activities you've carried out, the tasks you've completed, and the milestones you've reached vis-à-vis your project plan. A progress report is typically written for a supervisor, colleagues, or client. You might write it on your behalf or work with your teammates to produce a team progress report. Depending on the scope and complexity of the project, you might need to give a progress report weekly or monthly, or for every 25% project milestone.
* **Policies and Procedures for Organization.** It is designed to influence and determine all major decision and actions, and all activities take place within the boundaries set by them. Policies-address important issues such as what constitutes acceptable behavior by employee. Procedure-sequence of step to be followed in consistent manner such as how organization will respond to any policy violation.

**Write a note on Substance of Technical Writing**

Organizations produce technical reports for both:

1. Internal use
2. External use **Internal use:**

Internally reports such as feasibility studies, technical notes, and memorandums go from superiors to subordinates from subordinates to superiors and between colleagues at the same level.

Company policy, tact and the need-to-know are important considerations for intracompany paperwork.

**External use:**

Externally, letters and reports of many kinds go to other companies, the government, and to the users of the company’s products. Let us cite few of many possibilities:

* A computer must prepare **instructional manuals** to accompany its computers.
* A university department prepares a **proposal** to a state government offering to provide research services.
* An architectural firm prepares **progress reports** to inform clients about the status of contracted building programs.
* An insurance company must write **letters** accepting or denying claims by its policy holders.
* Many government agencies, scientific laboratories and commercial companies make **research** their principal business.
* Universities and colleges publish books, journals articles and papers for professional societies. Many reports are prepared for public consumption.
* Myriad applications such company memos and reports, government publications, research reports, public relation releases create a great flood of paperwork.

Some of it is only for passing interest while some of it makes history. All of it is prepared by report writers and professionals, scientists, and technologist.

**Describe the nature of technical writing**

Technical writing is most certainly a specialty within the field of writing. Beginning technical writers must serve an apprenticeship. They must gain a knowledge of their subject matter and terminology. They must learn to develop a prose style that is clear, objective, and economical. They must learn report style, variations in format, standards for abbreviations, the use of tables and graphs, the kinds of people who read technical reports and their expectations.

* **No-nonsense approach**: The writing is marked by a no-nonsense approach to the subject it treats. It is single-minded and earnest. Interesting points are seldom introduced for their interest value alone; they must also be pertinent.
* **purpose of writing:** The purpose of the article or paper is usually spelled out in the opening paragraph or two. All included information bears upon the accomplishment of the stated purpose. For example, a technical paper on smoke detectors may set forth only one major objective: to determine the relative effectiveness of photoelectric and ionization chamber types in detecting smoldering fires, flaming fires, and high temperatures. Other major topics would be re-served for other papers.
* **Specialized vocabulary:** The vocabulary tends to be specialized. Some of the terms may not appear in general dictionaries. If the audience shares the writer's professional specialization, the specialized terms may not be defined within the text, on the assumption that professional colleagues will be familiar with them.

|  |  |
| --- | --- |
| **Sentences:** | |
| **Format:** |  |

* Sentences are highly specific, and fact filled.

•

* When appropriate to **the material, numbers and dimensions** are numerous. These are usually in Arabic form and are exact rather than rounded out to the nearest whole number.
* **Signs, symbols, and formulas** may pepper the prose. The terms may be listed and defined in accompanying glossaries.
* **Graphs and tables** may substitute for prose or reinforce and expand upon the surrounding prose. Figures and illustrations of all sorts are widely used, sometimes to supplement prose, sometimes to replace it.

• **Documentation and credits**: In good technical writing documentation and credits appear in notes and bibliographies.

As these listed characteristics perhaps make clear, audience analysis is tremendously important to successful technical reporting.

|  |  |
| --- | --- |
| **List the characteristics of good technical writer** | |
| **Who are Technical writers?** |  |

A Technical writer who understands topics clearly and makes a blog, documentation, online user help, user guide, and so on. With the assistance of users, the way to use products or services. In short Professional writers who take complicated technical issues and transform them into a version that’s more understandable for the commoner are referred to as technical writers.

**The Qualities Of A Good Technical Writer:**

One writer, who knew well the nature and substance of technical reporting, summed up the way to be successful with three imperative:

|  |  |  |
| --- | --- | --- |
| **(1) Know your reader** |  | |
| **(2) Know your objective** | |  |
| **(3) Be simple, direct, and concise** | | |

To write clear and effective reports, writer have to build upon the natural talents he/she has in communicating ideas to others. But how can a writer build successfully? What skills, characteristics, and attitudes are of most value to the report writer?

* **Be objective**: Try not to get emotionally attached to anything that have written; be ready to chuck any or all of it into the wastebasket. While reading own prose or that of the colleagues, does not ask whether you or they are to be pleased but whether the intended audience will be pleased, informed, satisfied, and persuaded.
* **Be professional:** As a professional, keep in mind that most of what writers do will eventually have to be presented in writing. Good writers do the work so that it will be honestly and effectively reportable. He Record what he does and learns.
* **Knowledge required:** Accurately like all other jobs, you’ll need certain things to shine at your job.

Technical Writers should be quite knowledgeable in writing.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| o | ability to analyse, evaluate, simplify and communicate technical information | | | |
| o | knowledge of the professional area they’re writing on. |
| o | ability to edit, design and plan technical documentation | |
| o | skills in information science, web publishing, and graphic design. | | |

* **Reasonably methodical**: Writers must be reasonably methodical and painstaking. Plan work for the day and for the rest of the week. Look up from time to time to take stock of what he and the others are doing, so that he does not squander his time and energy on minor tasks that should be put off or dispensed with altogether. File his correspondence. Keep at desk the supplies needed to do the work. Keep a clear head about ways and means for accomplishing the purpose.
* **Clarity:** Good writers Remind themselves frequently that clarity is the most important attribute. Until the sense of a piece of writing is made indisputably clear, until the intended reader can understand it, nothing else can profitably be done with it.
* **Understanding the Topic:** A Technical writer possesses to be extremely attentive and alert in putting down the words. Content should be highly explicit and informative. content chosen by a Technical writer isn’t for entertainment purposes, therefore one has got to make content in such how that the reader doesn’t have any problem in understanding and gets to understand the content during a pretty simple and transparent language. A Technical writer has got to keep this in mind because this is often one among the talents and qualities of a Technical writer.
* **Critical thinking:** Critical thinking is the objective analysis and evaluation of an issue in order to form a judgement. Critical thinking skills are intimately connected to how glorious we address. Writing may be a big puzzle and it’s up to you as writers to work out the way to put the puzzle together. The straightforward elements of the puzzle are the audience and purpose. However, beyond these aspects, the weather that structure the particular document which determine whether the reader will understand or not.
* **Analytical Skills:** Must be able to identify and define problems, extract key information from data and develop workable solutions for the problems identified in order to test and verify the cause of the problem and develop solutions to resolve the problems identified. Analytical skills are important because it allows you to seek out solutions to common problems while you write and make decisions about what actions to require next.

|  |  |
| --- | --- |
| **Describe the qualities of good technical writing** | |
| **The Qualities of a Good Report** |  |

Good report writers turn out good reports. Because the qualities of good reports vary from report to report, depending upon audience and objective. The good report is free from typo graphical errors, grammatical slips, and misspelled words. Little flaws distract attention from the writer's main points. The good report:

* Arrives by the date it is due.
* Makes a good impression when it is picked up, handled, and
* flipped through.
* Has the necessary preliminary or front matter to characterize the
* report and disclose its purpose and scope.
* Has a body that provides essential information and that is written
* clearly without jargon or padding.
* When they are needed, has a summary, or set of conclusions to
* reveal the results obtained.
* Has been so designed that it can be read selectively: for instance, by some users, only the abstract; by other users, only the intro-duction and conclusions; by still other users, the entire report.
* Has a rational and readily discernible plan, such as may be revealed by the table of contents and a series of headings through-out the report.
* Reads coherently and cumulatively from beginning to end.
* Answers readers' questions as these questions arise in their minds.
* Conveys an overall impression of authority, thoroughness, soundness, and honest work.

|  |  |
| --- | --- |
| **Differentiate technical writing from other forms of writing** | |
| **They write to educate.** |  |

An author, and even a journalist, might seek to entertain or even persuade an audience. But a technical writer's work exists solely to inform the reader about a specific product. Everything a technical writer creates on the job is about factual, statistically-based or usability-based information. Personal opinions, or even comparisons to other products on the market, are not included in technical writing.

**They write without emotion.**

Technical writing is strictly objective. The technical writer is not employed to share emotions or opinions. They present facts in clear, detailed and non-dramatic ways.

**Chapter 2: Fundamentals of Technical Writing**

* 1. **Compose good technical report**
  2. **Identify the topic and purpose of a technical writing**
  3. **Draft and revise technical report**
  4. **Use fundamentals of technical writing to write good report**
  5. **Plan a technical writing with several writers**
  6. **Identify different readers of technical writers**
  7. **Search literature for topics in technical writing**
  8. **Write letter of inquiry**
  9. **Write report with list and tables**
  10. **Compose technical report that is grammatically correct and readable**

**What are Fundamentals of Technical Writing?**

**Fundamentals of technical writing are as follows:**

* **Composing:** prewriting, drafting and revision of technical writing.
* **Cooperative Writing:** Plan technical writing with several writers.
* **Readers of Technical Writing:** identify readers of technical writing
* **Collecting and Verifying Information:** search literature and write letters of inquiry.
* **Readable Style:** Write skimmable report with lists and tables.

**What is composing? How is a good technical report composed?**

Composing is a process of planning and writing. For most skilled and experienced writers, the composing process breaks u p roughly into three parts.

|  |  |
| --- | --- |
| **Prewriting:** | Writers |
| **Writing and Revising:** | |

1. think about audience, topic, and the purpose of writing.
2. Writers create a draft and focus on different issues like logic, completeness, style, and visuals of writing.
3. **Editing:** Writers edit the final work to satisfy the requirements of good format.

Time spent on these parts is not usually equal. Prewriting fora complicated piece of work may take 80 per cent or more of the time you have for the project. For an easy piece of routine writing, prewriting may take a few minutes, and writing may take up the bulk of the time. Some situations call for careful, scrupulous editing; others do not.The process is often not linear. If the writing bogs down, you may have to return to the prewriting stage to resolve the problem. Writing and revising may alternate as you write for a while, then stop to read and revise. **Prewriting:**

The first part is often called prewriting. Prewriting is a thought process where writers think about the readers and purpose of writing It's that time when you're trying to bring a thought from nowhere to somewhere. It's a time when you think about such things as:

* + Your Audience
  + Your Topic
  + Your Purpose

In prewriting, you “invent" or "discover" the material you need to satisfy your purpose and your audience. That discovery process may go on completely within the trillion cells of your brain or, as is often the case in technical writing, in libraries, laboratories, and workplaces as well. When the discovery stage is about complete, you pass into a stage where you arrange your material. That is, before writing a draft you may rough out a plan for it or even a complete outline.

# Writing And Revising

With your arrangement in hand, you are ready for the second part of the composing process, the writing and revising of your document. In this stage you come to the actual writing of your paper. We do not try to convince you that writing is an easy mechanical job. It is not. But we do give you suggestions that should make a tough job easier. During the formal revision process, you will want to revise from different perspectives. You may want to revise several times and focus on different issues like logic, completeness, style and visuals of your writing. **Editing:**

In the third part of the writing process, you edit your work to satisfy the requirements of standard English and to meet the requirements of good format. Editing is a critical writing requirement. In complex reports, you will want to perform several “edits”: one for mechanics—spelling, usage, punctuation, sentence structure. Editing is a critical writing requirement. In complex reports, you will want to perform several “edits”: one for mechanics—spelling, usage, punctuation, sentence structure. When your word processing program, usually a green line under a sentence or phrase—suggests that there’s a problem with your sentence, stop and check the sentence carefully. Another edit focuses on citing sources: Check your documentation to be sure that you give credit or sources of all information you have used. Be sure that when you use graphics and ideas from other sources you give credit to the source. A third edit focuses on the document as a whole: How does it look? How does it sound? Is the important information easy to locate? Is the document complete? In short, don’t try to check for every error at once, in one reading. Editing requires care, objective reading, and diligence.

|  |  |
| --- | --- |
| **What is cooperative writing?** | |
| Collaborative writing involves two or more persons working together to produce a written document. | Also |

called group writing, it is a significant component of work in the business world, and many forms of business writing and technical writing depend on the efforts of collaborative writing teams. Members can work in spaces that are face-to-face or virtual.

Collaboration involves a mindset that sees the whole as more important than its parts. In other words, when people decide to collaborate, they are deciding to set aside their individual goals for the good of the group or company they represent. Collaboration seeks to combine multiple skill sets, knowledge bases, ideas and engagement from a number of people for the sole purpose of accomplishing a goal that benefits all – regardless of position or title.

**Who are the readers of technical writing?**

In technical writing, your audience is often going to fit into one of the following categories:

1. Executives: Those who are funding the product.
2. Experts: Those who are coming up with ideas about the product.
3. Technicians: Those who are building the product.
4. Non-specialists: The end-user.

**What sources can be used for collection of data in technical report?**

Information gathering, whether in the library or elsewhere, is usually an important part of any major writing project. In addition to information-gathering methods, you will need some techniques for checking and reviewing your information as you gather it, both to stay on course and to correct your course as necessary. The methods and techniques you may use include but are not limited to the following:

* Searching the Literature
* Inspecting Local Sites and Facilities
* Preparing and Administering a Questionnaire
* Checking Readers' Attitudes and Requirements
* Interviews
* Letters of Inquiry
* Performing Calculations and Analyses
* Reviewing the Information Already Gathered

**What is a letter of inquiry and what is its purpose?**

A letter of enquiry is a letter written to enquire about something that you want to know. When writing a letter of enquiry, make sure to mention a list of all the details you would want to gather about the product you would like to purchase or the service you would like to avail. Inquiries can be sent as a formal business letter (outside of your company) or as an e-mail. Before sending your inquiry, you should be certain that the information is not available through other means, such as the company website. **How lists and table of content help a reader in technical report?**

A table of contents is a list of the main subject headings and subheadings of the document. Hence, a table of contents not only **helps readers find materials in the report but also outlines the topics of the report**.

The table of contents is often prepared from the document's outline.

Lists, when used correctly, can be a technical writer's—and reader's—best friend. Lists allow you to emphasize important ideas. They also increase the readability of text by simplifying long sentences or paragraphs and adding aesthetic passive space to make reading more pleasant. **Why determining a purpose is important in writing a technical report?**

It’s impossible to think of a piece of written communication without a purpose. You should be clear about what you want to achieve with a piece of written communication or a publication before you can think about design or the nature of your content. Unfocused publications don’t communicate effectively, just as unclear, disorganized, or poorly supported arguments are far less likely to persuade a reader.

|  |
| --- |
| **Why knowing your readers is important in writing a technical report?** |
| Knowing your audience is also critical in technical writing. If your content isn't catered to the right audience, |

your readers may be turned off by your copy. They may not understand the critical information you're trying to convey.

Your audience is your intended reader, or who you’re writing for. In technical writing, your audience is often going to fit into one of the following categories:

* Executives: Those who are funding the product
* Experts: Those who are coming up with ideas about the product
* Technicians: Those who are building the product
* Non-specialists: The end-user

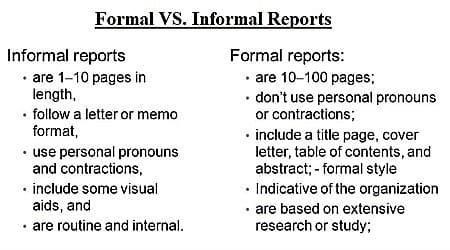
Your document’s goal typically determines its audience. For instance, if you’re writing for funding, your audience is going to be executives. If you’re writing an instruction manual, your audience is going to be the end-user of the product. This is important because the way you write your document is determined by the scope of your audience.

**Chapter 3: Techniques to Technical Writing**

* 1. Write readable report that informs
  2. Use visual language, analogy, and process description to write technical report
  3. Write readable report that define and describe
  4. Write readable report that describe a process
  5. Write readable and persuasive report that argue
  6. Compose technical writing that persuade

**What is difference between formal and informal report?**

Reports are categorised according to their purpose and readership. The most simple division is 'informal' and 'formal'. The essential difference between the two types is that **the formal or complex reports require some kind of investigation and research, whereas the informal one does not**.



|  |  |
| --- | --- |
| **What are the techniques of technical writing?** | |
| Following are the four techniques of technical writing: |  |

1. Informing
2. Defining
3. Describing
4. Arguing

|  |  |
| --- | --- |
| **What is informing in technical writing? How do you write a report that informs?** | |
| Writing to Inform means you are **communicating factual details about particular topics**. Examples |  |
| include newspaper articles, reference books, textbooks, instruction manuals and informative web sites such | |
| as government or non-profit sites. Techniques that are useful when your primary purpose is to inform: |  |

1. **chronological arrangement:**

**Chronological order** is listing, describing, or discussing when events happened as they relate to time. Basically, it is like looking at a timeline to view what occurred first and what happened after that. Let's say that you are asked to create a document showing the past changes and new ideas for a popular toy. A chronological pattern would allow you to explain what the toy looked like when it was first created, what it currently looks like, and what suggestions you would have to improve the toy in the future.

1. **Topical arrangement:**

A topical pattern arranges information according to different sub-topics within a larger topic, or the "types" of things that fall within a larger category. Using this pattern, each "type" represents a main section of information. For example, if your speech is on trees, you might talk about oak trees, pine trees, and birch trees. You would describe the specific characteristics of one tree, then move on to your description of the next tree.

1. **Exemplification:**

Exemplification means to provide examples about something. In this type of essay, examples act as supporting material to explain or clarify a generalization. The key to a good exemplification essay is to use enough detailed and specific examples to get the point. Exemplification writing uses specific, vivid examples for the purpose of adding more information to explain, persuade, define, or illustrate a general idea

## 4. analogy

|  |  |
| --- | --- |
| Analogy is a literary device that compares seemingly unrelated things to one another. For example, a | |
| common analogy used in middle school biology is “Mitochondria are the battery of the cell.” |  |

When a biology teacher calls mitochondria a battery, they are not giving a figurative description of microscopic Duracells scattered throughout the human body. They are conveying a message about mitochondria’s function: they power the cell the same way a battery powers a cell phone. Similes and metaphors also use comparison to vividly express an idea.

**5. Classification and Division.**

Classification is taking the items and putting them into different categories. Division essays identify the parts or subsystems of something in relation to the whole. Description or narration can be used to illustrate those parts or subsystems after the parts or subsystems have been defined and related to the whole.

|  |  |
| --- | --- |
| **What is technique of defining in technical writing?** | |
| You should define any term that you feel is not in your reader's normal vocabulary. The less expert your | |
| audience, the more you will need to define. | Definitions range in length from a single word to long essays or |

even books. Sometimes, but not usually, a synonym inserted into your sentence will do. You might write, "The oil sump, that is, the oil reservoir, is located in the lower portion of the engine crankcase." Synonym definition serves only when a common interchangeable word exists for some bit of technical vocabulary you wish to use.

Most often you will want to use at least a one-sentence definition containing the elements of a logical definition To make sure you are understood, you will often want to extend a definition beyond a single sentence. The most common techniques for extending a definition are description and example.

**What is description in technical writing?**

In technical writing you will chiefly have to describe three things: places, mechanisms, and processes. After explaining some preliminary concepts of description, we deal with the three. So, there are three types of descriptions:

**1. Place description:**

Writers of technical material must often describe places. Place descriptions appear in research reports when the location of the experiment has some bearing on the research. Highway engineers must describe the locations of projected highways. Surveyors have to de-scribe the boundaries of parcels of property. Police officers have to describe the scene of an accident. When describing a place, you must be aware of your point of view—that is, where you are positioned to view the place being described. When describing a place, if you, in your mind's eye, position yourself physically before you begin to write, you'll avoid confusing and annoying your readers with an inconsistent jumping about in your description. You can shift your point of view as our archaeologist has done but be aware when you are making the shift. Have a good reason for doing it, and don't do it too often. Most often the reason will be to allow yourself to give an overview and then proceed to a close-up of selected details. That is evident in the fore-going passage.

### 2. Mechanism Description

The physical description of some mechanism is perhaps the most common kind of technical description. It is a commonplace procedure with little mystery attached to it. For example, we see a friend having little success struggling to unplug a clogged sink drain by using a plunger. Professionals frequently describe mechanisms for reasons of technology transfer. Technology transfer is a rather fancy term fora common but important part of the technical and scientific life. Technical people exchange concepts through their technical journals. Sometimes the transfer is from one discipline to another. Very often the concept described concerns a mechanism. Consider these questions about the mechanism:

What are the purpose and function of the mechanism? How can the mechanism be divided?

* What are the purpose and function of the parts?
* How do the parts work together?
* How can the parts be divided? Is it necessary to do so?
* What are the purpose and function of the subparts?
* How do the parts and subparts work together?

**Impact of IT on business**

# IT Improvements:

**Off the shelf Systems:**

* One major benefit of the IT development in the opportunity to buy off-the-shelf systems that support many business requirements
* Off the shelf software are standardised software applications that are mass-produced, available to the general public, and fit for immediate use.

**Integrated Systems:**

* Integrated system, such as customer relationship and management information systems, provide access to a range of information that would be previously be stored on paper.

**Databases:**

Databases are simpler to use and provide filtered information in report or graphical format, which are easier to interpret.

**Communication Technologies:**

* To improve efficiency, businesses can increase their network, or incorporate a range of communication technologies for staff on the move, around the globe.

**Web Presence:**

* Wb presence is visibility through a website; promoting a product, service, company or individual(s) by featuring their presence on the internet.
* Smaller businesses, particularly a small trade such as a plumber or electrician, might wish to explore having a web presence to promote their business more widely during tough, economic times.

**Management Reports:**

* Businesses of any size will require management reports which can be more easily and remotely produced using technologies.
* By logging all business transactions, generating reports is not only simple, but also provides a more efficient approach to business practice.
* For example, a business using an accounting package can generate standard report such as expenditure, cash flow and income.

**What is cyber crime**

Cybercrime is a crime in which a computer is used for the. crime like hacking, spamming, phishing etc.

Cybercriminals use internet and computer technology to. hack user's personal computers, smartphone data, personal. details from social media, business secrets, national.

**What cybercrime law protects?**

Cybercrime law identifies standards of acceptable behaviour for information and communication technology (ICT) users; establishes socio-legal sanctions for cybercrime; protects ICT users, in general, and mitigates and/or prevents harm to people, data, systems, services, and infrastructure, in particular; protects human

**What is the best Defence against cyber crime?**

* Back up your data. ...
* Secure your devices and network. ...
* Encrypt important information. ...
* Ensure you use multi-factor authentication (MFA) ...
* Manage passphrases. ...
* Monitor use of computer equipment and systems. ...
* Put policies in place to guide your staff. ...
* Train your staff to be safe online.

**What are the Top 5 cyber crimes?**

Here are 5 of the top cybercrimes affecting businesses and individuals in 2020:

* Phishing Scams. ...
* Website Spoofing. ...
* Ransomware. ...
* Malware. ...
* IOT Hacking.

**What are the rules of cyber crime?**

In Simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the respective Penal Code.

**Why is it important to prevent cybercrime?**

Cybersecurity is important because it protects all categories of data from theft and damage. ... Without a cybersecurity program, your organization cannot defend itself against data breach campaigns, which makes it an irresistible target for cybercriminals.

**What causes cyber crime?**

* Operating systems are programmed by developers who are humans, thereby, making the codes vulnerable to errors. ...
* They can slip in through these loopholes and make the operating system malicious for the users. The complex coding can often become the common cause of cybercrimes.

**Impact of Development in IT:**

* Developments in IT have had a major impact on the way organizations operate. Few organizations in the developed world are able to survive in a competitive market without utilizing IT in some way.
* New technologies are being developed all the time and organizations are often compelled to upgrade their computer systems if only to keep up with the competition.
* To cope with the challenges facing organisations and to monitor the effectiveness of the IT system, an organisation should implement a technical infrastructure.

**Cost:**

Organizations looking to upgrade their systems will have to consider the cost. Most organizations will have a budget and the desire to upgrade may be outweighed by the amount of money they are able to spend. Some organizations might take the view that they will make cut-backs in other areas of their organizational budget in order to upgrade their systems or invest in more technology.

Managers are likely to carry out a cost-benefit analysis to justify any additional spending. As mentioned earlier, the use of technology could benefit an organization by increasing profitability, but it might also result in redundancies. They also have to consider costs that are indirectly associated with the increase or upgrading of technology, such as upskilling staff.

**Impact on procedures:**

* All organisations require sound and robust procedures in order to function efficiently. Some businesses use external companies to validate their quality procedures and systems. When ways of working change, or the tools and in this case the computer systems and associated software change, procedures need adjusting to accommodate that change.
* All change is challenging to manage. One factor that makes coping with change difficult is the time it takes to put new procedures or staff into place.
* This also has a cost implication, for example a receptionist in a doctor's surgery who has been used to keeping a paper appointments book is likely to have a fairly simple, although not foolproof, system for making changes to appointments. With the introduction of an electronic system the basic procedure will no longer be effective.

**Dealing with redundancies**

* **﻿**Changes to the ways in which an organization operates impact on the number of staff it requires or can afford. Organizations must deal with redundant skills and employees in order to avoid unnecessary costs. For example, if an organization is considering moving towards apaper-less office or outsourcing some of its services, it needs to think carefully about the job role (not the person) being made redundant and whether the salary saved benefits the business sufficiently.
* The organization will have to balance different considerations in order to decide which roles to make redundant. In addition, there are the overhead costs to consider such as office space, resources and possibly company cars. The organization might benefit financially from making a director redundant, but also risks losing expertise. The organization also needs to consider any redundancy payment it will have to offer - the size of this will depend on the length of time the employee has been with the organization and also the size of their current salary.
* Some organizations ask for volunteers to take redundancy.

**Impact on staff:**

* ﻿The fast pace of change brought about by developments in IT requires organizations to recognize the need for upskilling and training the workforce. Specialist skills are needed to use IT, for example the company may need someone who can use Dreamweaver to design web pages. ﻿
* Fewer organizations employ secretaries today and so staff and managers are increasingly expected to be administrators in addition to their main job role, for example sales representative, marketing manager, financial director. This will mean that they will need IT skills in using administrative software, such as word processing and spreadsheets. However, the cost of managers carrying out their own administrative tasks may be greater to the organization per hour than that of employing administrative staff.
* It is highly unlikely that the workforce (staff and managers) can simply 'pick up and run' with the introduction of new systems, software and even apparently basic or simple devices. Staff might be moved into jobs they do not particularly want and they might not have the necessary skills to carry out their new jobs efficiently and effectively straight away. There may be resistance from staff. Not everyone adapts to change easily.

**Balancing core employees with contractors and outsourced staff:**

* When considering staff reductions, changes to job roles and outsourcing of services, a strategy is needed before making any change to the staffing structure. For example, if all the sales staff are made redundant, who will sell the company's products? Devising a suitable strategy will create a delay and therefore has a cost implication.
* Consideration of the balance of core employees (those who are employed by the company as a minimum for the organization to operate effectively) against those who are contracted or outsourced is important.
* Core employees are permanently employed by the organization and receive a regular salary. They are an ongoing cost to the organization. Contractors (those who are outsourced) are not on the payroll and therefore are not an ongoing cost (although are likely to cost more per hour). Outsourced staff might include those on temporary contracts - these could be long- term contracts, but are not permanent. These staff will not be subject to the same terms and conditions as those on permanent contracts and are likely to be less cost-effective.

**Information Technology’s Impact on Business Operations:**

* **Accounting** - provides quantitative information about the finances of the business including recording, measuring, and describing financial information.
* **Finance** - deals with the strategic financial issues associated with increasing the value of the business, while observing applicable laws and social responsibilities.
* **Human resources** - includes the policies, plans, and procedures for the effective management of employees (human resources).
* **Sales** - the function of selling a good or service and focuses on increasing customer sales, which increases company revenues.
* **Marketing** - the process associated with promoting the sale of goods or services. The marketing department supports the sales department by creating promotions that help sell the company’s products.
* **Operations management** - includes the methods, tasks, and techniques organizations use to produce goods and services. Transportation (also called logistics) is part of operations management

**INFORMATION TECHNOLOGY BASICS:**

* For an organization to succeed, every department or functional area must work together sharing common information.
* Information technology can enable departments to more efficiently and effectively perform their business operations.
* Information Technology affects the accuracy of business operations.
* I.T. also allows companies to communicate easily regardless of distance
* ***Information technology (IT)*** – a field concerned with the use of technology in managing and processing information
* Information technology is an important *enabler* of business success and innovation.
* When beginning to learn about information technology it is important to understand the following:
  + Data, information, and business intelligence
  + IT resources
  + IT cultures

**ADVANTAGES OF TECHNOLOGY TO BUSINESS:**

* Customer Relations
* Business Operations
* Corporate Culture
* Security
* Research Opportunities
* Corporate Reports
* Industrial Productivity
* Business Mobility
* Research Capacity

**Interrupts:**

* Embedded systems often perform some tasks which are infrequent and possibly unpredictable
  + Hang up a VOIP phone when receiver is dropped
  + Apply brakes when brake pedal is pressed
* Regular tasks must be temporarily stopped to deal with the event
* Interrupts are the unusual events
* Interrupt handlers, or interrupt service routines, are programs which perform necessary tasks
* Interrupt can be invoked at any time
* Regular code must stop for a while

**Saving and Restoring Context;**

* Interrupt should not interfere with normal tasks
* Need to **save all used registers** at the beginning and **restore them at the end**
* Stack is typically used for temporary storage
  + Last in, first out (LIFO)
  + push, pop

**Disabling Interrupts:**

* Some events should be ignored completely
* Some tasks are **time-critical** and should not be interrupted
  + X-ray emitter in radiation therapy
* Interrupts can be disabled (usually by setting a register)
* **Nonmaskable** interrupt cannot be disabled
  + For critical events (like loss of power)

**Interrupt Vectors:**

* **Interrupt vector** is a pointer to an interrupt in memory
* Interrupt number is used to index the table
* **Interrupt vector table** holds pointers to all interrupts
* Table location may be fixed or placed in a known register

**Interrupt Latency:**

**Contributing Factors:**

1. Maximum length of time when interrupts are disabled
2. Time required to execute higher priority interrupts
3. Time between interrupt event and running interrupt code
4. Time required to complete ISR code execution

**Reducing Interrupt Latency:**

* **Make interrupt code short**
  + Reduces ISR execution time and time for higher priority interrupts
* **Reduce time during which interrupts are disabled**
  + Minimize size of critical regions

**Enabling/Disabling Interrupts:**

* ATmega contains a status register called **SREG**
* Bit 7 of SREG , the **I bit**, is the **Global Interrupt Enable**
* Clearing I bit disables interrupts, setting I bit enables them
* I bit is automatically cleared when an interrupt starts, set when interrupt is done
  + Interrupts are not interrupted
* Use the **SEI()** and **CLI()** macros to set and clear in C

**ATmega Timers:**

* ATmega 2560 has 6 timers, 2 8-bit and 4 16-bit
* Detailed descriptions found in the datasheet
* Timers can be used to **generate interrupts**
* Can be used to generate **pulse width modulated (PWM)** signals
  + PWM good for controlling motors (fake analog output)
  + We won't look at these functions

**General Timer Control:** **Need to control:**

**1. Start point of the timer (initial value)**

**2. “End” point of the timer (when the interrupt is generated)**

**- May be just overflow event**

**3. Clock rate timer receives, to increase/decrease count speed**

**- Typically uses a prescalar**

**- Slows down clock by dividing down with another counter**

**Timer0 Operation:**

* Timer0 is an 8-bit counter
* Can count from 0 to 255
* Timer0 increments every clock cycle (by default)
* Overflow event occurs when after counter reaches 255
* Counter is then reset to 0 (by default)

# IT Recent Development in Business Organization:

**Digital assistants:**

* Digital assistants are various types of software that are capable of performing rule-based work processes and communicating with people through writing and speech. The digital assistants are represented by technologies such as the Robotics Process Automation (RPA) and voice assistants. These assistants are new digital colleagues that will help the organisations of the future meet the demands for productivity and accessibility, as well as supporting the shift from “doing-jobs” to activities that add value for analogue employees.
* Digital assistants are a good solution for businesses that want to increase accessibility and quality, as well as improve response times in relation to their customers or employees.

**Internet of things:**

* The Internet of Things (IoT) comprises objects, often electronics and sensors, that are identifiable and can communicate with each other and exchange data via the Internet and cloud solutions. Third parties are also part of this network from time to time, and can offer insights and services to users. IoT objects could be anything from a sensor that monitors a pump at a manufacturing facility to the smartphone you use to unlock your car or house.
* IoT is opening the door to opportunities that entail more than just the improvement and digitalisation of individual processes. In order to succeed, businesses must be willing to develop new business and operational models around networks of connected devices.

**Artificial intelligence (AI):**

* AI (artificial intelligence) is a broad term that refers to a computer program’s or computer’s ability to appear intelligent. AI usually has the ability to capture data about its environment and can learn or adapt in order to achieve a given goal. In order to build an AI system that adds value, large volumes of data and an algorithm are used that are suitable for what the system is intended to achieve. After consuming the data, the system can make decisions based on the knowledge it has built up.
* In order to benefit from AI, it is necessary to have a clear strategy and plan regarding how data can be captured and utilised, serving as a basis for improved decisions, greater insight and optimisation of business processes.

**Blockchain:**

* A blockchain is a distributed transactional database in which all the parties are always in possession of the same information about the transactions. It is not possible to change information in the database unless the majority of participants agree that the change complies with the rules defined for a transaction to be approved. A blockchain therefore makes it possible to carry out transactions securely between multiple parties without the need for the transaction to be verified by a third party (such as a bank). Blockchains establish trust between the parties in a network who will be interacting.
* It is not known when blockchains will have a serious impact on the business world, but there is little doubt that the technology has the potential to play a central role in relation to value creation and innovation.

**3D printing:**

* 3D printing is a digitally-operated manufacturing technology in which physical objects are printed by a 3D printer based on the specification of a digital 3D model. The manufacturing process is additive, which means that an object is produced layer by layer rather than milling or turning a larger object down to the desired shape. Production using a 3D printer is carried out by allowing an object to be printed in successive horizontal layers of materials such as plastic or metal until the object has been fully produced. Each of these layers can be viewed as a thinly cut horizontal cross-section of the object being produced.
* 3D printing uses fast and precise machinery that prints complex three-dimensional objects with a high level of quality.

**Drones:**

* A drone is an unmanned aircraft that can fly (or dive) autonomously using software or be remotely controlled by people. For example, drones can be used for searching, surveillance and transportation. Several Norwegian companies are contributing on the front line in the development and commercialisation of drone technology, and the Norwegian Government has drawn up its own drone strategy to establish good framework conditions for the use of drones and growth in the drone sector.
* Businesses are investing in drone technology in order to explore how the technology is contributing to increased efficiency in operational processes, as well as access to new and improved data.

**Robotics and automation:**

* Automation of physical work duties is a growing trend within several sectors. This means that physical robots and machines are increasingly taking over work duties previously carried out by human employees. At present, this development has come furthest within processes associated with warehousing, logistics and surveillance, but it is also moving into a number of other sectors.
* Physical automation of work processes improves quality and increases uptime in processes, while freeing up human resources to work with other tasks that add value.

# Need Analysis of Hardware Upgrade in an Organization

**Increased Security:**

* Older systems are more at risk to hackers or viruses as they have been around longer and their security vulnerabilities have been exposed. New systems are typically more secure.
* It’s important to update your hardware. Software developers and designers are consistently upgrading software to prevent hacking but if the hardware is too old for the new update or version, your security is still at risk.

**Reduced Costs:**

Older hardware is more expensive to maintain than to replace. When hardware or software fails, it can overload the IT department or IT professionals and stall productivity. This can lead to additional pay for overtime hours or expensive repair bills

**Increased Productivity:**

* Newer hardware is more streamlined, has less load time and are often easier to use.
* Faster hardware devices can increase employee productivity and can also increase employee morale.
* Many employees want to learn newer hardware as a sign the company is committed to making their jobs easier and to helping them succeed.
* Investing in newer technology is an excellent way to show your employees you are investing in them.

**Increased Productivity:**

* It’s important to pay attention to the efficiency of your hardware.
* Paying attention to when items need to be repaired, refreshed or upgraded will save you money, keep your data safe and increase productivity among your staff.
* An IT consultant or your IT department can help you monitor the effectiveness of your IT software and hardware.

# Need Analysis of Software Upgrade in an Organization:

**What is software upgradation?**

Installation of new version of the Software that includes new and/or different features from the previous version.

# Software Update vs Upgrade:

**Software Update:**

* Software updates are a way for software developers to fine-tune a product to make it the best.
* Updates sometimes run automatically in the background. Other times, software updates (commonly referred to as ‘patches’) come in the form of a free download. They’re usually necessary for your product to continue running successfully.

**Software Upgrade:**

* Software upgrade is a new version of the software product entirely.
* Software upgrade, then, supersedes the old product.
* Software upgrade is less common than an update

**Why Software Upgradation?**

There are several factors that influence organisations to upgrade their systems, such as:

* Performance
* Efficiency
* Cost
* Time

**Advantages:**

* Job creation
* Business Development
* Customer Relation
* Globalization

# To set up remote environment:

**What is remote working style?**

* Remote work is a working style that allows professionals to work outside of a traditional office environment.
* Instead of commuting to an office each day to work from a designated desk, remote employees can execute their projects and surpass their goals wherever they please.

**The Impact Of The Remote Work Environment:**

* Work from remote location has become business as usual. Not even a year ago, working remotely was an opportunity for just a small percentage of the workforce. Then along came the Covid-19 pandemic, and that caused an instantaneous change.
* Companies in traditional office spaces were forced to send their employees home to work remotely—and many of these employees will continue to work from home, long after the pandemic is over**.**
* People won’t be commuting to their offices. Few few cars on the road. That’s good for climate change and emissions.
* Less traffic tickets, which is bad for government.
* Less gasoline usage, which is good for employees and employers but impacts oil companies. Lower gasoline sales means less tax collected, again bad for government.

**The Impact Of The Remote Work Environment:**

* Office Buildings: If people don’t have to come to an office, why lease office space? The demand for office space will drop.
* Buildings will lose tenants. Expect to see downtown properties repurposed from commercial office space into residential and other uses.
* Downtown restaurants and other businesses in commercial districts will see fewer customers.
* Tea/Coffee shops, restaurants, dhabas and local retailers dependent on the daily foot traffic will be hit hard.

# To study role of IT in modern and fully automated organization:

**Automation process:**

* Automation software handles the processes entirely on its own
* Software needs no human input to complete the tasks

**Fully Automated Organization:**

* A fully automated organization is a company that’s transformed itself. For the better.
* Automated organizations use AI to discover automation opportunities from their existing workflows, processes, and applications.

**IT Transformation – a practical reality:**

* Where automation forms the connective conduit for systems, software, and applications, enabling them to work smoothly together.
* Where personal robots step in to take on repetitive tasks, freeing people for higher-value work.

Where artificial intelligence (AI) easily brought to workflows, analyses, and decisions, delivering AI into every facet of business operations

# Understand How Organizations responds to IT developments:

**Adapting business processes:**

* With the expansion of technology globally, organizations are exploiting how technology can benefit their business
* Organizations leverage technology to enhance business operations, such as Tesco's introduction of loyalty cards in 1995, which drive sales by rewarding returning customers
* Online purchases often trigger personalized follow-up emails offering discounts, creating a sense of urgency to buy. This marketing tactic capitalizes on limited-time offers, encouraging immediate purchases. Small-time grocers and retailers face challenges competing with multinational corporations' purchasing power and sophisticated marketing strategies

**Sales and marketing strategies for global opportunities:**

* The internet facilitates swift and cost-effective global marketing, enabling sales negotiations through various channels like telephone and email, reducing travel expenses.
* Cost savings from quicker deals are often passed on to customers, enhancing competitiveness. Viral marketing incentive sharing product messages, amplifying reach online.
* Not all viral marketing campaigns are malicious-some are quite welcome and work well because they build a sense of community among recipients, who actually want to pass on the message. Viral marketing works particularly well among groups with highly developed social networks, such as teenagers.
* Organizations often collaborate with others to promote complementary products or services on their websites, benefiting both customers and businesses. Examples include camera suppliers linking to websites selling compatible printers and computer sellers directing users to purchase software or peripherals elsewhere.
* Pop-up ads, disliked by users for their intrusive nature, and shocking online advertisements exist, differing from television standards.
* Spam emails, especially post-purchase follow-ups, are frowned upon for their intrusive and often unsavory content. Specialized software aids in monitoring sales, enabling mass customization by adapting product ranges based on consumer feedback. Loyalty card data and software analysis help tailor offers, though some consumers feel uneasy about perceived surveillance and targeted marketing practices.
* Specialist software monitors sales, providing insights for masscustomization and adaptation of product ranges. Tracking individual purchases via loyalty cards enables targeted marketing efforts, guiding consumers towards additional purchases.

**Purchasing strategies for automated ordering:**

* **As a result of developments that make it easier for organizations to talk to each other through their systems, automated ordering becomes easier and quicker. One such example is the systems that large superstores use to monitor the stock on the shelves-tracking sales and using EDI for automatic reordering before stock runs out.**
* **Calculations are carried out in an attempt to avoid stocks running out at critical times based on the likelihood of products selling at peak times. An effective system calculates the optimum level of stock about storage capacity and with the least impact on cash flow.**
* **These new purchasing mechanisms are also referred to as channel management, as all the different potential channels to market are managed. Organizations decide how to sell their products and services - through catalogs, over the phone, on the Internet, etc. - choosing the method that seems to be the most effective.**

**Customer support processes for online systems:**

* New technology has revolutionized customer support, offering various channels like website queries, emails, and FAQs. However, automated telephone systems and scripted support staff can frustrate consumers with lengthy menus and scripted responses, often resulting in unresolved queries.
* Despite being cost-effective and accessible beyond regular hours, these approaches are generally unpopular with customers.

**Financial systems for secure funds transfer:**

* New technology has revolutionized customer support, offering various channels like website queries, emails, and FAQs. However, automated telephone systems and scripted support staff can frustrate consumers with lengthy menus and scripted responses, often resulting in unresolved queries.
* Despite being cost-effective and accessible beyond regular hours, these approaches are generally unpopular with customers.

**Automating manufacturing processes:**

* Over the past two decades, work dynamics have transformed significantly. The fax machine revolutionized communication in the mid-1980s, preceding advancements like networked computers and diverse software applications now ubiquitous in UK businesses.
* In manufacturing, robots have automated tedious tasks such as car building and precision processes in industries like Formula 1. Robots also tackle hazardous activities like undersea drilling and sweet manufacturing, streamlining production and packaging processes.

IT Troubleshooting

Knowledge Base System & Knowledge?

* **What is Knowledge Base System** ?

A System which is built around a knowledge base i.e collection of knowledge taken from human, store in such way that system can reason with it

* **What is Knowledge** ?

knowledge is a sort of information that People use to solve problem

**Data, Information, and Knowledge**

* Data is raw bits and pieces of information
  + Quantitative – numeric
  + Qualitative – descriptive
  + Alone is not useful
* Information is when data is given context and more specific
* Knowledge is developed when information has been aggregated and analyzed to make decisions, set policies, and spark innovation
* Wisdom is the combination of knowledge and   
  experience
  + May take years to develop

**Databases:**

* Organized collection of related information to generate knowledge for decision making purposes
  + For example, a university transcript database may contain information on students, classes taken, and grades received
* A separate university database would be created to maintain your financial information
* Relational databases (such as Microsoft Access) where data in organized into one or more tables
  + Tables are a collection of fields
    - E.g., Student ID, Course ID, Grade Earned
  + Record is an instance in the table
    - E.g., your specific information in the table

**Database Management Systems:**

* Knowledge Management (KMDatabase Management Systems (DBMS) is an application that allows data to be:
  + Entered, Modified, and Deleted
  + Read
  + Reported
* Has a user friendly interface to design the database
* Relational databases use Microsoft Access installed on one machine with one user access at a time
* Enterprise Databases serve the entire   
  organization

**Knowledge Management (KM):**

* Companies and individuals accumulate knowledge
* Not consistently written down or saved
* If recorded, not consistently organized
* KM is the process of formalizing   
  the capture, indexing, and   
  storing of knowledge

**Technical Manuals:**

A technical manual is a “how-to guide or manual” created for a single objective of making it simple for the end-user to understand the technicality of using a product or service. Technical manual contains instructions for installation, use, maintenance, and steps for effective deployment of equipment.

**Types of Technical Manuals:**

* Service manual — helps technicians and other trained people service, maintain, and repair equipment. ...
* User manual — assists people to use a particular system or device. ...
* Operation manual — provides guidance for the staff to perform their functions correctly and efficiently

**Frequently Asked Questions (FAQs):**

* The letters (or word) FAQ stands for Frequently Asked Questions. A FAQ page is usually a list of common questions people have asked about a specific product or service.
* Every business and product website comes with a set of default pages like an “About” page, “Contact” page, “Privacy Policy” page, and more. A FAQ page is one of the few must-have pages on this list.
* Think of a FAQ page as an automated customer support page or a simplified product manual. Where users can figure out answers to product-related questions all by themselves**.**

**PURPOSE OF FAQs:**

The purpose of a FAQ is generally to provide information on frequent questions or concerns; however, the format is a useful means of organizing information, and text consisting of questions and their answers may thus be called a FAQ regardless of whether the questions are actually frequently asked.

**IMPROTANCE OF FAQs:**

Frequently asked questions, or FAQs as they are known, are a great way to improve your customer's experience of your website. It allows you to answer the questions that are most commonly asked surrounding your product or service. At the same time, there are also many other benefits to having FAQs on your website

**ARE FAQS ARE GOOD?**

FAQs are a good indicator that there may be an issue with your content. Most are created because people think by bringing frequently asked questions together on a single page, they will make it easier for people to find the answers they are looking for.

**Discussion Forum:**

A meeting at which people can exchange ideas and opinions about at topic. Several well attended public discussion forums are held in the community.

**Purpose of Discussion Forum**

The purpose of discussion forum is to engage different groups of the same space together so they discuss some topic or give the opinion about some thing or provide useful information that can help other person or group and solve their problems

**Popular Discussion Forums & Websites :**

* Reddit
* Quora
* Stack Overflow
* XDA Developers
* Games Spot
* Final Thoughts

**MANUFACTURES WEB SITES:**

The manufacturing is the production of goods through the use of labour, machinery, tools and biological or chemical processing.

**Manufactures Websites**

The different manufacturing companies sell their products through internet. To achieve this goal they create website of their companies on which the information about those products is provided. This sort of online selling strategy is also called E-Commerce

**TYPES OF REMEDIES:**

**Repair or Replace Hardware**

Computer hardware repair technicians install, examine, test and repair computer hardware and peripheral components. They test computers' functionality, identify the problems and replace damaged components and parts

**Communication Paths**

Communication paths refer to the tracks of potential communications which may occur between communication objects (humans or computers

**Fixing Communication Paths**

* If you're experiencing slow or no signal, the problem may be resolved by refreshing your computer's IP address.
* Restart all Internet connections.
* Check for a temporary service interruption.

Unplug the modem, then plug it back in after some time.

**Software Remedy**

The Remedy Action Request System, also know as Remedy or ARS, is a client-server trouble ticketing application produced by BMC and used by organizations to track internal problems and customer-reported issues.

**Reconfigure Software**

A software reconfiguration pattern is a solution to a problem in component-based software systems where the configuration needs to be updated while the system is operational**Applying software Patch**

In the Patch section, click the executable link and then click Save on the File Download screen to save the executable to your server's hard drive. When the download completes, double-click the executable to launch it on the server. Click Finish once you are prompted that the update completed successfully.

**Data Backup Strategies:**

In information technology, a backup, or data backup is a copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event.

**Importance of Backup**

The main reason for a data backup is to have a secure archive of your important information, whether that's classified documents for your business or treasured photos of your family, so that you can restore your device quickly and seamlessly in the event of data loss**.**

**Data Backup Types**

**Following are three main data backup types:**

* Full Backup
* Incremental Backup
* Differential Backup

**Full Backup**

A full backup is a complete copy of a business or organization's data assets in their entirety. This process requires all files to be backed up into a single version. ... However, making a full backup demands copying a large volume of data, making this backup type a highly time-consuming process.

**Incremental Backup**

An incremental backup is **one in which successive copies of the data contain only the portion that has changed since the preceding backup copy was made**. ... Incremental backups are often desirable as they reduce storage space usage, and are quicker to perform than differential backups.

**Incremental Backup Example**

An incremental backup scenario requires one full backup and then subsequent incremental over a period of time. For example, if a full backup was performed on Monday, Tuesday's incremental will take a snapshot and back up all new or changed files since Monday's backup.

**Differential Backup**

A differential backup is a cumulative backup of all changes made since the last full backup, i.e., the differences since the last full backup. The advantage to this is the quicker recovery time, requiring only a full backup and the last differential backup to restore the entire data repository

**Difference between Incremental and Differential Backup**

The main difference between incremental and differential backups is how they save space and time by storing only changed files. However, the effectiveness of incremental backups is very different from differential backups.

**Difference between Full and Incremental Backup**

A Full Backup is a complete backup of all files on the designated hard drive. An Incremental Backup is a backup of all changed files since the last Full or Incremental backup.

**Data Recovery:**

Data recovery is the process of restoring data that has been lost, accidentally deleted, corrupted or made inaccessible. In enterprise IT, data recovery typically refers to the restoration of data to a desktop, laptop, server or external storage system from a backup

**DATA RECOVERY PROCEDURE:**

**Hard Drive Recovery**

A large percentage of data recovery services comes from hard drive failures and is increasing.

**RAID Recovery**

RAID recovery is the process of data recovery from a RAID array which failed for whatever reason, may it be a controller problem, member hard drive failure, or something else.

**Tape Recovery**

Tape recoveries are performed in dust-free cleanroom environments. Tapes and tape drives are carefully dismounted, examined and processed.

**Removable Data Recovery**

*Removable* storage media *data recovery software* is programmed for recovering lost and accidentally deleted data from all types of *removable* storage media.

**Digital Recovery**

Data recovery is **the process of accessing and recovering information from digital media that is not accessible through standard means**. This is a necessary service in a variety of situations from user error and deletion, to mechanical and physical damage on your storage device.

**Maintaining Security:**

**Virus**

A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. If this replication succeeds, the affected areas are then said to be "infected" with a computer virus, a metaphor derived from biological viruses

**Antivirus**

is a kind of software used to prevent, scan, detect and delete viruses from a computer. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.

**Types of Virus**

* **Boot Sector Virus.**
* **Web Scripting Virus**
* **Browser Hijacker**
* **Resident Virus.**
* **Direct Action Virus.**
* **Polymorphic Virus.**
* **File Infector Virus.**
* **Multipartite Virus**

Access Rights are the permissions an individual user or a computer application holds to read, write, modify, delete or otherwise access a computer file, change configurations or settings, or add or remove applications.

**The impact of organisationalpolicies on diagnosis and repair:**

This deals with making decisions about how and when to repair equipment and the impact that it can cause. We will be considering the following:

• Customer issues

• External considerations

• Organisational considerations

* The management team of an organisation is responsible for making decisions, for example about how much time is set aside for maintenance of computer systems and how many support staff are provided to help the workforce.
* There are many issues that arise within organisations that can impact on the support team: security, costs, systems downtime, disruption, resource allocation, prioritisation, contractual requirements and trend analysis.

**Out Sourcing:**

* An organisation may choose to outsource part or all of its support needs, such as the care of IT equipment.
* A service level agreement (SLA) may be set up with a third party specifying what cover is provided.
* The cost of this support will be included in the budget and will be renegotiated yearly.

**Network Management**

**. Performance management** deals with monitoring and managing the various parameters that measure the performance of the network

**2. Fault management** is the function responsible for detecting failures when they happen and isolating the failed component.

**3. Configuration management** deals with the set of functions associated with managing orderly changes in a network.

**4. Security management** includes administrative functions such as authenticating users and setting attributes such as read and write permissions on a per-user basis. From a security perspective, the network is usually partitioned into domains, both horizontally and vertically. Vertical partitioning implies that some users may be allowed to access only certain network elements and not other network elements.

**5. Accounting management** is the function responsible for billing and for developing lifetime histories of the network components. This function is the same for optical networks.

**Why Measure Network Performance**

The demands on networks are increasing every day, and the need for proper network performance measurement is more important than ever before. Effective network performance translates into improved user satisfaction, whether that be internal employee efficiencies, or customer-facing network components such as an e-commerce website, making the business rationale for performance testing and monitoring self-evident.

**Network Performance Measurement Tools**

Network performance measurement tools can be broadly categorized into two types - [passive and active](https://www.applicationperformancemanagement.org/network-monitoring/network-monitoring-tools/).

**Passive network measurement** tools monitor (or measure) existing applications on the network to gather data on performance metrics. This category of tool minimizes network disruption, since no additional traffic is introduced by the tool itself.

**Active networking performance measurement tools** generate data that can be tailored to baseline performance using pre-set routines. This testing requires an additive level of data traffic by nature, so it must be scheduled appropriately to minimize impact on existing network traffic

**Network Performance Measurement Parameters**

* **Latency**

With regards to network performance measurement, latency is simply the amount of time it takes for data to travel from one defined location to another. This parameter is sometimes referred to as [delay](http://www.techsoupforlibraries.org/planning-for-success/networking-and-security/tools/network-performance-metrics-defined). Ideally, the latency of a network is as close to zero as possible.

* **Packet Loss**

With regards to network performance measurement, packet loss refers to the number of packets transmitted from one destination to another that fail to transmit. This metric can be quantified by capturing traffic data on both ends, then identifying missing packets and/or retransmission of packets. Packet loss can be caused by [network congestion](https://www.annese.com/blog/what-causes-packet-loss), router performance and software issues, among other factors.

* **Throughput and Bandwidth**

Throughput is a metric often associated with the manufacturing industry and is most commonly defined as the amount of material or items passing through a particular system or process. A common question in the manufacturing industry is how many of product X were produced today, and did this number meet expectations. For network performance measurement, throughput is defined in terms of the amount of data or number of data packets that can be delivered in a pre-defined time frame.

* **Jitter**

Jitter is defined as the variation in time delay for the data packets sent over a network. This variable represents an identified disruption in the normal [sequencing of data packets](https://datapath.io/resources/blog/what-is-network-jitter/).

* **Latency vs Throughput**

While the concepts of throughput and bandwidth are sometimes misunderstood, the same confusion is common between the term’s latency and throughput. Although these parameters are closely related, it is important to understand the difference between the two.

* **Response time**

Response time, in the context of computer technology, is the elapsed time between an inquiry on a system and the response to that inquiry. Used as a measurement of system performance, response time may refer to service requests in a variety of technologies. Low response times may be critical to successful computing.

* **Line utilization**

"Utilization" is the percentage of a network's bandwidth that is currently being consumed by network traffic. Consistently high (>40%) utilization indicates points of network slowdown (or failure) and a need for changes or upgrades in your network infrastructure.

## Planning a network installation

**Network operations**

1. **Data Logging:**

Almost all information technology systems generate a log, which serves as a record of all the activity that the system conducted in its operation. Such logs are generated by network infrastructure devices (firewalls, switches, domain name service devices, routers, load balancers), computer platforms (servers, appliances, and smartphones), operating systems (Windows, Linux, IOS) and applications (client/server, web applications, cloud-based utilities).

The importance of managing these logs for operational and security reasons, and various tools that synthesize such logs so that functionality and security issues can be identified.

Proper maintenance of network logs is imperative to assure proper operation of the application and for forensic investigation of suspected security issues.

Maintenance of network logs consists primarily of two distinct, but complementary, activities.

**Activity 1:** Ensure the availability of the network log. Application developers typically limit the size of a log event file so that it does not end up growing to a point that its size impacts storage space availability or some other function of the application. Once a log event file hits its size limit, some applications start another file and preserve the previous files. Other applications will typically 'roll' the event logs. This means that when a new log is written, an older log is deleted, which ensures the file size doesn't exceed its maximum limit.

Activity 2: Ensure the integrity of the network log. Log files provide crucial information about how the application is performing, about attempted access to resources, and other aspects of the application's behavior. When an investigation requires performing forensics on the logs to determine the source of an application problem or a security incident, investigators must know that the log file is intact and has not been tampered with.

Security attacks against applications often include efforts by the attackers to modify log files in the application in order to hide their activity. Again, exporting logs to a dedicated log manager is a recognized way to improve the protection of the integrity of the logs.

**Format of Log Data**

The most commonly used formats for data interchange are XML and JSON. These two formats are universal because they are flexible to store numerous types of data.

XML and JSON using plain text file format, which makes it possible to open them in Notepad and easily read the log entries.

* **How important is Data Logging?**

The short answer is – it’s not just important, it is crucial. A strong data logging mechanism in place can give system administrators red flags about performance and security issues ahead of time before the entire system crashes and eventually freeze your operations.

When examining the fleet of data logs, it is possible to arrive at the cause of the issue. Armed with this useful information, it allows you to respond to issues faster and avoid serious consequential damages.

* **Why Do I Need Monitoring and Logging Tools?**
* **Resource Management:** Log data can assist in the management, maintenance, and troubleshooting of your IT systems. You can gauge system health by monitoring real-time inactivity and anomalies, identifying configuration or performance issues, and drilling down into data to perform root cause analysis on failures
* **Application Troubleshooting:** Log data can help your IT personnel investigate the details of application issues. It assists with pinpointing poor performance areas, assessing and troubleshooting application health, and diagnosing the root cause of run-time errors and installation issues.
* **Business Analytics:**  Log data can help you understand business process health, customer SLAs, revenue per hour, and transactional data like transactions per second.
* **Marketing Insights:** Marketing professionals can use log data to examine how a campaign is affecting conversions, traffic, sales, and overall visibility. Log data can also help with identifying new areas where SEO could be optimized, because log files can reveal how bots are crawling your site.

1. **Network Traffic Monitoring:**

Network traffic monitoring, or network flow monitoring, is the process by which a person or program can track what devices are connected to a network, what kinds of data the devices are accessing, and how much bandwidth each device is using.

The key objective behind network traffic monitoring is to ensure availability and smooth operations on a computer network. Network monitoring incorporates network sniffing and packet capturing techniques in monitoring a network. Network traffic monitoring generally requires reviewing each incoming and outgoing packet.

Some of the technologies that incorporate network traffic monitoring include:

* Firewalls
* Intrusion detection and prevention systems
* Network monitoring, managing and performance software
* Anti-virus/Anti-malware software

1. **Network Management Reporting:**

Network management reporting is an essential tool for network administrators. Comprehensive network management reporting provides IT teams with data to monitor their infrastructure, increase productivity and aid in decision-making. From reporting on the total number of unresolved issues, to CPU utilization, interface errors, application performance or rogue wireless activity, reports hold the key to capacity planning, network architecture validation and SLA compliance.

Your network management software should be able to collect and analyze data from all components of the network, including devices, systems and applications, and present it as cohesive reports that identify network trends; assess overall performance metrics and provide comprehensive troubleshooting solutions.

### **Consider Usage Requirements**

Determine the number of people that will be using the network to get a rough idea of the computers and peripherals it must support. Consider how users will interact with the system to define the features you will need. For example, what sort of access is required to the network (e.g. will each user have their own computer? or will several users be sharing the same computer?) Will any users need to access the network remotely (e.g. from home or other office sites)?

### **Gather Input**

Factor the needs of the various teams and departments within your organization into your network plan. Start by defining the requirements of each group and determine the relative costs of incorporating the different requirements into the network plan. This may be in terms of money or time saved.

### **Plan for the future**

Detail or factor in, to the best of your knowledge, the direction your organization is likely to take in the near future (3-5 years). As you think about expansion, identify any plans that might affect your network needs (e.g. new staff or volunteers, office expansion, remote working, or the installation of new [software](http://www.icthubknowledgebase.org.uk/index.php?id=glossary&glossary_id=68&tx_a21glossary%5Bback%5D=planningnetworkinstallation&cHash=108803ea34) packages). Doing this now will be less expensive and time-consuming than replacing an inadequate network later.

### **Decide who will manage the network**

As your network solution becomes more defined, you will need to decide whether you have the resources in-house to install and maintain it yourself or whether you require a consultant or external company to handle it.

### **Security Issues**

Ensure you build security features into your network plan to protect your organizations most important asset - its information. Common network security precautions include passwords, virus protection, an external [firewall](http://www.icthubknowledgebase.org.uk/index.php?id=glossary&glossary_id=24&tx_a21glossary%5Bback%5D=planningnetworkinstallation&cHash=fd1fb7ac45) and data encryption.

### **Other Considerations**

You may enhance the foundation of your network plan by addressing other issues that may affect the integration, use and maintenance of your network. These include:

#### **Information Management**

Consider how to manage information on your server so that users can easily find what they need. Create standardized naming conventions for files on the server and establish rules for the creation of new files and folders.

#### **Remote Access**

If some staff members travel frequently or work from locations outside your office, you may want to build remote access capabilities into your network. This can be done through remote dial-in, or securely over the [Internet](http://www.icthubknowledgebase.org.uk/index.php?id=glossary&glossary_id=34&tx_a21glossary%5Bback%5D=planningnetworkinstallation&cHash=ee11bf8017) using a [VPN](http://www.icthubknowledgebase.org.uk/index.php?id=glossary&glossary_id=83&tx_a21glossary%5Bback%5D=planningnetworkinstallation&cHash=daaacf6e74).

#### **Staff Training**

While working with a network is relatively simple, it may demand that employees adopt new habits. A training program will enable workers to take full advantage of your network's timesaving and productivity enhancing features.

## Network pre-installation checklist

This checklist of questions will help you cover the main areas when it comes to planning and installing a new or upgraded network.

### **Planning**

* How many people will use the network?
* How many users are local or on-site?
* How many users are remote or off-site and will require access to the network?
* How many on-site computers will be connected to the network?

### **Network hardware requirements**

* What other devices will your network support (e.g. back-up devices, Uninterruptible Power Supplies, Network printers, etc.)?
* Do you have enough network points for these network devices?

### **Network design**

* What network topology will you use
* Do all workstations have the correct Network interface cards (NICs) to support this technology?
* Which network operating system will you use (e.g. Windows 2000 Server, Linux, Novell etc.)?

### **Security, back-up and power**

* What security measures will you be putting in place? Virus protection, user passwords, firewalls, data encryption etc.
* Do you need to physically secure your server (e.g. lock it away in a cupboard)?
* How will you back up data on your network?

**Network Operating System**

Network Operating System is a computer operating system that facilitates to connect and communicate various autonomous computers over a network.

An Autonomous computer is an independent computer that has its own local memory, hardware, and O.S. It is self-capable to perform operations and processing for a single user. They can either run the same or different O.S.

The Network O.S. mainly runs on a powerful computer, that runs the server program. It facilitates the security and capability of managing the data, user, group, application, and other network functionalities.

The main advantage of using a network OS. is that it facilitates the sharing of resources and memory amongst the autonomous computers in the network. In other words, the Network O.S. is mainly designed to allow multiple users to share files and resources over the network.

The Network O.S. is not transparent in nature. The workstations connected in the network are aware of the multiplicity of the network devices. The Network Operating Systems can distribute their tasks and functions amongst connected nodes in the network, which enhances the system overall performance.

It can allow multiple access to the shared resources concurrently, which results in efficiency. One of the major importance of using a Network O.S. is remote access. It facilitates one workstation to connect and communicate with another workstation in a secure manner.

For providing security, it has authentication and access control functionality. The network OS. implements a lot of protocols over the network, which provides a proper implementation of the network functionalities. One drawback of Network O.S. is its tightly coupled nature in the network.

**Some examples of Network O.S.**

* Novel Netware
* Microsoft Windows server (2000, 2003, 2008,2012,2016)
* Unix,
* Linux, etc.

There are mainly two types of Network O.S., they are:

* [**Peer-to-Peer**](https://afteracademy.com/blog/what-are-peer-to-peer-networks-and-server-based-networks)
* [**Client-Server**](https://afteracademy.com/blog/what-are-peer-to-peer-networks-and-server-based-networks)

**Peer-to-Peer**

[Peer-to-Peer](https://afteracademy.com/blog/what-are-peer-to-peer-networks-and-server-based-networks) Network Operating System is an operating system in which all the nodes are functionally and operationally equal to each other. No one is superior or inferior. They all are capable to perform similar kinds of tasks.

All the nodes have their own local memory and resources. Using the Network O.S., they can connect and communicate with each other. They can also share data and resources with one another.

One node can also communicate and share data and resources with a remote node in the network by using the authentication feature of the Network O.S. The nodes are directly connected with each other in the network with the help of a switch or a hub.

***Advantages:***

1. Easy to install and setup.
2. The setup cost is low.
3. There is no requirement for any specialized software.
4. The sharing of information and resources is fast and easy.

***Disadvantages:***

1. The performance of autonomous computers may not be so good when sharing some resources.
2. There is no centralized management.
3. It is less secure.
4. It does not have backup functionalities.
5. There is no centralized storage system.

**Client-Server**

The [Client-Server](https://afteracademy.com/blog/what-are-peer-to-peer-networks-and-server-based-networks) Networking Operating System operates with a single server and multiple client computers in the network.

The Client O.S. runs on the client machine, while the Network Operating System is installed on the server machine. The server machine is a centralized hub for all the client machines. The client machines generate a request for information or some resource and forward it to the server machine.

The server machine, in turn, replies to the client machine by providing appropriate services to it in a secure manner.

The server machine is a very powerful computer, that is capable of tackling large calculations and operations. It can also have the ability to administer the whole network and its resources. It can be multiprocessing in nature, which can process multiple client requests at the same time. The Network O.S. enhances the reach of client machines by providing remote access to other nodes and resources of the network in a secure manner.

***Advantages:***

1. It has centralized control and administration.
2. It has a backup facility for lost data.
3. The shared data and resources can be accessed concurrently by multiple clients.
4. It has better reliability and performance.

***Disadvantages:***

1. The setup cost is very high.
2. There is a requirement of specialized software for client and server machines to function properly.
3. There is a need for an administrator to administer the network.
4. There may be network failure, in case of central server failure.
5. A huge amount of client requests may overload the server.

***functionalities of the Network Operating System:***

1. Data and Resource sharing
2. Performance
3. Security capabilities such as [**user authentication**](https://searchsecurity.techtarget.com/definition/user-authentication) and [**access contro**](https://searchsecurity.techtarget.com/definition/access-control)**l**
4. Robustness
5. Scalability
6. Memory management
7. Backup and web services
8. Common file system and database sharing

**Examples:**

**Novell NetWare:** Novell NetWare was one of the first network operating systems. It made possible the networking of computers running MS-DOS. NetWare used DOS to boot the server and then installed itself as an alternative operating system.

Although today Novell NetWare uses TCP/IP, its original [file transfer protocol](https://www.sciencedirect.com/topics/computer-science/file-transfer-protocol) was IPX. Novell NetWare requires a server running the server software and client software on all machines. Novell client software is included in recent Windows releases but must be purchased separately for other operating systems. Novell NetWare is the least commonly used of the major NOSs today and is the least likely to be installed in a new, small network.

**Microsoft Windows:** Current desktop releases of Windows support peer-to-peer networking. In addition, Windows server software provides a full range of network services.

**Mac OS X Server:** Like desktop versions of Windows, Mac OS X supports a variety of peer-to-peer networking services. However, if you want to use a Mac OS X server, you will need the separate server software.

**UNIX:** The many variations of the UNIX operating system incorporate TCP/IP as their networking foundation. The open source version of UNIX that is the most commonly used UNIX in small offices.

**Networking Protocols**

* **Transmission Control Protocol (TCP):** TCP is a popular communication protocol which is used for communicating over a network. It divides any message into series of packets that are sent from source to destination and there it gets reassembled at the destination.
* **Internet Protocol (IP):** IP is designed explicitly as addressing protocol. It is mostly used with TCP. The IP addresses in packets help in routing them through different nodes in a network until it reaches the destination system. TCP/IP is the most popular protocol connecting the networks.
* **User Datagram Protocol (UDP):** UDP is a substitute communication protocol to Transmission Control Protocol implemented primarily for creating loss-tolerating and low-latency linking between different applications.
* **Simple mail transport Protocol (SMTP):** SMTP is designed to send and distribute outgoing E-Mail.
* **Post office Protocol (POP):** POP is an old and very simple protocol for downloading email from an email server. POP3 uses TCP as the transport protocol on port 110.
* **IMAP (Internet Access Message Protocol)** is an email protocol that deals with managing and retrieving email messages from the receiving server.

**Difference b/w POP and IMAP?**

POP3 downloads the email from a server to a single computer, then deletes the email from the server.

On the other hand, IMAP stores the message on a server and synchronizes the message across multiple devices.

**Should you be using POP3 or IMAP?**

It depends on how you want to access your emails.

Generally speaking, IMAP is more powerful and the recommended method for receiving email if you’re working across multiple devices.

Alternatively, if you prefer to have all emails accessible offline, and if you have a designated device for email, then POP could be a suitable option.

* **File Transfer Protocol (FTP):** FTP allows users to transfer files from one machine to another. Types of files may include program files, multimedia files, text files, and documents, etc.
* **Hyper Text Transfer Protocol (HTTP):** HTTP is designed for transferring a hypertext among two or more systems. HTTP is designed on Client-server principles which allow a client system for establishing a connection with the server machine for making a request. The server acknowledges the request initiated by the client and responds accordingly.
* **Hyper Text Transfer Protocol Secure (HTTPS):**HTTPS is abbreviated as Hyper Text Transfer Protocol Secure is a standard protocol to secure the communication among two computers one using the browser and other fetching data from web server. The transferring of data is done in an encrypted format.
* **Telnet:** Telnet is use for remote login. The system which requests for connection is the local computer, and the system which accepts the connection is the remote computer.
* **NTP(Network Time Protocol)** is a network protocol used for clock synchronization between computer systems over packet switched, variable latency data networks.
* **DNS - Domain Name System** - translates network address (such as IP addresses) into terms understood by humans (such as Domain Names) and vice-versa.
* **DHCP - Dynamic Host Configuration Protocol** - can automatically assign Internet addresses to computers or users
* **What is SNMP?**

SNMP is one of the widely accepted protocols to manage and monitor network elements. Most of the professional–grade network elements come with bundled SNMP agent. These agents have to be enabled and configured to communicate with the [network monitoring tools](https://www.manageengine.com/network-monitoring/network-monitoring-tools.html) or network management system (NMS).

**SNMP basic components and their functionalities:**

**NMP Manager:**

A manager or management system is a separate entity that is responsible to communicate with the SNMP agent implemented network devices. This is typically a computer that is used to run one or more network management systems.

SNMP Manager’s key functions

* Queries agents
* Gets responses from agents
* Sets variables in agents
* Acknowledges asynchronous events from agents

**Managed Devices:**

A managed device or the network element is a part of the network that requires some form of monitoring and management e.g. routers, switches, servers, workstations, printers, UPSs, etc...

**SNMP Agent:**

The agent is a program that is packaged within the network element. Enabling the agent allows it to collect the management information database from the device locally and makes it available to the SNMP manager, when it is queried for. These agents could be standard (e.g. Net-SNMP) or specific to a vendor (e.g. HP insight agent)

SNMP agent’s key functions

* Collects management information about its local environment
* Stores and retrieves management information as defined in the MIB.
* Signals an event to the manager.
* Acts as a proxy for some non–SNMP manageable network node.

**Design considerations:**

**Scalability and Modularity**

A well-designed network should be scalable. The chosen topology should be able to accommodate projected growth. A modular approach to design converts a complex system into smaller, manageable ones, simplifies implementation and ensures that it can easily isolate a failure.

**Performance**

Three aspects to consider:

* Bandwidth and effective throughput are the most important aspects of network performance and response time.
* Media and Voice over IP applications impose additional demand on the Quality of Service guarantees that the network can provide.
* How scalable is the network, with respect to the performance requirements?

**Availability and Reliability**

* Availability and reliability require redundancy. Your network equipment must be redundant to support the redundant set of Genesys Suite components, including an HA pair of SIP Servers.
* Implement a network management system, to monitor the health of the network, ascertain operating conditions, and isolate faults. Use standard network monitoring and management tools to monitor SIP Server networks.
* Virtualization is an overall trend in IT. Your hardware platform should provide virtualization to ensure redundant and high-performance network connectivity.
* Network design should accommodate SIP Server specifics. For instance, deployment of dual NIC is required when network devices don’t support the required Quality of Service.

**Designing Security into a Network:**

* Security on top of an existing network can be expensive and difficult to implement properly.
* Separating assets of differing trust and security requirements should be an integral during design phase.
* Organization to use small numbers of network security devices, such as **firewall** and **intrusion**-**detection** **system**, to secure and monitor multiple application system.

**PERFORMANCE**

* Network are getting faster and faster, evolving from 10 megabit to 100 megabit to gigabit speeds.
* The bandwidth requirements projected for two or three year in the future. otherwise expensive replacements or upgrades may be required.
* Application and networks that low tolerance for latency, such as those supporting video and voice streaming.
* The Cisco Hierarchical Internetworking model is an extremely common design implemented in large scale network today. This model is derived from Public Switched Telephone Network (PSTN) model.

Classically, network management consists of several functions, all of which are important to the operation of the network:

**1. Performance management** deals with monitoring and managing the various parameters that measure the performance of the network

**2. Fault management** is the function responsible for detecting failures when they happen and isolating the failed component.

**3. Configuration management** deals with the set of functions associated with managing orderly changes in a network.

**4. Security management** includes administrative functions such as authenticating users and setting attributes such as read and write permissions on a per-user basis. From a security perspective, the network is usually partitioned into domains, both horizontally and vertically. Vertical partitioning implies that some users may be allowed to access only certain network elements and not other network elements.

**5. Accounting management** is the function responsible for billing and for developing lifetime histories of the network components. This function is the same for optical networks.

**Why Measure Network Performance**

The demands on networks are increasing every day, and the need for proper network performance measurement is more important than ever before. Effective network performance translates into improved user satisfaction, whether that be internal employee efficiencies, or customer-facing network components such as an e-commerce website, making the business rationale for performance testing and monitoring self-evident.

**Network Performance Measurement Tools**

Network performance measurement tools can be broadly categorized into two types - [passive and active](https://www.applicationperformancemanagement.org/network-monitoring/network-monitoring-tools/).

**Passive network measurement** tools monitor (or measure) existing applications on the network to gather data on performance metrics. This category of tool minimizes network disruption, since no additional traffic is introduced by the tool itself.

**Active networking performance measurement tools** generate data that can be tailored to baseline performance using pre-set routines. This testing requires an additive level of data traffic by nature, so it must be scheduled appropriately to minimize impact on existing network traffic

**Network Performance Measurement Parameters**

* **Latency**

With regards to network performance measurement, latency is simply the amount of time it takes for data to travel from one defined location to another. This parameter is sometimes referred to as [delay](http://www.techsoupforlibraries.org/planning-for-success/networking-and-security/tools/network-performance-metrics-defined). Ideally, the latency of a network is as close to zero as possible.

* **Packet Loss**

With regards to network performance measurement, packet loss refers to the number of packets transmitted from one destination to another that fail to transmit. This metric can be quantified by capturing traffic data on both ends, then identifying missing packets and/or retransmission of packets. Packet loss can be caused by [network congestion](https://www.annese.com/blog/what-causes-packet-loss), router performance and software issues, among other factors.

* **Throughput and Bandwidth**

Throughput is a metric often associated with the manufacturing industry and is most commonly defined as the amount of material or items passing through a particular system or process. A common question in the manufacturing industry is how many of product X were produced today, and did this number meet expectations. For network performance measurement, throughput is defined in terms of the amount of data or number of data packets that can be delivered in a pre-defined time frame.

* **Jitter**

Jitter is defined as the variation in time delay for the data packets sent over a network. This variable represents an identified disruption in the normal [sequencing of data packets](https://datapath.io/resources/blog/what-is-network-jitter/).

* **Latency vs Throughput**

While the concepts of throughput and bandwidth are sometimes misunderstood, the same confusion is common between the term’s latency and throughput. Although these parameters are closely related, it is important to understand the difference between the two.

* **Response time**

Response time, in the context of computer technology, is the elapsed time between an inquiry on a system and the response to that inquiry. Used as a measurement of system performance, response time may refer to service requests in a variety of technologies. Low response times may be critical to successful computing.

* **Line utilization**

"Utilization" is the percentage of a network's bandwidth that is currently being consumed by network traffic. Consistently high (>40%) utilization indicates points of network slowdown (or failure) and a need for changes or upgrades in your network infrastructure.

### **Consider Usage Requirements**

Determine the number of people that will be using the network to get a rough idea of the computers and peripherals it must support. Consider how users will interact with the system to define the features you will need. For example, what sort of access is required to the network (e.g. will each user have their own computer? or will several users be sharing the same computer?) Will any users need to access the network remotely (e.g. from home or other office sites)?

### **Gather Input**

Factor the needs of the various teams and departments within your organization into your network plan. Start by defining the requirements of each group and determine the relative costs of incorporating the different requirements into the network plan. This may be in terms of money or time saved.

### **Plan for the future**

Detail or factor in, to the best of your knowledge, the direction your organization is likely to take in the near future (3-5 years). As you think about expansion, identify any plans that might affect your network needs (e.g. new staff or volunteers, office expansion, remote working, or the installation of new [software](http://www.icthubknowledgebase.org.uk/index.php?id=glossary&glossary_id=68&tx_a21glossary%5Bback%5D=planningnetworkinstallation&cHash=108803ea34) packages). Doing this now will be less expensive and time-consuming than replacing an inadequate network later.

### **Decide who will manage the network**

As your network solution becomes more defined, you will need to decide whether you have the resources in-house to install and maintain it yourself or whether you require a consultant or external company to handle it.

### **Security Issues**

Ensure you build security features into your network plan to protect your organizations most important asset - its information. Common network security precautions include passwords, virus protection, an external [firewall](http://www.icthubknowledgebase.org.uk/index.php?id=glossary&glossary_id=24&tx_a21glossary%5Bback%5D=planningnetworkinstallation&cHash=fd1fb7ac45) and data encryption.

### **Other Considerations**

You may enhance the foundation of your network plan by addressing other issues that may affect the integration, use and maintenance of your network. These include:

#### **Information Management**

Consider how to manage information on your server so that users can easily find what they need. Create standardized naming conventions for files on the server and establish rules for the creation of new files and folders.

#### **Remote Access**

If some staff members travel frequently or work from locations outside your office, you may want to build remote access capabilities into your network. This can be done through remote dial-in, or securely over the [Internet](http://www.icthubknowledgebase.org.uk/index.php?id=glossary&glossary_id=34&tx_a21glossary%5Bback%5D=planningnetworkinstallation&cHash=ee11bf8017) using a [VPN](http://www.icthubknowledgebase.org.uk/index.php?id=glossary&glossary_id=83&tx_a21glossary%5Bback%5D=planningnetworkinstallation&cHash=daaacf6e74).

#### **Staff Training**

While working with a network is relatively simple, it may demand that employees adopt new habits. A training program will enable workers to take full advantage of your network's timesaving and productivity enhancing features.

## Network pre-installation checklist

This checklist of questions will help you cover the main areas when it comes to planning and installing a new or upgraded network.

### **Planning**

* How many people will use the network?
* How many users are local or on-site?
* How many users are remote or off-site and will require access to the network?
* How many on-site computers will be connected to the network?

### **Network hardware requirements**

* What other devices will your network support (e.g. back-up devices, Uninterruptible Power Supplies, Network printers, etc.)?
* Do you have enough network points for these network devices?

### **Network design**

* What network topology will you use
* Do all workstations have the correct Network interface cards (NICs) to support this technology?
* Which network operating system will you use (e.g. Windows 2000 Server, Linux, Novell etc.)?

### **Security, back-up and power**

* What security measures will you be putting in place? Virus protection, user passwords, firewalls, data encryption etc.
* Do you need to physically secure your server (e.g. lock it away in a cupboard)?
* How will you back up data on your network?

# **ISA Server (Internet Security and Acceleration Server):**

# Microsoft's ISA Server is the successor to Microsoft's Proxy Server 2.0 and is part of Microsoft's ([.NET](https://searchwindevelopment.techtarget.com/definition/NET)) support.

# ISA Server provides the two basic services of an [**enterprise**](https://searchwindowsserver.techtarget.com/definition/enterprise)[**firewall**](https://searchsecurity.techtarget.com/definition/firewall?_ga=2.15840816.723670437.1615175173-1511631273.1604386388&_gl=1*16yrab9*_ga*MTUxMTYzMTI3My4xNjA0Mzg2Mzg4*_ga_RRBYR9CGB9*MTYxNTE3NTE3My40LjEuMTYxNTE3NTgwMS4w) and a **Web proxy/**[**cache server**](https://whatis.techtarget.com/definition/cache-server). ISA Server's firewall screens all [packet](https://searchnetworking.techtarget.com/definition/packet)-level, [circuit](https://whatis.techtarget.com/definition/circuit)-level, and [application](https://searchsoftwarequality.techtarget.com/definition/application)-level traffic. The Web cache stores and serves all regularly accessed Web content in order to reduce network traffic and provide faster access to frequently-accessed Web pages. ISA Server also schedules downloads of Web page updates for non-peak times.

# ISA Server allows administrators to create policies for regulating usage based on user, group, application, destination, schedule, and content type criteria. ISA Server is designed to work with [Windows 2000](https://searchenterprisedesktop.techtarget.com/definition/Windows-2000) and later operating systems and to take advantage of Windows' [Kerberos](https://searchsecurity.techtarget.com/definition/Kerberos) security. ISA Server includes a software development kit ([SDK](https://whatis.techtarget.com/definition/software-developers-kit-SDK)).

(*Kerberos is a protocol for authenticating service requests between trusted hosts across an untrusted network, such as the internet. Kerberos is built in to all major operating systems, including Microsoft Windows, Apple OS X, FreeBSD and Linux.)*

# ISA Server comes in two editions, Standard Edition and Enterprise Edition. Standard Edition is a stand-alone server that supports up to four [processor](https://whatis.techtarget.com/definition/processor)s. Enterprise Edition is for large-scale deployments, server array support, multi-level policy, and computers with more than four processors. Licenses are based on the number of processors.

# **Installation of ISA Server**

# The easiest and least problematic way to install ISA Server 2004 is to do a "clean" install (rather than an upgrade of an ISA Server 2000 computer). If installation doesn't begin, double-click isaautorun.exe.

# If you've been running an evaluation version of ISA Server 2004, you should use the ISA backup tool to back up the configuration and then uninstall the eval version before installing the licensed copy.

# Click the links to view the release notes and setup/feature guide. Then click Install ISA Server 2004. This invokes the Setup Wizard. Go through the first pages to accept the license agreement, enter your name and organizational information, and provide the product key.

# You can choose from these setup types: Typical (this installs the main features and requires about 27 MB of disk space, exclusive of space needed for caching); Complete (this installs all features); and Custom (this lets you pick the features you want to install). You can also click the Change button to change the path location to which the ISA files will be installed.

# When you select the Custom option, by default the following features are installed: firewall services, ISA Server Management, and Advanced Logging (this allows you to log to a Microsoft data engine or MSDE database).

# You can select to optionally install the Message Screener. You can use this feature to filter spam and e-mail attachments. The IIS 5.0 or 6.0 SMTP service must be installed before you install the Message Screener.

# You'll need to define addresses on the default internal network. You can enter the IP addresses manually or click the Select Network Adapter button to use the routing table entries to determine which addresses are on the internal network. If you choose the latter, you'll see a message warning you that the routing table must be properly configured.

# The internal network contains "trusted network services" such as DNS server, DHCP servers, Active Directory Domain Controller, terminal servers, and workstations used for management. ISA Server 2004 doesn't have a local address table (LAT) as did ISA Server 2000.

# After you've defined the internal network, you can select whether to allow computers running earlier versions of the firewall client to connect (this would include the Proxy Server 2.0 Winsock Proxy and the ISA 2000 firewall client). I suggest that you update the client computers to the ISA 2004 firewall client as soon as possible for best functionality, but you might need to allow older clients to connect in the meantime.

# A big security advantage of the ISA 2004 firewall client is that the communications between the ISA Server and the firewall clients is encrypted when you update all the firewall clients to the new software.

# Before installation actually begins, the SNMP and IIS Admin services will be stopped, and the Internet Connection Firewall (ICF), Internet Connection Sharing (ICS), and RRAS NAT service will be disabled. ICF, ICS, and RRAS NAT conflict with ISA Server and cannot be used in conjunction with it.

# When you get to the Ready To Install page of the wizard, click Install, and then click Finished on the Installation Wizard Completed page. You'll need to restart the server after installation completes.

# **The default configuration:**

After your ISA Server installation is complete, the following defaults are in effect until you make changes:

* There is one default access rule (called Default Rule), which is a Deny rule that does not allow any traffic to pass through the ISA Server firewall from any network to another. This is for high security.
* The default system policies permit selected traffic to go to and from the ISA Server. These are only to allow needed services.
* There is a NAT relationship set between the internal network and the default external network.
* Caching is disabled.

Note that, by default, only local administrators will be able to make changes to policies.

# **Customizing your ISA Server configuration**

Since the ISA Server is very secure, but not very functional in its default configuration, you'll want to make some immediate changes. To do so, log on as an administrator. Open the ISA Management Console (Start | All Programs | Microsoft ISA Server | ISA Server Management).

The first thing you'll want to do is create some access rules. To provide functionality, you should create rules to allow internal network clients to access the DHCP server on the ISA Server and to allow the ISA Server to send DHCP messages to the client computers (if you've installed DHCP services on the ISA Server).

If you have a DNS server on the internal network, you should also create a rule to allow the internal DNS server to use the ISA Server for its DNS server. If you don't have a DNS server on the internal network, you need to create a rule to allow clients on the internal network to access the ISA Server's caching-only DNS server.

Next, you need to create rules to allow clients on the internal network to access Internet sites and protocols through the ISA Server. To test the ISA Server, you can create an "all open" rule to allow access to all Internet sites and protocols; but in a production environment, you'll want to limit access.

# **Assigning administrative roles:**

You can delegate administration of the ISA Server and assign different administrative roles to users or groups based on what each firewall administrator needs to be able to do. This allows for better security. There are three defined administrative levels:

* **Basic Monitoring:**These users can monitor the server but can't configure monitoring tasks, such as configuring the logs or defining alerts.
* **Extended Monitoring:** These users can monitor the server and configure all monitoring tasks.
* **Firewall Administrator:** These users can completely manage the ISA Server, create rules and policies, apply network templates, and perform all configuration tasks for firewall and caching.

You can define administrative roles by invoking the Administration Delegation Wizard. In the ISA Server Management Console, click the name of the ISA Server in the left pane. On the Tasks tab in the right pane, click Define Administrative Roles. This starts the wizard, which will walk you through the process of delegating control to users or groups. I recommend that you assign roles to groups rather than individual users

## **What is a Firewall?** A firewall is a type of cybersecurity tool that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons.

The primary goal of a firewall is to block malicious traffic requests and data packets while allowing legitimate traffic through.

## **8 Types of Firewalls:** Firewall types can be divided into several different categories based on their general structure and method of operation. Here are eight types of firewalls:

* Packet-filtering firewalls
* Circuit-level gateways
* Stateful inspection firewalls
* Application-level gateways (a.k.a. proxy firewalls)
* Next-gen firewalls
* Software firewalls
* Hardware firewalls
* Cloud firewalls

**Packet-Filtering Firewalls:** This is the oldest firewall type out there. They are designed to create checkpoints at individual routers or switches. The packet-filtering firewalls will check the data packets that try to come through, without inspecting the contents. If the information trying to come through looks suspicious, it cannot get through the network. This is a simple firewall that does not impact network performance too much.

**Circuit-Level Gateways:** Circuit-level gateways are much like packet-filtering firewalls in that they quickly and easily check and approve or deny traffic. They do it without being heavy on resources, too. Circuit-level gateways work by verifying the transmission control protocol handshake. It doesn’t check the packet directly, so there is a risk of malware getting through. These are not the best ones to protect your business.

**Stateful Inspection Firewalls:** A combination of the two firewalls above, the stateful inspection firewalls offer a higher level of protection for your business. The problem with these is that they take up more resources, which can slow down the legitimate packet transfer.

**Proxy Firewalls (Application-Level Gateways/Cloud Firewalls):** If you want firewalls that operate at the application layer to filter traffic, proxy firewalls do the job. These are cloud-based most of the time, and they establish traffic connections and examine data packets coming through. The difference between these and the stateful inspection firewalls is that the proxy firewalls can also do a more in-depth inspection to check the packet contents. The drawback to these is that they can create a [network slowdown](https://www.extnoc.com/blog/denying-the-true-cost-of-network-downtime/) because of all the extra steps – but it’s all in the name of the security for your business.

**Next-Generation Firewalls:** There’s no real insight into what makes a firewall today “next-generation” besides the time it was created. There are commonalities between these firewalls and the originals, and those include TCP handshakes and packet inspections. Next-generation firewalls also use IPS – intrusion prevention systems – to stop network attacks.

**Software Firewalls:** These are any firewalls installed on local devices. The biggest draw for these in that they can create a useful, in-depth defense path. Maintaining these on more than one device is not easy, though, so you may need more than one for each asset.

**Hardware Firewalls:** Hardware firewalls use physical appliances, and they act like a traffic router. The intercept data packets before they are connected to a network server. The weakness here is that they can be easily bypassed, which goes against your need for a firewall.

**Cloud Firewalls:** Cloud solutions are also called FaaS – firewalls as a service. They often go hand in hand with proxy firewalls, and the most significant benefit to these is that they grow with your business. They work to filter large amounts of traffic away from your company, where it’s malicious.

## **Method 1: Set Windows Automatic Metric to Combine Connections**

Windows operating system has a metric value that is assign to an IP route to indicate the cost associated with using that route. When you have multiple active Internet connections on your computer, Windows automatically computes the cost of using them and assign a metric value to each of them. Then Windows set the most cost effective connection as default and keeps other active connections for backup (fail safe) purpose.

You can manually assign this metric value. If you set this value the same for all active connections you can force Windows to use all the connections.

* Open **Control Panel**
* Go to **Network and Sharing Center** > **Change Adapter Settings**
* Double click on your active Internet connection
* Select **Internet Protocol TCP/IP Version 4**
* Click on **Properties** button.
* A new box will open. Click on **Advance** button
* Another box will come up. Uncheck **Automatic Metric**
* Type value **15** in the box labelled **Interface metric**.
* Repeat the above steps for all the active connections your have
* Disconnect all your connections
* Restart your computer and reconnect all the Internet connections

That’s it! You will have the combined the power of all your Internet connections!

**Method 2: Use Bridge Connections Feature of Windows**

Windows also provides a feature of bridging connections. To use this feature, you have to have at least two active LAN/WAN connections on your computer.

* Open **Control Panel**
* Go to **Network and Sharing Center**
* Here you will see all the available active Internet connection
* Select all the active connection (use **CTRL+Click** to select multiple connections)
* Right click on one of the selected connections and choose **Bridge Connections**
* A network bridge will be created and thus your selected Internet connections will be combined.

## **Method 3: Combine Internet Connections With Load Balancing Router**

Several load balancing routers are available in the market. When you search for it in Google, TL-R480T+ comes as the first choice. There are routers from better known companies like Cisco as well. But load balancing router from TP-Link is cheapest and could be affordable by individuals and small businesses.

This router providers 4 WAN ports where you can plug in up to four wired connections. This piece of hardware comes with built-in advanced algorithm that guarantees maximum Internet speed after you combine several connections.

TL-R480T+ router is available for about $65 at present. Join all your connections and then output them as one single connection. Then you can distribute the combined speed through a wifi router, LAN hub or you can directly connect it to your computer.

After running the setup of the router, go to the configuration page as instructed in the user manual.

* Go to **Advanced** > **Load Balancing** option
* Uncheck **Enable Application Optimized Routing** option
* Uncheck **Enable Bandwidth Based Balance Routing** option
* You should also set the Maximum Transmission Unit (MTU) of router to avoid timeout errors.
* Make sure that the IP address assigned to load balancing router is different from the default gateway address of the WAN connections. The default IP of router is 192.186.0.1 (as usual)… change your default gateway IP if it is the same.

# **Network Performance Monitoring and Security:**

what we’re really stressing is the importance of a strong relationship between network performance monitoring (NPM) and security monitoring (SM). In fact, the most secure networks implement a risk management strategy to include both NPM and SM because of their similar features. For example, NPM and SM both use key performance indicators (KPI) as a benchmark to provide us with key information that is essential to network performance

# **3 Key Metrics for Efficient Performance Monitoring:**

Today’s networks have evolved and become more complex to manage. Network administrators are inundated with so many network monitoring tools on the market today, that choosing the right ones can be challenging.

One of the most effective solutions for network monitoring is a network performance monitoring and diagnostic tool (NPMD). In short, NPMD tools provide the ability to detect, identify, and prevent issues related to the many applications that pass through the Internet and the networking devices and appliances that are part of the physical infrastructure.

**It’s all about the metrics**

There are many metrics network admins track daily and all provide relevant information regarding network performance. We’ve selected our top 3 metrics we think every network admin should monitor:

**1**. Link Utilization

**2.** TCP Retransmissions

**3**. Network and Server Response Time

**Link Utilization**

Have you ever experienced latency and dropped packets? We’ve all been victims of slower networks and packet loss, so bandwidth occupancy is one key metric you want to keep your eye on. It’s important to know what’s happening in the network links in case they become congested. If they are, you will notice an increase in packet drops occurring at the routers.  Secondly, make sure the bandwidth occupancy you’re measuring is shown with millisecond granularity. Believe it or not, critical network issues such as buffer oversubscription can occur within milliseconds so if your current tools only show per second analysis, you’re not seeing the complete picture. Think about it, a millisecond advantage in preventing a critical network issue translates to improved customer experience, better business outcomes and greater revenue.

You should also consider which IP is occupying most of the traffic in order to isolate any sources of network congestion and/or anomalous behavior. Typically, the network’s top talkers will identify the specific data flows that represent most of the bandwidth usage. Figure 1 below shows a dashboard measuring bandwidth and top talkers.

**TCP Retransmission**

Transmission Control Protocol (TCP) retransmission rate is a good indicator of network health and one of the most valuable metrics to measure. By definition, retransmission is the resending of packets that have been damaged or lost. Packet retransmissions are a healthy function of modern TCP networks. They can occur when a receiving node doesn’t acknowledge when a packet is sent from a sending node. While these are expected to occur on a normal network, a sustained increase in retransmissions warrant further investigation. For example, there could be a saturated network link and/or some segment of the network that is causing packets to drop. If left unresolved, a large count of retransmissions will negatively impact the performance of your applications. Figure 2 below shows a dashboard with retransmission and response time metrics.

**Network and Server Response Time:**

Many applications today are based on TCP protocol and a client/server model. The Application response time metric measures the time it takes for a server to respond to a data request with application data. This metric can tell us how quickly the application is responding to requests. If the response time increases, this indicates that the application is running slowly.

Network Round Trip Time (RTT) is another great indicator of overall network health, as well as the health and response time of the TCP/IP stack of your server. Basically, it’s the amount of time (typically in milliseconds), that it takes for a server to respond to a packet sent by a client. If a server is overwhelmed with requests, such as during a DDoS attack, its ability to respond efficiently is inhibited, resulting in increased round trip time.

**NETWORK MANAGEMENT:**

Network management is the process of administering and managing computer networks. Services provided by this discipline include fault analysis, performance management, provisioning of networks and maintaining quality of service

**Network hardware requirements:**

* What other devices will your network support (e.g. back-up devices, Uninterruptible Power Supplies, Network printers, etc.)?
* Do you have enough network points for these network devices?

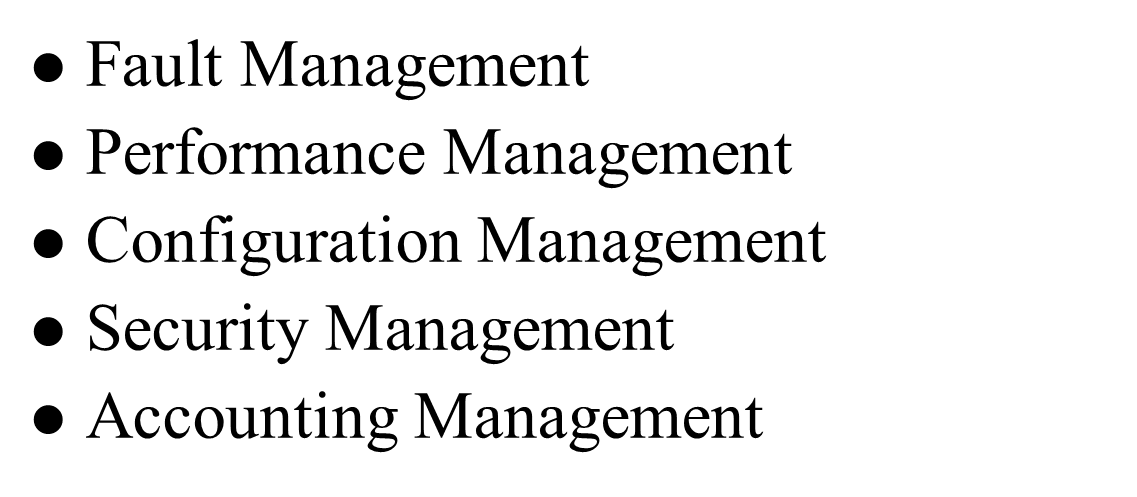
**Network Design:**

* What network topology will you use

• Do all workstations have the correct Network interface cards (NICs) to support this technology

• Which network operating system will you use (e.g. Windows 2000 Server, Linux, Novell etc.)

**Network Management Functions:**



***Fault Management:***

*Fault management is about finding network problems and correcting them. It also identifies and prevents potential or know problems that may occur in future.*

**Fault Detection and Diagnosing (FDD)**

The system discovers that service delivery has been interrupted or its performance has degraded. FDD is the process of uncovering errors in physical system while attempting to identify the source of problem

**By Passing**

Reconfiguration or bypassing involves acting redundant resources specially assigned to back up critical entities. Fault administration service ensures that faults are not lost or neglected.

**Repairing**

An implicit repair can occur when faulty component is replaced or removed

**Reporting**

Report store data on faults and device running condition

**PERFORMANCE MANAGEMENT:**

Network performance management (NPM) is the collection of methods that manage, enable and ensure a computer network optimal performance level. Typically network performance management demands the routine monitoring of quality and performance services

**Performance Variables:**

The goal of performance management is **to measure and make available various aspects of network performance** so that internetwork performance can be maintained at an acceptable level. Examples of performance variables that might be provided include network throughput, user response times.

**Throughput**

For network performance variable through put is defined in terms of the amount of data or number of data packets that can be delivered in predefined time frame.

**User Response**

The number of users or devices on a network can affect the performance on a network, as the available bandwidth will be shared amongst different users. The more users, the more divided the available bandwidth would be**.**

**Network Resources Utilization:**

Network utilization is the proportion of the current network traffic to the maximum amount of traffic that can be handled. It indicates the bandwidth consumption in the network. While high network traffic means that the network is overloaded, low network traffic means that the network is not busy.

* **Network Evaluation**

A network evaluation may consider a range of questions and adopt a variety of options for undertaking the evaluation depending on factors such as the type, size, stage of development and purpose of the network. Networks may be closed (bound) or open (unbounded).

* **Behaviour**

Network behaviour analysis (NBA) is a network monitoring program that ensures the security of a proprietary network. NBA helps in enhancing network safety by watching traffic and observing unusual activity and departures of a network operation. Conventional methods of defending a network against harmful data include packet checking, signature recognition and real-time blocking of malicious sites and data

**Configuration Management:**

Network configuration management (NCM) is a broad term for the organization and management of a computer network. Network configuration management involves collecting different information about hardware devices, software programs and other elements of the network in order to support administration and troubleshooting

**Importance**

Configuration management is essential to keep accurate network configuration records and to help organizations avoid potential challenges or problems within their networks. IT teams can't manage a network if they lose track of connected devices, device configurations and an accurate picture of the device connections.

***Network device discovery***

*Network device discovery, also referred to as topology discovery, is the first step when mapping and monitoring network infrastructure. Network device discovery involves locating devices connected to a network and collecting detailed information to generate a comprehensive network inventory.*

***Configuration backup***

*Configuration backup is the process of extracting configuration settings from a system and writing it to disk. The configuration restore process uses backup configuration data files for the system to restore a specific system configuration.*

**Configuration change management**

Configuration and change management (CCM) is the process of maintaining the integrity of hardware, software, firmware, and documentation related to the configuration and change management process.

**Network Account**

Account is a set of credentials for participating in a network. In a typical network, each user needs an account to access resources on the network, such as shared folders, printers, or applications. Accounts provide a way of identifying users on a network and are the foundation for network security

**Types of Network User Accounts:**

* System accounts
* Super user account
* Regular user account
* Guest user account
* User account vs Group account
* Remote service accounts

**Security Management**

Network security management includes various rules and procedures adopted by network administrators to ensure that unauthorized users do not obtain access. Security involves a host of policies that limit access. The process makes the network secure and protects and manages network operations.

**Types of Security Management:**

* Firewall. Firewalls control incoming and outgoing traffic on networks, with predetermined security rules.
* Network Segmentation.
* Remote Access VPN.
* Email Security. ...
* Data Loss Prevention (DLP) ...
* Intrusion Prevention Systems (IPS) ...
* Sandboxing. ...
* **Importance**
* Network security management protects customer data and prevents it from getting leaked, breached, manipulated or modified. No matter how good your product or service may be, ensuring security and protection to customer data is extremely important to provide your customers with great customer experience

**Network Operating Systems:**

A network operating system (NOS) is an operating system that manages network resources: essentially. An operating system that includes special functions for connecting computers and devices into a local/Wide area network (LAN/WAN)

**Advantage of Network Operating System**:

* It allows multiple computers to connect so that they can share data, files and hardware devices.
* Provide basic operating system features such as support for processors, protocols, automatic hardware detection and support multi-processing of applications.
* Provide security features such as authentication, login restrictions, and access control.
* Provide name and directory services.
* Provide file, print, web services and back-up services.
* Support Internetworking such as routing and WAN ports.
* User management and support for logon and logoff, remote access; system management, administration, and auditing tools with graphical interfaces.

**Severs**

A server is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network. In theory, whenever computers share resources with client machines they are considered servers. There are many types of servers, including web servers, mail servers, Application Servers etc.

**Work Stations**

A high-performance computer system that is basically designed for a single user and has advanced graphics capabilities, large storage capacity, and a powerful central processing unit. A workstation is more capable than a personal computer (PC) but is less advanced than a server

**Interconnection Devices:**

Interconnected devices are physical objects that can send and receive information or data to and from the internet. Some interconnected devices can also send information or commands to other products. Common interconnected devices include: smart phones, computers, laptops and tablets.

**HUB**

A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices.

**Switches**

Switches can be used to connect together a number of end-user devices such as workstations, or to interconnect multiple network segments. A switch that interconnects end-user devices is often called a workgroup switch.

**Bridge**

A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

**TYPES OF BRIDGES :**

**Transparent Bridges**:- These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.

**Source Routing Bridges**:- In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination

**ROUTER**

A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

**BRouter:**

It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks, and working as the bridge, it is capable of filtering local area network traffic.

**GATEWAY:**

A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. Gateway is also called a protocol converter.

**NETWORK PROTOCOLS:**

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design. Network protocols are the reason you can easily communicate with people all over the world, and thus play a critical role in modern digital communications.

**Simple Network Management Protocol:**

Simple Network Management Protocol (SNMP) is a networking protocol used for the management and monitoring of network-connected devices, defined by (Internet Engineering Task Force)

**Simple Network Management Protocol Components:**

**Manager**

* Centralised system used to monitor network

**Agent**

Software Management Utility installed on managed device

**Management Information**

* Consists of information of resources which are to be managed

**Secure Messaging Protocol:**

A secure messaging protocol (SMP) allows remote users to send messages (and more) to each other securely over an untrusted (and possibly adversarial) network such as the Internet. In general, to use an SMP, participants first have to go through some type of trusted setup, often called “contact discovery

**Manager**

A manager is a server running some kind of software system that can handle management tasks for a network. Managers are often referred to as Network Management Stations.

**Agent**

a piece of software that runs on the network devices you are managing. Most IP devices come with some kind of SNMP agent built in. In Network Management System, the agent keeps performance information in a database.

**Design Consideration:**

Network design is the practice of planning and designing a communications network. Network design includes things like network analysis, IP addressing, hardware selection, and implementation planning. In simple networks, like those found in most homes and small offices, network design is a straightforward process.

**Speed**

Network speed measures the transfer rate of data from a source system to a destination system, network bandwidth is the amount of data that can be transferred per second. Combine the two, and you have what is known as network throughput.

**Usability**

Usability is the degree of ease with which products such as Network software and Web applications can be used to achieve required goals effectively and efficiently. Usability assesses the level of difficulty involved in using a user interface.

**Functionality**

Computer networks share common devices, functions, and the features of computer network like clients, server, transmission media, shared data, shared printers and other hardware and software resources, Network Interface Card (NIC), Local Operating System (LOS), and the network operating system.

**Cost**

Network costs means the costs incurred by the Host Council in hosting the Network, including but not limited to, hardware, software licences, lease payments, interest and fees incurred on leases, communication costs, stationery, courier charges and any other resources associated with operating the network.

The term flexibility is commonly defined as the ability to adapt to changes. For networks, flexibility would refer to the ability to adapt the available network resources, such as flows or topology, to changes of design requirements.

**Principle of computer network**

# Chapter # 1:

## TYPES OF NETWORK SYSTEMS AND RELATED STANDARDS:

Local area network (LAN):

* A **local area network** (LAN) is a computer network in a small area like a home, office, or school.
* Many computers can be connected to share information and Internet connections. Most LANs use Ethernet to connect together.
* Router does not use as forwarding devices between LAN devices.

Wide area network (WAN):

* A **WAN** (wide area network), in comparison to a MAN, is not restricted to a geographical location, although it might be confined within the bounds of a state or country. A WAN connects several LANs, and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive. The Internet is an example of a worldwide public WAN.

**Leased lines :** When permanent dedicated connections were required, a point-to-point link using copper media was used to provide a pre-established WAN communications path from the customer premises to the provider network. Point-to-point lines could be leased from a service provider and were called “leased lines”.

**Circuit-Switched:**

* Circuit-switched connections are provided by Public Service Telephone Network (PSTN) carriers.

**Public Service Telephone Network (PSTN)**

* Dialup WAN access uses the PSTN as its WAN connection. Traditional local loops can transport binary computer data through the voice telephone network using a voiceband modem. The modem modulates the digital data into an analog signal at the source and demodulates the analog signal to digital data at the destination. The physical characteristics of the local loop and its connection to the PSTN limit the rate of the signal to less than 56 kbps.

**Integrated Services Digital Network (ISDN)**

* ISDN is a circuit-switching technology that enables the PSTN local loop to carry digital signals. This provided higher capacity switched connections than dialup access. ISDN provides for data rates from 45 Kbps to 2.048 Mbps.
* ISDN has declined greatly in popularity due to high-speed DSL and other broadband services. ISDN is considered a legacy technology with most major providers discontinuing this service.
* Packet switching segments data into packets that are routed over a shared network.
* Circuit-switched networks require a dedicated circuit to be established. In contrast, packet-switching networks allow many pairs of nodes to communicate over the same channel.
* There are two traditional (legacy) packet-switched connectivity options.

**Frame Relay**

* Frame Relay is a simple Layer 2 non-broadcast multi-access (NBMA) WAN technology that is used to interconnect enterprise LANs. A single router interface can be used to connect to multiple sites using different PVCs. PVCs are used to carry both voice and data traffic between a source and destination, and support data rates up to 4 Mbps, with some providers offering even higher rates.
* Frame Relay creates PVCs which are uniquely identified by a data-link connection identifier (DLCI). The PVCs and DLCIs ensure bidirectional communication from one DTE device to another.
* Frame Relay networks have been largely replaced by faster Metro Ethernet and internet-based solutions.

**Asynchronous Transfer Mode (ATM):**

* Asynchronous Transfer Mode (ATM) technology is capable of transferring voice, video, and data through private and public networks. It is built on a cell-based architecture rather than on a frame-based architecture. ATM cells are always a fixed length of 53 bytes. The ATM cell contains a 5-byte ATM header followed by 48 bytes of ATM payload. Small, fixed-length cells are well-suited for carrying voice and video traffic because this traffic is intolerant of delay. Video and voice traffic do not have to wait for larger data packets to be transmitted.
* The 53-byte ATM cell is less efficient than the bigger frames and packets of Frame Relay. Furthermore, the ATM cell has at least five bytes of overhead for each 48-byte payload. When the cell is carrying segmented network layer packets, the overhead is higher because the ATM switch must be able to reassemble the packets at the destination. A typical ATM line needs almost 20 percent greater bandwidth than Frame Relay to carry the same volume of network layer data.
* ATM networks have been largely replaced by faster Metro Ethernet and internet-based solutions.

**Value added network (VAN):**

* A VAN (value added network) is a private network provider that focuses on offering network services such as secure email, message encryption and management reporting. Their goal is to facilitate EDI (electronic data interchange) among online companies, providing a convenient way for ecommerce businesses to securely communicate and share data.

**How a VAN is created**

* When a common carrier such as a telecom company leases communication lines to a network provider and that provider then enhances those lines by adding additional services, it has created a Value Added Network. While EDI is the primary focus of VANs, the improvements or enhancements a network chooses to add is what differentiates networks.

**Benefits of VANs:**

**1.Error correction** VANs help in error correction, as they reduce human involvement, and improve recordkeeping. They can perform checks at the transaction level and ensure minimal error.

**2. Improved exchange** The exchange of data becomes real-time with VANs. This improves decision-making and record-keeping and provides essential business intelligence to generate insights about operations.

**3. Secure** Electronic data transfers can be made securely using encryption. All communication between businesses can be encrypted to protect business secrets.

**4. Standardized** VANs transfer data using standard formats, such as XML and CSV. They allow the data to be read by the various Enterprise Resource Planning (ERP) software used by companies. They also enable the use of newer technologies without making changes to existing technology.

* **Physical topology** can be considered as a layout of the network media that shows the interconnections of the devices on the network. It specifies which geometric shape the linked devices form with each other.
* The physical topology does not give much comprehensive detail about the type of devices, the mechanism used for interacting with other devices in the network, and how data is transferred from one device to another.

**Types of Physical Topology:**

1. **Bus topology** – Comprised of a single main cable, with which all the devices or pc’s are connected. There is a terminator attached with the cable, in the end, to absorb the signals when it reaches the end of the line.
2. **Ring topology** – This topology connects all the devices of the network by forming a ring and the flow of data will always be in one direction. It does not require any termination of the cable, as a result, each device has an equal opportunity to access the media. There are two types of ring topology – single ring and dual ring.
3. **Star topology** – In this topology, all the devices are linked to a central hub by its own cable.
4. **Mesh topology** – This topology link each device with every other devices in the network.

**Logical Topology:**

* Unlike physical topology, the logical topology emphasis on the manner in which data is transmitted between network nodes instead of the physical layout of the path that data follows. An important fact regarding these topologies is that both physical and logical topologies are independent regarding a network, whether it is of any shape and size.

**Types of Logical Topology**

1. Logical Bus – The data follows a linear pattern from the source to all destinations.
2. Logical Ring – In this topology, the data travels in the form of a ring from a device to another and reaches to the beginning of the circle.

**Network access methods:**

**CSMA/CD (Carrier Sense Multiple Access/Collision Detection):**

* In CSMA/CD (Carrier Sense Multiple Access/Collision Detection) Access Method, every host has equal access to the wire and can place data on the wire when the wire is free from traffic. When a host want to place data on the wire, it will “sense” the wire to find whether there is a signal already on the wire. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time (Backoff Timer) and again the data will be retransmitted, to avoid collision again.

**CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)**

* In CSMA/CA, before a host sends real data on the wire it will “sense” the wire to check if the wire is free. If the wire is free, it will send a piece of “dummy” data on the wire to see whether it collides with any other data. If it does not collide, the host will assume that the real data also will not collide.

**Token Passing**

* In CSMA/CD and CSMA/CA the chances of **collisions** are there. As the number of hosts in the network increases, the chances of **collisions** also will become more. In token passing, when a host want to transmit data, it should hold the token, which is an empty packet. The token is circling the network in a very high speed. If any workstation wants to send data, it should wait for the token. When the token has reached the workstation, the workstation can take the token from the network, fill it with data, mark the token as being used and place the token back to the network.

**Application Layer:**

* This is the only layer that directly interacts with data from the user.
* The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users.
* A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

**Presentation Layer**:

* The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

**Session Layer**:

* The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends.
* The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.

**Transport Layer**:

* The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer.
* The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

**Network Layer:**

* The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end.
* The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

**Data Link Layer**:

* The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination.
* This layer is composed of two parts—
  + **Logical Link Control (LLC),** which identifies network protocols, performs error checking and synchronizes frames.
  + **Media Access Control (MAC)** which uses MAC addresses to connect devices and define permissions to transmit and receive data.

**Physical Layer**:

* The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.

**Advantages of OSI Model**:

1. Determine the required hardware and software to build their network.
2. Understand and communicate the process followed by components communicating across a network.
3. Perform troubleshooting, by identifying which network layer is causing an issue and focusing efforts on that layer

**Network protocols and standards:**

* A protocol is the set of rules used when computers communicate.
* Network standards and protocols are necessary because different people use different networks therefore they need to have a common platform to communicate to each other.
* The standards and protocols are like languages – you have to understand them and be able to speak them to communicate effectively.
* For the communication to be successful two devices need to communicate the same way –with the same language or code- for the communication to be successful.
* If both devices are not following the same protocol then the communication won’t be successful due to the fact that both devices won’t understand each other.

**What is TCP/IP?**

* TCP/IP stands for Transmission Control Protocol/Internet Protocol and is a suite of communication protocols used to interconnect network devices on the internet.
* TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into [packets](https://www.techtarget.com/searchnetworking/definition/packet), addressed, transmitted, routed and received at the destination.

**The 4 layers of the TCP/IP model:**

TCP/IP functionality is divided into four layers, each of which includes specific protocols:

1. The **application layer**provides applications with standardized data exchange. Its protocols include HTTP, FTP, [Post Office Protocol 3](https://whatis.techtarget.com/definition/POP3-Post-Office-Protocol-3), [Simple Mail Transfer Protocol](https://whatis.techtarget.com/definition/SMTP-Simple-Mail-Transfer-Protocol) and Simple Network Management Protocol. At the application layer, the payload is the actual application data.
2. The **transport layer**is responsible for maintaining end-to-end communications across the network. TCP handles communications between hosts and provides flow control, multiplexing and reliability. The transport protocols include TCP and [User Datagram Protocol](https://www.techtarget.com/searchnetworking/definition/UDP-User-Datagram-Protocol), which is sometimes used instead of TCP for special purposes.
3. The **network layer**, also called the *internet layer*, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are IP and Internet Control Message Protocol, which is used for error reporting.

The **physical layer**, also known as the *network interface layer*or *data link layer*, consists of protocols that operate only on a link -- the network component that interconnects nodes or hosts in the network. The protocols in this lowest layer include Ethernet for local area networks and [Address Resolution Protocol](https://www.techtarget.com/searchnetworking/definition/Address-Resolution-Protocol-ARP)

**UDP:**

* **User Datagram Protocol (UDP)** is a Transport Layer protocol.
* it is an **unreliable and connectionless protocol.** So, there is no need to establish a connection prior to data transfer.
* For real-time services like computer gaming, voice or video communication, live conferences; we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP, so it also saves bandwidth.
* User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth
* **Source Port:** Source Port is a 2 Byte long field used to identify the port number of the source.
* **Destination Port:** It is a 2 Byte long field, used to identify the port of the destined packet.
* **Length:**Length is the length of UDP including the header and the data. It is a 16-bits field.
* **Checksum:**Checksum is 2 Bytes long field. It is the 16-bit one’s complement of the one’s complement sum of the UDP header, the pseudo-header of information from the IP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

**Applications of UDP:**

* Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control.
* UDP is used for some routing update protocols like RIP(Routing Information Protocol).
* Normally used for real-time applications which can not tolerate uneven delays between sections of a received message.
* Following implementations uses UDP as a transport layer protocol:
  + NTP (Network Time Protocol)
  + DNS (Domain Name Service)
  + BOOTP, DHCP.
  + NNP (Network News Protocol)
  + Quote of the day protocol
  + TFTP, RTSP, RIP.

**802.2** (Logical Link Control):

* 802.2 is "the standard for the upper Data Link Layer sublayer also known as the Logical Link Control layer. It is used with the 802.3, 802.4, and 802.5 standards (lower DL sublayers).“
* 802.2 "specifies the general interface between the network layer (IP, IPX, etc) and the data link layer (Ethernet, Token Ring, etc).
* Basically, think of the 802.2 as the "translator" for the Data Link Layer. 802.2 is concerned with managing traffic over the physical network. It is responsible for flow and error control.

**802.3 (Ethernet):**

* IEEE 802.3 is a set of standards and protocols that define Ethernet-based networks.
* Ethernet technologies are primarily used in LANs, though they can also be used in MANs and even WANs.
* IEEE 802.3 defines the **physical layer** and the **medium access control (MAC) sub-layer** of the data link layer for wired Ethernet networks.

**FDDI (Fiber Distributed Data Interface):**

* FDDI (Fiber Distributed Data Interface) is a network standard that uses [fiber optic](https://www.techtarget.com/searchnetworking/definition/fiber-optics-optical-fiber) connections in a local area network ([LAN](https://www.techtarget.com/searchnetworking/definition/local-area-network-LAN)) that can extend in range up to 200 kilometers (124 miles).
* The FDDI protocol is based on the [token ring](https://www.techtarget.com/searchnetworking/definition/Token-Ring) protocol.
* A FDDI LAN can support thousands of users. While FDDI is frequently used on the backbone for a wide area network ([WAN](https://www.techtarget.com/searchnetworking/definition/WAN-wide-area-network)) or campus area network ([CAN](https://www.techtarget.com/searchnetworking/definition/campus-network)), it has been largely superseded by other networking technologies.

**Features:**

* FDDI uses optical fiber as its physical medium.
* It operates in the physical and medium access control (MAC layer) of the Open Systems Interconnection (OSI) network model.
* It provides high data rate of 100 Mbps and can support thousands of users.
* It is used in LANs up to 200 kilometers for long distance voice and multimedia communication.
* It uses ring based token passing mechanism and is derived from IEEE 802.4 token bus standard.
* It contains two token rings, a primary ring for data and token transmission and a secondary ring that provides backup if the primary ring fails.
* FDDI technology can also be used as a backbone for a wide area network (WAN).
* Token-passing networks move a small frame, called a token, around the network. Possession of the token grants the right to transmit.
* If a node receiving the token in order to transmit data, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the [information](https://ecomputernotes.com/fundamental/information-technology/what-do-you-mean-by-data-and-information) that it wants to transmit, and sends this [information](https://ecomputernotes.com/fundamental/information-technology/what-do-you-mean-by-data-and-information) to the next station on the ring. Since only one station can possess the token and transmit data at any given time, there are no collisions.

**Wireless technologies:**

* Wireless technology involves transmitting electromagnetic signals over the air. Interference and obstacles that block RF signals are common problems with wireless technology.
* Wireless technology allows users to communicate simultaneously over the same medium without their signals interfering with one another.

**Infrared:**

* Infrared (IR) is a wireless mobile technology used for device communication over short ranges. IR communication has major limitations because it requires line-of-sight, has a short transmission range and is unable to penetrate walls. IR transceivers are quite cheap and serve as short-range communication solutions.
* In fact, Infrared Data Association (IrDA) device communication is usually exchanged on a one-to-one basis. Thus, data transmitted between IrDA devices is normally unencrypted.

**Bluetooth:**

* Bluetooth technology is a high-speed low powered wireless technology link that is designed to connect phones or other portable equipment together. It is a specification (IEEE 802.15.1) for the use of low-power radio communications to link phones, computers, and other network devices over short distances without wires. Wireless signals transmitted with Bluetooth cover short distances, typically up to 30 feet (10 meters).
* It is achieved by embedded low-cost transceivers into the devices.

**Factors affecting range and speed of wireless technologies:**

* Physical Obstructions: Wireless signals can have trouble penetrating solid objects which can be any numbers of things such as hills, buildings, single walls or even people.
* Network Range & Distance between Devices: The further apart the networked devices that are trying to communicate with each other are, the more the signal strength drops.
* Wireless Network Interference: Signals operating at similar frequencies can cause interference with each other and have a significantly negative effect on the performance of the network. Other wireless technologies can cause identical interference such as mobile phones and microwave ovens that operate within the same ranges (2.4GHz)
* Signal Sharing: Wireless Networks allow more than 1 person to communicate with another network source at any one time. This sharing of connection means that the more subscribers utilizing the network, the more devices the access point has to try and communicate with instantaneously. The point of access has to delegate its resources to each subscriber.

**Application layer protocols:**

**DNS :**

The Domain Name System ([DNS](https://www.cloudflare.com/learning/dns/what-is-dns/)) is the phonebook of the Internet. When users type domain names such as ‘google.com’ or ‘nytimes.com’ into web browsers, DNS is responsible for finding the correct [IP address](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/) for those sites. Browsers then use those addresses to communicate with [origin servers](https://www.cloudflare.com/learning/cdn/glossary/origin-server/) .

**How do DNS servers resolve a DNS query?**

There are four servers that work together to deliver an IP address to the client: recursive resolvers, root nameservers, TLD nameservers, and authoritative nameservers.

1. The DNS recursor (also referred to as the DNS resolver) is a server that receives the query from the DNS client, and then interacts with other DNS servers to hunt down the correct IP. Once the resolver receives the request from the client, the resolver then actually behaves as a client itself, querying the other three types of DNS servers in search of the right IP.
2. First the resolver queries the root nameserver. The root server then responds to the resolver with the address of a Top Level Domain (TLD) DNS server (such as .com or .net) that stores the information for its domains.
3. Next the resolver queries the TLD server. The TLD server responds with the IP address of the domain’s authoritative nameserver. The recursor then queries the authoritative nameserver, which will respond with the IP address of the origin server.
4. The resolver will finally pass the origin server IP address back to the client. Using this IP address, the client can then initiate a query directly to the origin server

**DHCP:**

* A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices.
* **How DHCP works:**
* DHCP is a client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.
* Clients configured with DHCP broadcast a request to the DHCP server and request network configuration information for the local network
* The DHCP server responds to the client request by providing IP configuration information . This includes a specific IP address, as well as a time period -- also called a ***lease***-- for which the allocation is valid.
* If a node is relocated in the network, the server identifies it using its Media Access Control ([MAC](https://searchnetworking.techtarget.com/definition/MAC-address)) address, which prevents the accidental configuration of multiple devices with the same IP address.

**Static vs. dynamic DHCP leases**

* Each time a device with a dynamic IP address is powered up, it must communicate with the DHCP server to lease another IP address.
* On the other hand, static devices -- such as web servers and switches -- are assigned permanent IP addresses.

**HTTP:**

* HTTP (Hypertext Transfer Protocol) is a Protocol for transferring files -- such as text, images, sound, video and other multimedia files -- over the web
* **How HTTP works**
* Client devices send requests to servers for the resources needed to load a web page; the servers send responses back to the client to fulfill the requests.
* **The specific version of HTTP followed.** HTTP and [HTTP/2](https://www.techtarget.com/searchnetworking/definition/HTTP-2-protocol) are the two versions.
* **A URL.**This points to the resource on the web.
* **An HTTP method**. ‘GET’ and ‘POST’; a ‘GET’ request expects information back in return (usually in the form of a website), while a ‘POST’ request typically indicates that the client is submitting information to the web server (such as form information, e.g. a submitted username and password)..
* **HTTP request headers.** This includes data such as what type of browser is being used and what data the request is seeking from the server. It can also include [cookies](https://searchsoftwarequality.techtarget.com/definition/cookie), which show information previously sent from the server handling the request.
* **An HTTP body.** This is optional information the server needs from the request, such as user forms -- username/password logins, short responses and file uploads -- that are being submitted to the website.

**Response:**

* **HTTP status code**, which indicates the status of the request to the client device. Responses may indicate success, an informational response, a redirect, or errors on the server or client side.
* **HTTP response headers**, which send information about the server and requested resources.
* **An HTTP body (optional).** If a request is successful, this contains the requested data in the form of HTML code, which is translated into a web page by the client browser.

**HTTP status codes:**

* **200 OK.** This means that the request, such as GET or POST, worked and is being acted upon.
* **300 Moved Permanently.** This response code means that the URL of the requested resource has been changed permanently.
* **401 Unauthorized.** The client, or user making the request of the server, has not been authenticated.
* **403 Forbidden**. The client's identity is known but has not been given access authorization.
* **404 Not Found.** This is the most frequent error code. It means that the URL is not recognized or the resource at the location does not exist.
* **500 Internal Server Error.** The server has encountered a situation it doesn't know how to handle.

**FTP (File Transfer Protocol):**

* FTP stands for File transfer protocol.
* FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
* It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
* It is also used for downloading the files to computer from other servers.

**Objectives of FTP:**

* It provides the sharing of files.
* It is used to encourage the use of remote computers.
* It transfers the data more reliably and efficiently.

**There are two types of connections in FTP:**

* Control Connection: Through control connection, we can transfer a line of command or line of response at a time. The control connection remains connected during the entire interactive FTP session.
* Data Connection: The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

**SMTP:**

* SMTP is a push protocol and is used to send the mail whereas POP or IMAP are used to retrieve those emails at the receiver’s side.
* The client who wants to send the mail opens a TCP connection through port 25 to the SMTP server and then sends the mail across the connection.

# Chapter # 2 UNDERSTAND THE HARDWARE AND SOFTWARE USED IN NETWORKING:

Network devices:

**Workstations:**

**workstation**, a high-performance computer system that is basically designed for a single user and has advanced graphics capabilities, large storage capacity, and a powerful CPU. 

**Print servers :**

* Print servers, or printer servers, are devices or programs that connect printers to computers over a network. They act as an intermediary between computers and printers, accepting printing jobs from computers and sending them on to the right printer. They do this by storing and queueing print requests locally and to avoid overloading a busy printing device.

**Mail server :** A mail server is a computer system that sends and receives email. In many cases, web servers and mail servers are combined in a single machine. However, large ISPs and public email services (such as Gmail and Hotmail) may use dedicated hardware for sending and receiving email.

Mail servers can be broken down into two main categories:

* outgoing mail servers (SMTP)
* incoming mail servers (POP, IMAP)

**File server :**

A **file server** is a computer containing files available to all users connected to a local-area network (LAN). In some LANs, a microcomputer is designated as the file server, while in others it is a computer with a large disk drive and specialized software.

* **web server :**
* A web server is software and hardware that uses HTTP (Hypertext Transfer Protocol) and other protocols to respond to client requests made over the World Wide Web. The main job of a web server is to display website content through storing, processing and delivering webpages to users.
* **proxy server :** A proxy server is a computer system or router that functions as a relay between client and server. It helps prevent an attacker from invading a private network and is one of several tools used to build a firewall.  
    
  The word proxy means "to act on behalf of another," and a proxy server acts on behalf of the user. All requests to the Internet go to the proxy server first, which evaluates the request and forwards it to the Internet. Likewise, responses come back to the proxy server and then to the user.
* **network interface cards (NIC):**
* A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.

Interconnection devices:

* **Modem** :
* A **modem** or **broadband modem** is a hardware device that connects a computer or router to a broadband network. For example, a cable modem and DSL modem are two examples of these types of Modems.
* Short for **modulator/demodulator**, a **modem** is a hardware device that allows a computer to send and receive information over telephone lines. When sending a signal, the device converts ("modulates") digital data to an analog audio signal, and transmits it over a telephone line. Similarly, when an analog signal is received, the modem converts it back ("demodulates" it) to a digital signal.
* **Repeater:** Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters.When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. Repeaters amplifies the attenuated signal and then retransmits it.
* **HUB:**A hub is basically a multiport repeater. It is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN.
* A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination or not.
* Types of network hubs
* Active hubs repeat and strengthen incoming transmissions. They are also sometimes referred to as repeaters.
* Passive hubs simply serve as a point of connectivity, without any additional capabilities.
* **Bridge:** A bridge works at the **data link layer,** and it also helps to make interconnection in between multiple networks with using of same protocol.
* Network Bridge divides the large network into small segments, and these segments represent a separate collision domain, and it also helps to decrease the number of collision over the network. Every collision domain contains the own individual **bandwidth**, so its performance is getting to improve.
* **Switch:**
* A switch is a data link layer networking device which connects devices in a network and uses packet switching to send and receive data over the network.
* When a data frame arrives at any port of a network switch, it examines the destination address and sends the frame to the corresponding device(s). Thus, it supports both unicast and multicast communications**.**
* **Router:**
* A router is a layer 3 or network layer device. It connects different networks together and sends data packets from one network to another. It transfers data in the form of IP packets. In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.
* Routers have a routing table in it that is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.
* **Gateway:**
* Gateways serve as an entry and exit point for a network as all data must pass through or communicate with the gateway prior to being routed.
* The gateway is implemented at the edge of a network and manages all data that is directed internally or externally from that network. When one network wants to communicate with another, the data packet is passed to the gateway and then routed to the destination through the most efficient path.
* **Wireless access points :**
* A wireless access point (WAP) is a hardware device or configured node on a local area network (LAN) that allows wireless capable devices and wired networks to connect through a wireless standard, including Wi-Fi or Bluetooth. WAPs feature radio transmitters and antennae, which facilitate connectivity between devices and the Internet or a network.
* A WAP is also known as a hotspot.

Media types:

* **Coaxial cable:**
* Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield . The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

 Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors

* There are two types of Coaxial cable:
  + Thinnet (10Base2 )  maximum segment length is 185 meters.
  + Thicknet (10Base5 ) maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor.
* **UTP:** UTP stands for Unshielded Twisted Pair. In the mantle of a UTP cable you will find eight separate wires. All the wires are twisted in four pairs. A connector can be placed on the end of these cables. These connectors are also known as RJ45 plugs.
* The twist helps to improve its immunity to electrical noise and EMI.
* UTP Cat5, has a transfer rate of 100mbit/s and a bandwidth of 100Mhz
* UTP Cat5e, has a transfer rate of 1.000mbit/s and a bandwidth of 100Mhz
* UTP Cat6, has a transfer rate of 1.000mbit/s and a bandwidth of 250Mhz
* UTP Cat6a, has a transfer rate of 10.000mbit/s and a bandwidth of 500Mhz
* **Fiber Optic Cable:**
* Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials. It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference.
* Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds.
* Two common types of fiber optics are:
  + Single-mode fiber (SMF)
  + Multi-mode fiber (MMF)
* **shielded twisted-pair (STP) :**
* STP Cabling is twisted-pair cabling with additional shielding to reduce crosstalk and other forms of electromagnetic interference (EMI).
* Shielded twisted-pair (STP) cabling is more expensive than unshielded twisted-pair (UTP) cabling. It has an impedance of 150 ohms, has a maximum length of 90 meters.
* **Single-mode fiber**
* Single-mode fiber is used for longer distances due to the smaller diameter of the glass fiber core. This smaller diameter lessens the possibility for attenuation, which is a reduction in signal strength.
* Single-mode fiber also has a considerably higher [bandwidth](https://www.techtarget.com/searchnetworking/definition/bandwidth) than multimode fiber. The light source used for single-mode fiber is typically a laser. Single-mode fiber is usually more expensive as it requires precise calculations to produce the laser light in a smaller opening.
* **Wireless:** Wireless Communication is a method of transmitting information from one point to other, without using any connection like wires, cables or any physical medium. The information can be transmitted through the air by using electromagnetic waves like IR, RF, satellite.
* The main advantage of wireless communication is mobility . This kind of communication provides flexibility and very easy to use and Install.
* **Types of Wireless Communication:**
  + Satellite Communication
  + Infrared Communication
  + Bluetooth Technology
  + Broadcast Radio
  + Microwave Communication
  + Wi-Fi
  + Mobile Communication Systems

**Microwave and satellite links**:

* **Microwave:**

Microwave transmission in the atmosphere can only take place when there is a direct line of sight between the sender's and receiver's antenna. This is why microwave transmission towers are speckled with antennas pointing in many directions -- they actually point at different microwave transmission towers. The absorption of microwaves in the atmosphere also means that there is very little interference between different microwave towers

* **satellite:**
* In satellite communication, the signal (a beam of modulated microwave) is sent near the satellite then, the satellite amplifies the signal and sent it back to the antenna receiver which is located on the surface of the earth. Satellite communication contains two main components like the space segment and the ground segment. The ground segment consists of fixed or mobile transmission, reception, and ancillary equipment and the space segment, which mainly is the satellite itself.

**Software**:

* **Network operating system:**
* Network Operating System is a computer operating system that facilitates to connect and communicate various autonomous computers over a network.
* The Network O.S. mainly runs on a powerful computer, that runs the server program. It facilitates the security and capability of managing the data, user, group, application, and other network functionalities.
* The main advantage of using a network O.S. is that it facilitates the sharing of resources and memory amongst the autonomous computers in the network. It can also facilitate the client computers to access the shared memory and resources administered by the Server computer. In other words, the Network O.S. is mainly designed to allow multiple users to share files and resources over the network.
* **Virus checker:** A virus scan is the process of using anti-virus software to scan and identify viruses in a computing device.
* It is an information security process that aims to review and identify threatening viruses and programs. It is the core feature of anti-virus software.
* **Firewall:** A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.
* Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer’s entry point, called ports, which is where information is exchanged with external devices. For example, “Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."
* **Types of Firewalls**

**Packet filtering**

* A small amount of data is analyzed and distributed according to the filter’s standards.

**Proxy service**

* Network security system that protects while filtering messages at the application layer.

**Stateful inspection**

* Dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.

**Next Generation Firewall (NGFW)**

* Deep packet inspection Firewall with application-level inspection.
* **Email Client:** An email client, email reader or, more formally, message user agent (MUA) or mail user agent is a **computer program used to access and manage a user's email**.

# Directory Services:

What is a Directory Services?

Directory services are used to store, retrieve, and manage information about objects, such as user accounts, computer accounts, mail accounts, and information on resources available on the network.

**Active Directory:**was developed by Microsoft for networks running Windows 2000 Server, Windows 2003 Server, or Windows 2008.

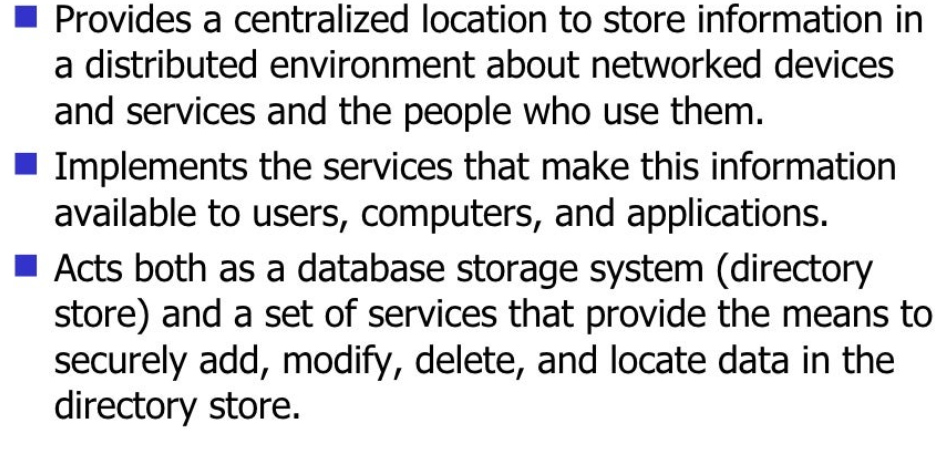
**eDirectory :** was developed by Novell for Novell NetWare networks. Previous versions for Novell NetWare 4.x and 5.x were called Novell Directory Services (NDS).

**OpenLDAP:** was developed by Apple for networks running Mac OS X Servers.

**Common Features of DS**:

* Provide file sharing .
* Authenticate Users.
* Provides services, Such as Email, Access to internet, print services ETC.
* Control access to services and sharing.

**Key Features of Active directory**:



**AD Terminologies**:

* Attribute
* Object
* OU (Organizational Unit)
* Domain
* Tree
* Forest

**Lightweight Directory Access Protocol (LDAP) (IETF)** is a protocol that enables clients to access information within a directory service, allowing the directory to be searched and objects to be added, modified, and deleted.LDAP was created after the X.500 (ITU) specification that uses the Directory Access Protocol (DAP).

## Telecommunication services:

* **E-mail**, in full **electronic mail**, messages transmitted and received by digital computers through a network.
* The process starts with an email client’s help by connecting it through a server called Simple Mail Transfer Protocol through the internet. A dedicated port is assigned to the server to help the client transfer the messages through the mail. It is necessary to keep the header information intact so that the recipient’s email address should be correct. SMTP converts the information to transfer the mail content across the ports. The @ sign acts as a divider between the name and mail server, and hence SMTP looks for the mail server after @ sign.
* There are different clients for emails such as Outlook, Gmail, thunderbird etc. and mails can be sent and received from different clients. When the domains are different, SMTP looks for the domains in Domain Name System, and with the help of an IP address, a signal is sent to the recipient’s server saying about the email. Now the gateways are opened, and the mail is sent to the new server, and the communication happens.

**IRC - Internet Relay Chat** is a system for chatting that involves a set of rules and conventions and client/server software.

* There are hundreds of IRC channels (discussion areas) around the world, hosted on servers, on which people type their messages to others on the same channel interested in the same subject.
* There are client IRC programs which provide graphical interfaces which make it easier for people log on and access active channels and send and receive the messages. IRC chat, at present, is not limited to two people, unlike earlier versions.

**Discussion board**:

* A discussion board (known also by various other names such as discussion group, discussion forum, message board, and online forum) is a general term for any online "bulletin board" where you can leave and expect to see responses to messages you have left. Or you can just read the board.
* The first discussion boards were available on bulletin board systems. On the Internet, USENET provides thousands of discussion boards; these can now sometimes be viewed from a Web browser.

**What is remote access?**

Remote access is the ability for an authorized person to access a computer or network from a geographical distance through a network connection.

This is especially important for employees who work at branch offices, are traveling or telecommute.

* **Remote desktop**:
* Remote desktop is a program or an operating system feature that allows a user to connect to a computer in another location, see that computer's desktop and interact with it as if it were local.
* **Remote desktop protocols**
* A remote desktop connection relies upon any of a number of protocols, including Remote Desktop Protocol ([RDP](https://searchenterprisedesktop.techtarget.com/definition/Remote-Desktop-Protocol-RDP)), virtual network computing ([VNC](https://www.techtarget.com/searchnetworking/definition/virtual-network-computing)), NX technology and Independent Computing Architecture (ICA).
* People use remote desktop access capabilities to do a variety of things, including the following:
  + Access a workplace computer from home or when traveling.
  + Access a home computer from other locations.
  + Fix a computer problem.
  + Perform administrative tasks.
  + Demonstrate something, such as a process or a software application
* What Is Social Networking?
* The term social networking refers to the use of internet-based [social media](https://www.investopedia.com/terms/s/social-media.asp) sites to stay connected with friends, family, colleagues, customers, or clients. Social networking can have a social purpose, a business purpose, or both, through sites like Facebook, Twitter, LinkedIn, and Instagram.

**File services**:

* A file server provides a central location on your network where you can store files and share them with users across your network.
* AN organizations need to share information and data between people. Instead of *emailing* or using USB drives to move data, for example, a file server can be used as a central place for many people to store files.
* **File server protocols and programs:**
  + **Server message block (**[**SMB**](https://www.techtarget.com/searchnetworking/definition/Server-Message-Block-Protocol)**) :** is the most common protocol for LAN file servers. SMB is natively supported for Windows and macOS operating systems (OSes).
* **Network File System (**[**NFS**](https://searchenterprisedesktop.techtarget.com/definition/Network-File-System)**):**is primarily used by Linux and Unix OSes.
* **File Transfer Protocol (**[**FTP**](https://www.techtarget.com/searchnetworking/definition/File-Transfer-Protocol-FTP)**)**and **Secure FTP (**[**SFTP**](https://searchcompliance.techtarget.com/definition/SFTP-Secure-File-Transfer-Protocol)**)**are designed to serve files over the internet. FTP is generally used to download and upload files; it is not designed for clients to execute the data from the remote file system directly. Some examples of FTP server software are FileZilla and Microsoft Internet Information Services.

**Application Software**:

* **Database:** A database is **an organized collection of structured information, or data, typically stored electronically in a computer system**.
* A database is usually controlled by a database management system (DBMS).The data can then be easily accessed, managed, modified, updated, controlled, and organized.
* Types of databases:
  + [**Relational databases**](https://www.oracle.com/database/what-is-a-relational-database/)**:**Items in a relational database are organized as a set of tables with columns and rows. Relational database technology provides the most efficient and flexible way to access structured information.
  + **Object-oriented databases:** Information in an object-oriented database is represented in the form of objects, as in object-oriented programming.
* **Distributed databases :** A distributed database consists of two or more files located in different sites. The database may be stored on multiple computers, located in the same physical location, or scattered over different networks.
* **NoSQL databases:** A [NoSQL](https://www.oracle.com/database/nosql-cloud.html), or nonrelational database, allows unstructured and semi-structured data to be stored and manipulated. NoSQL databases grew popular as web applications became more common and more complex.
* **Cloud databases:** A [cloud database](https://www.oracle.com/database/what-is-a-cloud-database/) is a collection of data, either structured or unstructured, that resides on a private, public, or hybrid cloud computing platform.

**Web**:

* The Web is the common name for the World Wide Web, a subset of the Internet consisting of the pages that can be accessed by a Web browser.
* Web pages are formatted in a language called Hypertext Markup Language (HTML). It this language that allows users to click through pages on the Web via links.
* The Web uses HTTP protocol to transmit data and share information. Browsers such as Internet Explorer, Google Chrome or Mozilla Firefox are used to access Web documents, or Web pages, which are connected via links.
* The Web is just one of the ways that information is shared over the Internet; others include email, instant messaging and File Transfer Protocol (FTP).

**Shared resources**:

* Shared resources, also known as network resources, refer to computer data, information, or hardware devices that can be easily accessed from a remote computer through a local area network (LAN) or enterprise intranet. E.g. files, data, multimedia and hardware resources like printers, fax machines and scanners.
* Printer sharing is the process of allowing multiple computers and devices connected to the same network to access one or more printers.
* In Windows 7 and 8, the printer sharing function can be activated in the Control Panel as follows: click on the Network and Sharing Center icon and then click "Change advanced sharing settings"; under "File and printer sharing", select the "Turn on file and printer sharing" radio button.

**Voice over Internet Protocol (VoIP):**

* Voice over Internet Protocol (VoIP), is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line.
* Some VoIP services may only allow you to call other people using the same service, but others may allow you to call anyone who has a telephone number - including local, long distance, mobile, and international numbers.
* Also, while some VoIP services only work over your computer or a special VoIP phone, other services allow you to use a traditional phone connected to a VoIP adapter.

**Mobile Working:**

* A mobile workforce is **a group of employees that isn't bound by a central physical location**. Instead, the employees are connected by various types of mobile technology: computers, smartphones and other mobile devices.
* The idea of a mobile workforce goes well beyond simply working from home.

**Authentication**:

* Authentication is **the process of recognizing a user's identity**.
* Different systems may require different types of credentials to ascertain a user's identity. The credential often takes the form of a password, which is a secret and known only to the individual and the system.
* **User Authentication:**
  1. Identification. Users have to prove who they are.
  2. Authentication. Users have to prove they are who they say they are.
  3. Authorization. Users have to prove they're allowed to do what they are trying to do.
* **Hardware Authentication:**
* Endpoint authentication is a security mechanism designed to ensure that only authorized devices can connect to a given network, site or service. The approach is also known as device authentication. ... The password response sent from the registered device verifies that the user is connecting from an authorized endpoint.