**Practical - 1**

* WHAT IS NIC

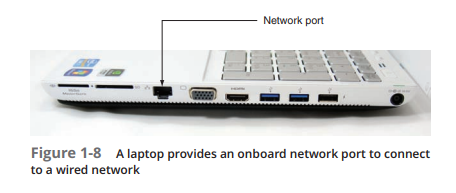
A network interface card (NIC) is a hardware component, typically a circuit board or chip, installed on a computer so it can connect to a network. Modern NICs provide functionality to computers, such as support for input/output interrupt, direct-memory access interfaces, data transmission, network traffic engineering and partitioning.

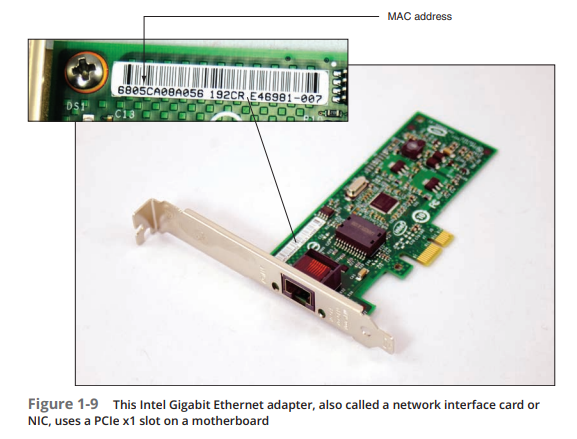
A NIC provides a computer with a dedicated, full-time connection to a network. It implements the physical layer circuitry necessary for communicating with a data link layer standard, such as Ethernet or Wi-Fi. Each card represents a device and can prepare, transmit and control the flow of data on the network.

* TYPES OF NIC

**Internal Network Cards**

In internal networks cards, motherboard has a slot for the network card where it can be inserted. It requires network cables to provide network access. Internal network cards are of two types. The first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA).





**External Network Cards**

In desktops and laptops that do not have an internal NIC, external NICs are used. External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network. They are useful while traveling or accessing a wireless signal.



* HOW NIC WORKS

It is a physical card or chip, which contains MAC addresses, helps to identify the device on the network.

NIC works on the physical layer and the data-link layer. Actually, NIC collects the data from the computer and sends it to the transmission Channel. It acts as a middleman between your computer and the data network. It is responsible to exchange the computer's data with a network. Any incoming data that comes from the network medium is received by the NIC

**How NIC transmits the data?**

* For outgoing data, first, the network protocol transfers a packet to the buffer which presents on the NIC card
* Then the source and destination MAC address are attached as the frame header and calculate the CRC
* CRC (Cyclic Redundancy Code) is a numerical value, is a powerful type of checksum, which has the purpose of detecting errors
* Lastly, NIC transmits frames onto the medium as bit signals.

**How NIC receive the data?**

* Bit signals travel along with the medium and are recerved by NIC, then the received bits are formatted into a frame
* First, CRC (a type of checksum) is calculated and compared to CRC in the frame trailer
* If they don't match that means the frame is damaged or changed, and frame is discarded
* If CRC is okay, then the destination MAC address is checked.
* Once the MAC address is checked and verified, the frame header and trailer are romoved and the packet comes out from for further processing the frame which is sent to the network protocol for further processing.

* WHAT ARE THE COMPONENTS OF NIC

Network Interface Card contains the following essential components -

1. Memory

Memory is one of the most important components of the NIC. It is used to store the data during communication.

2. Connectors

connectors are used to connect the cables to the Ethernet port.

3. Processor

Processor is used for converting the data message into a suitable form of communication.

4. Jumpers

Jumpers are the small device that is used to control the communication operations without the need of any software. It is also used to determine settings for the interrupt request line, I/O address, upper memory block, and type of transceiver.

5. Routers

To provide wireless connectivity, routers are used.

6. MAC address

MAC address is also referred to as a physical network address. It is a unique address that is present to the network interface card where ethernet packets are communicated with the computer.

* ADVANTAGES AND DISADVANTAGES

**Advantages of NIC**

A list of advantages of NIC is given below -

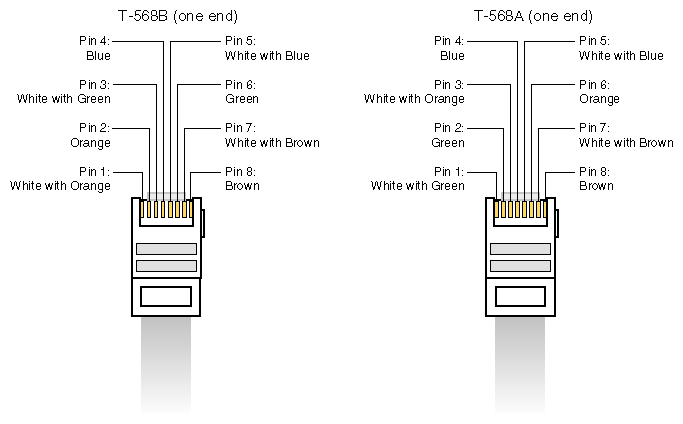
* As compared to the wireless network card, NIC provides a secure, faster, and more reliable connection.
* NIC allows us to share bulk data among many users.
* It helps us to connect peripheral devices using many ports of NIC.
* Communication speed is high.
* Network Interface cards are not expensive.
* NICs are easy to troubleshoot.

**Disadvantages of NIC**

A list of disadvantages of NIC is given below -

* NIC is inconvenient as compared to the wireless card.
* For wired NIC, a hard-wired connection is required.
* NIC needs a proper configuration to work efficiently.
* NIC cards are not secure, so the data inside NIC is not safe.

ETHERNET



* WHAT IS ETHERNET

Ethernet is the most widely used LAN technology and is defined under IEEE standards 802.3. The reason behind its wide usability is that Ethernet is easy to understand, implement, and maintain, and allows low-cost network implementation. Also, Ethernet offers flexibility in terms of the topologies that are allowed. Ethernet generally uses a bus topology. Ethernet operates in two layers of the OSI model, the physical layer and the data link layer. For Ethernet, the protocol data unit is a frame since we mainly deal with DLLs. In order to handle collisions, the Access control mechanism used in Ethernet is CSMA/CD.

Although Ethernet has been largely replaced by wireless networks, wired networking still uses Ethernet more frequently. Wi-Fi eliminates the need for cables by enabling users to connect their smartphones or laptops to a network wirelessly. The 802.11ac Wi-Fi standard offers faster maximum data transfer rates when compared to Gigabit Ethernet. However, wired connections are more secure and less susceptible to interference than wireless networks. This is the main justification for why so many companies and organizations continue to use Ethernet.

* WHY IS EHTERNET USED

Over the last few years, Wi-Fi has grown in popularity. Technology advancements have resulted in Wi-Fi with better speeds and more consistent coverage. Wi-Fi signals can only handle a certain number of devices at any given moment. Because there are so many Wi-Fi-enabled gadgets competing for signal, the service may be weak or inconsistent. In old buildings, Wi-Fi drop zones are frequent. When Wi-Fi signals pass through barriers, they can become poor. Other common household items can also interfere with Wi-Fi signals like such as wireless telephones, TV satellite receiver, microwave etc.

* ADVANTAGES AND DISADVANTAGES

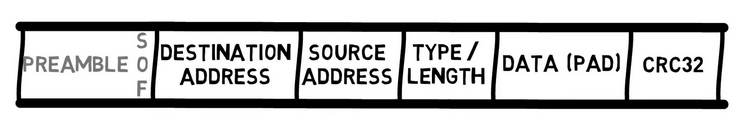
Advantages of Ethernet :

* The fastest speed provide by Gigabit ethernet is of 1Gbps. The speed ranges from more than 10 times Fast Ethernet.
* To form an Ethernet, we don’t need much cost. It is relatively inexpensive. Total cost induced is less.
* In Ethernet, all the node have an equivalent privileges. It does not follow client-server architecture.
* It does not require any switches or hubs
* Maintenance and administration are simple.
* The cable wont to connect systems in ethernet is strong to noise.
* As it is strong to the noise, the standard of the info transfer doesn’t degrade. The data transfer quality is good.
* With latest versions such as gigabit ethernet and wireless ethernet (IEEE 802.11ac/11ad) transfer speeds in data with the speed of 1-100Gbps.

Disadvantages of Ethernet :

* It offers a nondeterministic service.
* It doesn’t hold good for real-time applications because it requires deterministic service.
* As priority packets cannot be set, it’s not suitable for a client-server architecture.
* In an interactive application, data is extremely small and wish quick data transfer. In ethernet, there’s a limit of the minimum size of the frame to 46B. As a result, it’s not an honest choice for interactive applications.
* If you’re using it for interactive applications, you’ve got to feed dummy data to form the frame size 46B which is mandatory.
* Not suitable for traffic-intensive applications. In case the rate of traffic on the Ethernet goes up the efficiency of the Ethernet goes down.
* It provides connectionless communication over the network.
* The receiver cannot able to send any knowledge after receiving the packets.
* If there’s any problem in ethernet, it’s difficult to troubleshoot what cable or node within the network causing an actual problem.
* The 100Base-T4 version does not support full-duplex data communication mode.
* HOW ETHERNET WORKS

**Ethernet Frame Overview**

****

Ethernet works by breaking up information being sent to or from devices, like a personal computer, into short pieces of different sized bits of information called frames. Those frames contain standardized information such as the source and destination address that helps the frame route its way through a network.

And because computers on a LAN typically shared a single connection, Ethernet was built around the principal of CSMA/CD, or carrier-sense multiple access with collision detection. Basically, the protocol makes sure that the line is not in use before sending any frames out. Today, that is far less important than it was in the early days of networking because devices generally have their own private connection to a network through a switch or node. And because Ethernet now operates using full duplex, the sending and receiving channels are also completely separate, so collisions can't actually occur over that leg of their journey.

* EVOLUTION OF ETHERNET

- The History of Traditional Ethernet

First developed by Xerox PARC in the 1970s and ratified by IEEE as a standard in 1983, the evolution of Ethernet has taken this LAN technology through dozens of specifications.

For hundreds of years, scientists believed a mysterious substance known as ether served as the medium for light to disperse through space.

The notion was ultimately dismissed once physicists discovered that photons act as both particles and waves. But the archaic word lives on in the modern term Ethernet - the technology by which bits of information travel through complex computer networks.

- Traditional Ethernet - The First Local Area Network (LAN)

The first LAN in the world was the original version of Ethernet. Robert Metcalfe and his coworkers at Xerox designed it more than forty years ago. On May 22, 1973, Bob Metcalfe (then at the Xerox Palo Alto Research Center, PARC, in California) wrote a memo describing the Ethernet network system he had invented for interconnecting advanced computer workstations, making it possible to send data to one another and to high-speed laser printers.

The first Ethernet standard was published in 1980 by a consortium of Digital Equipment Corporation, Intel, and Xerox (DIX). Metcalfe wanted Ethernet to be a shared standard from which everyone could benefit, and therefore it was released as an open standard.

- The History of Carrier Ethernet

Carrier Ethernet (CE) is a marketing term for extensions to Ethernet to enable telecommunications network providers to provide Ethernet services to customers and to utilize Ethernet technology in their networks. The CE story is today moving on. New capabilities and features are being deployed that go further than the minimum requirements established by the Metro Ethernet Forum (MEF), ushering in the age of Carrier Ethernet (CE).

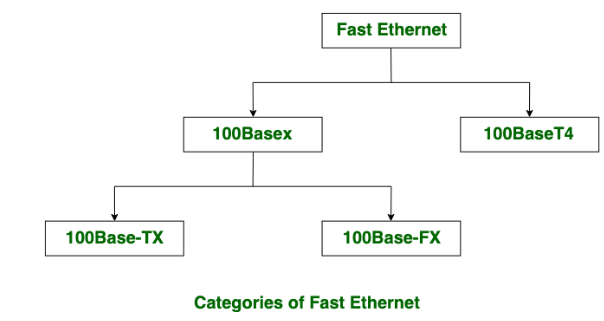
Carrier Ethernet supports 802.1ad Provider Bridging and can deliver and transport MEF services using MPLS/ H-VPLS and PBB-TE technologies, along with SDH-like 50ms restoration capabilities. By supporting these important technologies, Carrier Ethernet enables carriers to leverage existing network investments and select, mix, and match the wide-area services that best meet their needs today and in the future.

* TYPES OF ETHERNET

Fast Ethernet is the Successor of 10-Base-T Ethernet. It is more popular than Gigabit Ethernet because its configuration and implementation is simple. It is faster than its successors. Its variants are:

* 100Base-T4
* 100Base-Tx
* 100Base-Fx

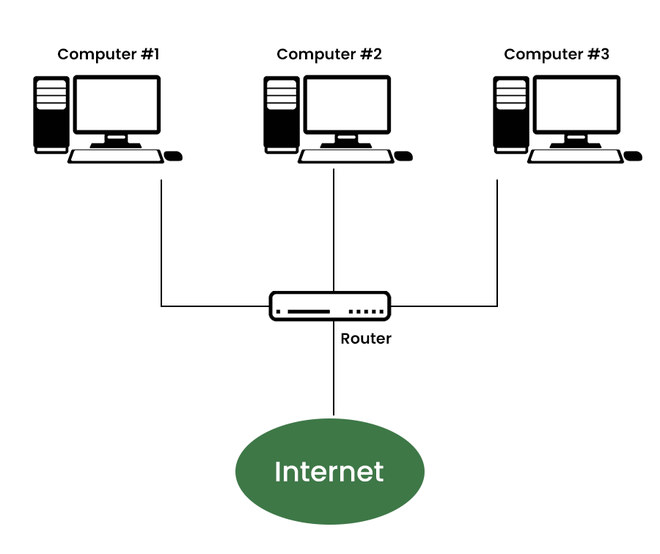
The coverage limit of Fast Ethernet is up to 10 km and its round-trip delay in Fast Ethernet is 100 to 500 bit times.



Gigabit Ethernet was created to provide greater transmission rates of up to 1 Gbps and covers a distance of up to 70 kilometres. The initial goal was to create a system that could be used with existing networking hardware. It is based on Ethernet protocols like CSMA/CD and supports both full duplex and half duplex modes, like fast Ethernet. The IEEE 802.3ab standard established the applicability of Gigabit Ethernet for 1000 Base T networks while also permitting the use of existing UTP cabling.

**PRACTICAL 3**

**INTERNET**



* WHAT IS INTERNET

The Internet is a global network of billions of computers and other electronic devices. With the Internet, it's possible to access almost any information, communicate with anyone else in the world, and do much more.

You can do all of this by connecting a computer to the Internet, which is also called going online. When someone says a computer is online, it's just another way of saying it's connected to the Internet.

* WHO INVENTED INTERNET

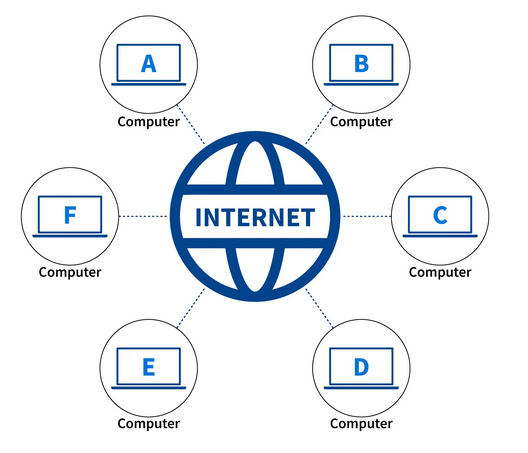
The internet has been the result of gradual development rather than a flash of inspiration that can be attributed to a single person. There are definitely some key figures along this path who deserve to be celebrated.

Like many of the technologies that we take for granted nowadays, it got its start during the Cold War as the U.S. government sought to gain an edge over its bitter rival, the Soviet Union. In 1957 the USSR successfully launched the world’s first satellite into orbit, a move that is widely seen as marking the start of an era in which these two global powers battled for technological supremacy. This was reflected in the foundation of new U.S. government programs such as the National Aeronautics and Space Administration (NASA) – as well as a key player in our story, the U.S. Department of Defense’s Advanced Research Projects Agency (ARPA).

Computer scientists Vinton Cerf and Robert Kahn can be found on every shortlist of people credited as inventors of the internet. This is because they came up with the Transmission Control Protocol and Internet Protocol (TCP/IP), aka the standard for how information is shared between different networks.

* HOW DOES INTERNET WORS

An internet is a huge network of networks that helps us to connect millions of computers together. These computers that are connected to each other through the internet can interact with each other over the internet.



The Internet operates on a technique called packet switching. In packet switching, the data that is transferred among the different computers on the internet are transmitted in the form of packets. These packets contain information about the error control mechanisms, the address of the destination, and also the sequence in which the packets are to be transmitted.

Nowadays, whatever we do is directly or indirectly related to the internet. We chat with our friends on various social networking websites which actually use the internet to send messages. We order food using different mobile applications which also use the internet.

Internet uses a packet switching technique to transmit the data. Thus, the data to be sent is divided into packets and the data is sent in the form of packets only. Each packet of data contains various information like the address of the destination, error control information, etc.

Internet majorly uses protocols called Internet Protocol (IP) and Transmission Control Protocol (TCP) to transmit data from one computer to another.

Internet Protocol (IP) The internet protocol is a network layer protocol that is responsible for defining the rules that define how the information is sent over an internet connection from one computer to another.

Internet Protocol is responsible for gathering the addresses to which the data is to be transmitted.

Transmission Control Protocol (TCP) The transmission control protocol (TCP) is a transport layer protocol that works along with the internet protocol to transmit data over the internet. It is a connection-oriented and reliable protocol i.e. it establishes the connection first and then only, sends data over the established connection hence, there is no packet loss in the transmission control protocol.

Transmission Control Protocol is responsible for the delivery of data once the Internet protocol gets the IP address of the destination.

Also, there are several other protocols that are used by the internet for different purposes. For example, it uses Simple Mail Transfer Protocol (SMTP) to send mail from one client to another, it uses File Transfer Protocol (FTP) to transfer files over the internet, it uses Hypertext Transfer Protocol (HTTP) through which a browser (client) can interact with the internet server.

* ADVANTAGES AND DISADVANTAGES

Advantages of Internet -

* Connectivity − As we know we are connected to the internet to stay connected with our family, friends, colleagues, services, etc.
* Information − We can search and get many search results for our questions and the information can increase knowledge.
* Online Payment − Using payment modes such as Paytm, GPay, and Bhim UPI are many payment methods to pay online.
* Digital Marketing − We are making our websites and making business online.
* Net Banking Services − Banking services such as payment, debit, credit, changing our details, and scheduling payment are an integral part of secure payment.
* Productive Collaboration − As we experienced, after the Covid pandemic, we have worked from home and made things work better than ever before by connecting through video conferencing and saving mobility.

Disadvantages of Internet -

* Wastage of time − Considering today’s lifestyle, one prominent advantage of the Internet is addiction. People are getting addicted to the internet, watching videos and reels without realizing they are wasting so much of their time.
* Cybercrime − It is increasing rapidly as more information is shared and getting leaked.
* Accessibility of pornographic content − It is accessible to even children since there is complex information shared every day and it is hard to figure out the source of these images and videos. This is a big concern regarding children and their minds, parental security is necessary on mobile phones being used by children.
* Identity theft − It is one major concern on a bigger level such as higher organizations, government, and private sectors.
* Increase in cyber attacks in the banking sector and corporate sector − Information is getting leaked, shared, and misused for harm, theft, privacy violation, and harassment.
* Fake Information or Misleading − People nowadays can easily manipulate any information and reclaim it to be true this could mislead people and their reliability towards information shared.
* WHAT IS INTRANET

An intranet is a private network contained within an enterprise that is used to securely share company information and computing resources among employees. An intranet can also be used for working in groups and teleconferences.

Intranets encourage communication within an organization. They let employees easily access important information, links, applications, forms and databases of company records. A database that includes all the usernames of employees who have access rights to the network is often used to maintain intranet security.

* HOW INTRANET IS USED
* Central repository. Intranets become the main repository where important information and company data are stored.
* Collaboration. These internal networks provide a way to share information that makes it easier for employees to work together.
* Personalization. Intranets provide personalized content to employees based on their role within the company.
* Communication. They make employee directories, company news and organization charts readily available, improving internal corporate communications.
* Easy access to information. Intranets provide easy access to information about company policies, benefits and updates.
* Social elements. Social media features let employees create an account, post content and status alerts and browse a newsfeed.
* Project management. To-do lists, employee directories, status updates and other resources aid users in project management.
* Automation. Intranets streamline everyday activities by helping to automate repeatable tasks
* HOW INTRANET WORKS

A secure and reliable intranet requires a web server that manages requests for data hosted on the server. The web server finds requested files and delivers them to the appropriate user. A content management system should also be set up to control the creation, publication and management of intranet content.

An intranet may also consist of many interlinked local area networks (LANs), as well as leased lines connecting to wide area network resources. The intranet's web server uses TCP/IP, HTTP and other internet protocols. Typically, an intranet includes connections through one or more gateway computers to the outside internet and external resources.

To access their company intranet, employees must have a special network password and be connected to the company LAN. Remote employees access the intranet through a virtual private network (VPN) or another secure connection. The VPN lets users not actually connected to the required LAN sign into the intranet and access all the same information and functions that would be available had they been connected to the LAN.

* ADVANTAGES AND DISADVANTAGES OF INTRANET

Advantages of Intranet :

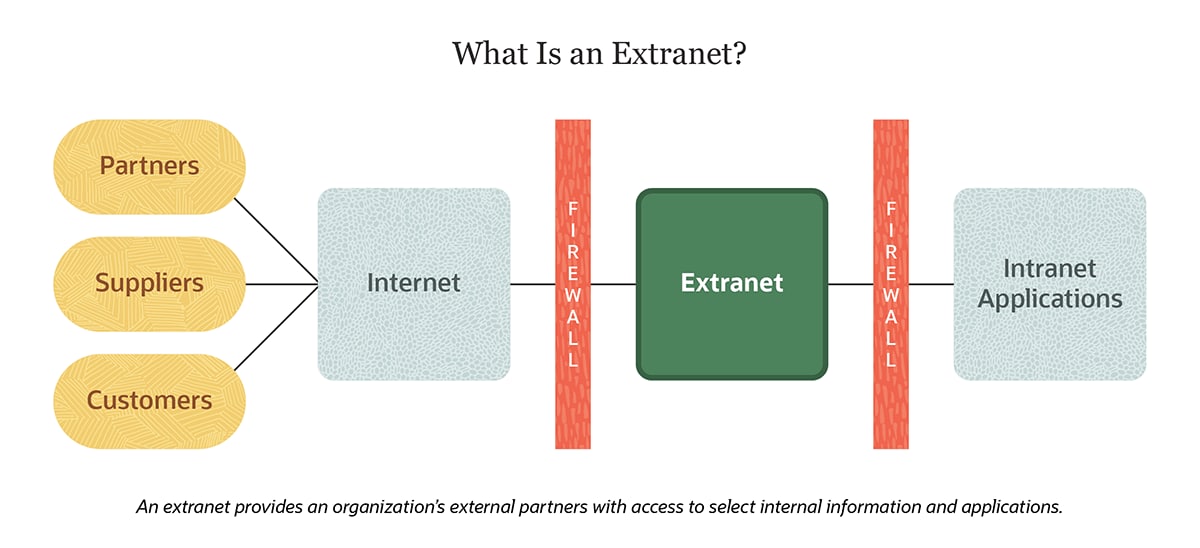
* Cost : The cost of conveying data utilizing the intranet is very low. The entire association can utilize the administrations of the intranet for a low membership charge. Also, there is no cost engaged with upkeep, printing, and others. This makes the intranet exceptionally savvy.
* Accessibility : Utilizing intranet workers can get to their data whenever and anyplace. Workers don’t need to sit infront of the PC. With the administrations of the cloud gateway, information can be gotten to in a split second any place you are on the planet. This makes turn out simpler for the representatives who are continually on the movement for their business.
* Data Exchange : Intranet can be utilized as a correspondence center point where workers store data at whatever point they needed. Inside a few seconds, records can be gotten to just as downloaded. Thus, organizations can guarantee that the data can connect with each condition of the organization.
* Correspondence : Intranet permits quick and conservative methods of correspondence inside an association. That too bothly (level just as vertical). In spite of the actual area, an intranet can alter, remark, and store information. The two organizations contain the choices of talks, gatherings, and messages so workers are allowed to communicate their suppositions. It additionally diminishes travel time as workers as representatives in the business undertakings can speak with one another with simply a solitary snap.
* Profitability : By and large, the profitability can be seen expanded utilizing intranet. It makes all the information promptly accessible so laborers won’t discover hard to look through them. In this manner, representatives can convey their work all the more productively and precisely. In the event that additional time is spent on finding the necessary records, it can contrarily affect the organization’s efficiency. Aside from the laborers, directors also can be profited by the intranet efficiency. The chief can invest more energy in investigating data.

Disadvantages of Intranet :

* Usage : The expense of actualizing intranets is normally high (Depending on the sort of intranet arrangements and the number of clients). Furthermore, it needs separate preparation and redesign for utilizing the intranet arrangement adequately. All these require time and exertion which makes troublesome the execution cycle.
* Unpredictability : Intranets are viewed as unpredictable in nature. Because of their multifaceted nature, numerous workers feel overpowered and reluctant to utilize it. And furthermore, intranet clients need to do isolate organizations which can be tedious.
* Security : Al however intranet frameworks do contain numerous safety efforts, it is as yet helpless against security hazards. Except if there are firewalls or entryways, your private information can be gotten to by an outsider. Along these lines, when utilizing the intranet there is a deficiency of security for the corporate.
* Onboarding : On intranet consistently the workers should be fulfilled for the purpose of dispatch. In the event that there is no esteemed substance, staff won’t utilize it any longer. In this manner, content assumes a significant part here.
* Updates : An intranet arrangement that gets oftentimes refreshed is less inclined to convenience issues. In any case, the issue stays in discovering one. It tends to be incredibly testing to discover an intranet arrangement that remains refreshed. These sorts of intranet frameworks most on occasion need client service. Henceforth, representatives of the organization will have an issue embracing it.
* WHAT IS EXTRANET

An extranet is a controlled private network, defined by Gartner as “a collaborative, internet-based network that facilitates intercompany relationships by linking an enterprise with its suppliers, customers or other external business partners.” Employing internet-derived applications and technology, organizations create extranets to securely extend their internal business data and processes to partners outside their four walls.

From a networking perspective, an IT team creates an extranet when they take an application built for internal users, often on their intranet, and extend it to select business partners or customers. The extranet can be used only by individuals who are granted secure access credentials.



* HOW EXTRANET WORKS

An extranet is implemented as a Virtual private network (VPN) that provides secure communication between the organizations. VPN creates a secure connection over a public network such as the internet. The VPN is formed on Internet Protocol security (IPsec) which provides an extra layer on the already present TCP/IP i.e. Transmission Control Protocol/ Internet Protocol.

The IPsec connection (tunneling) provides:

* Privacy: To maintain confidentiality between the sources.
* Integrity: To protect and share the data securely between the resources.
* Authentication: To allow only authorized users on the network.

IPsec Protocols: It makes use of two protocols Authentication Header (AH) or Encapsulating Security Payload (ESP). One or both of them could be used to protect the IP packet. Which protocol to used depends on the security needs of the network.

* Authentication Header (AH): It is used only for authentication and does not provide encryption. Data origin authentication, integrity, and anti-replay services are provided.
* Encapsulating Security Payload (ESP): It provides authentication, data integrity, anti-replay, and encryption. Both authentication and encryption services can be used or only one of them could be used while using these protocols.
* ADVANTAGES AND DISADVANTAGES OF EXTRANET

Advantages

* Security: Extranet is formed as a Virtual private network (VPN) as it assures a protected and secure communication across the network. The information shared between the organizations could be highly confidential and an extra level of security makes sure that none of it is lost or accessed by anyone else other than the parties involved.
* Data: Sometimes there could be a large amount of data to be transferred between organizations. An extranet allows a large amount of data transfer across the network in a secure fashion.
* Network Sharing: One or multiple organizations could connect via the extranet. For example, three organizations collaboratively working on the same project could make use of an extranet or an e-commerce site sharing its network with various small businesses.
* Communication: It is a medium for internal and external members to connect or organizations to connect to third parties. Instead of allowing third parties in the company’s intranet network and giving access to the internal resources, the extranet provides a lot more flexibility and security for everyone to communicate.

Disadvantage

* Complex Security: Extranet needs an additional firewall if hosted on its own server which expands workload and complex security mechanism.
* Hosting: Hosting could be an issue as it requires a high bandwidth internet connection. A High bandwidth internet connection may not be possible for everyone, which would lead to inefficiency in work.
* Expensive: It is costly compared to intranet due to the extra layer of security and hosting charges.
* limited: It can only be accessed through the internet. So, the work would came to halt or slow down if the internet goes down.

|  |  |  |
| --- | --- | --- |
| **Address Class** | **Range** | **Default Subnet Mask** |
| A | 1.0.0.0 to 126.255.255.255 | 255.0.0.0 |
| B | 128.0.0.0 to 191.255.255.255 | 255.255.0.0 |
| C | 192.0.0.0 to 223.255.255.255 | 255.255.255.0 |
| D | 224.0.0.0 to 239.255.255.255 | Reserved for Multicasting |
| E | 240.0.0.0 to 254.255.255.255 | Experimental |

Note : Class A addresses 127.0.0.0 to 127.255.255.255 cannot