





KEMENTERIAN PENGAJIAN TINGGI

ELECTRICAL ENGINEERING DEPARTMENT

Learn & Explore

DEP 50033

vol.1

Create a proper network technology design

RAHIMAH BINTI ABDUL RAHMAN SHARIPAH BINTI DAUD NORSYIRA ZURAIZA BINTI OMAR

INTRODUCTION TO NETWORKING

AUTHORS RAHIMAH BINTI ABDUL RAHMAN SHARIPAH BINTI DAUD NORSYIRA ZURAIZA BINTI OMAR

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher at the address below.

> Politeknik Tuanku Sultanah Bahiyah (PTSB) Kulim Hi-Tech Park, 09090 Kulim, Kedah.

> > e ISBN 978-967-2740-32-2

ABOUT THE AUTHORS

RAHIMAH BINTI ABDUL RAHMAN

Rahimah binti Abdul Rahman. Kulim Kedah. PhD in Professional & Teacher Education from University Science Malaysia, Penang (2020), M.Ed in TVET from University Tun Hussein Onn Malaysia (2007),B.eng Electrical Engineering in (Communication) from Colledge University Tun Hussein Onn (2005). Politeknik Sultan Abdul Halim Muadzam Shah (2007-2012), Politeknik Tuanku Sultanah Bahiyah (2011- Now). Experienced in teaching variety of Electrical and Electronic Engineering subjects.

SHARIPAH BINTI DAUD

Sharipah binti Daud. Pendang Kedah. M.Eng. in Electronic System from University Technical Malaysia, Malacca (2016), B.eng in Electrical Engineering from University Techology Mara (2007).Silterra (M) Sdn Bhd (2007–2008). Politeknik Sultan Abdul Halim Muadzam Shah (2008–2011), Politeknik Tuanku Sultanah Bahiyah (2011– Now). Experienced in teaching variety of Electrical and Electronic Engineering subjects.



NORSYIRA ZURAIZA BINTI OMAR



Norsyira Zuraiza Binti Omar. Kulim Kedah. MEng (Hons) in Electrical-Electronic Engineering (Telecommunication) from University Technology Malaysia, Johor (2010), B.Eng in Electronic Engineering from Staffordshire University, United Kingdom (2005). Agilent Technologies (M) Sdn Bhd (2006-2008), Politeknik Sultan Abdul Halim Muadzam Shah (2009-2013), Politeknik Tuanku Sultanah Bahiyah (2013- Now). Experienced in teaching variety of Electrical and Electronic Engineering subjects.



In the name of Allah, the Most Gracious an the Most merciful, Alhamdulillah, all the praises to Allah for the strength and His Blessings in completing this eBook.

We would like to express our appreciation to the Department of Polytechnic education, which gave us the idea to produce this eBook. Our sincerest appreciation also to Pn Ida Safinar as Head of Electrical Department of Polytechnic Tuanku Sultanah Bahiyah, Kedah for helping us with motivation, guidance and inspiration that help us to finish the eBook. We owe a profound feeling of appreciation for our deepest gratitude goes to our beloved parents and families for their endless love prayers and encouragement. To those who indirectly contributed to this eBook, your kindness means a lot to us. Finally, we would like to thank each other. None of us alone could have accomplished the work. Working with the team was always a privilege.





DATA COMMUNICATION AND NETWORKING exposes to the principle of data communication and networking. This e-books focus on basic concept of data communication and networking fundamental for a quality data transmission.

This e-books consists to Open Systems Interconnection (OSI) Model and Network Protocol. Other than that, this e-books covered the Introduction to Local Area Network and public digital network.





1 INTRODUCTION TO NETWORKING BASIC CONCEPT AND ELEMENTS OF COMPUTER NETWORK

DEFINE COMPUTER NETWORK FUNDAMENTAL TYPES OF NETWORKS THE COMMON ELEMENTS REQUIRED IN CLIENT/SERVER NETWORK

PG 7 - 42

STZ

Ш

F

Ζ

of CO

U

0

LOCAL AREA NETWORK(LAN) METROPOLITAN AREA NETWORK(MAN) WIDE AREA NETWORK (WAN) GLOBAL AREA NETWORK (GAN)

WIRING STANDARD IN NETWORKING

SET-UP TYPES OF WIRING STANDARD TIA/EIA-568-A OR TIA/EIA-568-B FOR THE NETWORK CABLING PREPARATION VERIFY UTP NETWOK CABLE TESTING USING CABLE TESTER

PG 67 - 82

NETWORK SECURITY

EXPLAINATION OF NETWORK SECURITY TYPES OF NETWORK SECURITY

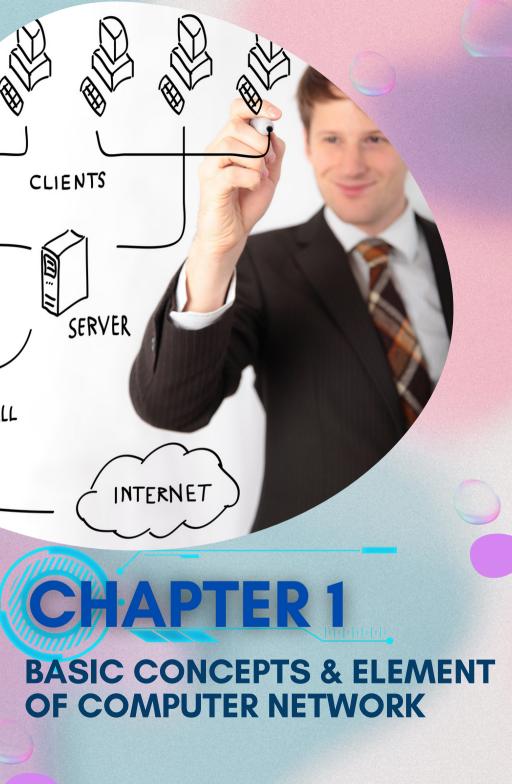
TUTORIAL

QUESTION & ANSWER

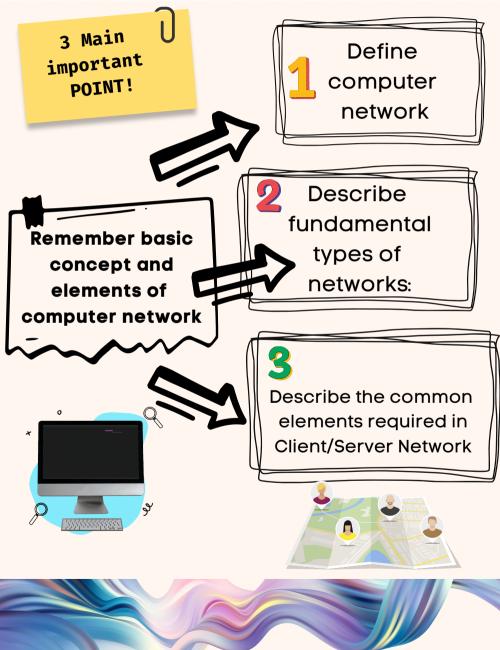
REFERENCES

PG 91- 118

PG 119



CHAPTER 1



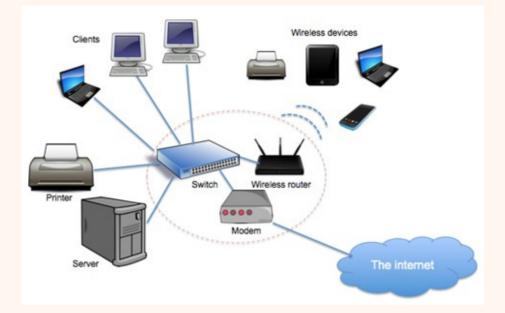
DEFINITION OF COMPUTER NETWORK

Computer networking may be consider a branch of computer science, computer engineering, and telecommunications, since it relies on the theoretical and practical application of the related disciplines. Computer networking was influence by a wide array of technology developments and historical milestones.

A computer network is a set of computers sharing resources located on or provided by network nodes. The computers use common communication protocols over digital interconnections to communicate with each other. These interconnections are made up of telecommunication network technologies, based on physically wired, optical, and wireless radiofrequency methods that may be arranged in a variety of network topologies. The nodes of a computer network can include personal computers, servers, networking hardware, or other specialised or generalpurpose hosts. They are identified by network addresses, and may have hostnames. Hostnames serve as memorable labels for the nodes, rarely changed after initial assignment. Network addresses serve for locating and identifying the nodes by communication protocols such as the Internet Protocol.

Computer networks may be classified by many criteria, including the transmission medium used to carry signals, bandwidth, communications protocols to organize network traffic, the network size, the topology, traffic control mechanism, and organizational intent.

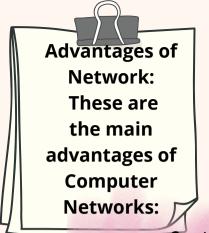
Computer networks support many applications and services, such as access to the World Wide Web, digital video, digital audio, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications.



Example of Computer Network

Advantages of Network: These are the main advantages of Computer Networks:





Etworks: <u>Central Storage of Data</u> Files can be stored on a central node (the file server) that can be shared and made available to each and every user in an organization.

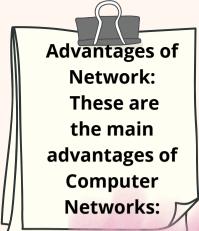
Anyone can connect to a computer network There is a negligible range of abilities required to connect to a modern computer network. The effortlessness of joining makes it workable for even youthful kids to start exploiting the data.

Faster Problem-solving

Since an extensive procedure is disintegrated into a few littler procedures and each is taken care of by all the associated gadgets, an explicit issue can be settled in lesser time.

4 <u>Reliability</u>

Reliability implies backing up information. Due to some reason equipment crashes, and so on, the information gets undermined or inaccessible on one PC, another duplicate of similar information is accessible on another workstation for future use, which prompts smooth working and further handling without interruption.



It is highly flexible

Files can be stored on a central node (the file server) that can be shared and made available to each and every user in an organization.

Security through Authorization Anyone can connect to a computer network There is a negligible range of abilities required to connect to a modern computer network. The effortlessness of joining makes it workable for even youthful kids to start exploiting the data.

D Faster Problem-solving

Since an extensive procedure is disintegrated into a few littler procedures and each is taken care of by all the associated gadgets, an explicit issue can be settled in lesser time.

Reliability Reliability implies backing up information. Due to some reason equipment crashes, and so on, the information gets undermined or inaccessible on one PC, another duplicate of similar information is accessible on another workstation for future use, which prompts smooth working and further handling without interruption.

Disadvantages of Network: These are the main disadvantages of Computer Networks:

1. <u>It lacks robustness</u>

If a PC system's principal server separates, the whole framework would end up futile. Also, if it has a bridging device or a central linking server that fails, the entire network would also come to a standstill. To manage these issues, gigantic systems ought to have a ground-breaking PC to fill in as a document server to influence setting up and keeping up the system less demanding.

2. It lacks independence

PC organizing includes a procedure that is worked utilizing PCs, so individuals will depend on a greater amount of PC work, rather than applying an exertion for their jobs that needs to be done. Besides this, they will be subject to the primary document server, which implies that, in the event that it separates, the framework would end up futile, making clients inactive.

Cont;nue

3. Virus and Malware

On the off chance that even one PC on a system gets contaminated with an infection, there is a possibility for alternate frameworks to get tainted as well. Infections can spread on a system effectively, in view of the availability of different gadgets.

4. Cost of the network

The expense of executing the system including cabling and equipment can be expensive.

PC systems administration will dependably be a quick and advantageous method for exchanging and sharing data, yet individuals ought to know about its outcomes too.

PES OF NET

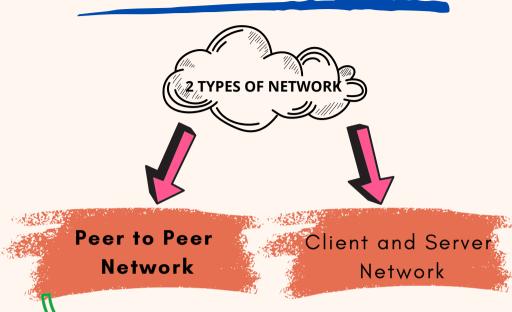
Peer to Peer Network

Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes.

Client and Server

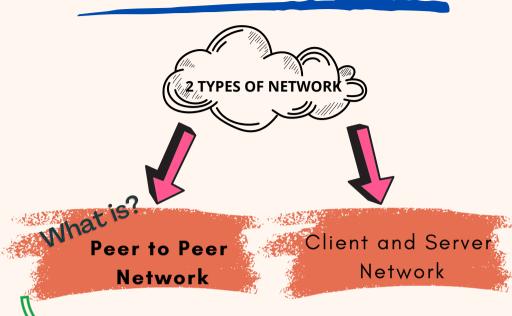
Network

Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts.

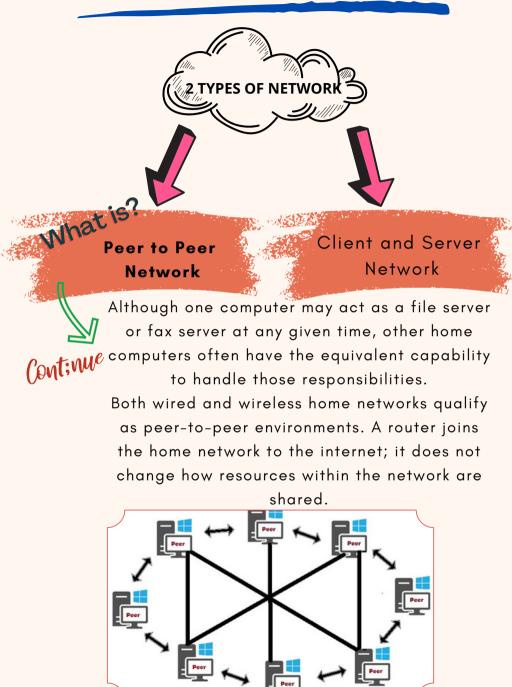


Continue

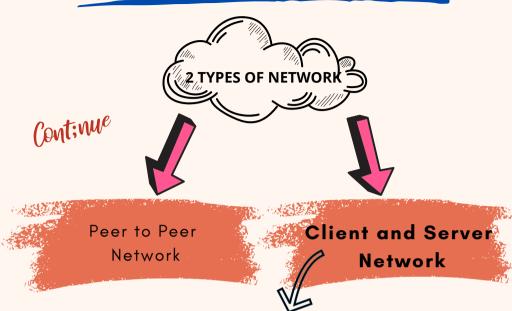
A P2P network connects devices directly without using another computer or device (like a server) as an intermediary. Although they have existed for many years, peer-to-peer computing technologies promise to radically change the future of networking.



Computers in a peer-to-peer network are typically situated physically near each other and run similar networking protocols and software. Before home networking became popular, only small businesses and schools built peer-to-peer networks. Most home computer networks today are peer-to-peer networks. Residential users configure their computers in peer workgroups to allow sharing of files, printers, and other resources equally among all devices.



Peer to Peer Network Diagram

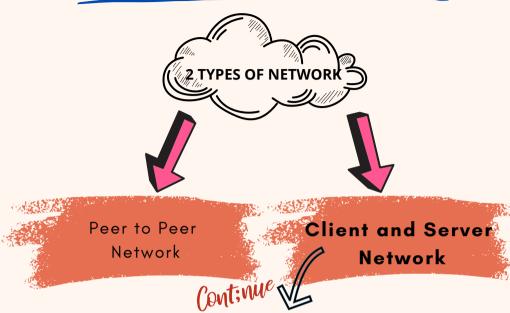


Client-server networking involves a central, powerful computer called a server, and a number of client computers that need to connect to the server to carry out specific tasks.

A server is a computer on a network that provides a resource that can be used by any authorised client station.

The level of access a server grants to a client is an important security consideration. Sometimes the data on a server is designed to be open and therefore the server will respond to any request it receives. In other

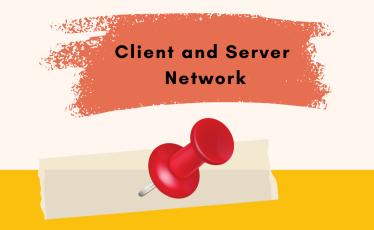
cases the data may be sensitive or commercially valuable, so the server will need to ensure the request is from a legitimate source. If it did not, it would risk exposing the data and potentially the network to malicious actors. Also, backup of data is managed centrally and can be automated in the server.



There are many types of server:

- <u>Web servers</u> are the most common type of server you will interact with. These servers store and provide web pages. This course is stored on a web server; every time you complete a step, your device will request the next one.
- <u>Email servers</u> direct email to the intended recipient and sometimes filter out spam.
- File servers provide files to users.
- <u>Database</u> servers provide data storage and manipulation.

When thinking about servers, most people think of huge stacks in massive warehouses. Whilst these are used by large internet services, there are also other types of servers. Companies can have their private servers for their employees, to access shared work or for video conferencing.



When thinking about servers, most people think of huge stacks in massive warehouses. Whilst these are used by large internet services, there are also other types of servers. Companies can have their private servers for their employees, to access shared work or for video conferencing. With cloud computing, anyone can rent and use a cloud server without having to invest in the physical machine. A client is a computer or computercontrolled device that provides a user with access to a network.

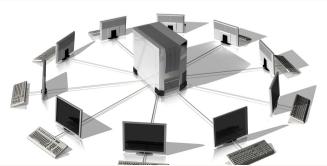
What is? Client

Clients are user-facing computers that run software to make requests to servers, and either interpret or display the responses. In particular, a client sends a request to the server. The server processes the request and then sends a response to the client. Clients do not hold the power to force a server to respond to a request. For example, if the server requires authentication that the client cannot provide, it will not get the data it has requested. Clients do not always have to be on and should be able to start up and connect to a server at any time, which is why it is useful to have servers on all the time. Some clients are dedicated hardware devices – speed cameras are a good example of this. Their entire functionality is to capture photos and license plate numbers, and to send a request to a central server to store and process them. Other clients include the software running on general purpose computers. A lot of applications turn your smartphone into a client. These apps are not processing or computing much themselves, but make requests to servers to do it for them. This model has granted immense computing power to mobile devices, allowing them to perform a wide range of networked tasks.

What is

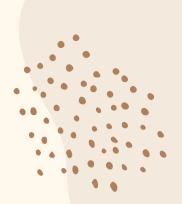
Cont;nue

Client



Client-Server Network Diagram





"Differences Between Peer To Peer (P2P) & Client Server Network (CSN)



Differences between P2P & CSN?

Definition

Peer to peer network is a distributed application architecture that partitions tasks or workloads between peers. Client server network is a distributed application structure based on resource or service providers called servers and service requesters called clients. This constitutes the difference between peer to peer and client server network.



Functionality



The main difference between peer to peer and client server network is that, in peer to peer network, each node can request for services and provide services. Whereas, in client server network, the client requests for service and server responds with a service

Network Type

Another difference between peer to peer and client server network is that the peer to peer network is a decentralized network while client server network is a centralized network.



Differences between P2P & CSN?

Reliability

There are multiple service providing nodes in a peer to peer network. So, it is more reliable. In client server network, the clients depend on the server. Failure in the server will disrupt the functioning of all clients. This is an important difference between peer to peer and client server network.





Access time for services

Moreover, as the service providing nodes are distributed in the peer to peer network, the service requesting node does not need to wait long. On the other hand, in client server network, multiple clients requests for services from a server. Therefore, the access time for a service is higher.

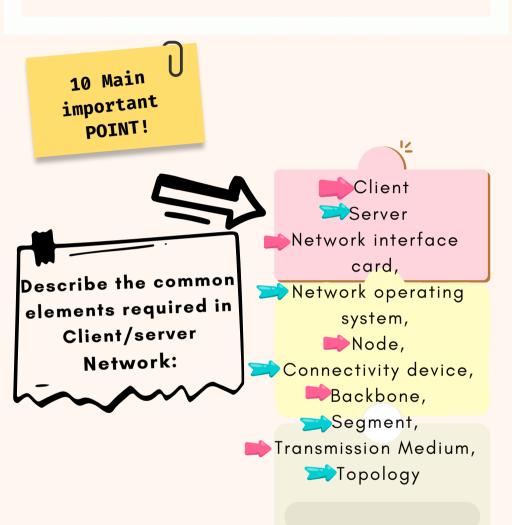
Cost

While a client server network is expensive to implement, a peer to peer does not require extensive hardware to set up the network.

Security

A client server network is more stable and secure than a peer-to-peer network. This is also a difference between peer to peer and client server network.

CHAPTER 1





COMMON ELEMENT REQUIRED IN CLIENT SERVER NETWORK

8 Common Element Required in Client Server Network

Network Interface Card (NIC) Network Operating System(NOS) Node Connectivity devices Topology Transmission media

NETWORK INTERFACE CARD (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.



NETWORK OPERATING SYSTEM (NOS)

A network operating system (NOS) is a computer operating system (OS) that is designed primarily to support workstations, personal computers and, in some instances, older terminals that are connected on a local area network (LAN). The software behind a NOS allows multiple devices within a network to communicate and share resources with each other.

The composition of hardware that typically uses a NOS includes a number of personal computers, a printer, a server and file server with a local network that connects them together. The role of the NOS is to then provide basic network services and features that support multiple input requests simultaneously in a multiuser environment.

NODE

A node is any physical device within a network of other tools that's able to send, receive, or forward information. A personal computer is the most common node. It's called the computer node or internet node. Modems, switches, hubs, bridges, servers, and printers are also nodes, as are other devices that connect over Wi-Fi or Ethernet. For example, a network connecting three computers and one printer, along with two more wireless devices, has six total nodes. Nodes within a computer network must have some form of identification, like an IP address or MAC address, for other network devices to recognize them. A node without this information, or one that's offline, no longer functions as a node.

CONNECTIVITY DEVICE

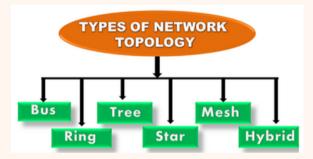


Network devices can relate PCs or other electronic tools to share documents or resources like printers or fax machines. Devices can install a Local Area Network

(LAN) are the general type of network devices used by the public. A LAN needed a hub, router, cabling or radio innovation, connection cards, and a high-speed modem if an online connection is necessary.

TOPOLOGY

Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.



1.BUS TOPOLOGY

The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable. Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable. When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.

RING TOPOLOGY



2.RING TOPOLOGY

Ring topology is like a bus topology, but with connected ends. The node that receives the message from the previous computer will retransmit it to the next node. The data flows in one direction.

The data flows in a single loop continuously known as an endless loop. It has no terminated ends, i.e., each node is connected to another node and has no termination point. The data in a ring topology flow in a clockwise direction.

The most common access method of the ring topology is token passing. Token passing is a network access method in which a token is passed from one node to another node. Token is a frame that circulates around the network.

STAR TOPOLOGY

Star Topology



3.STAR TOPOLOGY

Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.

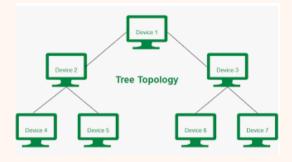
The central computer is known as a server, and the peripheral devices attached to the server are known as clients.

Coaxial cable or RJ-45 cables are used to connect the computers.

Hubs or Switches are mainly used as connection devices in a physical star topology.

Star topology is the most popular topology in network implementation.

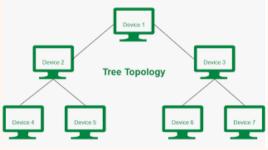
TREE TOPOLOGY



4 .TREE TOPOLOGY

Tree topology combines the characteristics of bus topology and star topology. A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion. The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node. There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

MESH TOPOLOGY



5. MESH TOPOLOGY

Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.

There are multiple paths from one computer to another computer.

It does not contain the switch, hub or any central computer which acts as a central point of communication.

The Internet is an example of the mesh topology.

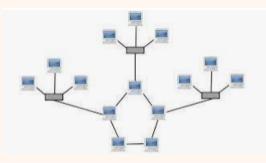
Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.

Mesh topology is mainly used for wireless networks.

Mesh topology can be formed by using the formula:

Number of cables = $(n^{(n-1)})/2$.

HYBRID TOPOLOGY



6. HYBRID TOPOLOGY

The combination of various different topologies is known as Hybrid topology.

A Hybrid topology is a connection between different links and nodes to transfer the data. When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

TRANMISSION MEDIA

1.GUIDED

A transmission medium is a route that transmits information from a source to a receiver. Transmission mediums lie underneath the physical layer and the physical layer regulates them. Communication channels are another name for transmission medium. There are 2 types of transmission media: 1. Guided 2. Unguided

Guided Transmission Media:

Bounded media and wired media are other names for guided transmission media. They consist of cables or wires that transfer data. They go by the name "guided" because they act as a physical link between the transmitter and recipient devices. The physical limitations of the medium limit the signal flowing via these mediums. They are:

Secure high-s<mark>peed l</mark>inks.

Generally used for shorter distances. Some of these most popular guided transmission media are Twisted Pair Cable, Coaxial Cable, and Optical Fibre Optic.

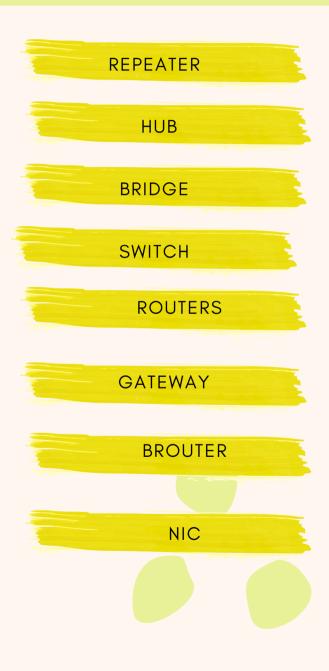
TRANMISSION MEDIA

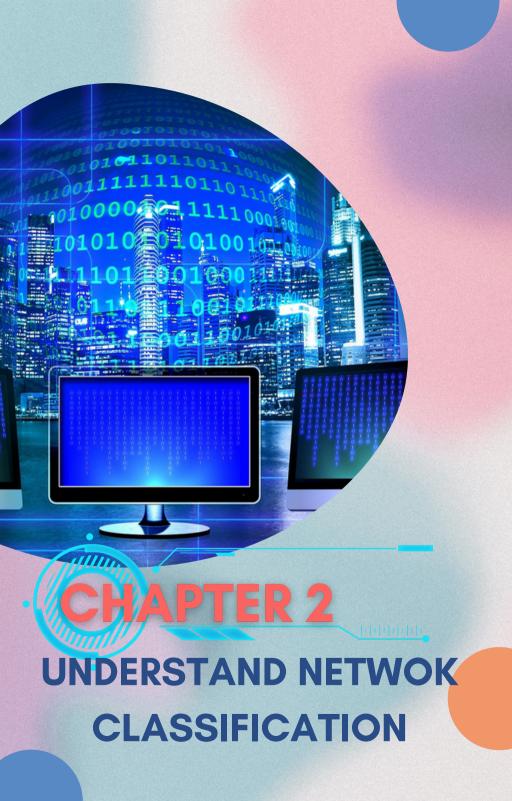
2. UNGUIDED

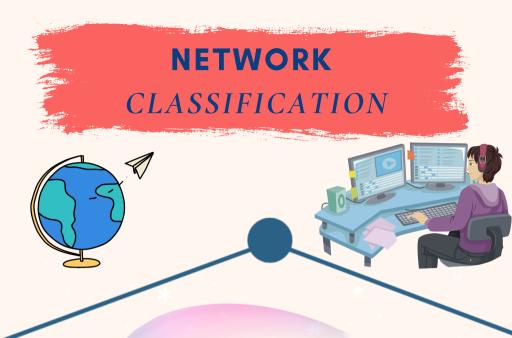
Unguided Transmission Media: Electromagnetic signals can also be transmitted without the use of a physical medium. These are also known as wireless or unbounded transmission media. Some properties of unguided media are: Less secure than guided media. Used for longer distances. Types of Unguided Transmission Media are infrared, radio wave, microwave and light transmission.



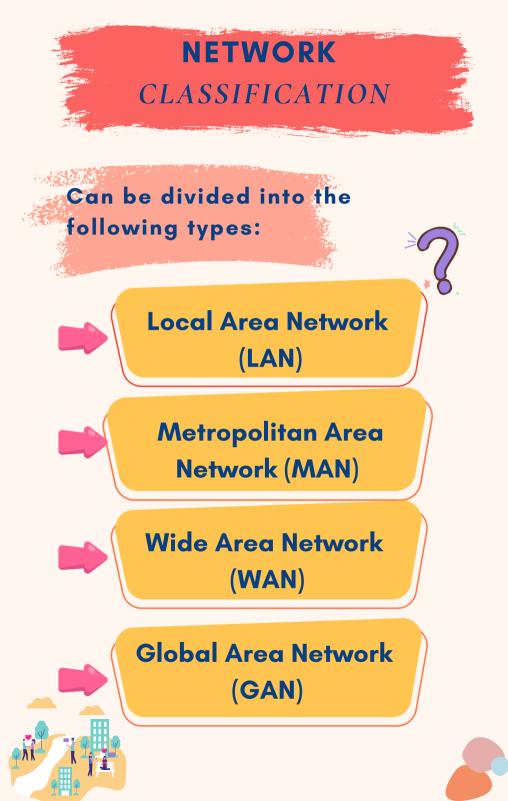
8 TYPES NETWORK DEVICES







A computer network is a system in WHICH MULTIPLE COMPUTERS ARE CONNECTED TO SHARE INFORMATION AND RESOURCES. Computer network varies with each other based on their functionality, geography, ownership, and communication media used.



 Θ

A local area network is a network, which is design to operate over a very small geographical or physical area such as an office, building, a group of buildings, etc.



 $\overline{\mathbf{\Theta}}$

Generally, it is used to connect two or more personal computers through a communication medium such as coaxial, twisted-pair cables, etc.



 Θ

A LAN can use either wired or wireless mode of communication. Wireless media for communication can be termed as WLAN (Wireless Local Area Network)



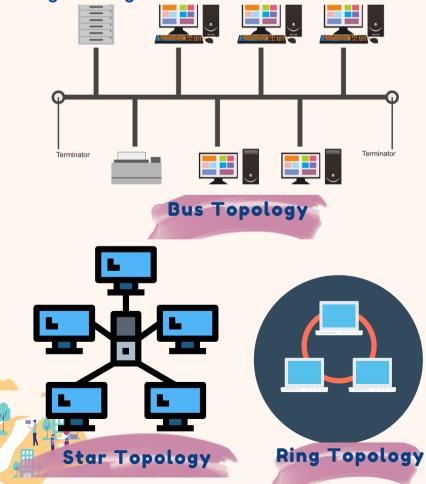
 Θ

LAN existence in around 1970s. IEEE developed the specifications for LAN. The speed of this network varies from 10mbps(Ethernet network) to 1 Gbps(FDDI or Gigabit Ethernet).



Cont; nue

In other word, a LAN connects a relatively small number of machines in a relatively close geographical area. Bus, Ring, and Star topology are generally used in a local area network. In LAN, one computer can become a server in a star topology, serving all other computers called clients. Two different buildings can be connected very easily in LAN using a 'Bridge'



Ethernet LAN is the most commonly used LAN. The speed of a Local Area Network also depends on the topology used. For example, a LAN using bus topology has a speed of 10mbps to 100mbps, while in ring topology it is around 4mbps to 16mbps. LAN's are generally privately owned networks.











FILE SERVING: IN LAN, A LARGE STORAGE DISK ACTS AS A CENTRAL STORAGE REPOSITORY.

 PRINT SERVING: PRINTERS CAN BE SHARED VERY EASILY IN A LAN BY VARIOUS COMPUTERS.

 ACADEMIC SUPPORT: A LAN CAN BE USED IN THE CLASSROOM, LABS, ETC. FOR EDUCATIONAL PURPOSES.

 HIGH RELIABILITY: INDIVIDUAT WORKSTATIONS MIGHT SURVIVE THE NETWORK IN CASE OF FAILURES













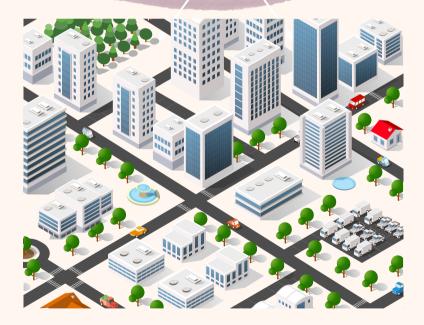


 Equipment and support may be costly

 Some hardware devices may not inter-operate properly

Metropolitan Area Network (MAN)

A Metropolitan Area Network is a bigger version of LAN that uses similar technology as LAN. It spans over a larger geographical area such as a town or an entire city.





Metropolitan Area Network (MAN)

It can be connected using an OPTICAL FIBRE cable as a communication medium. Two or more LAN's can also be connected using routers to create a MAN. When this type of network is created for a specific campus, then it is termed as CAN(Campus Area Network).







Metropolitan Area Network (MAN)

A MAN spans over a geographical area of about 50km. The best example of MAN is the cable television network that spans over the whole city.

The MAN can be either a public or privately owned network. Generally, a telephone exchange line is most commonly used as a communication medium in MAN. The protocols that are used in MAN are RS-232, Frame Relay, ISDN, etc.



Uses of MAN are as follows:

- MAN can be used for connecting the various offices of the same organization, spread over the whole city.
- It can be used for communication in various governmental departments.



ADVANTAGES OF MAN









The Propagation delay of MAN is moderate





It is hard to design and maintain a MAN

MAN is less fault-tolerant

It is costlier to implement

Congestions are more in a MAN



A Wide Area Network is the largest spread network. It spans over very large-distances such as a country, continent or even the whole globe. Two widely separated computers can be connected very easily using WAN. For Example, the Internet.

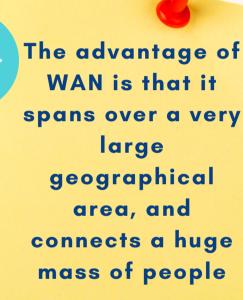


A WAN may include various Local and Metropolitan Area Network. The mode of communication in a WAN can either be wired or wireless. Telephone lines for wired and satellite links for wireless communication can be used in a wide area network.

In other words, WAN provides long distance transmission of data, voide, image, and video, over a large geographical area. A WAN may span

geographical area. A WAN may span beyond 100km range. It may be privately or publicly owned.

The protocols used in WAN are ISDN (Integrated Service Digital Network), SMDS (Switched Multi-Megabit Data Service), SONET(Synchronous Optical Network), HDLC(High Data Link Control), SDLC (Synchronous Data Link Control), etc.







The disadvantages of WAN:



The propagation delay is more in a WAN



The data rate is low



The error rate is high



It is very complex to design a WAN



These are the types of network according to geographical area.

Global Area Network (GAN)



A global area network (GAN) refers to a network composed of different interconnected networks that cover an unlimited geographical area. The term is loosely synonymous with Internet, which is considered a global area network

Unlike local area networks (LAN) and wide area networks (WAN), GANs cover a large geographical area.



Global Area Network (GAN)



The most sought-after GAN type is a broadband GAN. The broadband GAN is a global satellite Internet network that uses portable terminals for telephony. The terminals connect laptop computers located in remote areas to broadband Internet.





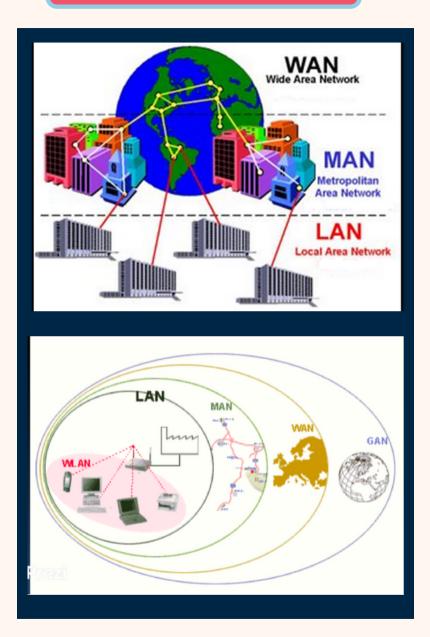
Global Area Network (GAN)

A global network such as the internet also referred to as the GAN. The internet is, however, not the only computer network but also internationally operating companies also support local networks that comprise of several WANs and connect company computers across the world. GANs use the fiber optic infrastructure from wide area networks and combine these with international undersea cables or satellite transmissions.





SUMMARY



Credit picture: https://prezi.com/lhfbc0vlp8_m/lan-wan-man-gan/ http://www.differencebetween.net/technology/difference-betweenlan-wan-and-man/

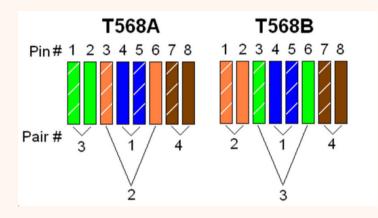
CHAPTER 3 WIRING STANDARD IN NETWORKING



T568A and T568B are the wiring standards that define the pinout for terminating twisted-pair network cable in eight-pin modular connector plugs and jacks. These wiring standards are one part of the TIA/EIA-568 telecommunications cabling standards.

T568B is commonly used in commercial installations, while T568A is prevalent in residential installations

DIFFERENCES BETWEEN WIRING CODES T568A VS T568B



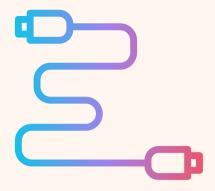
T568A and T568B are the termination standards used by Internet backbone infrastructure, Internet providers and all the way down to homeowners or businesses. The only real difference between these two pin-

to-pair assignments are the green and orange pairs. These two sets are swapped in the cable. Even though these are switched, they are still both effectively direct or "straight through" connections.

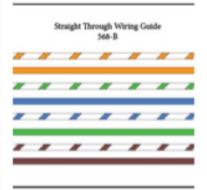


T568A T568B

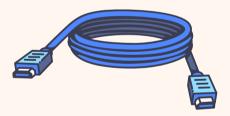
Pin	Color	Color
1	white /orange	white /green
2	orange	green
3	white /green	white /orange
4	blue	blue
5	white /blue	white /blue
6	green	orange
7	white /brown	white /brown
8	brown	brown

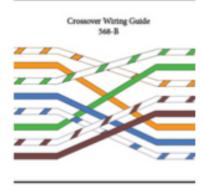


2 TYPES OF NETWORK CABLINGS



Straight-Through Wired Cables

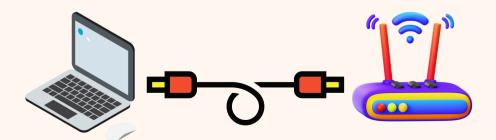




Crossover Wired Cables

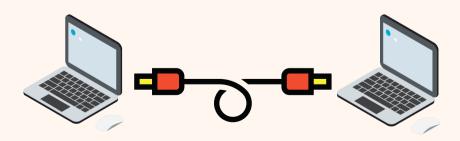


A straight-through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. This type of cable is also sometimes called a patch cable and is an alternative to wireless connections where one or more computers access a router through a wireless signal. On a straight-through cable, the wired pins match. Straight through cable use one wiring standard: both ends use T568A wiring standard or both ends use T568B wiring standard.





A crossover Ethernet cable is a type of Ethernet cable used to connect computing devices together directly. The RJ45 crossover cable uses two different wiring standards: one end uses the T568A wiring standard, and the other end uses the T568B wiring standard. The internal wiring of Ethernet crossover cables reverses the transmit and receive signals. It is most often used to connect two devices of the same type: e.g. two computers or two switches to each other.



How to make your own Ethernet cable

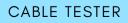
What you'll need:

Network cable Modular connector (RJ45) Crimping tools Cable Tester



MODULAR CONNECTOR (RJ45)

CRIMPING TOOL

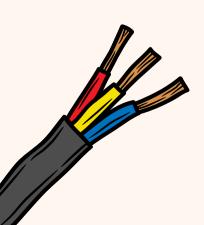




NETWORK CABLE

Networking cables are networking hardware used to connect one network device to other network devices or to connect two or more computers to share printers, scanners etc. Different types

of network cables, such as coaxial cable, optical fiber cable, and twisted pair cables, are used depending on the network's topology, protocol, and size. The devices can be separated by a few meters or nearly unlimited distances.





MODULAR CONNECTOR (RJ45)

An RJ45 connector (Registered Jack-45) is an 8-position, 8-contact (8P8C) modular plug or jack, frequently used for Ethernet networking.

The "45" refers to the number of the interface standard.

The jacks (female) are the recessed sockets, designed to accept an RJ45 plug (male) inserted into the socket.

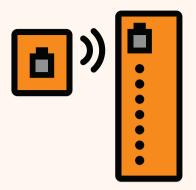


CRIMPING TOOLS

Crimping is a way of joining pieces of metal or other ductile material by deforming one or both of the pieces to hold the other, and this deformity is known as the "crimp".

A crimping tool is the tool used to deform the material and create the connection.

Crimping is commonly used in electrical work, to attach wires together or wire to other connectors.



CABLE TESTER

A cable tester is a device used to test the strength and connectivity of a particular type of cable or other wired assemblies.

There are many different types of cable testers. Each of them can test a specific type of cable or wire.

A cable tester can test whether a cable or wire is set up properly, connected correctly, and the communication strength between the source and destination.





Step by step to make Ethernet cable

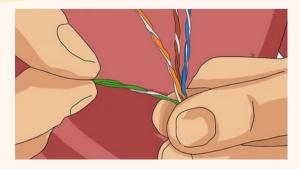
Step 1:

Strip the cable jacket about 1.5 inch down from the end.



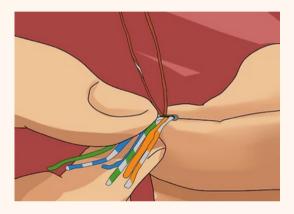
Step 2:

Spread the four pairs of twisted wire apart. For Cat 5e, you can use the pull string to strip the jacket farther down if you need to, then cut the pull string. Cat 6 cables have a spine that will also need to be cut.



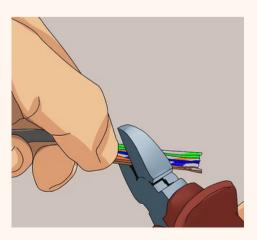
Step 3:

Untwist the wire pairs and neatly align them in the T568B orientation. Be sure not to untwist them any farther down the cable than where the jacket begins; we want to leave as much of the cable twisted as possible.



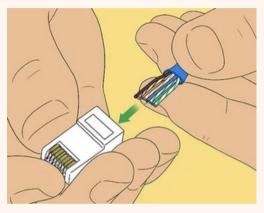
Step 4:

Cut the wires as straight as possible, about 0.5 inch above the end of the jacket.



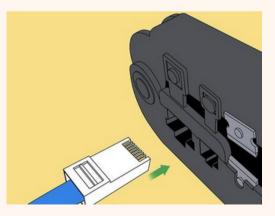
Step 5:

Carefully insert the wires all the way into the modular connector, making sure that each wire passes through the appropriate guides inside the connector.



Step 6:

Push the connector inside the crimping tool and squeeze the crimper all the way down.



Step 7:

Repeat steps 1-6 for the other end of the cable.

Step 8:

To make sure you've successfully terminated each end of the cable, use a cable tester to test each pin.



For crossover cables, simply make one end of the cable a T568A and the other end a T568B-

< 1 • min PTER 4 **NETWORK** SECURITY



NETWORK SECURITY is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies

There are many layers to consider when addressing network security across an organization. Attacks can happen at any layer in the network security layers model, so your network security hardware, software and policies must be designed to address each area.

Types of network security

- Network Access
 Control
- Antivirus and Antimalware Software
- Firewall
- Web security
- Packet filter
- Email security







To ensure that potential attackers cannot infiltrate your network, comprehensive access control policies need to be in place for both users and devices.

Network access control (NAC) can be set at the most granular level. For example, you could grant administrators full access to the network but deny access to specific confidential folders or prevent their personal devices from joining the network







ANTIVIRUS SOFTWARE

Antivirus and Antimalware Software

Antivirus and antimalware software protect an organization from a range of malicious software, including viruses, ransomware, worms and trojans.





A

The best software not only scans files upon entry to the network but continuously scans and tracks files.



Firewall

Firewalls, as their name suggests, act as a barrier between the untrusted external networks and your trusted internal network. Administrators typically configure a set of defined rules that blocks or permits traffic onto the network.







For

example, Forcepoint's Next Generation Firewall (NGFW) offers seamless and centrally managed control of network traffic, whether it is physical, virtual or in the cloud



Web security

Web security is also known as "Cybersecurity". It basically means protecting a website or web application by detecting, preventing and responding to cyber threats



1

Websites and web applications are just as prone to security breaches as physical homes, stores, and government locations. Unfortunately, cybercrime happens every day, and great web security measures are needed to protect websites and web applications from becoming compromised.



Anything that is applied over the Internet should have some form of web security to protect it.

Packet filter

Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports.

Packet filtering checks source and destination IP addresses. If both IP addresses match, the packet is considered secure and verified. Because the sender may use different applications and programs, packet filtering also checks source and destination protocols, such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).



Packet filters also verify source and destination port addresses.

Email security

Email security is the term for any procedure that protects email content and accounts against unauthorized access. Email service providers have email security measures in place to secure client accounts and information from hackers.

Such measures include email servers with strong password and access control mechanisms; encrypted email messages (both inboxes or in transit); web application firewalls; and spam filtering software.

Email is popular with hackers as a tool for spreading malware, spam, and phishing attacks. Email is also a main entry point for attackers looking to access an enterprise network and breach valuable company data.



TUTORIAL Questions & Answers







State the definition of a computer network.

2

Interpret the client/server network with a suitable diagram.

3

Show the difference between peer-to-peer and client-server networks in terms of reliability, cost, and access time for services.

ÿ

Describe the common elements required in Client/server Network

5

The Client-Server Network Model focuses on information sharing meanwhile the Peer-to-Peer Network Model focuses on connectivity to remote computers. Illustrate these TWO (2) types of networks.

QUESTIONS CHAPTER 2



1

What is an advantage of a Local Area Network?

2

Explain Metropolitan Area Network and Wide Area Network in Data Communication System.

3

Draw the configurations to show the network classification of three sets of Local Area Network (LAN) connected to Wide Area Network (WAN).

4

Mr. John is a small businessman who runs Hardware. He has been experiencing problems with his small accounting department, which he depends on to provide sales reports. Mr. John wants to share information between his 7 computer stations and have on central printing area. What type of network would you recommend to Mr. John?

QUESTIONS CHAPTER 3



1

EIA/TIA cabling and related standards have been developed to provide guidelines for designers, assemblers, end users, and manufacturers. This standard is to meet the requirements of telecommunication wiring systems for commercial buildings that support multiple network areas, data, sound and image or video systems. Using the appropriate diagram, construct TIA/EIA-568-B standard wiring using Cross Over types.

2

The types of wiring standard TIA/EIA-568-B for the network cabling preparation is a straight-through unshielded twisted pair (UTP) cable and cross-over UTP cable. Set-up a network cable for both types by using a suitable equipment with a proper procedures and diagram.





State the definition of Network Security.

2

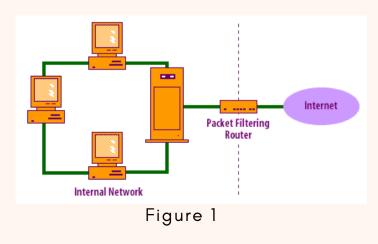
List FOUR(4) types of Network Security and explain TWO(2) of them.

3

Show the operation of the Firewall as network security with a suitable diagram.

4

Explain the operation of Packet Filtering in the block diagram below (Figure 1).







State the definition of a computer network.

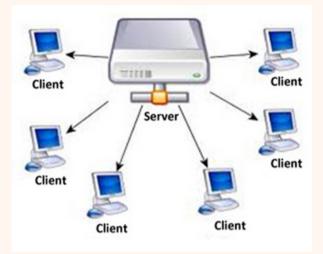
A computer network is a set of computers sharing resources located on or provided by network nodes. The computers use common communication protocols over digital interconnections to communicate with each other.

2

Interpret the client/server network with a suitable diagram.

Client-server networking involves a central, powerful computer called a server, and a number of client computers that need to connect to the server to carry out specific tasks.

A server is a computer on a network that provides a resource that can be used by any authorised client station.



Client server network diagram

3

Show the difference between peer-to-peer and client-server networks in terms of reliability, cost, and access time for services.

Reliability

There are multiple service providing nodes in a peer to peer network. So, it is more reliable. In client server network, the clients depend on the server. Failure in the server will disrupt the functioning of all clients. This is an important difference between peer to peer and client server network.

Cost

While a client server network is expensive to implement, a peer to peer does not require extensive hardware to set up the network.

Access time for services

Moreover, as the service providing nodes are distributed in the peer to peer network, the service requesting node does not need to wait long. On the other hand, in client server network, multiple clients requests for services from a server. Therefore, the access time for a service is higher.

4

Describe the common elements required in Client/server Network

Network Interface Card (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.

Network Operating System (NOS)

A network operating system (NOS) is a computer operating system (OS) that is designed primarily to support workstations, personal computers and, in some instances, older terminals that are connected on a local area network (LAN). The software behind a NOS allows multiple devices within a network to communicate and share resources with each other.

Node

A node is any physical device within a network of other tools that's able to send, receive, or forward information. A personal computer is the most common node. It's called the computer node or internet node. Modems, switches, hubs, bridges, servers, and printers are also nodes, as are other devices that connect over Wi-Fi or Ethernet.

Topology

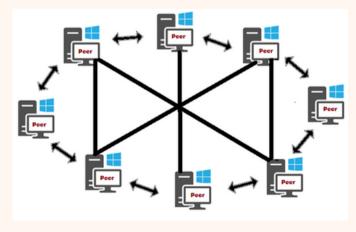
Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

Transmission media

A transmission medium is a route that transmits information from a source to a receiver. Transmission mediums lie underneath the physical layer and the physical layer regulates them. Communication channels are another name for transmission medium.

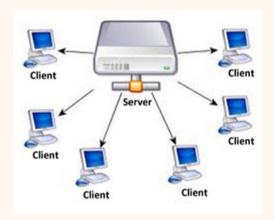
5

The Client-Server Network Model focuses on information sharing meanwhile the Peer-to-Peer Network Model focuses on connectivity to remote computers. Illustrate these TWO(2) types of networks.



Peer to Peer network diagram

Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers.



Client server network diagram

Client-server networking involves a central, powerful computer called a server, and a number of client computers that need to connect to the server to carry out specific tasks.

A server is a computer on a network that provides a resource that can be used by any authorised client station.

Servers are usually always on and connected to the internet, so that users can access their resources and services at any time.





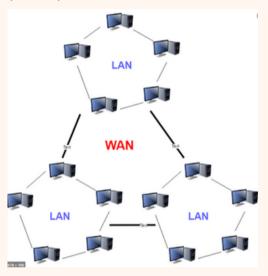
What is an advantage of a Local Area Network?

- File transfer and file access
- Resource or peripherals sharing
- Personal computing
- Document distribution
- Easy to design and troubleshoot
- Minimum propagation delay
- High data rate transfer
- Low error rate
- Easily scalable (devices can be added or removed very easily)

Explain Metropolitan Area Network and Wide Area Network in Data Communication System.

- A Metropolitan Area Network is a bigger version of LAN that uses similar technology as LAN. It spans over a larger geographical area such as a town or an entire city.
- It can be connected using an optical fiber cable as a communication medium. Two or more LAN's can also be connected using routers to create a MAN.
- The MAN spans over a geographical area of about 50km. The best example of MAN is the cable television network that spans over the whole city.
- MAN can be used for connecting the various offices of the same organization, spread over the whole city.
- It can be used for communication in various governmental departments.

Draw the configurations to show the network classification of three sets of Local Area Network (LAN) connected to Wide Area Network (WAN).



4

Mr. John is a small businessman who runs Hardware. He has been experiencing problems with his small accounting department, which he depends on to provide sales reports. Mr. John wants to share information between his 7 computer stations and have on central printing area. What type of network would you recommend to Mr. John?

Local Area Network (LAN)

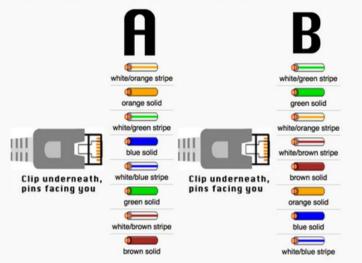


EIA/TIA cabling and related standards have been developed to provide guidelines for designers, assemblers, end users, and manufacturers. This standard is to meet the requirements of telecommunication wiring systems for commercial buildings that support multiple network areas, data, sound and image or video systems. Using the appropriate diagram, construct TIA/EIA-568-B standard wiring using Cross Over types.

In order to make Ethernet cross-over cable, we'll need:

- Ethernet cabling. CAT5e is certified for gigabit support, but CAT5 cabling works as well, just over shorter distances.
- A crimping tool. This is an all-in-one networking tool shaped to push down the pins in the plug and strip and cut the shielding off the cables.
- Two RJ45 plugs.
- Optional two plug shields.

Straight through network cable: both sides should be A Crossover cable: One side A, one side B



To start construction of the device, begin by threading shields onto the cable.

Next, strip approximately 1.5 cm of cable shielding from both ends. The crimping tool has a round area to complete this task.

After that, untangle the wires; there should be four "twisted pairs." Referencing back to the sheet, arrange them from top to bottom. One end should be in arrangement A and the other in B. Once the order is correct, bunch them together in a line, and if there are any that stick out farther than others, snip them back to create an even level. The difficult aspect is placing these into the RJ45 plug without messing up the order. To do so, hold the plug with the clip side facing away from you and have the gold pins facing toward you, as shown.

Next, push the cable right in. The notch at the end of the plug needs to be just over the cable shielding, and if it isn't, that means that you stripped off too much shielding. Simply snip the cables back a little more.

After the wires are securely sitting inside the plug, insert it into the crimping tool and push down. It should be shaped correctly, but pushing too hard can crack the fragile plastic plug.

Lastly, repeat for the other end but using diagram B instead.

To test it, plug it in and attempt to connect two computers directly. While LEDs differ by the device, one should show activity and the other should indicate speed.

The types of wiring standard TIA/EIA-568-B for the network cabling preparation is a straight-through unshielded twisted pair (UTP) cable and cross-over UTP cable. Set-up a network cable for both types by using a suitable equipment with a proper procedures and diagram.

Step 1: Strip

Using the stripping razor on the crimp tool, strip 3-5 millimeters off the sheath at the end of the cable. If somehow accidentally cut the internal wires, just cut the wire an inch down and try stripping again. (So, leave a few spare inches in case you mess up.) After striping process, there are eight color-coded wires inside.

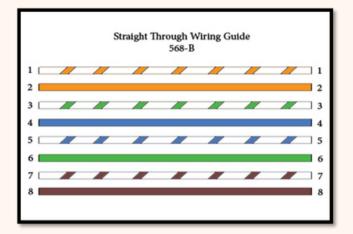
Step 2: Arrange

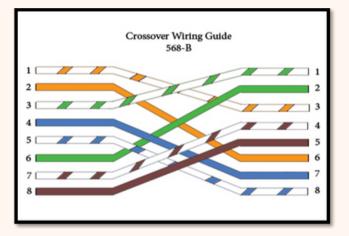
For making a standard cat 5 cable, arrange the color-coded wires in the same order on both ends. Use the 568B order below:

- 1. White/orange
- 2. Orange
- 3. White/green
- 4. Blue

5. White/blue

- 6. Green
- 7. White brown
- 8. Brown





Step 3: Crimp

Insert the wires into the cavity at the back of the RJ45 connector while making sure that the arrangement of the wires mentioned in the preceding step is not disturbed, and that each wire is properly seated into its corresponding channel. Push the wires all the way to the end of the cavity to ensure that the pins inside the RJ45 will pierce the individual wires and make good contact. Then, insert the plug into the crimp tool and squeeze. Cat 5 plugs contain metal "teeth" that pierce the colored wires during crimping to create electrical conductivity. Repeat this process for the other end

Step 4: Test

Test the cable to make sure you've successfully terminated each end of the cable using a cable tester.





State the definition of Network Security.

Network security is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies.

2

List FOUR(4) types of Network Security and explain TWO(2) of them.

- Network Access Control
- Antivirus and Antimalware Software
- Firewall
- Web security
- Packet filter
- Email security

Choose 4 from the answer above

Network Access Control

To ensure that potential attackers cannot infiltrate your network, comprehensive access control policies need to be in place for both users and devices.

Network access control (NAC) can be set at the most granular level. For example, you could grant administrators full access to the network but deny access to specific confidential folders or prevent their personal devices from joining the network.

Antivirus and Antimalware Software

Antivirus and antimalware software protect an organization from a range of malicious software, including viruses, ransomware, worms and trojans.

The best software not only scans files upon entry to the network but continuously scans and tracks files.

Firewall

Firewalls, as their name suggests, act as a barrier between the untrusted external networks and your trusted internal network. Administrators typically configure a set of defined rules that blocks or permits traffic onto the network.

For example, Forcepoint's Next Generation Firewall (NGFW) offers seamless and centrally managed control of network traffic, whether it is physical, virtual or in the cloud.

Web security

Web security is also known as "Cybersecurity". It basically means protecting a website or web application by detecting, preventing and responding to cyber threats.

Websites and web applications are just as prone to security breaches as physical homes, stores, and government locations. Unfortunately, cybercrime happens every day, and great web security measures are needed to protect websites and web applications from becoming compromised.

Packet filter

Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports.

Packet filtering checks source and destination IP addresses. If both IP addresses match, the packet is considered secure and verified. Because the sender may use different applications and programs, packet filtering also checks source and destination protocols, such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

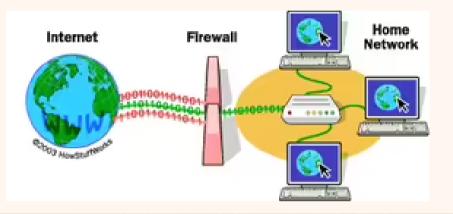
Email security

Email security is the term for any procedure that protects email content and accounts against unauthorized access. Email service providers have email security measures in place to secure client accounts and information from hackers.

Such measures include email servers with strong password and access control mechanisms; encrypted email messages (both inboxed or in transit); web application firewalls; and spam filtering software.

Choose 2 from the answer above

Show the operation of the Firewall as network security with a suitable diagram.

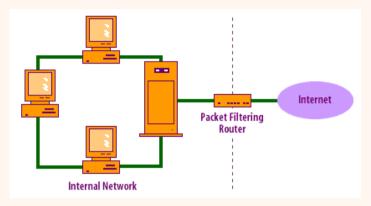


A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through.

A firewall acts as a gatekeeper. It monitors attempts to gain access to your operating system and blocks unwanted traffic or unrecognized sources. Firewalled system analyzes network traffic based on rules. A firewall only welcomes those incoming connections that it has been configured to accept. It does this by allowing or blocking specific data packets – units of communication you send over digital networks – based on pre-established security rules.

A firewall works like a traffic guard at your computer's entry point or port. Only trusted sources, or IP addresses, are allowed in.

Explain the operation of Packet Filtering in the block diagram below (Figure 1).



A packet filtering firewall is a network security feature that controls the flow of incoming and outgoing network data.

The firewall examines each packet, which comprises user data and control information, and tests them according to a set of preestablished rules.

If the packet completes the test successfully, the firewall allows it to pass through to its destination. It rejects those that don't pass the test. Firewalls test packets by examining sets of rules, protocols, ports and destination addresses.



Jerry FitzGerald, Alan Dennis, Alexandra Durcikova (2014). Business Data Communications and Networking. 12th Edition Wiley.

Jeffrey S. Beasley, Gary M. Miller (2013). Modern Electronic Communication. 10th Edition Pearson/Prentice Hall.

William Stallings (2015). Data And Computer Communications, International Edition. 10th Edition. Pearson Education Limited.

https://www.tutorialspoint.com/data_communic ation_computer_network/index.htm

https://www.techopedia.com/definition/6765/d ata-communications-dc

https://www.wikihow.com/Make-a-Network-Cable



