Piyush Mishra
Roll no: 727

Assignment :- Ethics and Technology

Q:1] Write a note on CIA triad.

Confidentiality - is a set of rules that limits access to information.

Integrity - is the assurance that the information is trustworthy and accurate.

Availability - is a gaurantee of reliable access to the information by authorized people.

At the core of information security is information Assurance, which means the act of maintaining CIA of information, ensuring that information is not compromised in any way when critical issues arise.

The CIA triad model acts as the backbone of information security.

Deals with such questions as:
Has the data been made disclosed to authorized Entities?

To prevent information from being made available or disclosed to unauthorized entities.
Applies to information while stored, being processed, or in transit.
To prevent all forms of disclosure such as printing and displaying including revealing the existence of information objects.

Mechanisms used to provide data Confidentiality include.
Encryption
physical Isolation.

Types of data Confidentiality Services.

① Prevent unauthorized disclousure of data
Connection - oriented Confidentiality.
Example: protecting all data transmitted between two Entities

Connectionless Confidentiality
Example: protecting only important messeges.

Selective field Confidentiality.
Example:- protecting the message field but not the addressed field.

② Traffic flow Confidentiality.
Origin destination patterns.
Example: who is talking to whom.
- message size.
Frequency of message transmission.

Data integrity.

To prevent the information from being altered or destroyed.
Includes preventing such actions as writing modifying, changing status, deleting, creating, delaying, resequencing and replaying.

Mechanisms used for data integrity include:

- Checksums
- Cyclic Redundancy check (CRC)
- Cryptographic checksums
- Message digest checksums
- One way hash

Availability.

Dead switch attack resulting in loss an reduction in availability of Computing and Communication resource

Addressed denial of Services attacks.

Possible to detect could be hard to prevent.

Mechanisms used to deal with.

Replicated Communication facilities
Replicated Computing resources
Reliability Scheme
Robusts Computing and Communication architecture.
Sophisticated load balancing and Routing Scheme.

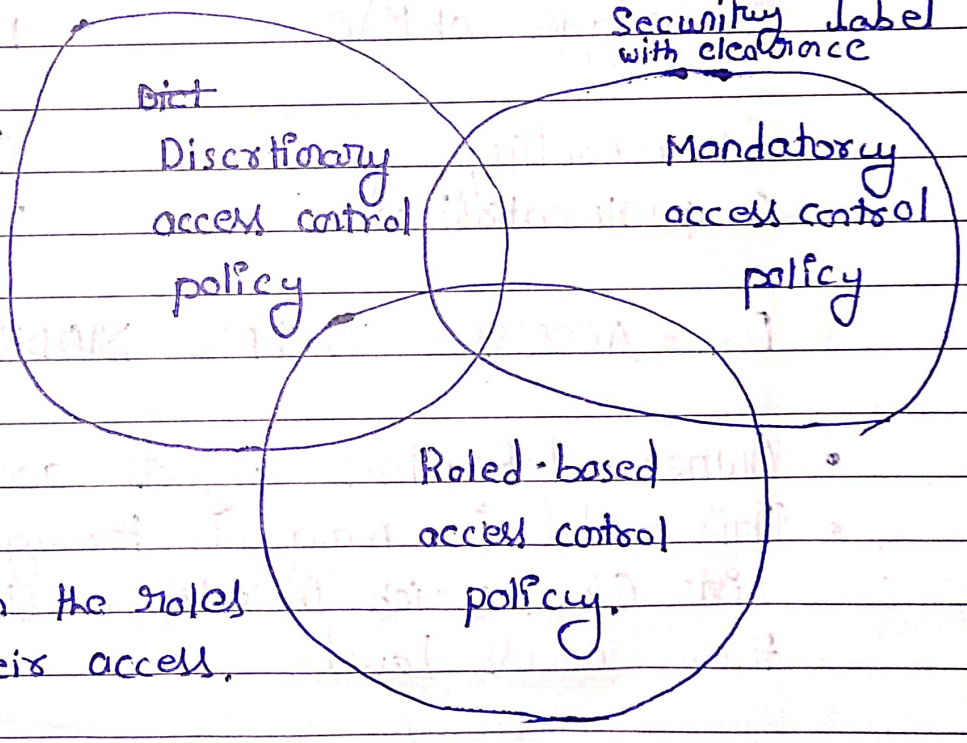
Q.2] What are different models of access control? Explain.

Mandatory Access Control (MAC)
Discreationary Access Control (DAC)
Role-Based Access Control (RBAC)

dictates
What types of access are permitted
under what circumstances,
by whom.

based on the identity of the requestor and on access rules.

based on comparing Security label with clearance



Based on the roles and their access.

MAC - ACCESS CONTROL Models

You define the sensitivity of the resource by means of a security label.
The security label is composed of Security level zero or more security categories. The security level indicates hierarchial classification of the information.

(For Example, Restricted, Confidential, or Internal)

The Security Category defines the category or group to which the information belongs (such as Project A or B). Users can access only information in a resource to which their Security labels entile them.

IF the user's Security label does not have Enough authority, the users cannot access the information in the resources.

Advantage of MAC	Disadvantages of MAC
Enforceability	Collaboration
Compartmentalization	Management burden.

DAC - ACCESS CONTROL MODELS

- Owner determines objects access privileges
- This model is managed through an access Control List (ACL) which includes a list of users with their access Levels

• Advantages of DAC.	• Disadvantages of DAC
• Conceptual Simplicity	• Limited Control.
• Responsiveness to business need	• Compromised security

Role-Based Access Control (RBAC)

- System administrators must assign access based on organizational roles. The idea is that an individual only has access to what is needed to do their job and nothing more.

- Advantages of RBAC

- Flexibility
- Ease of maintenance
- Centralized, non-discretionary policies.
- Lower Risk Exposure.

- DisAdvantages

- Complex deployment
- Balancing Security with Simplicity.
- Layered roles and permissions.

6.3) Explain the types of password vulnerabilities.

The two general classification of password vulnerabilities:

- Organizational or user vulnerabilities: This includes Lakes of password policies that are enforced within the organization and lack of security awarness on the parts of users.

- Technical vulnerabilities: This include weak Encription methods and unsecure storage of passwords on Computer System.

Organizational password vulnerability.

- its human nature who want Convenience, Especially when it Comes to remembring five, ten and often dozens of passwords for works and daily life. This desire for Conveniences makes password one of the Easiest barriers for an attackers to overcome.

- Almost 3 trillion Eight-character password Combination are possible by using the 26 letter of the alphabets and the numberals 0 through 9. The key to strong password are: 1) Easy to remember and 2) difficult to crack. However, most people just focus on the Easy-to-remben part. users like to use such password as password, their login name, abc123 or no password at all!

- Unless users are Educated and reminded about using Strong password, their password usually are.

- Easily to guess
- Seldom changed
- Reused for many Security point.

- When bad guys crack one password, they can often access Other System with that Same password and username.

- Write down in unsecure places.
- The more Complex a password is, the more difficult it is to Crack. However, when users create Complex passwords they are more likely to write them down External attackers and malicious insiders can find these passwords and use them against you and your business.

Technical password vulnerabilities.
you often Find these serious technical vulnerabilities often Exploiting organizational password vulnerabilities.

Weak password Encryption schemes.
Many vendards and developers believe that password are safe as long as they don't publish the source Code For their Encryption algorithem. wrong! A presistent, patient attackers can usually crack this Security by obscurity (a Security measures that hidden from plain view but can be Easily overcome)

Fairly quickly. After the code is cracked it is distributed across the internet and become public knowledge.

- program that store their password in memory unsecured files, and easily accessed databases.
- unencripted databases that provide direct access to sensitive information to anyone with database access, regardless of whether they have a business need to known.

Q.4) What are different types of Malware.

Ans Virus

- Vital information resource under seige.
- Software that replicates itself and spread by damaging and deleting the file.
- Virus enters your devices via attached images, greeting, audio, an video file download etc.

SPYWARE

- Spyware is a programe that get installed without the user information.
- It monitors the users activity on the internet and transmits the information to the third party.
- Example: kid logger.

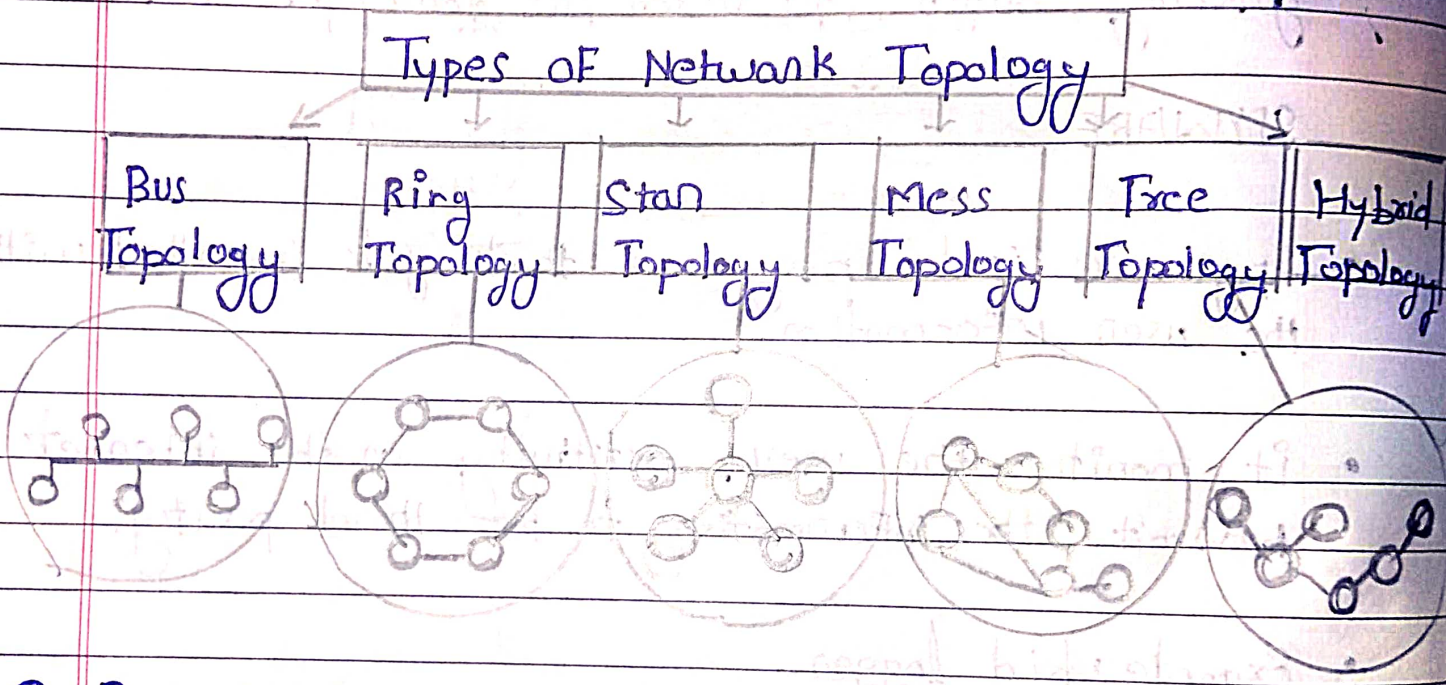
ADWARE

- Software advertising banners are displayed by any program is running.
- It automatically downloads to your devices by browsing any website.
- It is used by Companies for marcketing purpose.

WORMS

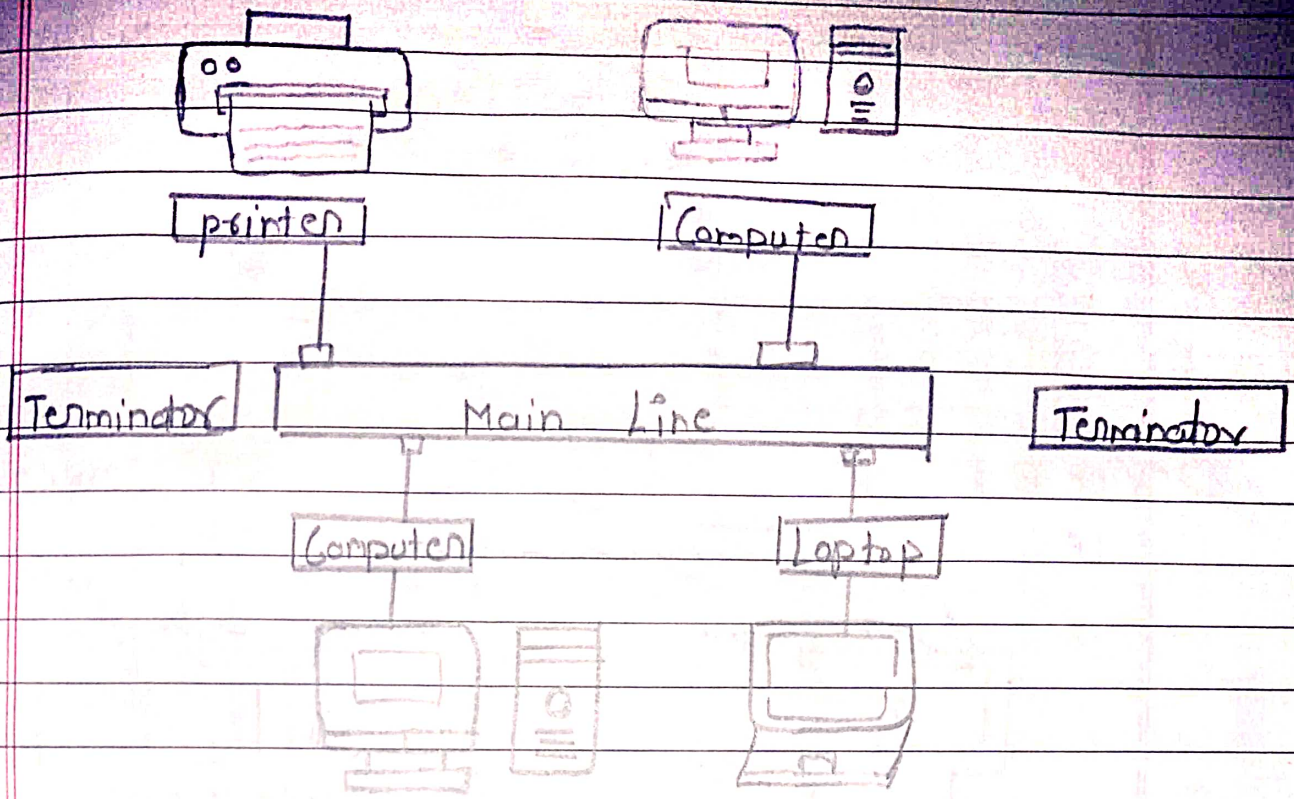
- Malicious program that make copies of itself on local device network share etc.
- They make the working of your devices slower.

Q.5] Explain different network topologies with diagram.



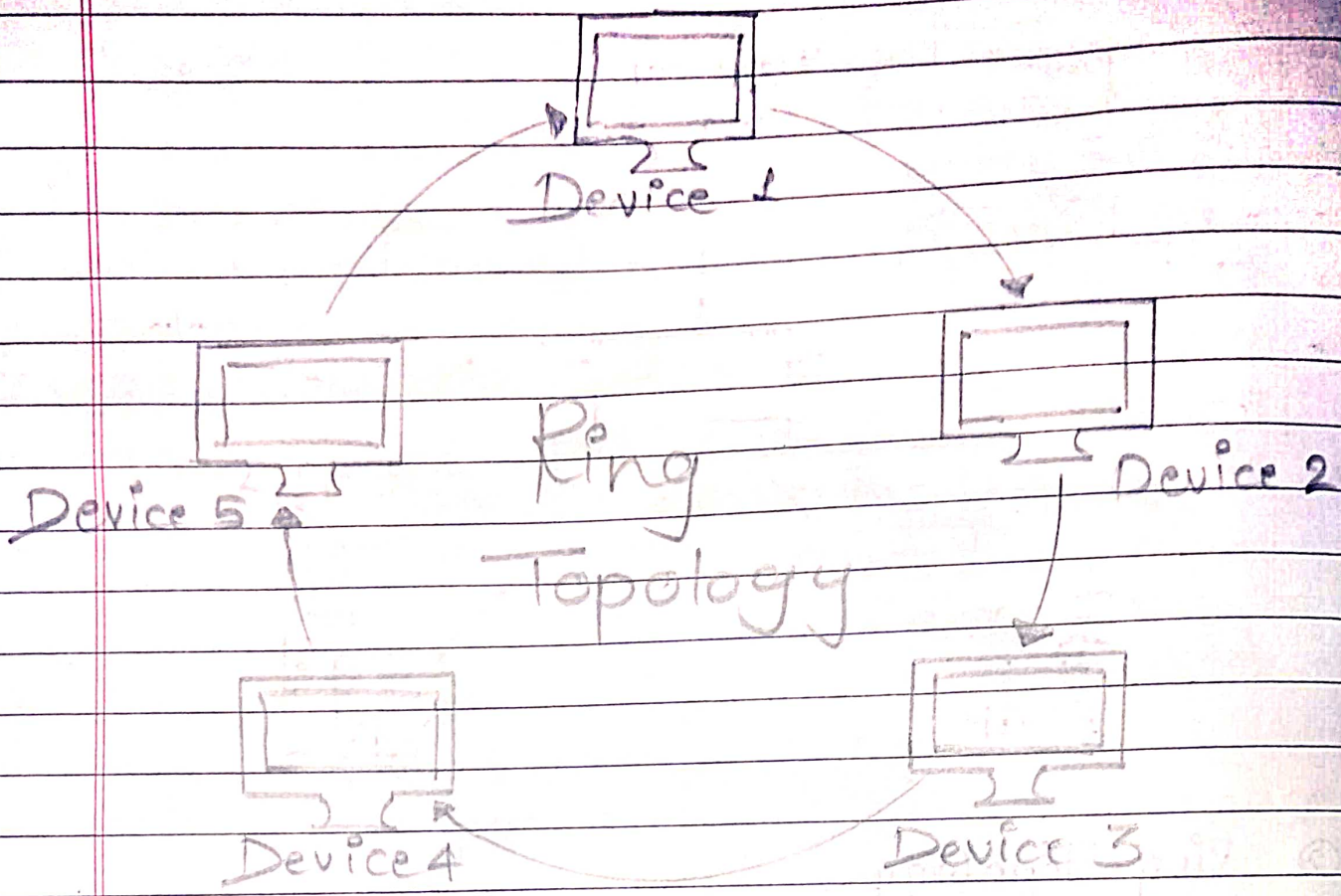
① Bus Topology.

The bus Topology connect each device on the network to a common main Cable, creating a single communication path for all nodes. One point transmits data along a single route to another point. we cannot transmit data in both ways. Linear Bus Bot topology is the term used for this topology when it has exactly two endpoints and is primarily utilized for small network.



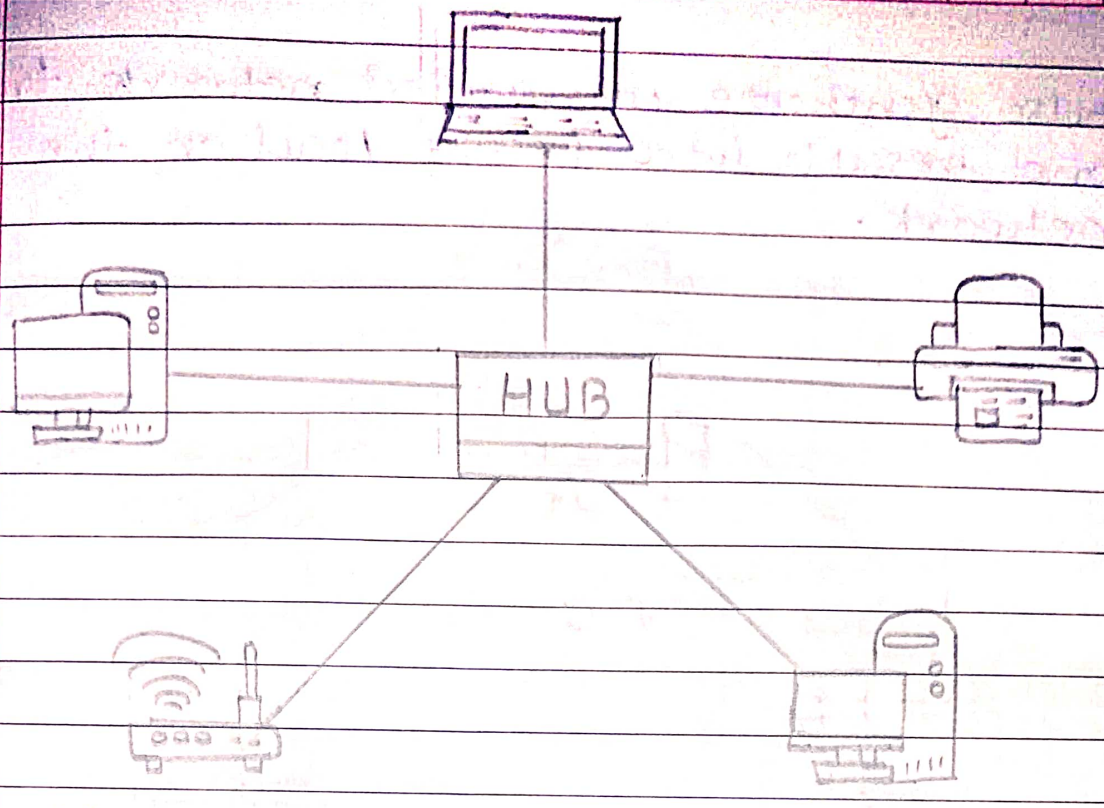
② Ring Topology

The devices in a ring topology, such as computers, pinters, or servers, are interconnected in a circular or ring-like pattern, which forms a closed loop. Two other devices link each other device in the Ring topology, positioned on either side. the last device in the chain connects to the first device, completing the circuit. Each device in a ring topology is linked to two other devices, ~~on the other devices~~, one on either side, forming a continuous ring or loop. In a ring topology, data is transmitted in one direction around the circle, with each device on the network reading and passing on the data until it reaches it's destination.



③ Star topology

In a star topology network, all devices directly link to a central switch or hub, serving as the central connection point, in this topology, devices transmit data through the central hub, which then distributes the data to all devices connected. Hubs can either be active or passive, with active hubs containing repeaters and passive hubs being classified as non-intelligent nodes. Each node is connected directly to a central node, which serves as a repeaters during data transmission.

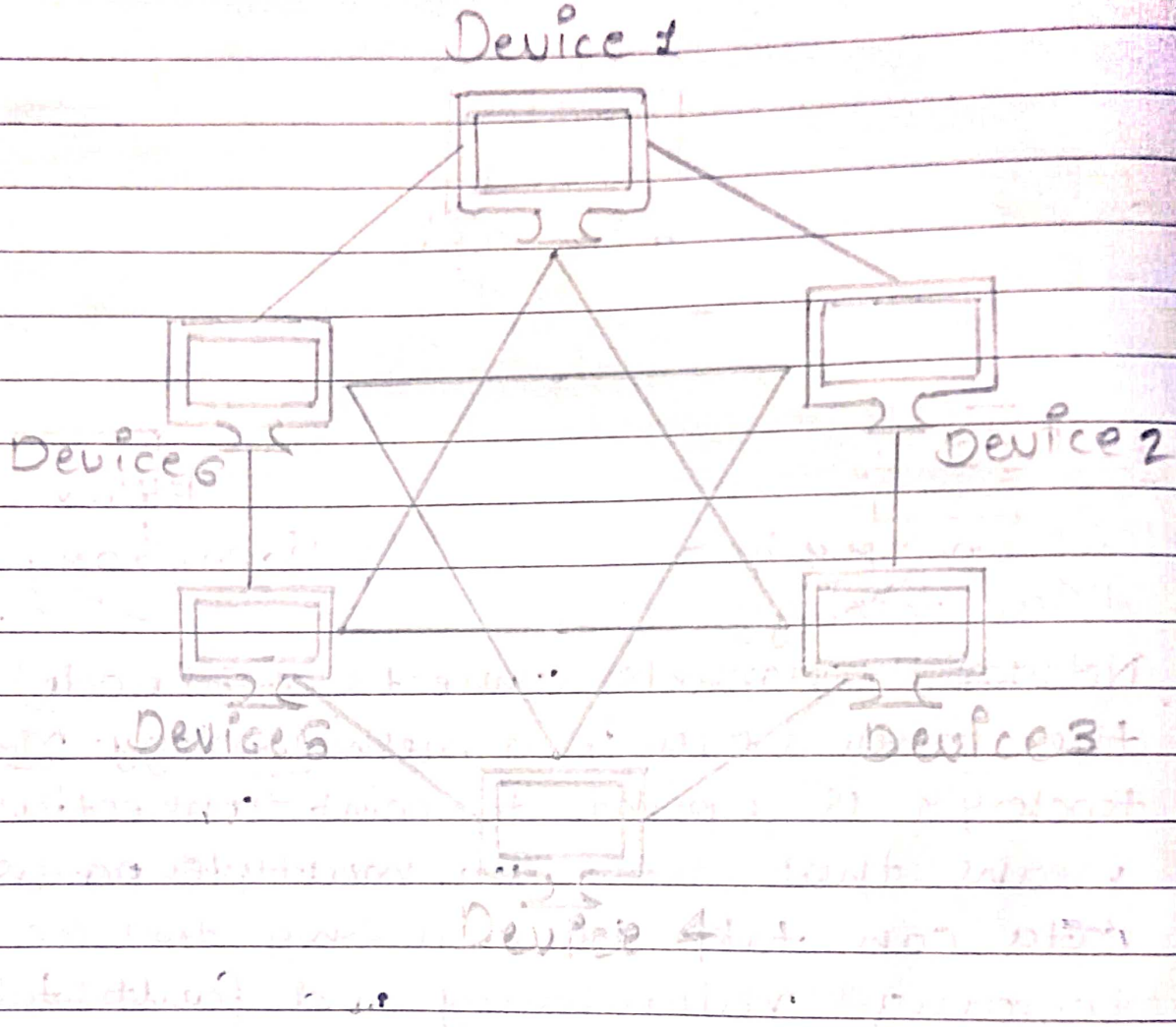


④ Mesh topology

Network channels connects each node to all the other nodes in a mesh topology. Mesh topology is a point-to-point connection, which means that there are multiple paths that data can take between any two devices, poviding redundancy and fault tolerance in a case of a network failure.

The mesh topology supports two data transmission techniques: routing and flooding. the routing technique the nodes with routing logic, such as selecting the sortest distance path to the destination node or avoiding routes with broken connections. On the eliminating the need for the routing logic. while this technique enhance the networks robustness, it may

also generate unwanted network traffic and result in a heavy load on the network.

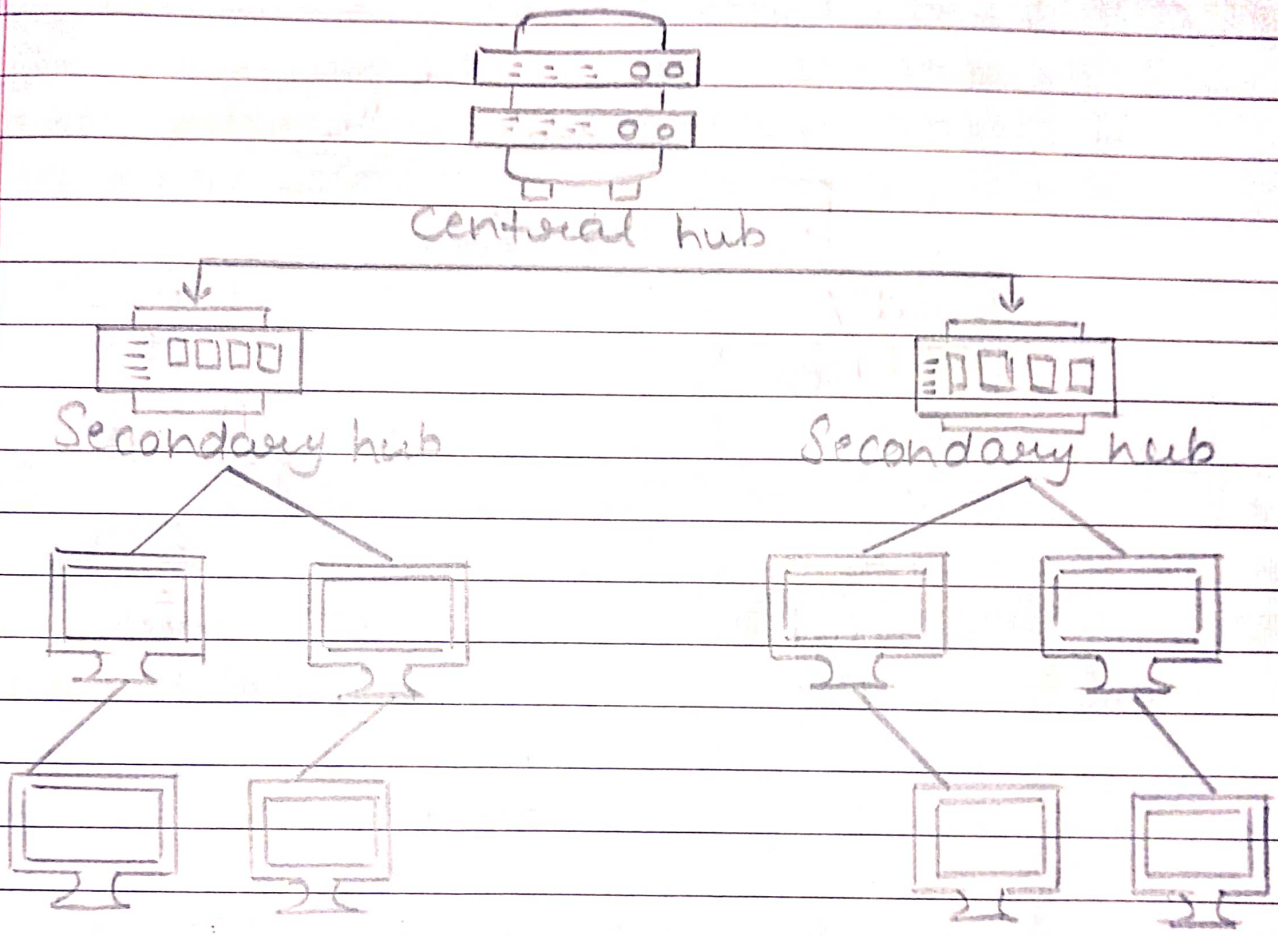


⑤ Tree topology

A tree topology consists of a hierarchical structure that resembles a tree. In this type of network topology, a central node, also known as root node, connects to one or more nodes, which in turn connect to additional nodes.

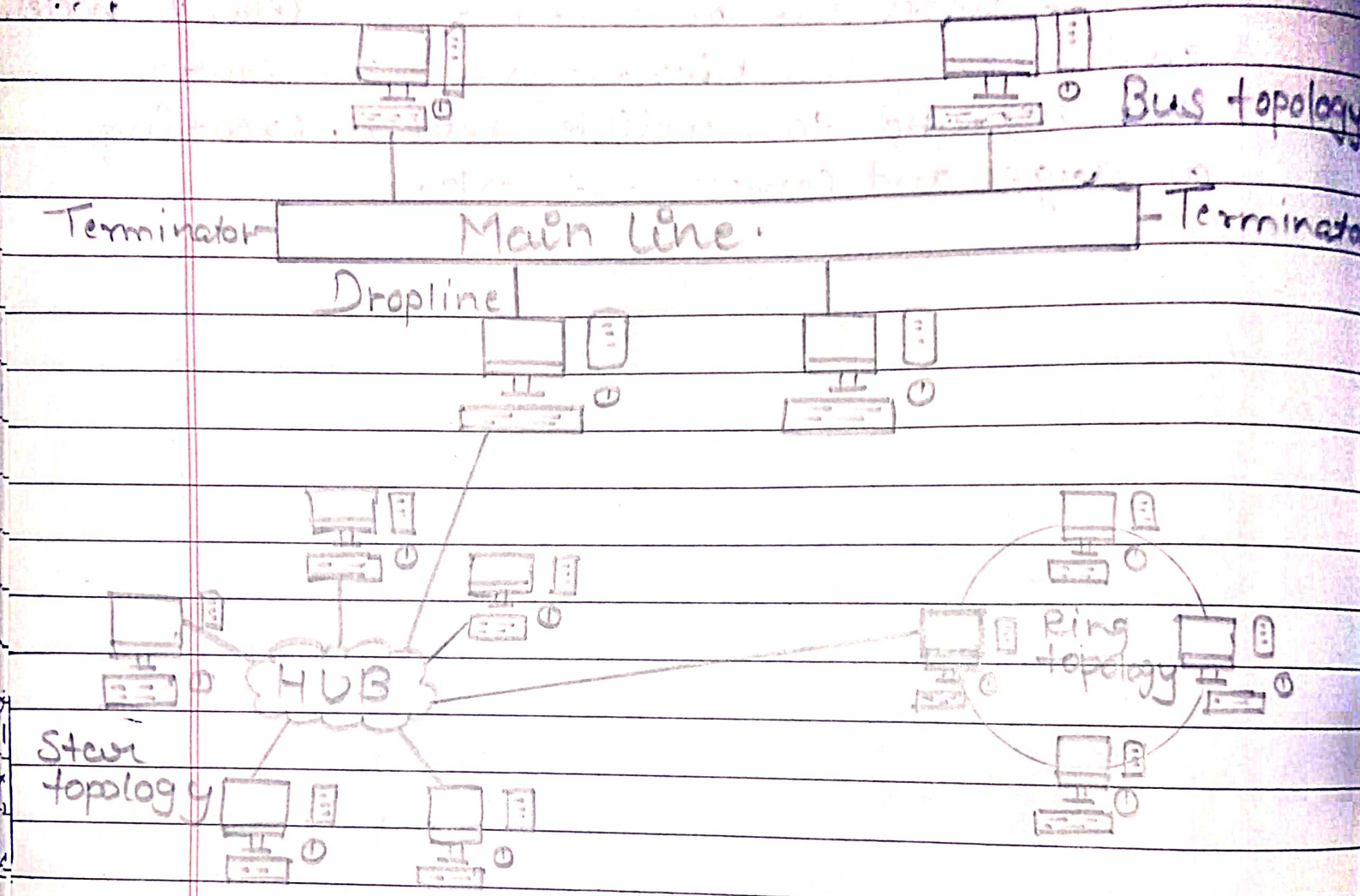
In a tree topology "level 1" nodes refer to the nodes directly connected to the root node, while nodes connected to

level 1 nodes are referred to as "level 2" nodes and so on. this hierarchical structure can expand to multiple levels, creating a large and complex network.



⑥ Hybrid topology

Hybrid topology refers to combining two or more different network topologies. It combines the advantages of each network topology to create a more robust and flexible network infrastructure.


Bus topology
Terminator
Main Line.
Terminator
Dropline
HUB
Star topology
Ring topology

Q.6] What are different network devices used.

① Router:

Function: Router Connect different network, such as Local area network (LANs) on the internet and direct data traffic between them, They use routing tables to determine the optimal path for data pack.

② Hub
Switch:

Function: Hubs are basic networking devices that Operate at the physical layer (Layer 1) and simply broadcast incoming data to all connected devices. The Lack the intelligence to selectively foward data Like Switches.

③ Bridge:

Function: Bridge operate at the data link layer and Connected two aspects network segment, allowing them to Communicate. They use MAC addresses to Filter and Forward data between the Connected Segment.

④ Firewall:

Function: ~~A Modern~~ modulator. Firewell are designed to monitor and control incoming and outgoing network traffic

based on predetermined security rules. They help protect networks from unauthorized access and cyber threats.

⑤ Modem

Function: A modem (modulator-demodulator) converts digital data from a computer into analog signals for transmission over telephone lines or cable systems. It also converts incoming analog signals back into digital data for the computer.

⑥ Repeater

Function: Repeaters amplify and retransmit signals in a network to extend the range of the network. They are commonly used in wireless networks to improve coverage.

Q7.] Encrypt 'tall trees' with playfair cipher using the key 'occurance'.

Ans Plaintext : tall trees

1. Key table setup.

o	c	u	r	e
n	a	b	d	f
g	h	i	k	l
m	p	q	s	t
v	w	x	y	z

2. Text preparation

ta	ll	tr	ee	sx

1. Encryption Rules

- If the letters are in the same row, replace each letter with the letter to its right.
- If the letters are in same column, replace each letter with the letter below it.
- If the letters are not in the same row or column, create a rectangle with these two letters and replace them with the letters at the other two corners of the rectangle.

2. Encrypt

- Applying the playfair cipher rules:
  - "ta" becomes "gr"
  - "ll" becomes "lk"
  - "tr" becomes "qr"
  - "ee" becomes "ds"
  - "sx" becomes "tv"

3. Encrypted Message.

gr	lk	qr	ds	tv

So, the encrypted form of "tall trees" using the playfair cipher with the key "occurrence" is "grlkqrdstv".

Q8.] Use the hill cipher to encipher the message "we live in an insecure world" with the key as $K = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$

Ans To encrypt the message 'we live in an insecure world' using the Hill cipher with the given key matrix $K = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$, follow these steps.

1. Message preparation:
Break the message into blocks of size equal to the dimension of the key matrix. In this case, the key matrix is 2×2, so we will group the message into pairs of letters.

we	li	ve	in	an	in	se	cu	re	wo	rl	d

1 Convert letters to Numbers:
Convert each pair of letters to numerical values using a simple mapping (e.g. A=0, B=1 ... Z=25)

we -> 22 04 | li -> 11 08 | ve -> 21 04 | in -> 08 13 |
an -> 08 13 | se -> 18 04 | cu -> 02 20 | re -> 17 04 |
wo -> 22 14 | rl -> 17 11 | d -> 03

1. Create matrices
Convert pairs of numbers into matrices

Matrix M = [22 04] Matrix K = [3 2]
[5 7]

[11 08]
[21 04]
[08 13]
[00 13]
[08 13]
[18 04]
[02 20]
[17 04]
[22 14]
[17 11]
[03]

1. Matrix Multiplication
Multiply the message matrix (MT) by the key matrix (K)

C = M X K

$$C = \begin{bmatrix} 22\times3+4\times5 & 22\times2+4\times7 \\ 11\times3+8\times5 & 11\times2+8\times7 \\ 21\times3+4\times5 & 21\times2+4\times7 \\ 8\times3+13\times5 & 8\times2+13\times7 \\ 0\times3+13\times5 & 0\times2+13\times7 \\ 8\times3+13\times5 & 8\times2+13\times7 \\ 18\times3+4\times5 & 18\times2+4\times7 \\ 2\times3+20\times5 & 2\times2+20\times7 \\ 17\times3+4\times5 & 17\times2+4\times7 \\ 22\times3+14\times5 & 22\times2+14\times7 \\ 17\times3+11\times5 & 17\times2+11\times7 \\ 3\times3+0\times5 & 3\times2+0\times7 \end{bmatrix}$$

Performing the calculations

$$C = \begin{bmatrix} 94 & 62 \\ 95 & 79 \\ 97 & 62 \\ 109 & 77 \\ 65 & 91 \\ 109 & 77 \\ 94 & 62 \\ 112 & 54 \\ 79 & 62 \\ 126 & 112 \\ 99 & 62 \\ 6 & 14 \end{bmatrix}$$

1. Convert Number to letters
Convert the elements of resulting matrix back to letters using the reverse mapping.

94 62 -> Yo
95 79 -> Zn
97 62 -> Ya
109 77 -> mn
65 91 -> ba
109 77 -> mn
94 62 -> Yo
112 54 -> pp
79 62 -> oz
126 112 -> bz
95 62 -> aZ
6 14 -> gf

Therefore, the encrypted message for "we live in an insecure world" using the hill cipher with key matrix K = $\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$ is

Yo ZV Ya mn ba mn Yo pp oz bz

Q.97 Encrypt and decrypt the message 'enemy attack tonight' with keyed columnar transposition cipher with encryption key 31452 and decryption key 25134.

Ans. Encryption

Encryption key : 31452
plaintext : enemy attack tonight

1. Write the message in colums based on the key

3	1	4	5	2
e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	

2. Arrange Columns in ascending order based on the number in the key

1	2	3	4	5
n	m	e	y	e
t	a	c	q	t
s	o	n	k	t
g	h	t	i	

1. Read the columns from left to right to get the ciphertext:

Ciphertext: nmtayeeactsonktghie

Decryption key: 25134

1. Write the ciphertext in columns based on the sky

2	5	1	4	3	4
n	m	t	g	y	
e	c	g	c	t	
s	o	n	k	t	
g	h	i	e		

1. Arrange columns in ascending order based on the numbers in the sky:

1	2	3	4	5
m	n	g	y	e
c	a	t	t	e
o	n	k	t	s
h	i	e	g	t

1. Read the columns from left to right to get the decrypted message

Decrypted message: mcohaingeabstet

the encrypted message using the keyed columnar transpotion cipher with the encryption key '31452' in 'nmtayecactsonktghie', and the decrypted message using the decryption key '25134' is 'mcctahingeatstekt'.