**With the help of suitable diagram, describe various network topologies.**

**(5 marks)**

* **Network topology refers to the arrangement of devices (such as computers, servers or network devices) in a network.**
* **Network topology describes how devices (like computers, servers, or other network devices) are connected to each other in a network.**
* **It’s like the blueprint of a network, showing how data flows between different devices.**

**Different types of network topologies with their features, advantages and disadvantages.**

1. **Bus Topology**
2. Star Topology
3. Ring Topology
4. Mesh Topology
5. Tree Topology
6. Hybrid Topology

1.Bus Topology

Description: All devices are connected to a single central cable. When a device wants to send data, it transmits the data onto the bus and data travels along the cable until it reaches its destination devices.

Advantages

1. Easy and cost-effective to set up for small networks.
2. Required less cable as compared to other topologies.

Disadvantages

1. A fault in the main cable brings down the entire network.
2. Slower performance when heavy traffic.

A diagram of a computer network

Description automatically generated

2.Star Topology

Description: All devices are connected to a central hub or switch. When a device wants to send data, it transmits the data to the central hub, which then forwards the data to the designated (target) device.

Advantages

1. Easy to add or remove devices without affecting the network.
2. Fault on one device doesn’t affect the others.

Disadvantages

1. A fault in the central hub can brings down the entire network down.
2. Required more cable as compared to bus topology.

A diagram of a computer network

Description automatically generated

3.Ring Topology

Description: All devices are connected in a circular loop, forming a “ring”. Each device is connected to two other devices, one on either side. When a device wants to send data, it transmits the data onto the ring in a specific format (often with a “token”). The data then travels around the ring, passing though each device until it reaches the designated(target) device.

Advantages

1. Easy and cost-effective to setup for small devices.
2. Data flows in a single direction, which helps to prevent collisions.

Disadvantages

1. If one device in the ring fails, can bring down the entire network.
2. Adding or removing devices can disrupt the entire network.

A diagram of a computer network

Description automatically generated

4.Mesh Topology

Description: All devices are connected to every other device, either fully or partially. Data can be transmitted along multiple paths.

Advantage

1. Failure of one link, doesn’t affect the entire network.
2. Data can be transmitted along multiple paths, so reduce network traffic.

Disadvantages

1. Expensive to setup.
2. Difficult to manage and maintain.

A diagram of a device and a device

Description automatically generated

5.Tree Topology

Description: A combination of bus and star topologies, where star networks are connected to central bus.

Advantages

1. Easy to add or remove devices without affecting the entire network.
2. Failure of one nodes doesn’t affect the other nodes.

Disadvantages

1. More complex to setup.
2. A failure in the central bus can brings down the entire network.

A diagram of a computer network

Description automatically generated

**Define IP Address. Explain the role of** **subnet mask in IP Addressing.** **When is static address assignment preferred over dynamic address assignment and vice versa? (3+4+3=10)**

An IP Address (Internet Protocol Address) is a unique address which is assigned to each device connected to a network. It allows devices to communicate with each other over the internet or a local network.

There are two types of IP Address

1. IPv4 (Internet Protocol Version 4): 32-bit address; represent in four sets of decimal number (e.g., 192.168.1.1)
2. IPv6(Internet Protocol Version 6): 128-bit address; represent in eight groups of hexadecimal numbers

**Roles of Subnet Mask in IP Addressing:**

1. Network and Host Identification: Subnet mask is used to define which part of an IP Address refers to the network and which part refers to the device(host).
2. Network Segmentation: It divides a large network into smaller, more manageable subnetworks. This improves network efficiency and security.
3. Routing: The subnet mask helps devices to decide where to send data. If the destination IP is in the same network, the data goes directly to the device. If it’s in a different network, the data is sent to the router for forwarding.
4. IP Address Allocation: Subnet mask assign only the needed number of address for each network.

**Static address assignment is preferred:**

1. When a device (like printers, routers, servers) needs fixed IP Address for reliable access.
2. When a Security System (like CCTV Camera) relies on specific IP Address for monitoring and access control.
3. When network administrator wants to full control over network because they know which devices uses which IP, so that they can manage network efficiently.

**Dynamic Address Assignment (via DHCP) is preferred:**

1. For large Network: Automatically assign IP Address to devices, which makes easier to manage multiple devices.
2. For devices that frequently join and leave: Devices like laptops and smartphones get automatic IPs when they connect.
3. Minimizes IP Address Duplication: DHCP reduces the chances of assigning duplicate IP Address.

What is Firewall? How does it work? Explain. 1+4=5

Firewall Definition: A firewall is a security system that monitors, and controls incoming and outgoing traffic network. It acts as a barrier between private network and public internet, protecting the network from unauthorized access and malicious attacks.

A diagram of firewall and firewall

Description automatically generated

How does firewall work?

A firewall works by following predefined set of rules by user.

1. Traffic Monitoring:
2. The firewall inspects incoming and outgoing data packets to decide whether they should be allowed or blocked.
3. Example: When you browse a website, the firewall monitors the website.
4. Rules Checking:
5. The firewall checks these data packets against its predefined rules.
6. Examples of Rules:

* Allow traffic from website 192.168.1.1
* Block access to suspicious domains like xyzmalicious.com.

1. Action:
2. Allow: If the data packet follows the rules, it is allowed.
3. Block: If the data packet violates the rules, it is blocked.
4. Example: If an email contains virus, the firewall blocks it before it reaches to the recipient.
5. Logging:
6. The firewall keeps records of traffic for monitoring and analysis.
7. Example: Network Administrator can review logs to detect unusual activities, like multiple times login attempt from unknown location.

Real world usage

1. Firewalls are commonly used in organizations, personal devices and web servers to protect sensitive information from cyber threats.

Importance

1. Without a firewall, a network is vulnerable to attacks like ransomware.

**What is the use of firewall in network security? Differentiate between IDS an IPS in network security management? 5 marks**

A screenshot of a white and black document

Description automatically generated

**How do you troubleshoot network connectivity problem? Explain. (5 marks)**

By following a systematic approach, we can identify and resolve the network connectivity problem.

steps

1)Identify the problem

1. **What’s going wrong?** Clearly describe the issue. Is your internet completely down, slow internet speed, or disconnecting on and off?
2. **Which devices are affected?** Check if the problem is happening on just one device (like your phone or laptop) or on all devices connected to a network.

2)Check Physical Connection

1. Ensure that all cables (like ethernet cables) are connected.
2. Make sure all devices like modems, routers are powered on.

3)Verify Device Configuration

1. Confirm the network settings like IP Address, firewall rules, DNS settings.
2. Confirm the device is connected to the current network.

4)Test Network Connectivity

1. Use ping command to test connectivity with the specific websites like ping google.com
2. Use the tracert command to trace the path of data packets to a destination, identifying failure nodes.

5)Check Network Equipment

1. Restart the router or network devices to reset the connection.
2. Verify that your router, modem, and network devices are UpToDate with the latest firmware

**What is Digital Signature? What are it's application. (5)**

A digital Signature is a cryptographic technique used to validate the authenticity and integrity of a digital message. It ensures that the message comes from a verified sender (authenticity) and has not been tampered during transmission (integrity). Digital Signature works on **public key infrastructure (PKI).**

1. Private key: used by the sender to create signature.
2. Public key: used by the recipient to verify the signature.

Application of Digital Signatures

1. Online Transactions: used in banking and e-commerce to validate transactions and ensure that the data is sent from authenticity source.
2. Legal Document Authentication: verify the authenticity of contracts, agreements, and official documents and ensure they haven’t been tampered after signing.
3. Secure Email: verify the authenticity of sender and ensure that the content of email has not been altered, provides secure communication.
4. Government Services: Governments use digital signatures to securely sign official documents, such as driving licenses, voting cards, and other identity-verifying documents.
5. Software Distribution: ensure that software, updates, and patches are genuine and haven't been tampered, keeping user safe from cyber threats.
6. Health Sector: ensure that medical reports, prescriptions, and patient forms are authentic and haven't been altered.

Conclusion

Digital Signature play a vital role in ensuring authenticity, integrity, trustworthy, security in various digital communication.

**How it works:**

**A diagram of hashtags and key

Description automatically generated**

1)Key Generation: A pair of key is generated: a public key and private key. The public key is shared with everyone, and private key is kept separate.

2)Signature Creation

b) First, the message is hashed using hashing algorithm (e.g., SHA-256) to produce fixed-size hash value.

c) This hash value is then encrypted with the private key to create digital signature.

3)Signature Verification

a) The recipient uses the senders public key to decrypt the digital signature and obtain the original hash value.

b) The same hashing algorithm is applied to the received message to produce new hash value.

c) If the two-hash value match, then it confirms that document has not been tampered.

**List out major duties of a network administrator and explain any one of them in detail. 4 + 6 = 10**

Major duties of Network Administrator

1) Network Implementation: This involves installing and configuring network hardware and software, such as firewalls, routers, switches, modem, and servers to establish a functional network infrastructure.

2)Network Controlling and Monitoring: This includes continuously monitoring the network to ensure optimal performance, identifying, and addressing security threats.

3)Network Security: They implement and maintain security measures such as firewalls, VPNs, other tools to protect networks against cyber threats.

4) User Support and Training: They provide technical support to users facing network-related problems and train them how to use network efficiently.

5) Backup and Disaster Recovery: They ensure that all critical data is backed up regularly and develop disaster recovery plan to minimize downtime in case of system failure.

Detailed Explanation of Network Security

Network Security is a critical responsibility of a network administrator. They implement security measures to protect the network form internal and external threats such as hacking, virus, cyber threats.

Key task in security management includes:

1. Firewall Implementation: Firewall are configured to inspects incoming and outgoing data packets, allowing safe packets while blocking suspicious threats.
2. Access Control: They assign roles and permission to users, ensuring only authorized user can access sensitive data.
3. Equipment Updates: They keep network software and hardware up-to-date. This helps to fix security vulnerabilities that hackers might exploit.
4. Data Encryption: Encrypting sensitive data during transmission to prevent unauthorized access.
5. Intrusion Detection System: They deploy tools to detect unusual activity within the network and prevent breaches.
6. Incident Response Plan: They have backup plan to respond to unexpected events such as security breaches, disaster, system failure. These plans help to minimize damage control and network is restored to normal operation as quickly as possible.

Detailed Explanation of Data Backup plan

Data Backup plan is a critical responsibility of network administrator. They implement security measures to protect critical data and minimize downtime in case of unexpected events such as system breach, hacking, natural disasters.

Key task in data backup management includes

1. Regular Data Backups: They ensure that critical data is backed up at regular intervals, either on physical storage or cloud-based solutions.
2. Backup Types: They implement different types of backups such as full backups, incremental backups and differential backups, for efficient restoration.
3. Testing Backup Data: They perform regular testing of backup data to confirm their integrity. This helps to ensure that data are not corrupted.
4. Cloud Backups: They utilized Cloud-based solution to protect your data. If your local data storage is damaged or destroyed due to fire or flood.
5. Incident Response Plan: They have backup plan to respond to unexpected events such as system breach, cyber-attacks, natural disasters. These plans help to minimize damage control and network is restored to normal operation as quickly as possible.

**What is Firewall? Explain the usages of firewall. (1 + 4 = 5 marks)**

**Usages of Firewall:**

1. **Network Security:**  
   Firewalls are configured to inspect incoming and outgoing data packets, allowing safe packets while blocking suspicious threats.
2. **Access Control:**  
   They assign roles and permissions to users, ensuring only authorized users can access sensitive data.
3. **Data Encryption:**  
   Encrypting sensitive data during transmission to prevent unauthorized access.
4. **Network Controlling and Monitoring:**  
   This includes continuously monitoring the network to ensure optimal performance, identifying, and addressing security threats.
5. **Preventing Cyber Attacks:**  
   Firewalls protect the system and network from cyber threats like hacking or Distributed Denial of Service (DDoS) attacks or other types of malicious activities. By blocking suspicious traffic, firewalls prevent these attacks.

**Discuss the importance of OSI Reference Model. Briefly explain each of the layer of OSI Reference Model. 3 +7 = 10**

**What is OSI reference model? Describe each layer and compare it with TCP/IP. 2 +8 = 10**

**Definition**

The OSI (Open Systems Interconnection) model is a conceptual framework that explains how different devices (such as computers, phones, servers) in a network communicate with each other. It divides the communication process into seven layers, each layer responsible for specific network function.

**Importance of OSI Reference Model**

1. **Standardization**: Provides a universal standard for reliable communication between devices.
2. **Design**: Allows developers to work on specific layers without affecting other layers, enhancing flexibility.
3. **Security**: Identifies vulnerabilities at specific layers and addressed that issues.
4. **Educational Tool**: widely used for education purpose; understanding for networking concepts

#### ****Explanation of OSI Layers****

**1. Physical Layer**

* **Function**: Only deals with the actual hardware (i.e., cables, routers, plugs, ports) and transmission of data.
* **Processes**: Transmits binary data (0s and 1s) over the physical medium.
* **Comparison with TCP/IP**: In the TCP/IP model, the **Network Interface Layer** combines both OSI Physical and Data Link Layers.

**2. Data Link Layer**

* **Function**: Ensures reliable data transfer between devices within the same network.
* **Processes**: Divides data into **frames**.
* **Protocols**: Ethernet (IEEE 802.3), PPP.
* **Comparison with TCP/IP**: This function is also part of the **Network Interface Layer** in TCP/IP, handling packet framing and MAC addressing.

**3. Network Layer**

* **Function**: Handles the routing of data packets across networks.
* **Processes**:
  + Assigns logical addresses to devices (e.g., IP addresses).
  + Determines the optimal path for data transmission.
* **Protocols**: IP, ICMP.
* **Comparison with TCP/IP**: The **Network Layer** in OSI corresponds to the **Internet Layer** in TCP/IP, responsible for logical addressing and routing.

**4. Transport Layer**

* **Function**: Ensures reliable data transfer between source and destination systems.
* **Processes**: Divides data into **segments**.
* **Protocols**: TCP, UDP.
* **Comparison with TCP/IP**: The **Transport Layer** in OSI is directly comparable to the **Transport Layer** in TCP/IP. Both use protocols like TCP and UDP for reliable data transfer between source and destination systems.

**5. Session Layer**

* **Function**: Establishes, manages, and terminates connections between applications.
* **Processes**:
  + Handles authentication.
  + Supports reconnection after interruptions.
* **Comparison with TCP/IP**: The **Session Layer** has no corresponding layer in the TCP/IP model, as session management is handled within the **Application Layer** of TCP/IP.

**6. Presentation Layer**

* **Function**: Ensures data is in a readable format for the application layer.
* **Processes**: Handles data encryption, compression, and formatting.
* **Examples**: JPEG, ASCII.
* **Comparison with TCP/IP**: The **Presentation Layer** has no corresponding layer in the TCP/IP model. Its functions are often combined with the **Application Layer** in TCP/IP.

**7. Application Layer**

* **Function**: Provides the user interface for network communication (e.g., web browsers, email clients).
* **Protocols**: HTTP, FTP, SMTP.
* **Comparison with TCP/IP**: The **Application Layer** in OSI corresponds to the **Application Layer** in TCP/IP, handling all user-network communication through protocols like HTTP and FTP.

**How can social media be a threat to an organization? What measures can be taken to avoid social media threats? Explain briefly. 2 + 3 = 5**

Social media can pose threat to an organization in several ways:

1.Reputation Damage: Fake news, negative comments or viral complaints can threat to an organization image.

2.Social Engineering and Phishing: Hackers gather sensitive information from social media to launch attacks, tricking employees into revealing credentials or downloading malware.

3.Intellectual Property Theft: Employees may unintentionally share confidential information or trade secrets on social media.

Measures to avoid social media threats

Social media Policy: set clear rules for employees regarding online behavior and the sharing information.

Employee Training: educate staff about phishing attacks, data privacy, and responsible social media use.

Monitoring Tools: continuously monitoring the social media to identify and address security threats earlier.

Access Control: assign roles and permissions to users, ensuring only authorized user can access sensitive information.

Incident Response Plan: develop backup plan to responds to unexpected events (i.e., social media threats), minimizing damage control as quickly as possible.

**How can social media be utilized by any government organization in service delivery? (5 marks)**

Social media can be effective tool for government organization to enhance service delivery. Here’s how:

1)Communication and Public Awareness: Social media platforms provides a direct way to share important services, policies, updates, and news with the citizens. For example, they can post about a new health program or issue emergency alerts during severe weather. This can quickly reach to broad people.

2) Public Engagement: Organization can use social media to interact with citizens by answering questions, gathering feedback. For instance, they can ask for improving public transportation. This helps them to identify citizens priorities.

3)Complaint Resolution: social media allows real-time monitoring of issues reported by the public. For example, a city might use a hashtag like #FixMyRoad for reporting potholes, so officials can respond faster. This helps faster issues fixed.

4)Service Delivery: Organization can use social media to provide service directly to people. For instance, someone could apply for a driving license or pay a bill online without visiting an office.

5)Transparency: social media helps Organization to share about their operations. For example, they can post, updates about how budgets are spent or explain the reason behind new policies. This shows they are accountable to the public.

**How can you use social media in governance? What is the use of anchor and meta tag? Explain with examples. 5 + 5 = 10**

This question is asking for an explanation of the practical ways social media can be utilized by government, public officials or governing organizations to improve administration and serve citizen.

**Use of Anchor and Meta Tags in the Web Development**

**Anchor Tag (<a>)**

**Purpose:** Anchor’s tag is used to create hyperlinks, allowing user to navigate to other web pages or specific section within the page.

Example: Clicking this links redirect the user to another website

A close-up of a website

Description automatically generated

**Additional example: Clicking this links redirect the user within the same page**

**A close-up of a computer code

Description automatically generated**

**Meta Tag(<meta>)**

Purpose: Meta tags provide additional information about web page, such as title, description, keywords, viewport settings. They are not visible to users but used by search engines or other web applications.

Example

A computer code with text

Description automatically generated with medium confidence

These tag help search engines and browsers understand the page content and display in the relevant search results.

**What is cyber-crime? Outline the major computer-related crime defined by electronic Transaction act and also mention the provision of punishment. 3 + 7 = 10**

**Cyber-Crime**  
Cyber-crime refers to criminal activities carried out using computers, digital devices, or the internet. These activities can include crimes like hacking, identity theft, and online fraud. Such crimes target individuals and organizations by exploiting vulnerabilities in digital systems.

**Major Computer-Related Crimes Defined by the Electronic Transaction Act (2063)**

1. **Piracy, Destruction, or Alteration of Computer Source Code**
   * **Punishment:** Imprisonment for up to 3 years, or a fine of up to NPR 2 lakhs, or both.
2. **Unauthorized Access to Computer Materials**
   * **Punishment:** Imprisonment for up to 3 years, or a fine of up to NPR 2 lakhs, or both.
3. **Damage to Any Computer or Information System**
   * **Punishment:** Imprisonment for up to 3 years, or a fine of up to NPR 2 lakhs, or both.
4. **Publication of Illegal Materials in Electronic Form**
   * **Punishment:** Imprisonment for up to 5 years, or a fine of up to NPR 1 lakh, or both.
5. **Computer Fraud**
   * **Punishment:** Imprisonment for up to 2 years, or a fine of up to NPR 1 lakh, or both.
6. **Operating as a Certifying Authority Without a License**
   * **Punishment:** Imprisonment for up to 2 years, or a fine of up to NPR 1 lakh, or both.
7. **Making False Statements to the Controller or Certifying Authority**
   * **Punishment:** Imprisonment for up to 2 years, or a fine of up to NPR 1 lakh, or both.
8. **Providing False Information About a License or Certificate**
   * **Punishment:** Imprisonment for up to 2 years, or a fine of up to NPR 1 lakh, or both.
9. **Divulgence of Confidential Information**
   * **Punishment:** Imprisonment for up to 2 years, or a fine of up to NPR 1 lakh, or both.
10. **Punishment for Offences Committed Outside Nepal**
    * **Punishment:** Punishment as applicable in Nepal.

**Mention any 5 strategies about how they contribute to achieving the objectives of ICT Policy, 2020.**

**List out any five goals/objective of ICT or IT Policy, 2072 (5 Marks)**

**Vision of IT/ICT Policy of Nepal, 2072**  
To transform Nepal into an information and knowledge-based society and economy.

**Mission of IT/ICT Policy of Nepal, 2072**  
To create conditions for the intensified development and growth of the ICT sector as a key driver for Nepal’s sustainable development and poverty reduction strategies.

**Objectives of ICT/IT Policy of Nepal, 2072**

1. **Empower Nepal in the Global Knowledge Society**
   * Enable Nepal to actively participate in the global digital community.
2. **Improve Government Delivery Service**
   * Use ICT to promote transparency, efficiency, and inclusiveness in government operations.
3. **Develop National ICT Infrastructure**
   * Build a secure, reliable, and sustainable ICT infrastructure that meets both local and international standards.
4. **Enhance Digital Literacy and Education**
   * Deploy ICT in schools and universities to improve education and make digital learning more accessible.
5. **Promote E-Commerce and SMEs**
   * Support small and medium enterprises (SMEs) in improving their work, especially in agriculture, tourism, and manufacturing.
6. **Encourage Research and Innovation**
   * Focus on ICT-based research to help low-income communities deal with environmental, economic, and social challenges.
7. **Support Local Content Development**
   * Encourage the creation and sharing of local content to help preserve Nepal’s culture and languages.
8. **Promote Tourism Through ICT**
   * Use ICT to promote Nepal’s tourist spots both locally and internationally.
9. Affordable Public Access Point

Establish innovative, low-cost public access point in villages or community to make ICT easily available for everyone.

10.Last -mile internet access

Provide affordable internet services to rural and undeserved areas so everyone can have equal access

11.Youth and Women Empowerment in ICT

Encourage youth and women to take part in ICT project, especially in creating media and content development.

**What is cybersecurity? What are the various common security threats? 2 + 3 = 5 marks**

Cybersecurity is the practice of protecting of computer system, network, servers, mobile devices and digital data from unauthorized access, theft, damage, cyberattacks. The goal of cybersecurity is to minimize the risk of cyber threats such as malware, phishing, ransomware, and hacking. This ensures the confidentiality and integrity of the digital assets.

**In today's world, what are the various types of security threats to the systems, data, and users? What are the safeguards and prevention mechanisms that need to be implemented in order to keep the data safe from them?**

**What is computer security threats? Explain its types. What are the effective remedies and protection measures to safeguard against them? 2 + 5 + 3 = 10**

**What are the common security threats? Give proper mechanism to mitigate.**

**5 + 5 = 10**

**What are common computer security threats and protection measures?**

**2.5 + 2.5 = 5 marks**

**Computer Security Threats**

Computer security threats refer to potential risks or vulnerabilities in computer systems that can be exploited to cause damage or gain unauthorized access. These threats can come from various sources, including malicious software and human error. Such threats can compromise the confidentiality and integrity of the system.

**Types of Computer Security Threats**

1. **Malware (Malicious Software)**
   * **Definition:** Software designed to damage or gain unauthorized access to a computer system.
   * **Examples:** Viruses, worms, Trojans, spyware, adware, ransomware.
2. **Phishing Attacks**
   * **Definition:** Tricking users to reveal sensitive information (such as login credentials or credit card details) by pretending to be trustworthy.
   * **Example:** A fake email that looks like it came from a bank, asking users to click a link and enter login credentials.
3. **Denial of Service Attacks (DoS)**
   * **Definition:** Flooding a network or server with traffic to make it unavailable to users.
   * **Example:** Multiple computers send traffic to a website, causing it to crash.
4. **Man-in-the-Middle Attack**
   * **Definition:** Intercepting communication between two parties; changing information or stealing data.
   * **Example:** Intercepting data between a user and a website to steal login credentials.
5. **Unauthorized Access**
   * **Definition:** Gaining access to another system or network without permission.
   * **Example:** Exploiting vulnerabilities in a system to gain unauthorized access.
6. **Social Engineering**
   * **Definition:** Hackers gather sensitive information from social media to launch attacks, tricking employees into revealing credentials or downloading malware.
   * **Example:** A scammer calls an employee, pretending to be from IT support and asking for login credentials to fix an issue.

**Effective Remedies and Protection Measures**

1. **Firewall Implementation**
   * Firewalls should be configured to inspect incoming and outgoing data packets, allowing safe packets while blocking suspicious threats.
2. **Access Control**
   * Assign roles and permissions to users, ensuring that only authorized users can access sensitive data.
3. **Regular Software and Hardware Updates**
   * Keep network software and hardware up-to-date. This helps to fix security vulnerabilities that hackers might exploit.
4. **Data Encryption**
   * Encrypt sensitive data during transmission to prevent unauthorized access.
5. **Intrusion Detection System (IDS)**
   * Deploy tools to detect unusual activity within the network and prevent breaches.
6. **Incident Response Plan**
   * Develop a backup plan to respond to unexpected events, such as security breaches or system failure. These plans help to minimize damage and ensure the network is restored to normal operation as quickly as possible.

**Define Routers, Hubs, and Switches. (**5 marks)

**Routers**

**Definition**:  
A router is a networking device that connects different networks and forwards data between them.  
It operates at the **Network Layer (Layer 3)** of the OSI model.

**Function**:

* **Check IP Address**: Routers analyze the IP address in each data packet header to determine its destination.
* **Use Routing Tables**: Routers use routing tables to determine the optimal path for the data packets based on their destination IP address.
* **Forward Data**: Once the optimal path is determined, it forwards the data packets to the destination network.

**Switch**

**Definition**:  
A switch is a networking device that connects multiple devices within the same network and forwards data based on the MAC address.  
It operates at the **Data Link Layer (Layer 2)** of the OSI model.

**Function**:

* **Check MAC Address**: Switches analyze the MAC address in each packet header to identify the destination device.
* **Forward to Specific Port**: Once the MAC address is identified, it forwards the data packets to the appropriate connected port.
* **Reduce Network Traffic**: By sending data packets only to the intended device, it minimizes network congestion.

**Hub**

**Definition**:  
A hub is a networking device that connects multiple devices in a network.  
It operates at the **Physical Layer (Layer 1)** of the OSI model.

**Function**:

* **Broadcast to All Devices**: The hub broadcasts incoming data to all connected devices, regardless of the destination.
* **Network Congestion**: Broadcasting data to all devices leads to network collisions.

**Provide a comparison between Hub, Switch, and Router.**

A screenshot of a computer

Description automatically generated

**Explain various security mechanism in details (10 marks).**

**1. Firewall Implementation**

* Firewalls should be configured to inspect incoming and outgoing data packets, allowing safe packets while blocking suspicious threats.

**2. Access Control**

* Assign roles and permissions to users, ensuring that only authorized users can access sensitive data.

**3. Equipment Updates**

* Keep network software and hardware up-to-date. This helps to fix security vulnerabilities that hackers might exploit.

**4. Data Encryption**

* Encrypt sensitive data during transmission to prevent unauthorized access.

**5. Intrusion Detection System (IDS)**

* Deploy tools to detect unusual activity within the network and prevent breaches.

**6. Incident Response Plan**

* Develop a backup plan to respond to unexpected events, such as security breaches or system failure. These plans help to minimize damage and ensure the network is restored to normal operation as quickly as possible.

**7. Multi-Factor Authentication**

* Ensure an extra layer of security to access sensitive information. This can include a password combined with a fingerprint or security code for additional protection.

**8. Network Controlling and Monitoring**

* This includes continuously monitoring the network to ensure optimal performance, identifying, and addressing security threats.

**9. Training**

* Provide cybersecurity training to users to protect them from threats like phishing attacks and social engineering. Teach them to use strong passwords and avoid clicking on links or downloading from malicious websites.

**10. Backup and Data Recovery**

* Ensure that all critical data is backed up regularly and ensure a data recovery plan to minimize downtime in case of system failure or security breach.

**What are the major functions, duties and powers of a controller as per electronic transaction act, 2063? 10 marks**

1.Issuing Licenses to Certifying Authorities

2.Supervising and Monitoring Certifying Authorities

3.The controller set the rules that certifying authorities must follow to verify digital signature.

4.The controller defines the rules that certifying authorities must follow to operate their business properly and legally.

5.The controller determines the format of digital certificates and the information that must be included in them.

6.The controller defines the procedures that certifying authorities must follow when interacting with subscribers to ensure clarity and security.

7.Then controller must maintain a record of information disclosed by certifying authorities and ensure it is stored in an accessible, regularly updated public databases.

8.The controller is responsible for carrying out other operations as required by law.