Question 1

a) Using the help of a diagram, explain the key differences between the OSI 7 Layer model and the TCP/IP Reference model.

OSI 7 Layer Model:

- Layers:
    i. Physical
    ii. Data Link
    iii. Network
    iv. Transport
    v. Session
    vi. Presentation
    vii. Application

TCP/IP 4 Layer Model:

- Layers:
    i. Network Interface (or Link)
    ii. Internet
    iii. Transport
    iv. Application

Key Differences:

1. Number of Layers:
    - OSI Model: 7 layers.
    - TCP/IP Model: 4 layers.
2. Layer Functions:
    - OSI separates presentation and session layers, which are part of the application layer in TCP/IP.
    - OSI's data link and physical layers are combined into the network interface layer in TCP/IP.
3. Usage:

- OSI is a theoretical framework; TCP/IP is a practical framework used in real-world networking.

Diagram:

```
OSI Model:                  TCP/IP Model:
+-----------+               +-----------+
| Application| <---> Application
+-----------+               +-----------+
| Presentation|
+-----------+
|    Session  |
+-----------+
|  Transport  | <---> Transport
+-----------+               +-----------+
|    Network  | <---> Internet
+-----------+               +-----------+
|  Data Link | <---> Network Interface
+-----------+               +-----------+
|   Physical  |
+-----------+
```

b) Which network devices operate at the following layers of the OSI Model?

i. Layer 1 (Physical Layer):

- Devices: Hubs, Repeaters, Physical cables (Ethernet cables, fiber optics)

ii. Layer 2 (Data Link Layer):

- Devices: Switches, Bridges, Network Interface Cards (NICs)

iii. Layer 3 (Network Layer):

- Devices: Routers, Layer 3 Switches

iv. Layer 1 up to Layer 7:

- Devices: Firewalls (Layer 3 to 7), Gateways (Layer 7), Network Management

Systems

c) Indicate the Protocol Data Unit (PDU) used at each layer of the OSI Layer Model.

1. **Physical Layer:** Bits
2. **Data Link Layer:** Frames
3. **Network Layer:** Packets
4. **Transport Layer:** Segments (TCP) / Datagrams (UDP)
5. **Session Layer:** Data
6. **Presentation Layer:** Data
7. **Application Layer:** Data

d) Using a diagram, describe data encapsulation/de-encapsulation within the OSI Reference Model.

Data Encapsulation Process:

1. **Application Layer:** Data is created.
2. **Presentation Layer:** Data is formatted and encrypted.
3. **Session Layer:** Data is added with session information.
4. **Transport Layer:** Data is segmented and headers are added.
5. **Network Layer:** Data is encapsulated into packets with network headers.
6. **Data Link Layer:** Data is encapsulated into frames with MAC headers and trailers.
7. **Physical Layer:** Data is converted into bits for transmission.

Data De-encapsulation Process:

1. **Physical Layer:** Bits are received.
2. **Data Link Layer:** Frames are processed and headers/trailers are removed.
3. **Network Layer:** Packets are processed and headers are removed.
4. **Transport Layer:** Segments are processed and headers are removed.
5. **Session Layer:** Session information is processed.
6. **Presentation Layer:** Data is decrypted and formatted.
7. **Application Layer:** Data is delivered to the application.

Diagram:

```
Sender:                                                 Receiver:
[Application] --- Data --->                             [Application]
[Presentation] --- Data --->                            [Presentation]
[Session] --- Data --->                                 [Session]
[Transport] --- Segment --->                            [Transport]
[Network] --- Packet --->                               [Network]
[Data Link] --- Frame --->                              [Data Link]
[Physical] --- Bits --->                                [Physical]
```

Question 2

Let's address each part of Question 2 based on the provided instructions.

a) Explain the differences between circuit switching and packet switching and provide examples of each technology.

Circuit Switching:

- Definition: Establishes a dedicated communication path between two endpoints for the duration of the communication session.
- Characteristics:
    - Fixed bandwidth.
    - Continuous transmission.
    - Connection-oriented.
- Examples:
    - Traditional telephone networks (PSTN).
    - ISDN (Integrated Services Digital Network).

Packet Switching:

- Definition: Data is broken into packets and each packet is transmitted independently over the network. The packets may take different paths and are reassembled at the destination.
- Characteristics:

        - Dynamic bandwidth allocation.
        - Bursty transmission.
        - Connectionless.
    - Examples:
        - Internet Protocol (IP).
        - Ethernet.

b) Differentiate between frame relay and DSL.

Frame Relay:

- Definition: A high-speed packet-switched WAN technology that provides a cost-effective way to connect local area networks (LANs) and transfer data between endpoints.
- Characteristics:
    - Utilizes virtual circuits.
    - Suitable for bursty data traffic.
    - Provides variable-length frames.
- Use Case: Used for connecting enterprise LANs to WANs.

DSL (Digital Subscriber Line):

- Definition: A family of technologies that provides internet access by transmitting digital data over the wires of a local telephone network.
- Characteristics:
    - Utilizes existing telephone lines.
    - Provides high-speed internet access.
    - Symmetric and asymmetric options (ADSL, VDSL).
- Use Case: Used for providing broadband internet access to homes and small businesses.

c) Recommend a primary and where relevant a backup network access media for the following scenarios:

i. Connecting 2 retail shops which are 100m apart.

- Primary: Ethernet (Cat6 cable).

- **Backup:** Wi-Fi with point-to-point bridge.

ii. **A new embassy based in Mauritius which needs to have a secured, reliable connection to its mother country.**

- **Primary:** Leased Line (dedicated, high-speed connection).
- **Backup:** VPN over a high-speed internet connection.

iii. **A new bank branch needs to connect to its Head Office which is 5kms away.**

- **Primary:** Fiber Optic Cable.
- **Backup:** MPLS (Multiprotocol Label Switching) network.

iv. **A recreational park on a mountainous region needs internet access - there is currently no fibre or copper connectivity.**

- **Primary:** Satellite Internet.
- **Backup:** 4G/5G LTE.

v. **A staff just moved to a new house and does not have an internet connection yet, he needs to urgently work from home.**

- **Primary:** Mobile Hotspot (4G/5G LTE).
- **Backup:** Wi-Fi from a nearby public network.

d) Draw the logical topology for a simple network - a company which has a router connecting to the internet, 2 switches which have 5 workstations connected to each switch, an access point and 2 laptops connecting through Wi-Fi.

Logical Topology:

```
          [Internet]
              |
          [Router]
              |
       -----------------
       |               |
   [Switch 1]       [Switch 2]
   |   |   |   |   | |   |   |   |   |
[PC1][PC2][PC3][PC4][PC5][PC6][PC7][PC8][PC9][PC10]

       [Access Point]
          /   \
      [Laptop1][Laptop2]
```

Question 3

Sure, let's break down and answer each part of the question:

Question 3 [20 Marks]

a) Explain the key differences between Link State routing protocols and Distance Vector protocols and give an example of each. (5 marks)

Link State Routing Protocols:

- Key Concept: Each router independently maps out the network topology.
- Method: Routers use information about the state of each link (i.e., how good or bad a connection is) to create a map of the network. This map is used to calculate the best path to a destination.
- Updates: Only when there is a change in the network topology, routers send updates.
- Examples: OSPF (Open Shortest Path First), IS-IS (Intermediate System to Intermediate System).

Distance Vector Routing Protocols:

- **Key Concept:** Routers share information about the distance to destinations with their immediate neighbors.
- **Method:** Each router calculates routes based on the distance (hop count) and direction (vector) to any given destination. The information is shared with neighboring routers.
- **Updates:** Periodically and whenever a change is detected in the topology, all or part of the routing table is sent to all neighbors.
- **Examples:** RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol).

b) Using a diagram, describe how OSPF works, what metric and algorithm this routing protocol uses to find the best path to a destination. (5 marks)

Explanation:

- **OSPF (Open Shortest Path First)**: OSPF uses the Dijkstra algorithm to calculate the shortest path tree for each route. The metric used by OSPF is cost, which is based on the bandwidth of the links.

Diagram:

1. **Link State Advertisement (LSA) Flooding:**
    - Each router broadcasts its link state to all other routers in the network area.
2. **Topology Database:**
    - Each router builds a topology database based on the LSAs received.
3. **Shortest Path Tree Calculation:**
    - Using Dijkstra's algorithm, each router calculates the shortest path tree to all destinations.
4. **Routing Table:**
    - The shortest path tree is used to populate the routing table with the best paths to each destination.

```
           [Router A]
           /    |    \
       [Router B] [Router C]
       /           /         \
[Router D] [Router E] [Router F]
```

c) Using a diagram, describe how BGP routes traffic between different Autonomous Systems. (5 marks)

Explanation:

- BGP (Border Gateway Protocol): BGP is used to exchange routing information between different Autonomous Systems (AS). It uses path vector routing and maintains a path (list of AS numbers) to reach a destination.

Diagram:

1. Autonomous Systems (AS):
    - Each AS is represented by a router or a set of routers.
2. BGP Peering:
    - BGP routers establish peering sessions with routers in other ASes.
3. Path Vector:
    - BGP advertises the entire path (sequence of AS numbers) to reach a destination network.
4. Decision Process:
    - BGP routers use path attributes like AS-path length, policy, and other criteria to select the best path.

```
      AS1           AS2           AS3
    [Router]----[Router]----[Router]
       |              |              |
[Network A]   [Network B]   [Network C]
```

d) Describe the 3-way handshake protocol for TCP Connection Establishment. (5 marks)

Explanation:

- Step 1: SYN
    - The client sends a SYN (synchronize) message to the server to initiate a connection.
- Step 2: SYN-ACK
    - The server responds with a SYN-ACK (synchronize-acknowledge) message to acknowledge the SYN request and to initiate a connection back to the client.
- Step 3: ACK
    - The client sends an ACK (acknowledge) message to the server to acknowledge the SYN-ACK, completing the connection establishment.

Sequence:

1. Client → Server: SYN (Seq=1000)
2. Server → Client: SYN-ACK (Seq=2000, Ack=1001)
3. Client → Server: ACK (Seq=1001, Ack=2001)

```
Client                            Server
   |         SYN (Seq=x)      --->    |
   |   <--- SYN-ACK (Seq=y, Ack=x+1) |
   |     ACK (Seq=x+1, Ack=y+1) ---> |
```

Question 4

a) Compare Twisted pair, Coaxial, and Fibre optics considering features such as network type, transmission distance, cost, security, and transmission speed. (5 marks)

Twisted Pair:

- Network Type: Commonly used in Ethernet networks.
- Transmission Distance: Up to 100 meters.
- Cost: Low cost.
- Security: Moderate; susceptible to electromagnetic interference and

eavesdropping.
- **Transmission Speed:** Up to 1 Gbps for Cat5e and Cat6 cables; up to 10 Gbps for Cat6a and higher.

Coaxial Cable:

- **Network Type:** Used for cable television, internet, and early Ethernet.
- **Transmission Distance:** Up to 500 meters for Ethernet.
- **Cost:** Moderate cost.
- **Security:** Better than twisted pair; more resistant to electromagnetic interference.
- **Transmission Speed:** Up to 10 Mbps for older standards, up to 1 Gbps with modern technology.

Fibre Optics:

- **Network Type:** Used for high-speed internet, backbone networks, and long-distance telecommunications.
- **Transmission Distance:** Several kilometers.
- **Cost:** Higher cost.
- **Security:** High; very secure against electromagnetic interference and eavesdropping.
- **Transmission Speed:** Up to 100 Gbps and beyond.

b) What are the differences between Single-mode and Multi-mode fibre? (5 marks)

Single-mode Fibre:

- **Core Diameter:** Smaller core (8-10 micrometers).
- **Light Source:** Laser.
- **Transmission Distance:** Longer distances (up to 40 km and beyond).
- **Bandwidth:** Higher bandwidth.
- **Applications:** Long-distance communication, high-speed networks.

Multi-mode Fibre:

- **Core Diameter:** Larger core (50-62.5 micrometers).
- **Light Source:** LED.

- **Transmission Distance:** Shorter distances (up to 2 km).
- **Bandwidth:** Lower bandwidth compared to single-mode.
- **Applications:** Short-distance communication, within buildings or campuses.

c) What are the components of an optical transmission system and explain how data is transmitted from source to destination? (5 marks)

Components:

1. **Transmitter:** Converts electrical signals into optical signals. Typically uses a laser diode or LED.
2. **Optical Fibre:** Transports the optical signals over a distance. Can be single-mode or multi-mode fibre.
3. **Optical Amplifiers:** Boost the strength of the optical signal without converting it to an electrical signal. Used for long-distance transmission.
4. **Receiver:** Converts optical signals back into electrical signals. Typically uses a photodetector or photodiode.
5. **Optical Regenerators:** Converts optical signals to electrical signals for regeneration and then back to optical signals. Used for very long distances to maintain signal integrity.

Transmission Process:

- The transmitter converts electrical data signals into light signals using a light source (laser or LED).
- The light signals are sent through the optical fibre, which guides the light over distances with minimal loss.
- Optical amplifiers may be used to boost signal strength if the distance is very long.
- At the destination, the receiver converts the light signals back into electrical signals using a photodetector.
- The electrical signals are then processed and interpreted by the receiving equipment.

d) You are a network administrator and you have been provided the prefix 192.168.5.129 /28. You have been requested to find out the network address, broadcast address, and the range of usable IP addresses that can be allocated to workstations. (5 marks)

Given:

- IP Address: 192.168.5.129
- Subnet Mask: /28

Calculations:

- **Subnet Mask in Dotted Decimal:** 255.255.255.240
- **Number of Hosts:** $2^{(32-28)} - 2 = 16 - 2 = 14$

Network Address:

- IP Address (Binary): 11000000.10101000.00000101.10000001
- Subnet Mask (Binary): 11111111.11111111.11111111.11110000
- Network Address (Binary): 11000000.10101000.00000101.10000000
- Network Address: 192.168.5.128

Broadcast Address:

- Broadcast Address (Binary): 11000000.10101000.00000101.10001111
- Broadcast Address: 192.168.5.143

Usable IP Addresses:

- Range: 192.168.5.129 to 192.168.5.142
- Usable IP Addresses: 192.168.5.129 to 192.168.5.142

Summary:

- **Network Address:** 192.168.5.128
- **Broadcast Address:** 192.168.5.143
- **Usable IP Range:** 192.168.5.129 to 192.168.5.142

Question 5

a) Describe the advantages of wireless networks over wired networks. (5 marks)

Advantages of Wireless Networks:

1. Mobility: Users can move around within the coverage area and remain connected to the network.
2. Ease of Installation: No need for extensive cabling, which makes setup faster and less disruptive.
3. Cost-Effective: Reduces the need for physical cables and the associated labor costs of installation.
4. Scalability: Easier to add new devices to the network without running new cables.
5. Flexibility: Ideal for places where wiring is difficult or impossible, such as historical buildings or outdoor areas.

b) Using a diagram, explain the concept of a Virtual Private Network and provide some common applications. (5 marks)

Explanation:

- A Virtual Private Network (VPN) creates a secure connection over a public network (such as the internet). It encrypts the data transmitted between the user's device and the VPN server, providing privacy and security.

Diagram:

```
[User Device] --encrypted-- [Internet] --encrypted-- [VPN Server] -- [Corporate Network]
```

Common Applications:

1. Remote Access: Employees can securely connect to their company's internal network from anywhere.
2. Privacy: Individuals can browse the internet securely and privately, protecting their data from eavesdroppers.
3. Geo-Restrictions: Users can access content that is restricted based on their

geographic location.
4. **Security:** Encrypts data transmitted over unsecured networks, such as public Wi-Fi hotspots.

c) What are some of the common applications of Bluetooth and describe some of the features of this protocol? (5 marks)

Common Applications of Bluetooth:

1. **Wireless Headsets:** For hands-free communication with mobile phones.
2. **File Transfer:** Between devices such as smartphones and laptops.
3. **Wireless Peripheral Devices:** Such as keyboards, mice, and printers.
4. **Health Monitoring Devices:** Such as fitness trackers and smartwatches.
5. **Automotive Systems:** For hands-free calling and audio streaming in cars.

Features of Bluetooth Protocol:

1. **Short-Range Communication:** Typically up to 10 meters, though newer versions can extend further.
2. **Low Power Consumption:** Designed for low energy usage, making it suitable for battery-powered devices.
3. **Frequency Hopping:** Uses frequency hopping spread spectrum (FHSS) to reduce interference from other wireless technologies.
4. **Secure Connections:** Supports encryption and authentication to ensure secure communication.
5. **Ad-Hoc Networking:** Allows devices to connect and communicate directly without a fixed infrastructure.

d) What are some common components of a Wireless LAN? (5 marks)

Common Components of a Wireless LAN:

1. **Wireless Access Points (APs):** Devices that allow wireless devices to connect to a wired network using Wi-Fi.
2. **Wireless Network Interface Cards (NICs):** Hardware installed in devices to enable wireless communication.
3. **Router:** Connects the wireless network to the internet and manages data traffic.
4. **Antennas:** Enhance the signal strength and coverage area of the wireless network.

5. **Wireless Controller:** Manages multiple access points and ensures seamless connectivity and network management.