1. Create a star, bus, ring and mesh topology network using a Cisco packet tracer simulator.

2. Set up a hybrid topology that includes all topologies in the Cisco packet tracer and simulate it.

3. Using the simulator, simulate a LAN network. Perform a ping operation between two virtual machines. What does a successful ping indicate? Use the "traceroute" command to trace the route between two hosts. What information does it provide?

A successful **ping** means that two devices are connected properly and can communicate over the network. It shows that the IP settings are correct, the cables and ports are working, and the network is set up correctly.

The `traceroute` command shows the path that data takes from one host to another. It lists all the routers (hops) between the source and the destination, along with the time it takes to reach each one. This helps in finding where delays or issues are happening in the network.

4. Configure a DNS server in the simulator and simulate hostname resolution using the "host" command. What is the role of DNS in network communication?

A DNS (Domain Name System) server translates website names (like www.google.com) into IP addresses (like 142.250.190.14). The role of DNS in network communication is to convert website names into IP addresses. This allows devices to find and connect to websites using names we can easily remember, instead of numbers.

5. Design a network with the IP address 192.168.1.0/24. Implement subnetting to create four subnetworks. What are the subnetwork addresses and subnet masks?

Subnetwork addresses (or subnet addresses) identify smaller parts of a larger network. They help organize and manage IP addresses more efficiently.

Subnet masks are used to divide an IP address into the network part and the host part, helping devices know if another IP is in the same network or not.A **subnet mask** is a 32-bit number used in conjunction with an IP address to determine the **network portion** and the **host portion**.It tells the device which part of the IP address refers to the network and which part refers to individual devices (hosts) within that network.

For example:

- **IP Address:** `192.168.1.100`
- **Subnet Mask:** `255.255.255.0`

The subnet mask of `255.255.255.0` means the first three octets (`192.168.1`) are the **network part**, and the last octet (`100`) refers to the **host part**.

6. **Using CIDR notation, design a network with a block of IP addresses from 172.16.0.0 to 172.16.3.255. What is the CIDR notation for this address block?**

Convert the range to size:

- Starting IP: 172.16.0.0
- Ending IP: 172.16.3.255
- Total IPs = (3 - 0 + 1) × 256 = 4 × 256 = 1024 IP addresses

Find the closest power of 2:

- 210=10242^{10} = 1024210=1024, so we need a /22 network (because 32 - 10 = 22)

CIDR Notation:

- The address block starts at 172.16.0.0
- So, CIDR = 172.16.0.0/22

7. Simulate a hub, switch and router in the network and explain how it operates. What are the limitations of a hub in terms of traffic management?

🚫 Limitations of a Hub in Traffic Management:

1. 🔁 Broadcasts All Traffic:
    - A hub forwards incoming data to *all* ports, not just the intended recipient.
    - This floods the network with unnecessary traffic.
2. 🧠 No Intelligence:

- Hubs don't read MAC addresses or manage routing — they work at Layer 1 (Physical Layer) of the OSI model.
- They can't distinguish between devices or decide where data should go.

3. 📶 One Collision Domain:
   - All devices connected to a hub share the same collision domain.
   - More devices = higher chances of data collisions = slower network.
4. 📉 Poor Scalability:
   - Adding more devices significantly reduces performance.
   - Not suitable for large or growing networks.
5. ⛔ No Full-Duplex:
   - Most hubs operate in half-duplex mode.
   - Devices can either send or receive at one time, not both — this increases latency and collisions.
6. 🛡️ No Security:
   - Anyone connected to the hub can potentially see all traffic — big security risk!

8. Configure a router in the simulator to connect two LANs. How does routing differ from switching in a network?

🔁 Routing vs. Switching

Feature	Routing	Switching
OSI Layer	Layer 3 (Network)	Layer 2 (Data Link)
Device	Router	Switch
Addressing	Uses IP addresses	Uses MAC addresses
Scope	Connects different networks (LANs)	Connects devices *within* a LAN
Traffic Control	Can make decisions based on IP path	Forwards frames based on MAC address
Speed	Slower due to complex decisions	Faster for local traffic
Security & Filtering	More control via ACLs, NAT, etc.	Less advanced in security features

9. Design a wired and wireless network using the Cisco packet tracer and enable DHCP (Dynamic Host Configuration Protocol). What is the role of DHCP in a wireless network?

DHCP automatically assigns IP addresses and other network settings (like gateway, DNS) to devices when they connect to the network — no need for manual setup.

Why it's important in wireless networks:

1. 🪄 **Plug-and-Play Connectivity**
    - When a device (like your phone or laptop) connects to Wi-Fi, it instantly gets an IP address from the DHCP server.
    - Makes the network user-friendly — no tech skills

needed to connect.

2. 📱 **Mobility Support**
    - Users frequently join and leave wireless networks.
    - DHCP handles this dynamic nature by leasing IP addresses for a limited time.
3. 📈 **Efficient IP Management**
    - Prevents IP conflicts by tracking which IP is assigned to which device.
    - Reclaims unused IPs when devices disconnect or go offline.
4. 🔌 **Simplifies Network Admin Work**
    - No need to manually assign IPs to every device.
    - Especially useful in places like cafes, schools, airports, etc.

10.Configure a web server in the Cisco packet tracer and host a simple webpage. Access the webpage from a client. What is the role of a web server in client-server communication?

Role of a Web Server in Client-Server Communication:

A **web server** acts as the intermediary between a **client** (such as a web browser) and the **web content** (like a website or web

application) on the server. Here's how it works in the context of client-server communication:

---

1. **Handling Client Requests**:
    - The **client** (usually a web browser) sends an **HTTP request** to the web server to access resources like web pages, images, or other files hosted on the server.
    - Example: When you enter a URL in the browser, it sends an HTTP request to the web server.
2. **Processing Requests**:
    - The **web server** receives the request and processes it. It can either serve a static file (like HTML, CSS, JavaScript, or image files) or dynamically generate content (by interacting with backend scripts, databases, etc.).
    - If dynamic content is required (e.g., PHP, Python, etc.), the web server passes the request to the relevant application or script for processing.
3. **Serving the Content**:
    - Once the request is processed, the web server responds with the requested content, usually in the form of an **HTTP response**. This might be an HTML page, a JSON object, or other resources that the client needs.
    - Example: The server sends back the HTML page that the browser requested, along with any necessary assets (like images or stylesheets).
4. **Communication Protocol (HTTP/HTTPS)**:
    - **HTTP (Hypertext Transfer Protocol)** or **HTTPS (secure version)** is the communication protocol used between the client and the web server. It governs how the requests and responses are formatted and transmitted.
5. **Stateless Communication**:
    - Web servers typically operate in a **stateless manner**, meaning each request from the client is treated independently. However, sessions or cookies may be used to maintain context between requests.
6. **Security**:
    - Web servers also handle security by implementing SSL/TLS encryption (for HTTPS), ensuring secure communication between the client and the server, especially for sensitive data like passwords or payment details.

11. Simulate a network with three routers and implement the RIP (Routing Information Protocol) routing protocol. Explain how RIP updates routing tables.

- RIP uses **hop count** as the metric for determining the best path.
- The **maximum number of hops** allowed is **15**. If a route has 16 hops, it is considered **unreachable**.
- RIP updates are sent **every 30 seconds**.

How RIP Updates the Routing Table:

1. **Periodic Updates**:
    - Every 30 seconds, each router sends its full routing table to its **directly connected neighbors**.
2. **Receiving Updates**:
    - When a router receives a RIP update from a neighbor, it checks the routes in that update.
    - For each route, it **adds 1 hop** to the hop count and compares it to its existing route.
3. **Routing Table Update**:
    - If the new route has a **lower hop count**, the router **updates its table** to use the new route.
    - If the hop count is **higher**, it ignores the update.

4. **Route Timeout**:
    - If a route is not updated within **180 seconds**, it is marked as **invalid**.
    - After **240 seconds**, it is **removed** from the table.
5. **Loop Prevention**:
    - RIP uses techniques like **split horizon**, **route poisoning**, and **hold-down timers** to avoid routing loops.

12. Set up OSPF (Open Shortest Path First) routing between routers in the simulator. Explain the advantages of OSPF over RIP.

Advantages of OSPF Over RIP

OSPF (Open Shortest Path First) is a **link-state routing protocol**, while **RIP (Routing Information Protocol)** is a **distance-vector protocol**. OSPF provides several benefits over RIP, especially in medium to large-scale networks.

---

1. Faster Convergence

- OSPF reacts quickly to network changes and updates only the affected routers.
- RIP takes up to 30 seconds to send updates, leading to slower convergence.

---

2. No Hop Count Limitation

- RIP supports a maximum of **15 hops**, making it unsuitable for large networks.
- OSPF has **no such limitation**, making it scalable for enterprise-level networks.

---

3. Better Metric Calculation

- RIP uses **hop count** as its metric, which may not always choose the best path.
- OSPF uses **cost based on bandwidth**, allowing more efficient and optimized routing.

---

4. Hierarchical Network Design

- OSPF supports network division into **areas** (including a backbone area), improving scalability and manageability.
- RIP uses a **flat topology** and does not support hierarchical design.

---

5. Lower Bandwidth Consumption

- RIP sends the **entire routing table every 30 seconds**, consuming more bandwidth.
- OSPF sends **only changes when they occur**, reducing unnecessary traffic.

---

6. Enhanced Security

- OSPF supports **authentication** (e.g., MD5) for secure routing updates.

- RIP has minimal or no authentication features.

---

8. More Reliable and Scalable

- OSPF is designed for **large, complex, and mission-critical networks**.
- RIP is simple and suitable only for **small networks**.

13. Simulate BGP (Border Gateway Protocol) routing between routers. What are the use cases for BGP in real world networks?

BGP is a **path vector routing protocol** used to exchange routing information **between autonomous systems (AS)** on the Internet. It is the **protocol that makes the Internet work** by managing how packets are routed across different organizations and networks.

🔹 **1. Internet Service Providers (ISPs)**

- **Primary use case** of BGP.
- ISPs use BGP to **connect and exchange routing information** with other ISPs and customers.
- Helps ensure **efficient and redundant Internet**

connectivity.

🔹 **2. Multi-Homing (Redundant Internet Connections)**

- Companies or data centers connect to **multiple ISPs** for high availability.
- BGP manages **which path to use** and provides **failover** in case one connection goes down.

🔹 **3. Data Centers and Cloud Providers**

- Large-scale data centers (e.g., Google, AWS, Microsoft Azure) use BGP to:
  - Connect to multiple networks.
  - Manage traffic **between different regions or availability zones**.
  - **Load balance** and ensure **reliability**.

🔹 **4. Traffic Engineering**

- BGP allows **manipulation of path selection**.
- Organizations use it to **control incoming/outgoing traffic** based on:
  - Path length
  - Policy
  - Bandwidth or reliability

🔹 **5. Content Delivery Networks (CDNs)**

- CDNs like Akamai or Cloudflare use BGP to:
  - Announce IP prefixes from **different locations**.
  - Serve content from **servers closest** to the user.

🔹 **6. Internet Backbone Routing**

- Global Internet routing depends on BGP to:
  - **Exchange routes** among thousands of autonomous systems.
  - Maintain **global reachability**.

🔹 **7. Enterprise WAN Routing**

- Large enterprises use BGP to:
  - Connect **multiple branch offices or sites**.
  - **Integrate with MPLS/VPN** or leased lines from ISPs.
  - Maintain **internal routing policies** across sites.

14. Set up HTTP, FTP,telnet,ssh, and servers in the Cisco packet tracer. Explain the functionality of each of these servers.

- **HTTP (HyperText Transfer Protocol)** allows users to access and view websites via a browser. It delivers web pages from the server to the client.

Functionality:

- **FTP (File Transfer Protocol)** is used to **upload and download files** between a client and server

Functionality:

- **DNS (Domain Name System)** translates domain names (e.g., google.com) into IP addresses, allowing users to access websites using easy-to-remember names.

15. Implement the RSA encryption and decryption processes in Python. Provide a step-by-step explanation of how the algorithm works.