Batch: C2	Roll No.:16010122323
Experiment / assignment / tutorial No.9	
Grade: AA / AB / BB / BC / CC / CD /DD	
Signature of the Staff In-charge with date	

Experiment No.:9

TITLE: Study and configure DHCP & DNS protocol using Cisco Packet tracer

AIM: To study and configure **DHCP/DNS** protocol using Cisco Packet tracer

Expected Outcome of Experiment:

CO:

Books/ Journals/ Websites referred:

1. A. S. Tanenbaum, "Computer Networks", Pearson Education, Fourth Edition
2. B. A. Forouzan, "Data Communications and Networking", TMH, Fourth Edition

Pre Lab/ Prior Concepts:

IPv4 Addressing, Subnetting, Link State Protocol, Router configuration Commands

New Concepts to be learned: DHCP/DNS Protocol and its configuration.

THEORY:

1. **Introduction**

DHCP (Dynamic Host Configuration Protocol) is a protocol used in IP networks to dynamically allocate IP addresses and other network configuration parameters to devices (known as DHCP clients) automatically. DHCP allows devices to join a network without the need for manual IP address configuration, which simplifies network administration and prevents issues such as IP address conflicts. The protocol is particularly useful in large networks where managing IP addresses manually can become cumbersome and prone to errors.

2. **DHCP Operation and the DORA Process**

DHCP follows a structured communication process known as the DORA process (Discover, Offer, Request, Acknowledge). The client and server interact in a sequence to assign an IP address and other settings.

3. **Discover:**
   - When a device (such as a laptop, PC, or smartphone) connects to a network, it sends a DHCP Discover message. This message is broadcast to all devices on the local network to find available DHCP servers.
   - The message contains the client's MAC (Media Access Control) address and asks for network configuration information like an IP address.
   - This is a broadcast message because the client doesn't yet know the IP address of the DHCP server.
4. **Offer:**
   - The DHCP servers on the network receive the Discover message and respond by sending a DHCP Offer message back to the client. The Offer contains the following details:
     - An available IP address for the client.
     - The subnet mask for the network.
     - The lease time (how long the client can use the IP address before needing to renew it).
     - The gateway address (the router's IP address).
     - DNS server addresses.

- Multiple DHCP servers may respond with an Offer, but the client will choose one.

5. **Request:**
   - After receiving multiple Offers, the client picks one and responds with a DHCP Request message, indicating that it accepts the offer from the selected DHCP server.
   - The DHCP Request message is sent as a broadcast, so all DHCP servers that made an offer know that the client has selected another server and will withdraw their offers.

6. **Acknowledge (ACK):**
   - The selected DHCP server sends a DHCP Acknowledge (ACK) message to confirm that the IP address and other network configuration settings have been assigned to the client.
   - The client is now fully configured with an IP address, subnet mask, default gateway, and DNS server information and can start using the network.

7. **DHCP Lease and Renewal**

- **Lease Time:** The IP address assigned by the DHCP server is leased to the client for a specified amount of time. Once the lease expires, the client must either renew the lease or obtain a new IP address. The lease time can vary depending on the network configuration.
- **Renewal Process:** Halfway through the lease period, the client automatically attempts to renew the lease by sending a request to the DHCP server. If the server is available and agrees to renew the lease, it sends an ACK message to extend the lease.

8. **DHCP Components**

- **DHCP Server:** The central server that holds a pool of IP addresses and assigns them to clients. It also provides the client with additional network configuration details.
- **DHCP Client:** Any device on the network that requests an IP address from the DHCP server. Common clients include computers, mobile devices, printers, and IoT devices.

- **IP Address Pool:** The range of IP addresses that the DHCP server can assign to clients. This is defined by the administrator in a DHCP scope.
- **DHCP Scope:** A range of IP addresses configured on the DHCP server, along with other configuration details like subnet mask, gateway, and DNS settings.
- **Subnet Mask:** A mask that defines the network portion of the IP address. This helps the device know which IP addresses are in its local network.
- **Default Gateway:** The IP address of the router, which allows the client to access other networks, including the internet.
- **DNS Server Address:** The IP address of a DNS server, which resolves domain names to IP addresses.

Advantages of DHCP

- **Simplifies Network Management:** DHCP automates the process of IP address assignment, reducing the need for manual configuration. This minimizes the chances of errors and makes it easier to add new devices to the network.
- **Reduces IP Conflicts:** Since the DHCP server controls the allocation of IP addresses, it ensures that no two devices are assigned the same IP address.
- **Dynamic Reassignment:** When devices leave the network, their IP addresses can be reassigned to new devices, optimizing IP address usage.
- **Centralized Management:** Network administrators can configure, manage, and monitor IP addressing centrally from the DHCP server.

Disadvantages of DHCP

- **Single Point of Failure:** If the DHCP server fails and there is no backup, devices will not be able to obtain IP addresses, causing network outages.
- **Security Risks:** Unauthorized devices could potentially connect to the network and receive an IP address from the DHCP server. Using techniques like DHCP snooping can mitigate this risk.
- **Limited to Local Networks:** DHCP uses broadcast messages, which do not traverse routers. This limits its functionality to a single network, but DHCP relay agents can help by forwarding requests to a DHCP server in another network.

Introduction:

DNS (Domain Name System) is a hierarchical, distributed naming system used to resolve human-friendly domain names (e.g., www.example.com) into machine-friendly IP addresses (e.g., 192.0.2.1). This allows users to access websites and other internet resources using easily remembered names rather than difficult-to-remember numerical IP addresses.

The DNS system acts like a phonebook for the internet. It translates domain names into IP addresses, allowing browsers to locate and retrieve the requested website or service.

1. **How DNS Works (DNS Resolution Process)**
2. **DNS Query:**
   - When a user enters a domain name (e.g., www.example.com) into a browser, the system first checks its local cache to see if the IP address corresponding to the domain name is already known.
   - If not found, the DNS client (resolver) sends a DNS query to a DNS server, asking it to resolve the domain name to an IP address.
3. **Root Servers:**
   - The DNS query starts by contacting a Root DNS Server. Root servers don’t know the IP address of specific domains, but they know which Top-Level Domain (TLD) servers (e.g., .com, .org) can provide further information.
4. **TLD Servers:**
   - The Root Server responds with the IP address of the TLD DNS server responsible for the domain extension (e.g., .com).
   - The DNS client then queries the TLD DNS server, which responds with the IP address of the Authoritative DNS Server for the specific domain.
5. **Authoritative DNS Servers:**

  - The authoritative DNS server contains the DNS records for the requested domain (e.g., example.com).
  - The server provides the IP address associated with the domain name, and the DNS resolver sends this information back to the user's browser, allowing it to access the website.

6. **DNS Caching:**
  - DNS responses are cached at multiple levels (client, DNS server, and browser) to improve response times for subsequent requests. Cached results are stored for a period defined by the TTL (Time to Live) value.

7. **DNS Records**

DNS records are the key pieces of information stored in DNS servers, and they define how queries are resolved. Common DNS records include**:**

- **A Record (Address Record)**: Maps a domain name to an IPv4 address.
- **AAAA Record**: Maps a domain name to an IPv6 address.
- **CNAME Record (Canonical Name):** Maps one domain name (alias) to another. Often used when a website has multiple subdomains or alternative names.
- **MX Record (Mail Exchange):** Specifies the mail server responsible for receiving emails for a domain.
- **NS Record (Name Server): Indicates which DNS server is authoritative for a domain.**
- **TXT Record:** Allows the domain owner to store text information in the DNS. It is often used for security purposes like verifying domain ownership or configuring email settings.

8. **DNS Components**

- **DNS Resolver (Client):** The device that initiates the DNS query. This is typically built into the operating system or browser.
- **Recursive DNS Server:** These servers handle DNS queries on behalf of the client by communicating with root servers, TLD servers, and authoritative DNS servers. They resolve the domain name and return the IP address to the client.
- **Root DNS Server:** The top of the DNS hierarchy. It directs queries to the appropriate TLD server.

- **Authoritative DNS Server:** Contains the DNS records for specific domains and provides the final resolution in a DNS query process.

Advantages of DNS

- **User-Friendly:** DNS allows users to access websites using easy-to-remember domain names instead of numeric IP addresses.
- **Distributed System**: DNS is decentralized, meaning that no single point of failure can bring down the entire system. This makes DNS highly resilient and scalable.
- **Caching:** DNS responses are cached at various levels, improving performance and reducing the load on DNS servers.

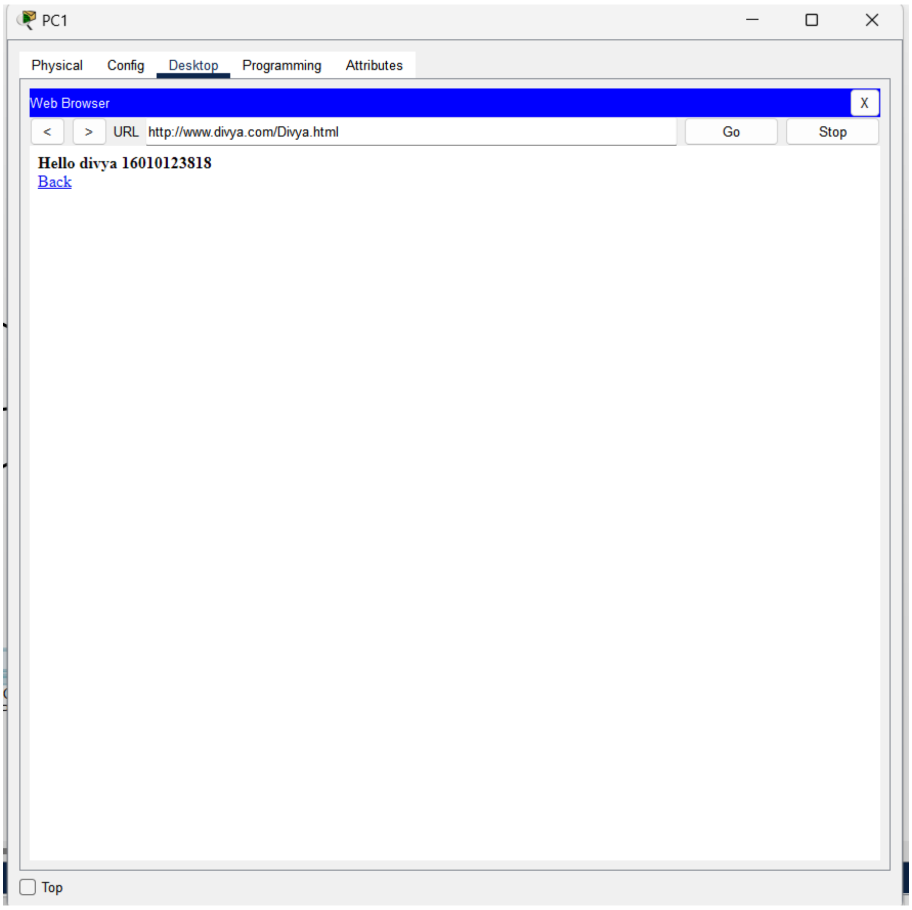
Disadvantages of DNS

- **DNS Spoofing (Cache Poisoning):** Attackers can alter the DNS cache to redirect users to malicious websites.
- **Latency:** DNS resolution can introduce delays in accessing websites, especially if the DNS query involves multiple servers.
- **Maintenance:** DNS requires careful maintenance to ensure domain names and IP addresses are up-to-date and configured correctly.

Security Considerations

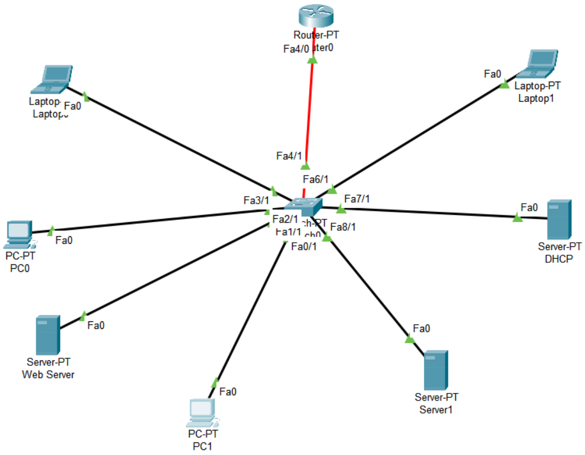
- **DNSSEC (Domain Name System Security Extensions):** A set of security extensions designed to protect DNS by ensuring that responses to DNS queries are authentic and have not been tampered with.
- **DNS Spoofing Prevention:** Network administrators should use techniques like DNSSEC and encrypted DNS (DNS over HTTPS or DNS over TLS) to secure DNS queries and prevent attacks.

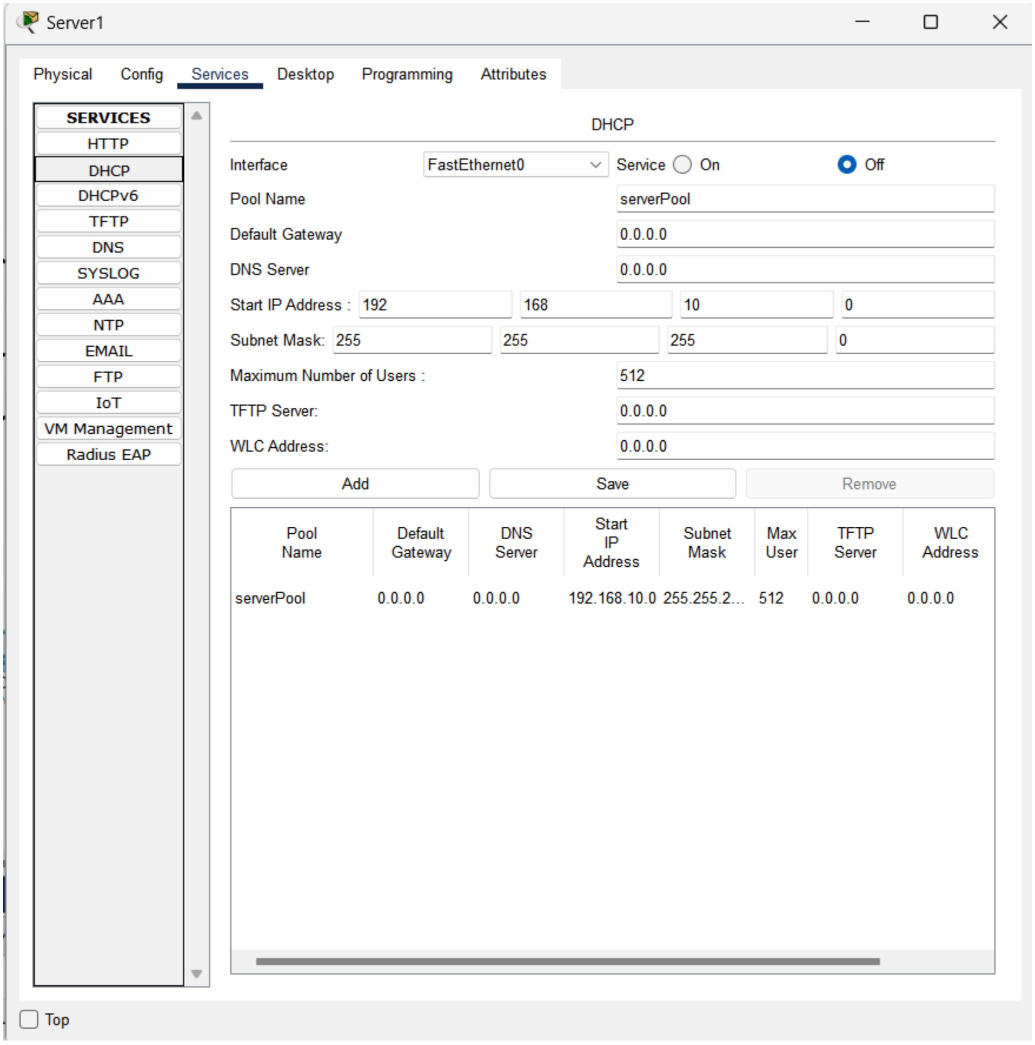
IMPLEMENTATION:



URL: http://www.divya.com/Divya.html

Hello divya 16010123818
Back





DHCP

Interface: FastEthernet0 Service ○ On ● Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address : 192 168 10 0

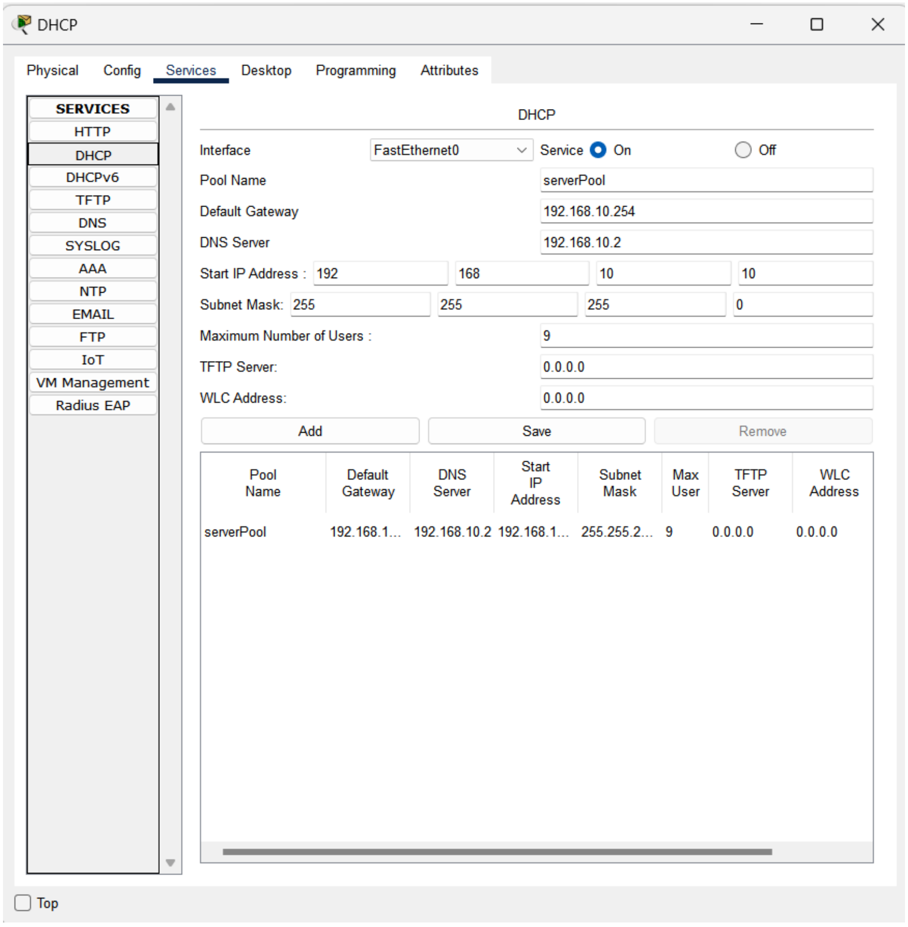
Subnet Mask: 255 255 255 0

Maximum Number of Users : 512

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	0.0.0.0	0.0.0.0	192.168.10.0	255.255.2...	512	0.0.0.0	0.0.0.0



DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 192.168.10.254

DNS Server: 192.168.10.2

Start IP Address : 192 168 10 10

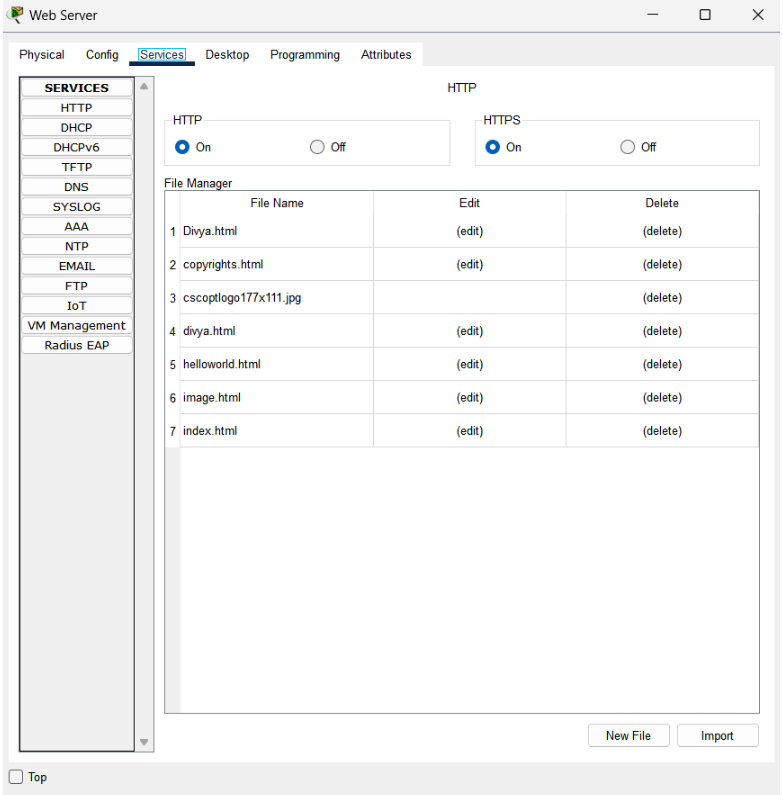
Subnet Mask: 255 255 255 0

Maximum Number of Users : 9

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.1...	192.168.10.2	192.168.1...	255.255.2...	9	0.0.0.0	0.0.0.0



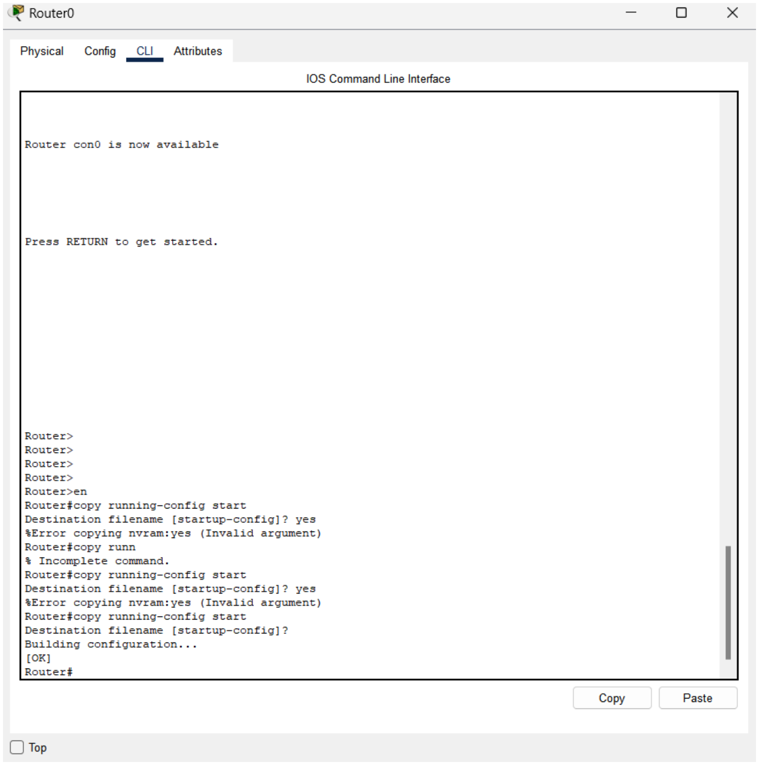
HTTP

HTTP: ● On ○ Off

HTTPS: ● On ○ Off

File Manager

	File Name	Edit	Delete
1	Divya.html	(edit)	(delete)
2	copyrights.html	(edit)	(delete)
3	cscoptlogo177x111.jpg		(delete)
4	divya.html	(edit)	(delete)
5	helloworld.html	(edit)	(delete)
6	image.html	(edit)	(delete)
7	index.html	(edit)	(delete)



```
Router con0 is now available



Press RETURN to get started.








Router>
Router>
Router>
Router>
Router>en
Router#copy running-config start
Destination filename [startup-config]? yes
%Error copying nvram:yes (Invalid argument)
Router#copy runn
% Incomplete command.
Router#copy running-config start
Destination filename [startup-config]? yes
%Error copying nvram:yes (Invalid argument)
Router#copy running-config start
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

CONCLUSION: Successfully Studied and configure DHCP & DNS protocol using Cisco Packet tracer

Date:24/10/2024 Signature of faculty in-charge