RNS INSTITUTE OF TECHNOLOGY

An Autonomous Institute under VTU
Accredited with NAAC A+ Grade

# PROJECT
# OFFICE NETWORK

Prepared By :

**MANOJ D**

**&**

**RAGHAV A**

DEPARMENT OF CYBER SECURITY

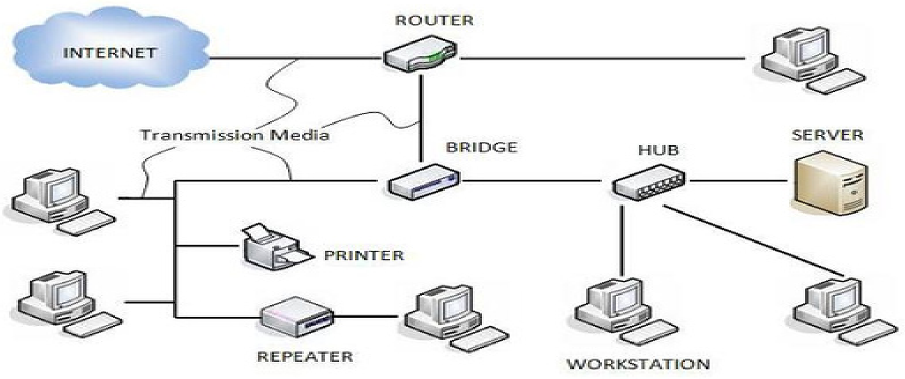
III SEMESTER

1RNCY25807

1RNCY25809

## Introduction to the Office Network

An **office network** is a private system designed to connect computers, printers, servers, and other devices within a single workplace or across multiple business locations. Its primary purpose is to enable seamless sharing of resources, data, and internet access among employees in a secure and managed environment.



## Core Goals

 Share resources: files, printers, applications, and internet.

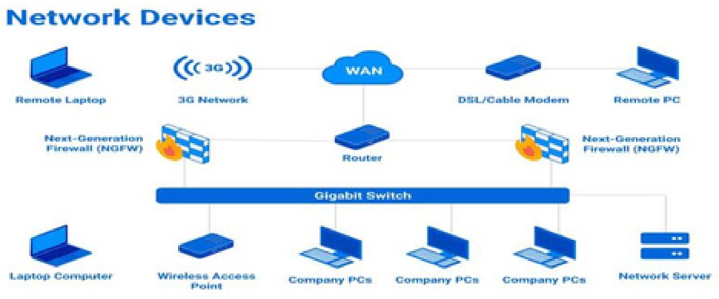
 Enable communication: email, VoIP calls, messaging, video meetings.

 Centralize management: user access, security policies, backups.

 Ensure security and reliability: protect data, maintain uptime.

## Key Components

- Router:Connects theoffice to the internet and different networks; performs Network Address Translation (NAT), routing, and often basic firewall functions.
- Switch: Connects devices inside the local network (LAN) and forwards frames to the correct ports using MAC addresses.
- Firewall: Enforces security rules; filters traffic between internal network and untrusted networks (internet), can be standalone or integrated with the router.
- Wireless Access Point (AP): Provides Wi-Fi so laptops and mobiles can join the LAN.
- DHCP Server: Automatically assigns IP addresses, subnet mask, gateway, and DNS to client devices; often runs on the router.
- DNS: Resolves human-friendly names (e.g., files.company.local) to IP addresses; can be internal or external.
- Servers/NAS: Provide shared storage, authentication (Active Directory), applications, backups.
- Cabling/Wi-Fi: Ethernet (Cat5e/Cat6) and fiber for wired; 2.4GHz/5GHz/6GHz radios for wireless.
- Endpoints: PCs, laptops, printers, IP phones, cameras, IoT devices



## Importance of Office Networks in Business

Office networks play a critical role in modern businesses ofall sizes, serving as the foundation that supports communication, collaboration, efficiency, and security. Here are the key reasons why office networks are vital for business success:

### 1. Seamless Communication and Collaboration

Office networks enable employees and departments to communicate and collaborate easily. Through email, instant messaging, video conferencing, and shared workspaces, teams can work together in real-time irrespective of physical location. This connectivity fosters faster decision-making, project management, and reduces downtime in workflow.

### 2. Resource Sharing

Networks allow multiple employees to share essential resources such as files, printers, scanners, and internet connections. Instead of duplicating hardware for each user, shared network resources reduce costs and improve convenience. For example, a central file server can store business-critical documents accessible by authorized personnel across the office.

### 3. Centralized Data Management

With an office network, all data can be stored and managed centrally on servers or cloud platforms. This centralization simplifies data backup, restores, updates, and security management. It also supports enterprise applications, such as Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP), essential for smooth business operations.

### 4. Enhanced Security

Office networks provide mechanisms to secure sensitive business information. Through firewalls, intrusion detection, user authentication, and encryption, networks control access and protect data from unauthorized users or cyber threats. Regular monitoring and security policies ensure compliance with industry standards and regulations.

5. Cost Efficiency

Networking reduces operational costs by optimizing hardware usage and streamlining IT management. Shared internet connections, printers, and servers minimize capital expenditure. Additionally, centralized IT administration reduces the need for on-site technical support, cutting maintenance and upgrade costs.

6. Improved Productivity

By enabling automated workflows, quick access to data, and reliable communication, office networks boost employee productivity. Employees spend less time on manual tasks and experiencing delays, enabling the business to respond promptly to clients, suppliers, and partners.

7. Scalability and Flexibility

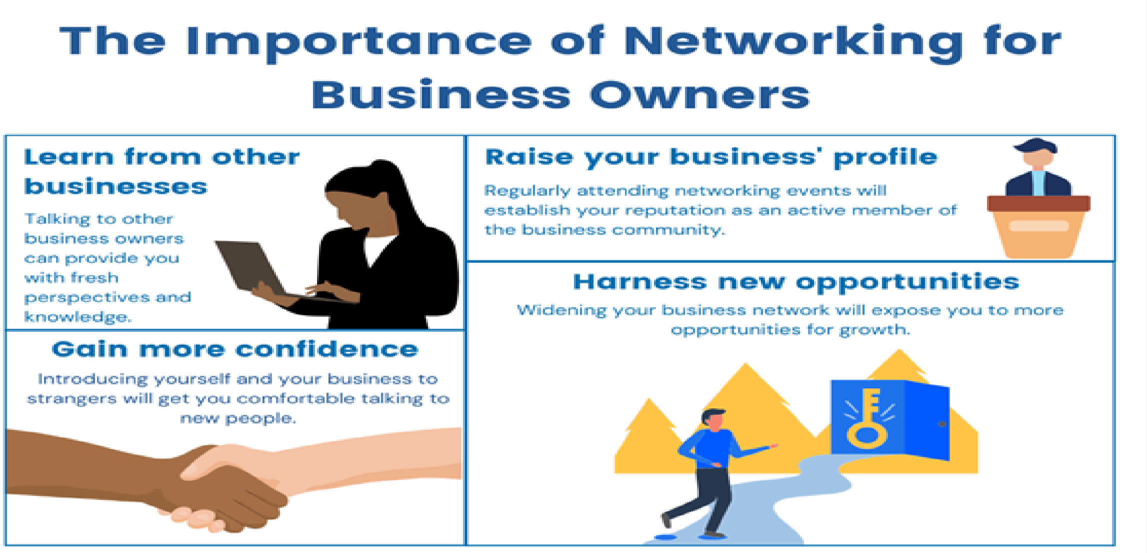
Office networks can grow with the business. New devices, users, or locations can be added with minimal disruption. Wireless networking adds flexibility for mobile devices and remote workforce integration, which is increasingly important in today's hybrid working models.

8. Business Continuity

Robust networking supports backup solutions, disaster recovery plans, and remote access to business systems. This ensures that operations can continue seamlessly despite outages or emergencies, protecting revenue and reputation.

9. Competitive Advantage

In today’s digital economy, businesses with well-designed and managed networks can innovate faster, enter new markets, and deliver superior customer experiences. Networks provide the infrastructure for emerging technologies, such as cloud computing, big data analytics, and Internet of Things (IoT).



The Importance of Networking for Business Owners

Learn from other businesses

Talking to other business owners can provide you with fresh perspectives and knowledge.

Raise your business' profile

Regularly attending networking events will establish your reputation as an active member of the business community.

Harness new opportunities

Widening your business network will expose you to more opportunities for growth.

Gain more confidence

Introducing yourself and your business to strangers will get you comfortable talking to new people.

# Network Architecture and Topologies

## Network Architecture

Network architecture refers to the organizational layout and design of a computer network. It defines how different components are arranged and interact with each other to enable communication and resource sharing. The architecture outlines the hardware, software, connectivity, protocols, and modes of transmission within a network.

### Key Elements of Network Architecture:

- **Physical topology:** How devices are physically connected.
- **Logical topology:** How data flows logically between devices, regardless of physical connections.
- **Protocols:** Rules that govern data transmission (e.g., TCP/IP).
- **Hardware components:** Routers, switches, servers, cables, etc.
- **Network services:** DHCP, DNS, authentication, etc.

Network architecture is essential for ensuring efficient data flow, scalability, security, and reliability in office networks.

# Network Topologies

Network topology is the specific arrangement or layout of devices and the connections between them. It dictates the path that data takes as it travels through the network.

## Common Network Topologies:

### 1.Bus Topology

- All devices are connected to a single central cable (bus).

- Data is sent in both directions; terminators prevent signal loss.
- Simple and cheap but difficult to troubleshoot and not scalable.

## 2.Star Topology

- All devices connect to a central device, usually a switch or hub.
- If one device fails, others continue working.
- Easy to manage and expand, common in office networks.

## 3.Ring Topology

- Devices are connected in a circular fashion.
- Data passes in one direction; each device acts as a repeater.
- Can be fast but if one device or link fails, the whole network may be affected

.

## 4.Mesh Topology

- Every device connects to every other device.
- Provides high redundancy and reliability.
- Expensive and complex; used mainly in critical network backbones.

## 5.Tree Topology

- Hierarchical form of multiple star topologies connected to a bus backbone.
- Scalable and well-organized for large networks.

## 6.Hybrid Topology

- Combination of two or more different topologies.

- Flexible to meet specific organizational needs.

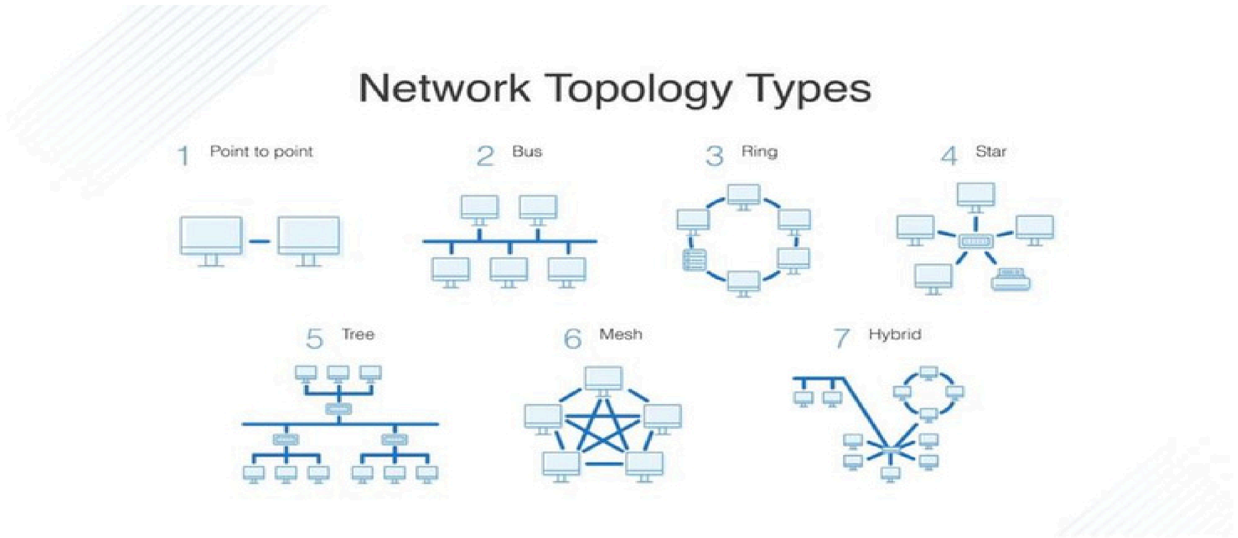
-

## Typical Office Network Architecture

In office environments, a **star topology** is most popular due to its simplicity, reliability, and scalability. Devices connect to switches, which interconnect to routers providing internet access and routing between different subnets or VLANs.

Large enterprise networks might employ hierarchical architectures comprising:

- **Core layer:** High-speed backbone switches/routers connecting different parts of the network.
- **Distribution layer:** Aggregates data from access switches, implements routing and policies.
- **Access layer:** Connects end-user devices and access points.



## Benefits of Structured Architecture and Topology

- **Improved performance** by reducing collisions and bottlenecks.
- **Scalability** toeasilyaddor remove devices.
- **Fault tolerance** throughredundancy.

- **Simplified troubleshooting and management.**

# IP Addressing and Subnetting

What is an IP Address?

An **IP address** (Internet Protocol address) is a unique numerical identifier assigned to every device connected to a network using the Internet Protocol, such as computers, printers, routers, or smartphones. It functions much like a home address, allowing devices to locate and communicate with each other within a network or over the internet.

- **IPv4 addresses** are 32-bit numbers, typically written in dotted-decimal notation, such as 192.168.1.10.
- **IPv6 addresses** are newer 128-bit addresses designed to provide far more unique addresses to overcome IPv4 limitations.

**Structure of an IP Address**

An IP address consists of two main parts:

1. **Network portion:** Identifies the specific network to which the device belongs.
2. **Host portion:** Identifies the specific device (host) on that network.

The division between network and host parts is determined by the **subnet mask**.

**What is a Subnet Mask?**

- A subnet mask is a 32-bit number that separates the IP address into the network and host portions.
- For example, the subnet mask 255.255.255.0 indicates that the first 24 bits are the network part, and the remaining 8 bits represent hosts.

□Subnet masks help routers determine if a destination device is on the local subnet or if the data needs to be routed outside the local network.

## Why Subnetting?

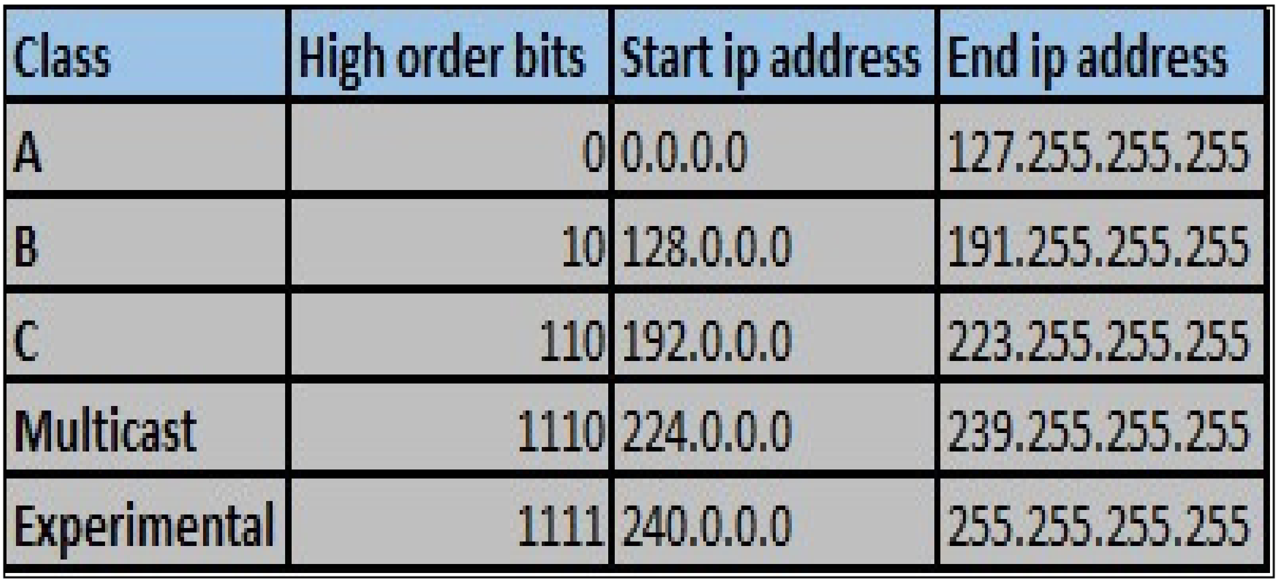
Subnetting divides a larger network into smaller, more manageable subnetworks (subnets), improving:

□ Network performance by reducing broadcast traffic.
□ Security by isolating segments.
□ Efficient IP address use.

-

## IP Address Classes (Classful Addressing)

IP addresses are historically divided into classes based on their leading bits



| Class | High order bits | Start ip address | End ip address |
|---|---|---|---|
| A | 0 | 0.0.0.0 | 127.255.255.255 |
| B | 10 | 128.0.0.0 | 191.255.255.255 |
| C | 110 | 192.0.0.0 | 223.255.255.255 |
| Multicast | 1110 | 224.0.0.0 | 239.255.255.255 |
| Experimental | 1111 | 240.0.0.0 | 255.255.255.255 |

Most office networks use **Class C** addresses because they support up to 254 hosts, which is suitable for small to medium-sized LANs.

-

## IP Address Assignment Methods

□**Static IP:** Address manually configured on a device (e.g., servers, printers).

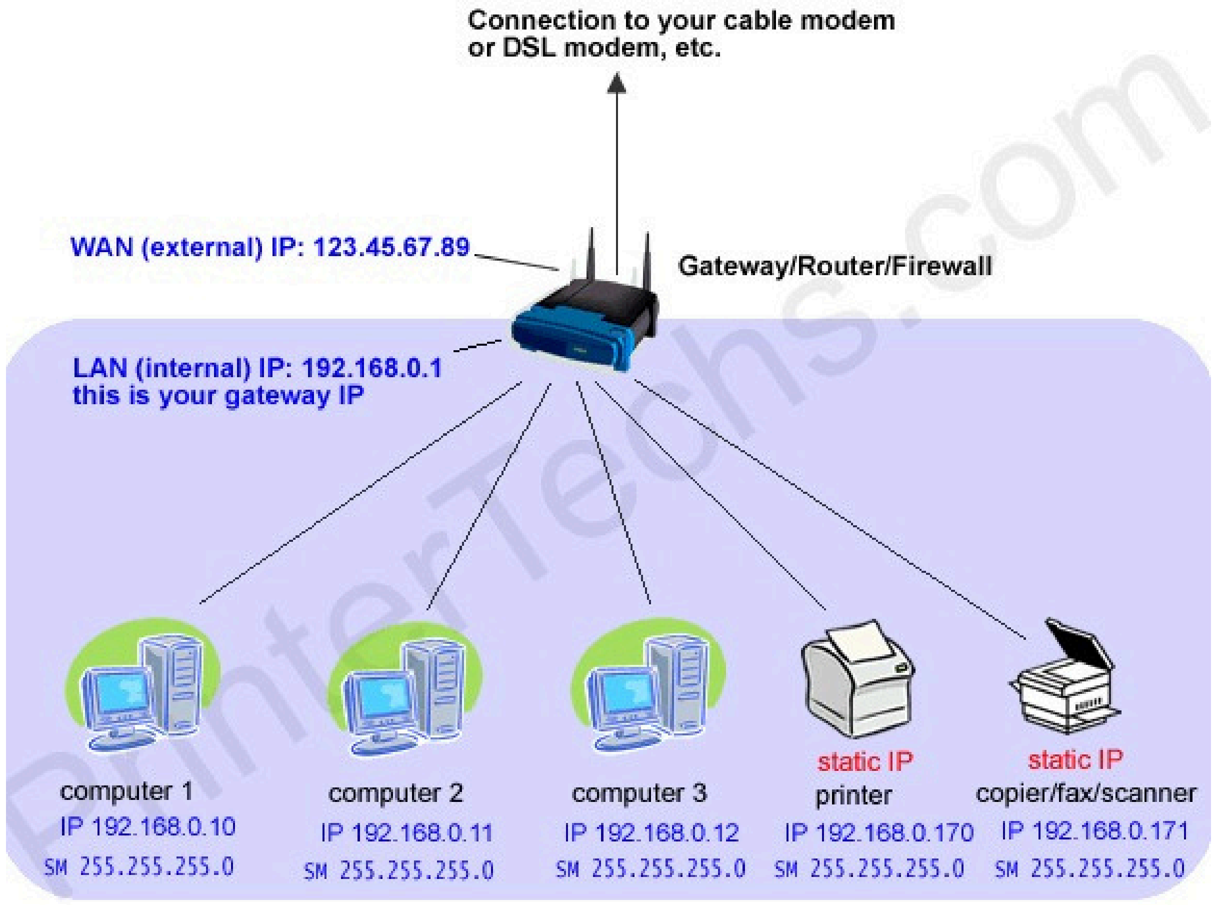
□ **Dynamic IP:** Automatically assigned by a DHCP (Dynamic Host Configuration Protocol) server, common for user devices for ease of management.

## How IP Addressing Works in an Office Network

1. Devices receivean IP addressand subnetmask indicatingtheir network boundaries.
2. If a device wants to communicate with another device:
   o It checks if the destination IP is within the same subnet.
   o If yes, it sends data directly within the LAN.
   o If no, the data is forwarded to the default gateway (router) to reach devices outsidethesubnet.

## Example: Small Office Network Addressing

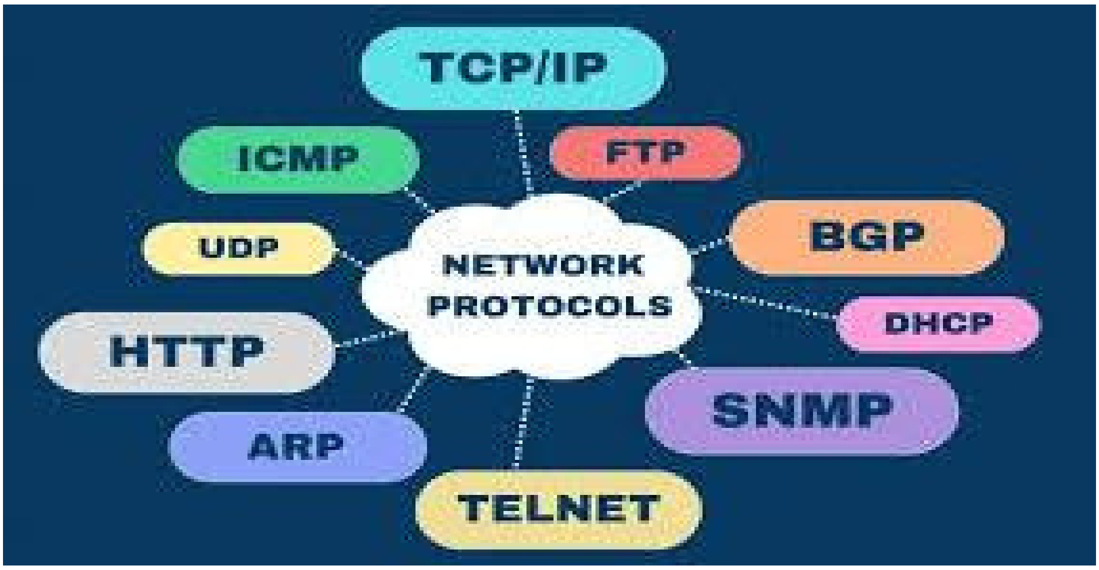
| Device | IP Address | Subnet Mask | Default Gateway |
|---|---|---|---|
| Router | 192.168.1.1 | 255.255.255.0 | - |
| PC0 | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 |
| PC1 | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| Printer | 192.168.1.10 | 255.255.255.0 | 192.168.1.1 |



## Network Protocols and Communication

### What Are Network Protocols?

Network protocols are standardized sets of rules and conventions that govern how data is transmitted, received, and interpreted between devices on a network. They ensure different devices, regardless of manufacturer or type, can communicate effectively, reliably, and securely



Key Network Protocols Used in Office Networks

1. **Transmission Control Protocol/Internet Protocol (TCP/IP)**
   - o The foundationalprotocolsuiteformostmodernnetworks, including office LANsandtheinternet.
   - o **TCP**: Ensures reliable,ordereddeliveryofdatapackets. It manages retransmissionoflostorcorruptedpackets.
   - o **IP**: Handles addressingandroutingofpacketsbetween devices, delivering data to thecorrectdestination.
   - o Together, TCP/IP enabledevicestoestablishconnections and exchange data accuratelyacrossnetworks

   .

1. **User Datagram Protocol (UDP)**
   - o Connectionless, lightweightprotocolidealforapplications requiring fast transmissionratherthanguaranteed delivery.
   - o Commonly used for videoconferencing,streaming, and online gaming where small datalossisacceptableforspeed.

1. **Hypertext Transfer Protocol (HTTP)/HTTP Secure (HTTPS)**
   - o Usedto transferwebpages from serverstoclient browsers.
   - o HTTPS adds encryption for secure communication.

1. **Domain Name System (DNS)**
    - Translates human-readabledomain names (like www.example.com) into IPaddresses.
    - Essential for locating servers and services on the internet and internal networks.

1. **Dynamic Host Configuration Protocol (DHCP)**
    - Automates IPaddressassignment for devices joining the network.
    - Simplifies network administration by managing IP pools and lease durations.

1. **Address Resolution Protocol (ARP)**
    - MapsIP addresses toMAC (hardware) addresses within a local network.
    - Enables devices to locate each other physically for data transmission.

1. **Internet Control Message Protocol (ICMP)**
    - Usedfornetwork diagnostics and errorreporting.
    - Commonly used by tools like ping andtraceroute to test connectivity and trace routes.

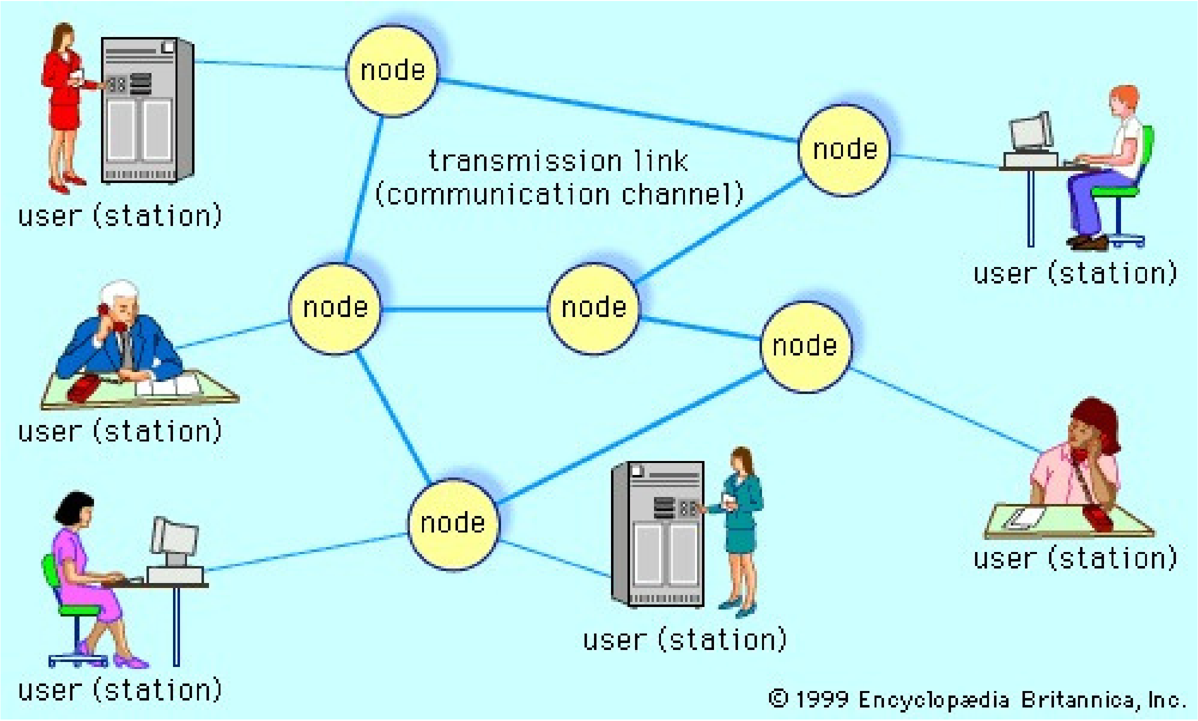
1. **File Transfer Protocol (FTP)**
    - Transfersfilesbetween client and server systems.
    - Secure versions (SFTP, FTPS) include encryption for data protection.

1. **Simple Network Management Protocol (SNMP)**
    - Usedby networkadministratorstomonitorand manage network devices.

-

## How Network Communication Works

- When a devicewants tosend data, thedatais broken into smaller units called **packets**.
- Each packet includes headers with information like source and destination IP addresses, sequencing information, and error-checking codes.
- The sending device uses protocols like TCP to ensure data integrity, sequencing, and retransmission if necessary.
- Packets travel through switches and routers, using IP addressing and routing protocols to find the best path.
- On arrival, packets are reassembled into the original data by the receiving device.



© 1999 Encyclopædia Britannica, Inc.

### Example: Sending an Email in an Office Network

1. Your email client uses TCP/IP to communicate with the mail server.
2. DNS translates the mail server domain name to an IP address.
3. Data packets are created and sent through the local network via switches.

4. The router forwards packets to the internet if the mail server is remote.
5. Communications are encrypted when using secure protocols like SMTP with TLS.
6. The recipient’s mail server receives and processes the packets, reassembling the original email.

## Network Security in Office Environments

Network security in office environments is critical to safeguarding sensitive business information, protecting users, and ensuring reliable network operations. It involves a combination of policies, technologies, and practices designed to prevent unauthorized access, misuse, data breaches, and cyber threats.

### Key Aspects of Office Network Security

1. **Firewalls**

- Act as a barrier between the trusted internal office network and untrusted external networks like the internet.
- Control incoming and outgoing network traffic based on security rules.
- Modern firewalls may include Intrusion Detection and Prevention Systems (IDS/IPS) to identify and block suspicious activity.

2. **Antivirus and Endpoint Protection**

- Installed on individual devices (PCs, laptops, servers) to detect and remove malware.
- Modern endpoint security solutions provide behavior monitoring, ransomware protection, and exploit prevention.

3. **Virtual Private Network (VPN)**

- Enables secure remote access to the office network over the internet.
- Encrypts data between remote users and company resources, protecting against interception.

4. **Secure Wi-Fi**

- Using strong encryption protocols (WPA2 or WPA3) to protect wireless networks.
- Employing unique, complex Wi-Fi passwords.
- Segregating guest Wi-Fi from the corporate network using VLANs to limit access.

5. **User Authentication and Access Control**

- Implementing strong password policies and multi-factor authentication (MFA) to verify user identities.
- Role-Based Access Control (RBAC) restricts users’ access to only the resources needed for their job.
- Network Access Control (NAC) ensures that only compliant and trusted devices connect to the network.

6. **Data Encryption**

- Encrypting data in transit (using TLS/SSL protocols) and data at rest (on servers and storage).
- Protects sensitive information such as financial data, customer records, and intellectual property.

7. **Regular Software Updates and Patch Management**

- Keeping network devices and software up to date to close vulnerabilities that attackers could exploit.
- Automated patching tools help maintain timely updates.

8. **Backup and Disaster Recovery**

- Regular backups of critical data protect against data loss from ransomware attacks, failures, or disasters.
- Recovery plans ensure business continuity.

9. **Security Monitoring and Incident Response**

- Continuous monitoring of network traffic and devices for anomalies.
- Incident response plans define how to react to security breaches effectively.

## Common Issues and Troubleshooting in Office Networks

Despite careful design and setup, office networks often encounter issues that can disrupt communication, reduce productivity, and compromise security. Understanding common problems and how to troubleshoot them is essential formaintaining smooth operations.

### 1. Connectivity Problems

- **Symptom:** Devices cannot connect to the network or internet.
- **Possible Causes:**
  - Faulty cables or disconnected hardware.
  - Incorrect IP configuration or DHCP failure.
  - Disabled network adapters.
- **Troubleshooting Steps:**
  - Check physical connections and replace faulty cables.
  - Verify IP settings; use ipconfig or ifconfig to check IP addresses.
  - Restart DHCP server or assign a static IP temporarily.
  - Enable andupdate network drivers.

### 2. IP Address Conflicts

- **Symptom:** Two deviceshavethe same IP, causing network interruptions.
- **PossibleCauses:**
  - Static IP overlaps with DHCP scope.
  - DHCP server malfunction.
- **Troubleshooting Steps:**
  - Check for duplicate IP addresses in network logs.
  - Adjust DHCP address pool or assign static IPs outside DHCP range.
  - Restart DHCP server.

### 3. Slow Network Performance

- **Symptom:** Slowfiletransfers,delayed response times.
- **Possible Causes:**

- o Network congestion due to heavy traffic.
- o Faulty hardware such as switches or routers.
- o Wireless interference or weak Wi-Fi signals.

□ **TroubleshootingSteps:**

- o Monitor traffic using network management tools.
- o Check and replace suspicious hardware.
- o Optimize Wi-Fi channels or increase access points.
- o Implement Quality of Service (QoS) policies to prioritize critical traffic.

## 4. Wireless Connectivity Issues

□ **Symptom:** Devices disconnect frequently or cannot connect to Wi-Fi.

☒ **PossibleCauses:**

o Signal interference from other devices or structures.

o Incorrect Wi-Fi settings or outdated drivers.

o AP overload due to many connected devices.

□ **Troubleshooting Steps:**

o Change Wi-Fi channels or bands (2.4 GHz vs 5 GHz).

o Update wireless adapters and access point firmware.

o Add more access points or limit concurrent connections.

## 5. Printer and Resource Sharing Problems

☒ **Symptom:** Users cannot access shared printers or files.

☒ **Possible Causes:**

o o Incorrect permissions or network discovery settings.

Devices on different VLANs without proper routing.

**TroubleshootingSteps:**

□

- o Verify sharing permissions and network profiles.
- o Ensure VLANs are correctly configured with inter-VLAN routing if required.
- o Restart file and print services.

## 6. Security Breaches and Malware

□ **Symptom:** Unusual network traffic, data loss, or unauthorized access.

- **Possible Causes:**
  - Weakpasswords or outdated security patches.
  - Phishingormalware infections.
- **Troubleshooting Steps:**
  - Run antivirus and malware scans.
  - Update software and change compromised credentials.
  - Audit firewall and access control settings.

## 7. DNS Resolution Failures

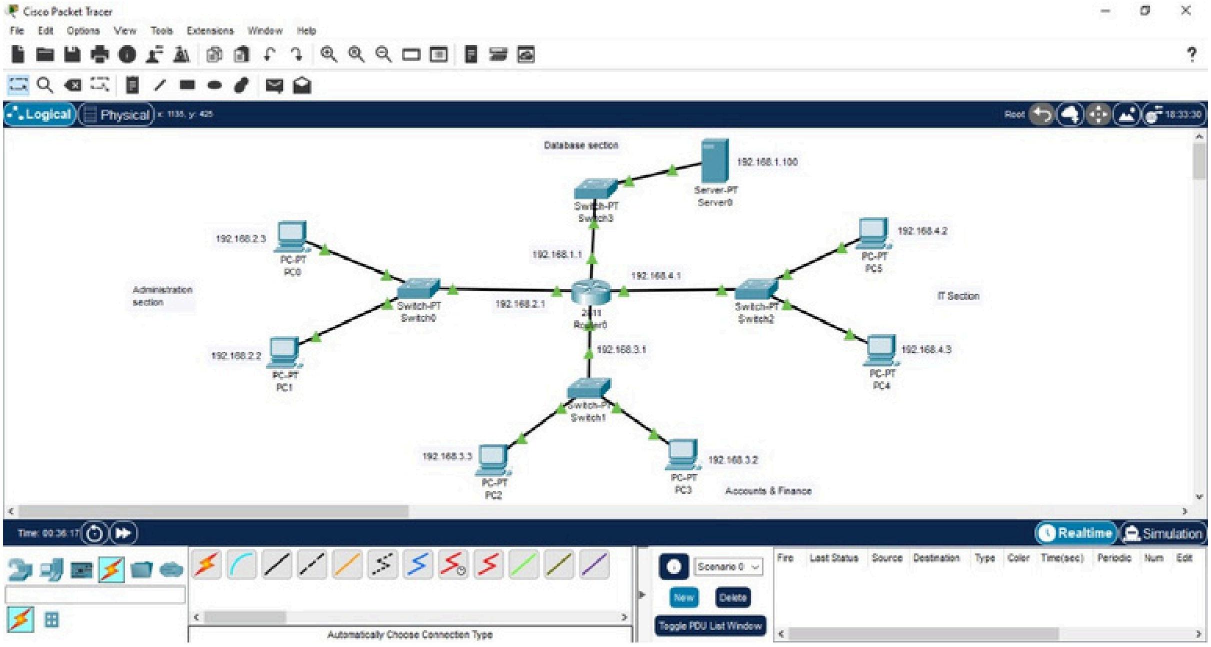
- **Symptom:** Unable to access websites or internal services using domain names.
- **Possible Causes:**
  - Incorrect DNS server settings.
  - DNS server outages.
- **Troubleshooting Steps:**
  - Verify DNS server IP settings on clients.
  - Restart or switch DNS servers (use public DNS like Google’s 8.8.8.8 temporarily).
  - Flush DNS cache (ipconfig /flushdns).

# Small Office Network Design

**Step 1:** Open the Cisco Packet Tracer.

**Step 2.:** After opening the Cisco Packet tracer, add a router, 4 switches, 6 PCs, and a server to build a network for a small organization.

| | |
|---|---|
| **Router** | 1 |
| **Switch** | 4 |
| **Server** | 1 |
| **PC** | 6 |

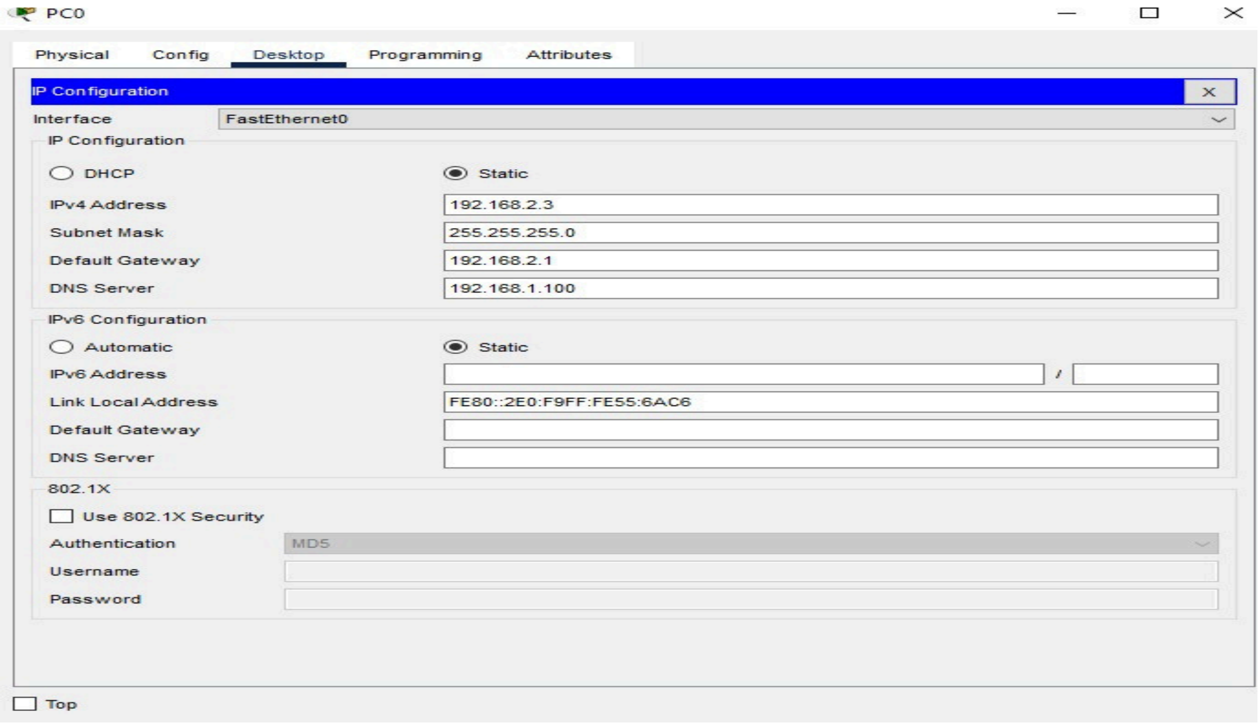


**Step 3:** Connect the router with 4 switches, 3 switches are connected with 2PCs each, and 1 switch is connected with the server using a cable. There are four different networks in this organization:- 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24, and 192.168.4.0/24.

**Step 4:** Give IP, subnet mask, default gateway, and DNS server to each PC and server in this network. To assign IP to each PC and server, click on each PC, go to Desktop, and then click on IP configuration.

| ompone nts | IP Address | Subnet Mask | Default Gateway | DNS server |
|---|---|---|---|---|
| PC0 | 192.168.2.3 | 255.255.255.0 | 192.168.2.1 | 192.168..1.100 |
| PC1 | 192.168.2.2 | 255.255.255.0 | 192.168.2.1 | 192.168.1.100 |
| PC2 | 192.168.3.3 | 255.255.255.0 | 192.168.3.1 | 192.168.1.100 |
| PC3 | 192.168.3.2 | 255.255.255.0 | 192.168.3.1 | 192.168.1.100 |

|  |  |  |  |  |
|---|---|---|---|---|
| PC4 | 192.168.4.3 | 255.255.255.0 | 192.168.4.1 | 192.168.1.100 |
| PC5 | 192.168.4.2 | 255.255.255.0 | 192.168.4.1 | 192.168.1.100 |
| Server | 192.168.1.100 | 255.255.255.0 | 192.168.1.1 | 192.168.1.100 |



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.2.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 192.168.1.100

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2E0:F9FF:FE55:6AC6

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

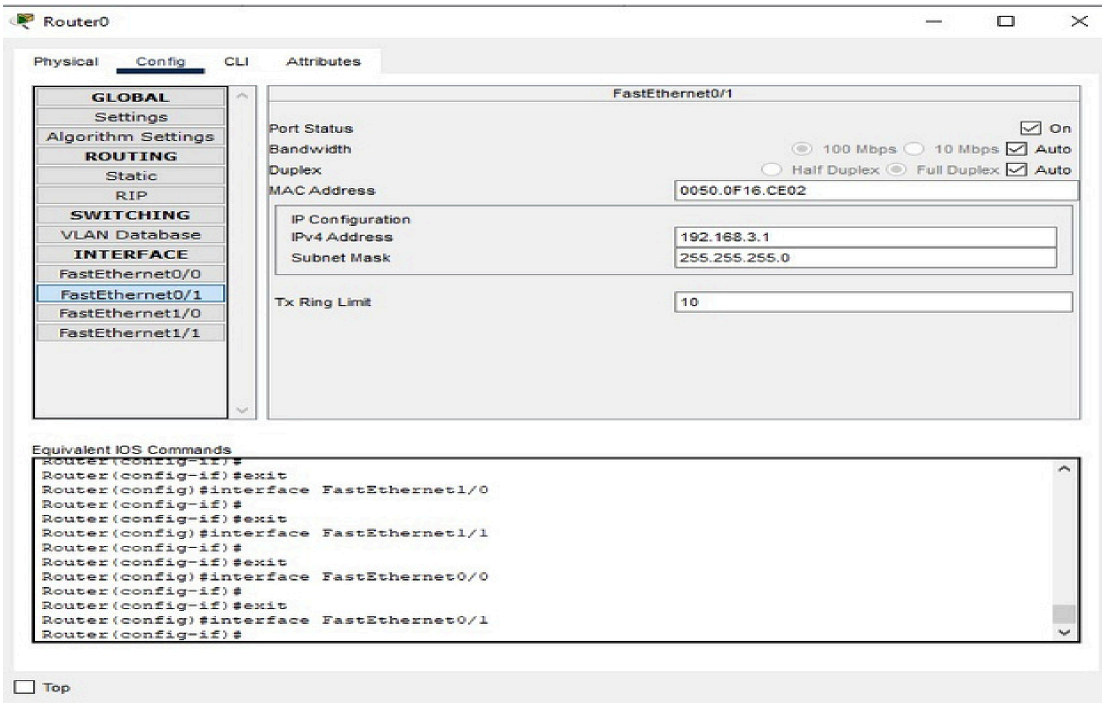
Username:

Password:

**Step 5:** Now, configure the router according to the details given below and then turn on the port status.

|  |  |  |
|---|---|---|
| FastEthernet0/0 | 192.168.2.1 | 255.255.255.0 |
| FastEthernet0/1 | 192.168.3.1 | 255.255.255.0 |
| FastEthernet1/0 | 192.168.1.1 | 255.255.255.0 |
| FastEthernet1/1 | 192.168.4.1 | 255.255.255.0 |

### For example, For FastEthernet0/1:



FastEthernet0/1

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0050.0F16.CE02

IP Configuration

IPv4 Address 192.168.3.1

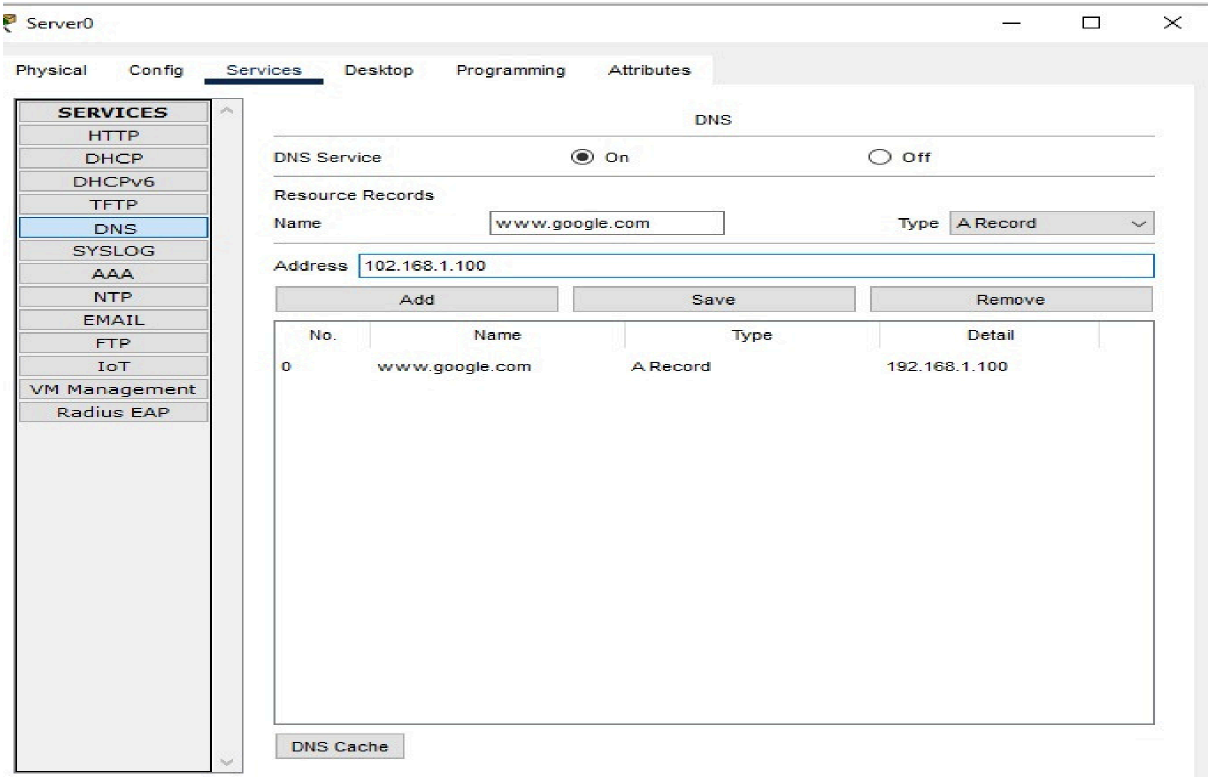
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet1/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
```

**Step 6:** Now, we've to maintain the DNS server. For this click on the server, go to the services section, and then click on DNS. Turn on the DNS server, Enter any domain in the 'Name' section For eg: "www.google.com" enter the IP address of the server in the 'Address section', and then click on save.



DNS Service ● On ○ Off

Resource Records

Name: www.google.com

Type: A Record

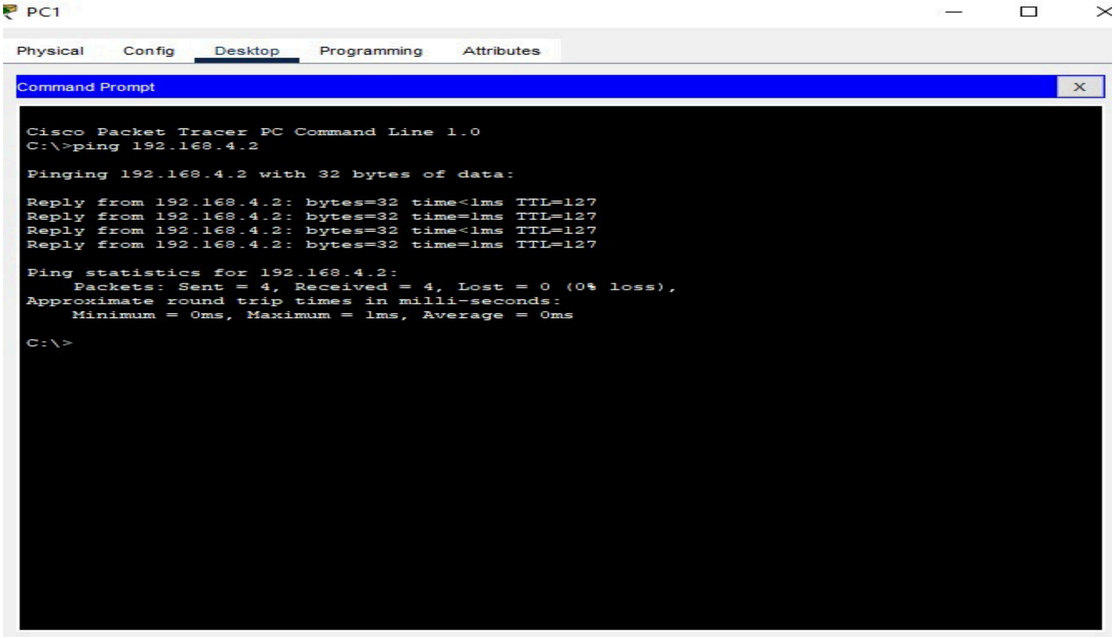
Address: 102.168.1.100

| No. | Name | Type | Detail |
|---|---|---|---|
| 0 | www.google.com | A Record | 192.168.1.100 |

**Step 7:** Again click on the server, go to services, and then click on HTTP. Turn on the HTTP and HTTPS services. You can also edit the index.html file which will show when you search the domain you entered in DNS in the web browser.

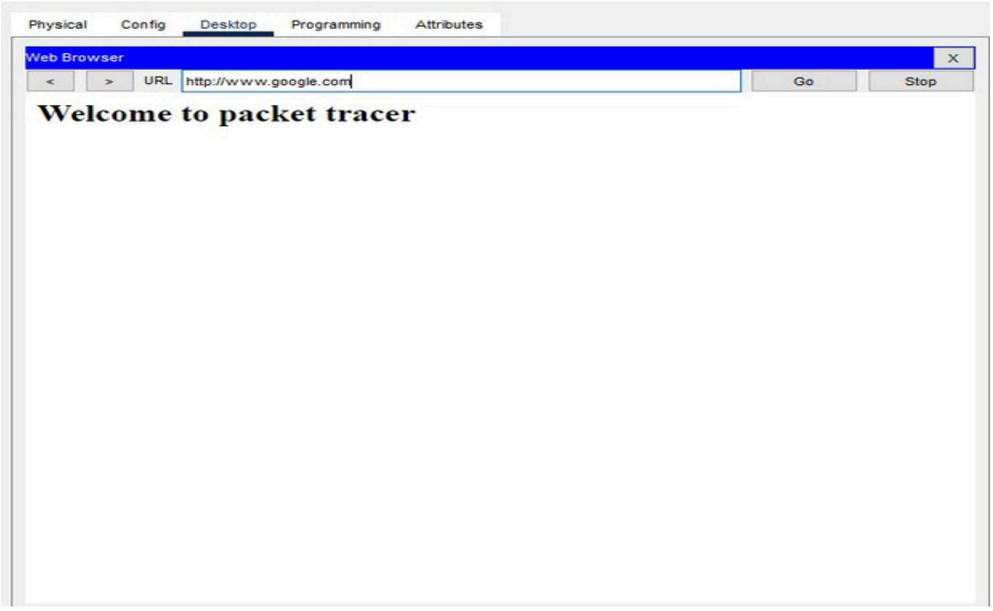
**Step 8:** To check the connection between PCs present in different networks in this organization, you can use the ping command. Click on any PC, go to Desktop, and then click on the command prompt, enter the ping command, and check if they're able to communicate with each other.

*For example, ping 192.168.3.1*



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time<1ms TTL=127
Reply from 192.168.4.2: bytes=32 time=1ms TTL=127
Reply from 192.168.4.2: bytes=32 time<1ms TTL=127
Reply from 192.168.4.2: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

**Step 9:** Click on any PC, go to the Desktop section, and then open the web browser. Enter the domain or address you've given in the DNS server and it will show the index.html file from HTTP services.



URL http://www.google.com

Welcome to packet tracer