**TASK SHEET : NETWORKING**

**Network Fundamentals and building networks**

**Task 1 : Create a diagram of the OSI Model with examples for each layer.**

| **Application layer**  **Examples: Resource sharing Remote file access. Remote printer access, HTTP (web browsing), FTP (file transfer), SMTP (email), DNS (domain name resolution).** |
| --- |
| **Presentation Layer**  **Examples: TSL, SSL, JPEG, MP3** |
| **Session layer**  **Examples: Remote desktop sessions, VoIP call setups, Network File System (NFS)** |
| **Transport layer**  **Examples: TCP (connection-based apps like web browsing), UDP (real-time apps like video streaming)** |
| **Network layer**  **Examples: IPv4, IPv6, OSPF, BGP, ICMP (ping/traceroute)** |
| **Data Link layer**  **Examples: ARP, VLAN tags, MAC, Switches, Bridge** |
| **Physical layer**  **Examples: Ethernet cables, Wi-Fi signals, USB Connectors (RJ-45, BNC), Hubs** |

**Task 2: Compare OSI and TCP/IP models with real-world examples.**

| Criteria | OSI Model | TCP/IP Model |
| --- | --- | --- |
| Full Form | Open Systems Interconnection | Transmission Control Protocol/Internet Protocol |
| Developed By | ISO (International Organization for Standardization) | U.S. Department of Defense (DoD) |
| Number of Layers | 7 | 4 |
| Layer Names | Application, Presentation, Session, Transport, Network, Data Link, Physical | Application, Transport, Internet, Network Access |
| Type of Model | reference model | Practical/implementation model |
| Usage | Used for teaching and design | Used in real-world networking and communication |
| Layer Functions | Each layer has a distinct function | Layers combine multiple OSI functions |
| Session & Presentation | Separate layers | Combined into Application Layer |
| Transport Layer Protocols | TCP, UDP | TCP, UDP |
| Network Layer Protocols | IP, ICMP, OSPF, etc. | IP, ICMP |
| Flexibility | More detailed and modular | Simpler and more efficient in practice |
| Data Flow | Vertical, from layer 7 to 1 and vice versa | Vertical, from Application to Network Access |

**Example: Sending a Text Message Using WhatsApp**

* You open WhatsApp on your phone, type a message, and send it to a friend.
* How OSI and TCP/IP Models Handle This on Sender side:

| OSI Layer | TCP/IP Layer | Sender side data flow |
| --- | --- | --- |
| Application | **Application**  **Application** | WhatsApp app formats the message and prepares it to be sent |
| Presentation | Message is encoded using Unicode, then encrypted using SSL/TLS |
| Session | WhatsApp creates a communication session with the recipient's phone |
| Transport | **Transport** | UDP (or TCP) is used to break message into packets and ensure (or not ensure) delivery |
| Network | **Internet** | IP assigns logical addresses and decides the route to deliver message to your friend |
| Data Link | **Network Access** | MAC address is used to send packets to the Wi-Fi router or mobile tower |
| Physical | Message bits are transmitted as electrical or radio signals through Wi-Fi or mobile network |

* How OSI and TCP/IP Models Handle This on receiver side:

| OSI Layer | TCP/IP Layer | Receiver’s Side data flow |
| --- | --- | --- |
| Physical | **Network Access** | Signal is received via Wi-Fi, mobile data, or Ethernet (electrical, optical, or radio signals) |
| Data Link | Signal is decoded into frames; MAC address is used for local delivery |
| Network | **Internet** | Packet is routed to the correct IP address (your device) |
| Transport | **Transport** | Packets are reassembled into a complete message using TCP or UDP |
| Session | **Application** | Session is maintained for the conversation (e.g., WhatsApp chat session) |
| Presentation | Data is decrypted (e.g., TLS), decompressed, and translated into readable format |
| Application | Message is passed to WhatsApp and displayed to the user |

**Task 3: Solve subnetting exercises and calculate valid subnets.**

**You are assigned 192.168.100.0/24**  
**Task:** Create subnets for:

* 1 subnet with 40 host
* 2 subnets with 30 hosts
* 1 subnet with 10 hosts
* **Step-by-Step VLSM (Variable Length Subnet Masking)**

We will assign IPs based on host requirements, starting with the largest.

So, here largest network with 40 hosts

**Subnet for 40 hosts**

* Need: 2^6 = 64 IPs → 255.255.255.192
* Subnet: 192.168.100.0/26
* Range: 192.168.100.1 – 192.168.100.62
* Broadcast: 192.168.100.63

**Subnet for 30 hosts**

* Need: 2^5 = 32 IPs → 255.255.255.224
* Subnet: 192.168.100.64/27
* Range: 192.168.100.65 – 192.168.100.94
* Broadcast: 192.168.100.95

**Subnet for 10 hosts**

* Need: 2^4= 16 IPs → 255.255.255.224
* Subnet: 192.168.100.96/28
* Range: 192.168.100.97 – 192.168.100.104
* Broadcast: 192.168.100.105

**Task 4: Document the steps to create a subnet plan.**

### **Step 1: Determine Network Requirements**

* Total number of devices (hosts)
* Number of required subnets (e.g., departments: HR, IT, Sales)
* Future growth
* Type of IP address**:** Private or Public

### **Step 2: Choose an IP Address Block or Range**

* Class A: 10.0.0.0 – 10.255.255.255
* Class B: 172.16.0.0 – 172.31.255.255
* Class C: 192.168.0.0 – 192.168.255.255

### **Step 3: Calculate the Number of Subnets and determine hosts per subnet.**

* Use the formula to calculate subnets:  
   2^n ≥ number of required subnets,
* where n is the number of bits borrowed from the host portion

### **Step 3: Figure Out How Many Subnets You Need and hosts per subnet.**

* Pick a subnet mask that provides enough IP addresses for each group without wasting unused addresses. Use formulas or subnet calculators to help. For example, a subnet with 64 addresses (/26) may be ideal for a group with up to 62 devices because two Ips are reserved one for network and another one for broadcast id.

**Example:**

* You are given 192.168.1.0/24
* Need to divide into 4 subnets
* Each department (HR, IT, Sales, Admin) needs up to 50 devices.

### **Step-by-Step Solution**

#### Step 1: Available Block

192.168.1.0/24 → 256 total IPs

#### Step 2: Determine Subnet Size

* + We need at least 4 subnets.  
     2^2 = 4 → Borrow **2 bits** from the host portion.
  + New subnet mask:  
     /24(Network bits) + 2(borrowed bits from host) = /26 **255.255.255.192**
  + Each /26 subnet provides:  
     2^6 = 64 IPs → 62 usable hosts

Perfect for 50 devices per department.

**HR department:**

Network address:192.168.1.0

Usable IP range: 192.168.1.1 to 192.168.1.62

Broadcast address: 192.168.1.63

**IT department:**

Network address:192.168.1.64

Usable IP range: 192.168.1.65 to 192.168.1.126

Broadcast address: 192.168.1.127

**Sales department:**

Network address:192.168.1.128

Usable IP range: 192.168.1.129to 192.168.1.190

Broadcast address: 192.168.1.191

**Admin department:**

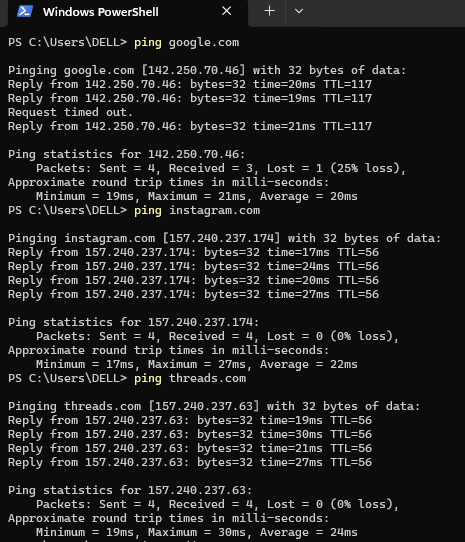
Network address:192.168.1.192

Usable IP range: 192.168.1.192 to 192.168.1.254

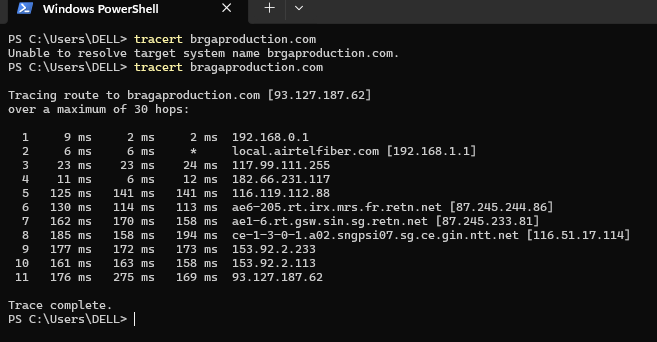
Broadcast address: 192.168.1.255

**Task 5: Report on the tools used and results obtained.**

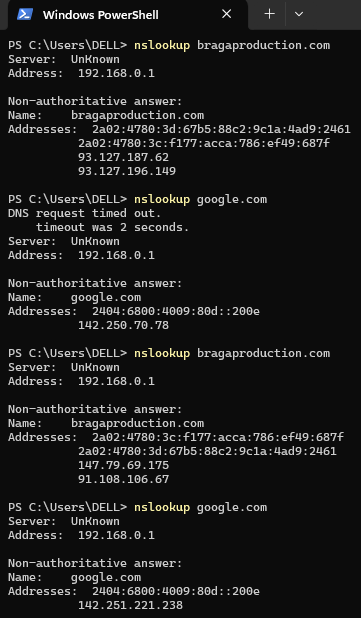
* **Ipconfig:** To check local network settings
* **Ping :** To check connectivity to an external server.



* **Traceroute :** To trace the route(path) taken by packets to reach the server.



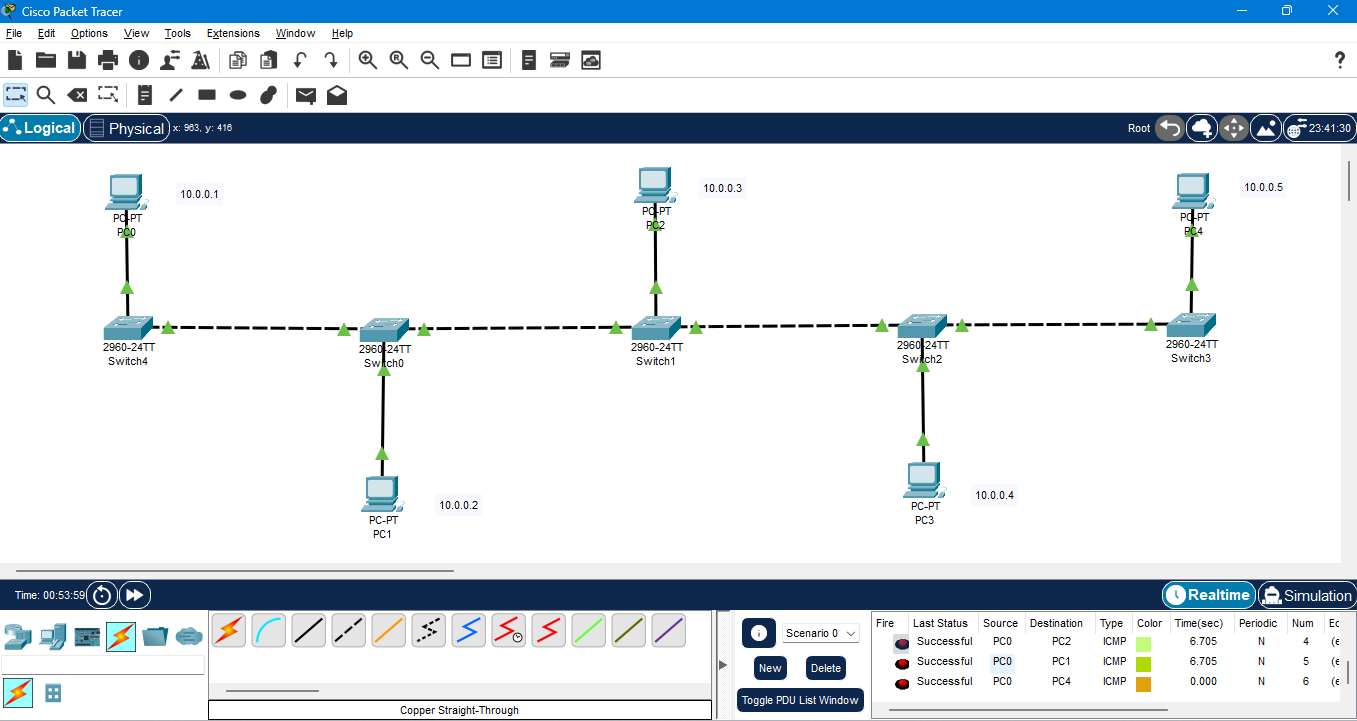
* **nslookup:** To resolve domain name in to IP address and visa versa.

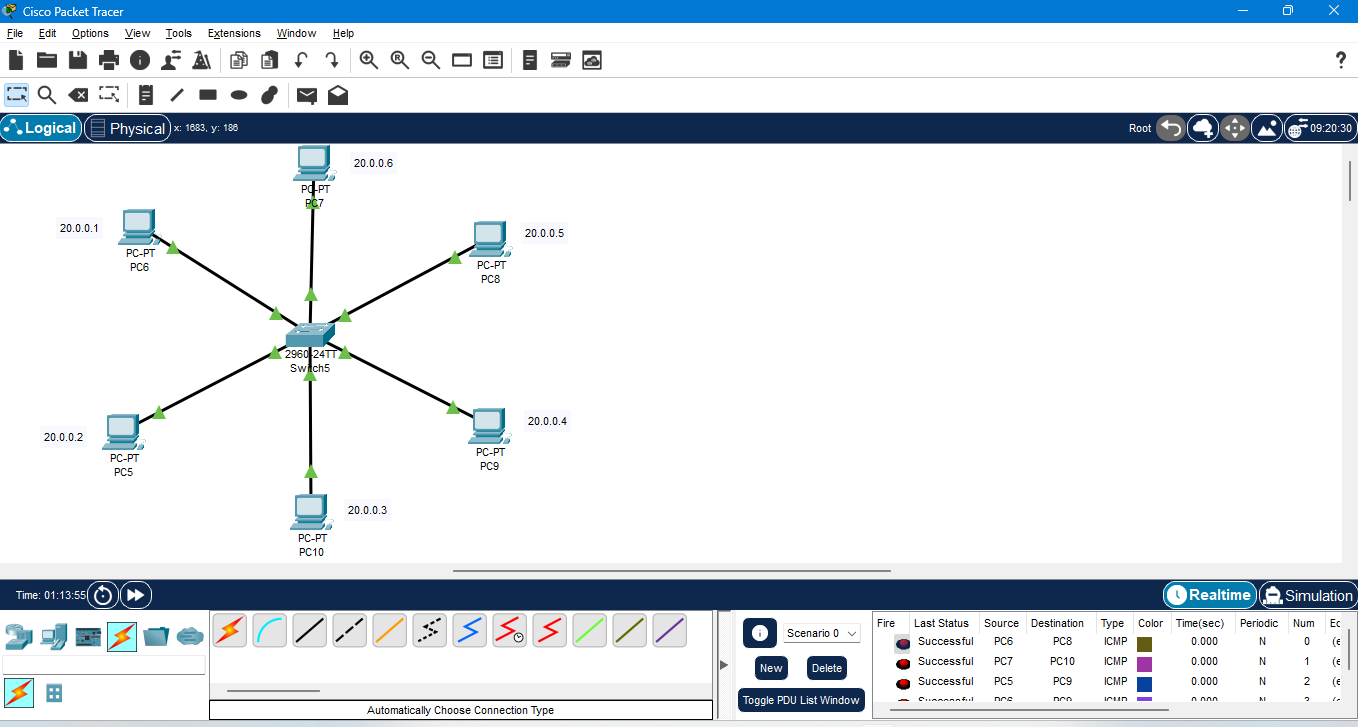


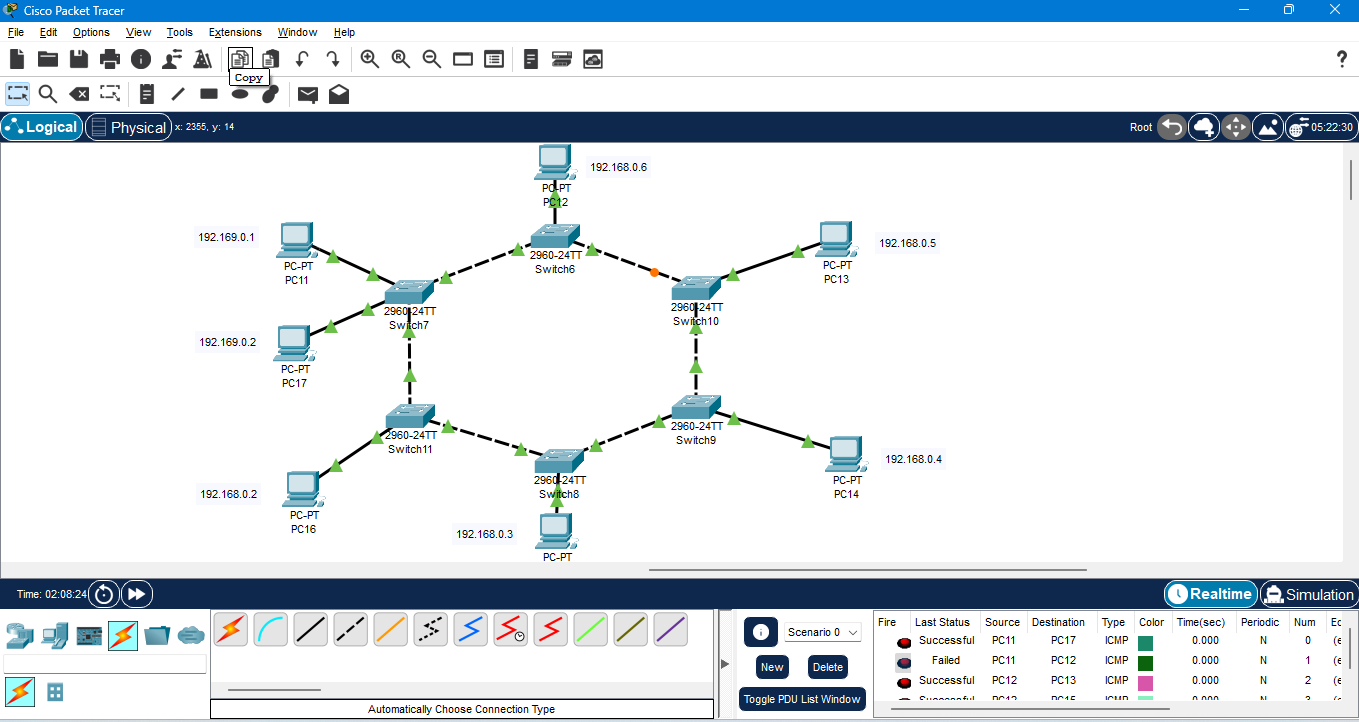
**Task 6: Create a table comparing network devices and their features.**

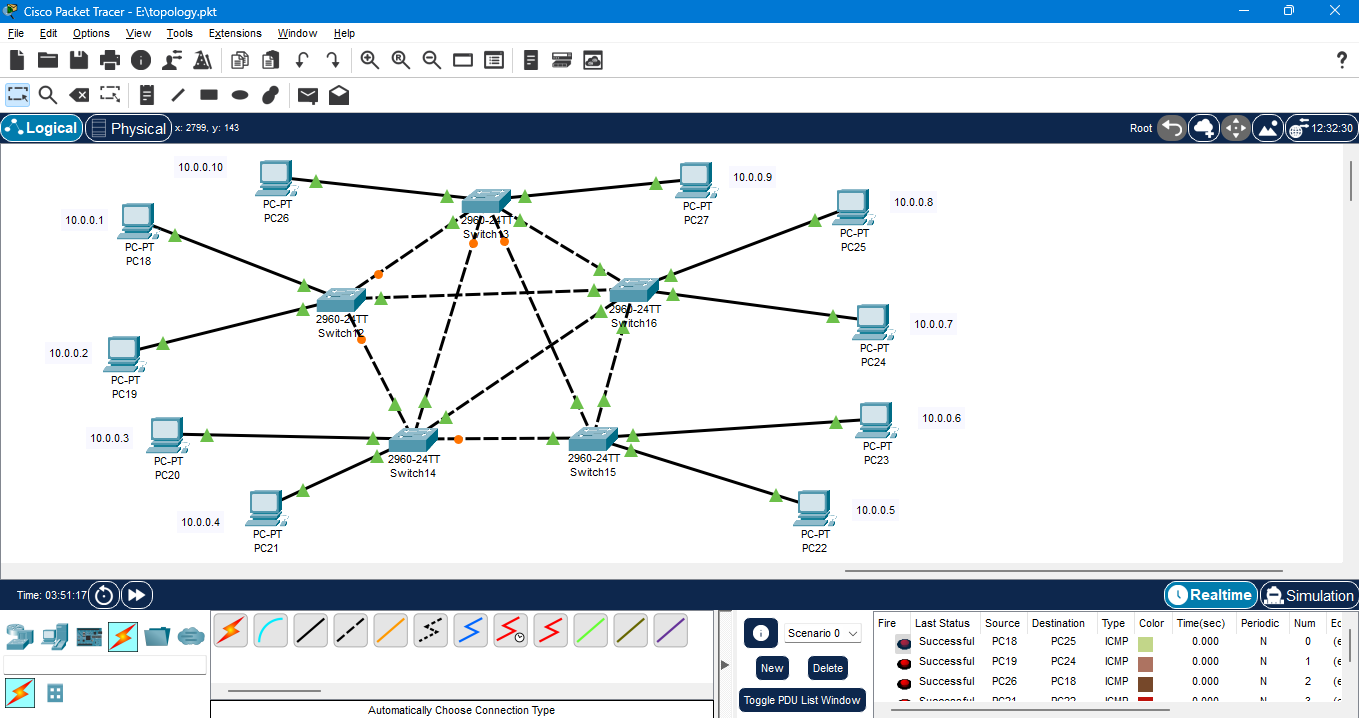
| Device | Main Function | Key Features |
| --- | --- | --- |
| Hub | Sends data to **all devices** in a network | - No intelligence  - Broadcasts data  - Collision is high  - Outdated |
| Switch | Sends data to the **correct device (MAC address)** | - Reduces collisions  - Full-duplex link  - Faster than hubs  - Traffic is minimal |
| Router | Connects **different networks** (e.g., LAN to WAN) | - Uses IP addresses  - Provides internet  - Supports DHCP/NAT |
| Firewall | **Secures** the network by controlling traffic | - Blocks unauthorized access  - Filters based on rules  - Can be hardware/software |
| Access Point | Provides **Wi-Fi** access to wired network | - Connects wireless devices  - Broadcasts SSID  - Supports encryption |
| Bridge | Connects **two LAN segments** | - Filters traffic  - Reduces traffic  - Learns MAC addresses  - No collision due to store and forward strategy |
| Repeater | **Boosts weak signals** | - Extends network range  - No filtering or logic  - Collision is maximum |
| Gateway | Connects **different protocols or networks** | - Protocol converter  - Used in hybrid networks  - Complex translations |
| Modem | Connects to **ISP and internet** | - Converts digital to analog  - Needed for DSL, fiber, cable internet |

**Task 7: Draw a diagram of topologies with examples.**

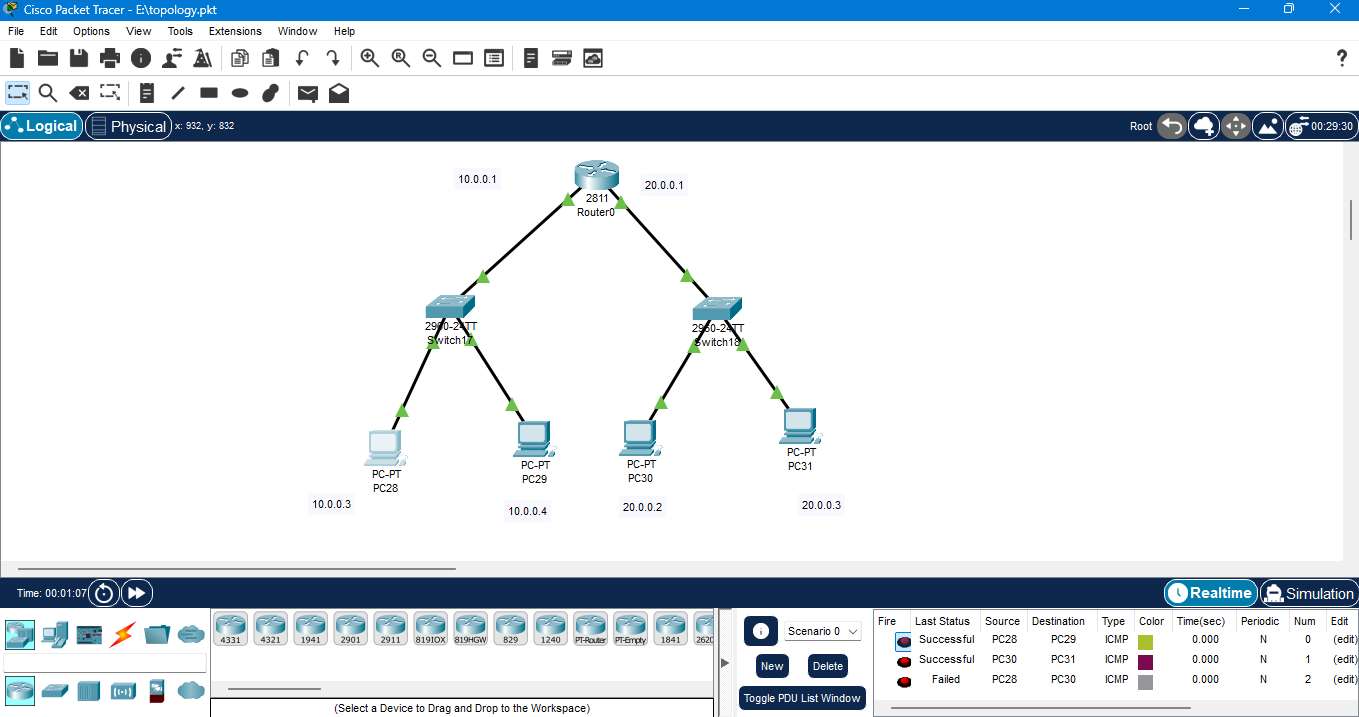
* **Bus topology**
* **Star topology**

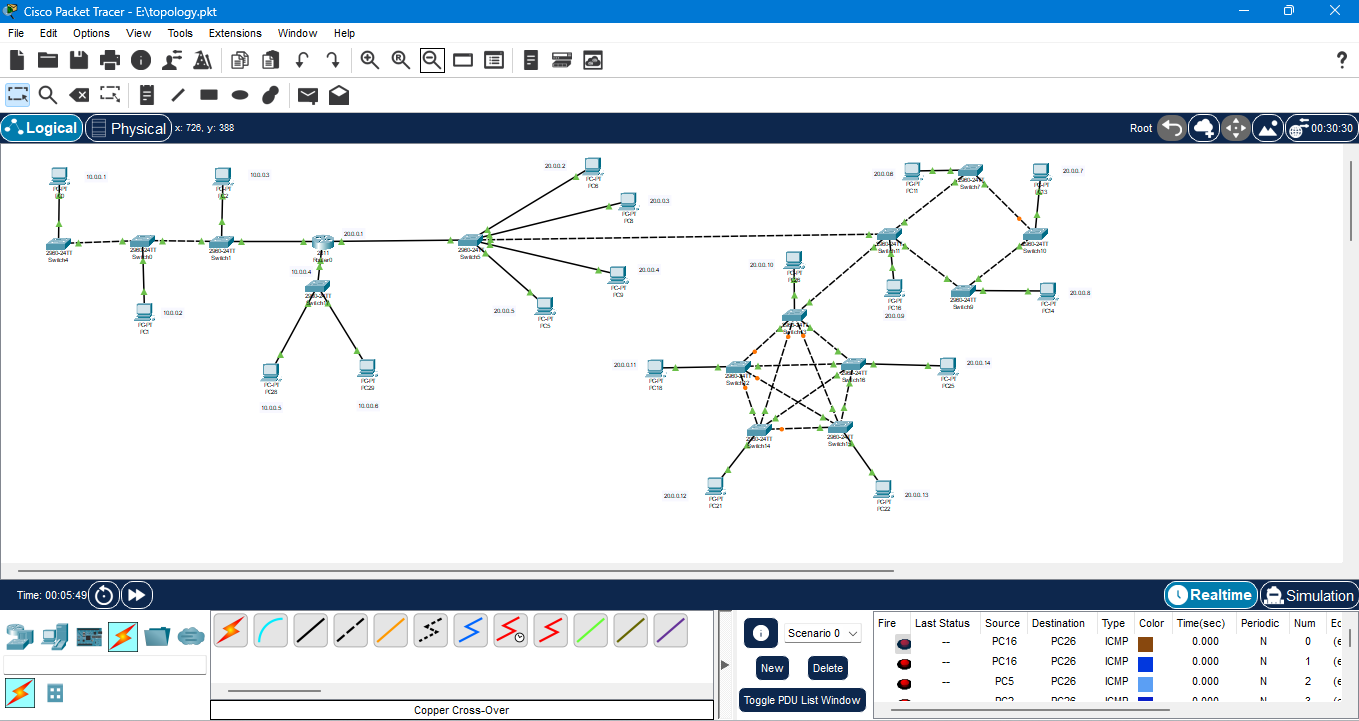


* **Ring topology**
* **Mesh Topology**





* **Tree Topology**
* **Hybrid topology**



**Task 8: Configure a static route between two routers in a simulation.**

To configure a static route between two routers in a simulation (e.g., using Cisco Packet Tracer), follow these step-by-step instructions. This will assume you're connecting Router0 and Router1 and want to enable communication between their LANs.

**Basic Network Topology**

* **Router0 LAN**: 192.168.1.0/24
* **Router1 LAN**: 192.168.2.0/24
* **Router0 ⇄ Router1 (WAN)**: 10.0.0.0/30

**Step-by-Step Configuration**

**1. Assign IP Addresses**

Router0:

Router0> enable

Router0# configure terminal

Router0(config)# interface gig0/0

Router0(config-if)# ip address 192.168.1.1 255.255.255.0

Router0(config-if)# no shutdown

Router0(config)# interface gig0/1

Router0(config-if)# ip address 10.0.0.1 255.255.255.252

Router0(config-if)# no shutdown

**Router1:**

Router1> enable

Router1# configure terminal

Router1(config)# interface gig0/0

Router1(config-if)# ip address 10.0.0.2 255.255.255.252

Router1(config-if)# no shutdown

Router1(config)# interface gig0/1

Router1(config-if)# ip address 192.168.2.1 255.255.255.0

Router1(config-if)# no shutdown

**Configure PCs (example)**

**PC0:**

* IP Address: 192.168.1.10
* Subnet Mask: 255.255.255.0
* Default Gateway: 192.168.1.1

**PC1:**

* IP Address: 192.168.2.10
* Subnet Mask: 255.255.255.0
* Default Gateway: 192.168.2.1

**Test Connectivity**

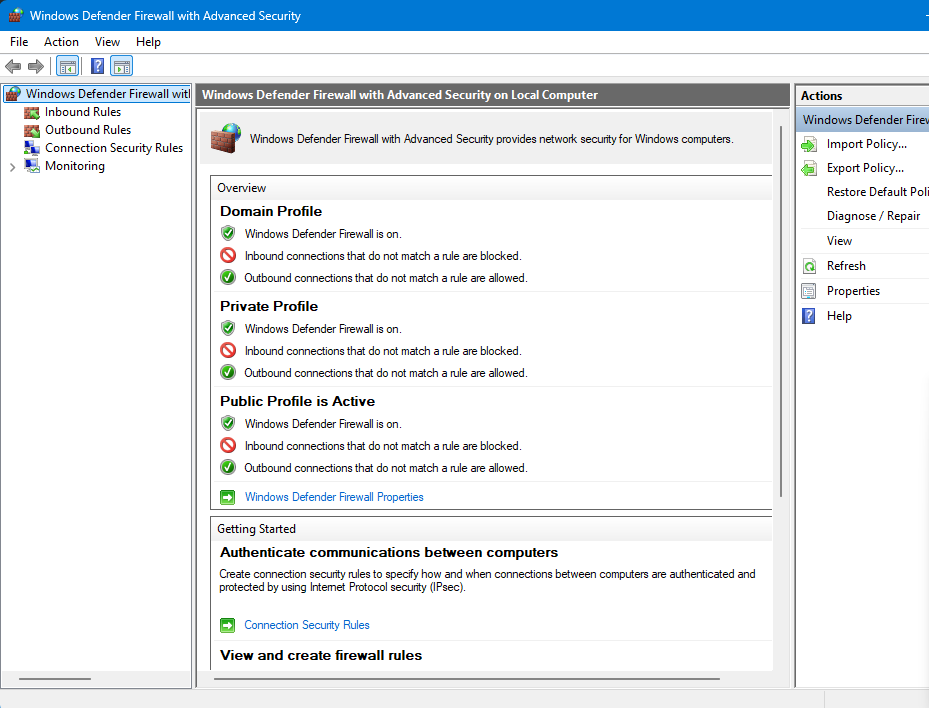
Use the ping command from **PC0 to PC1**:

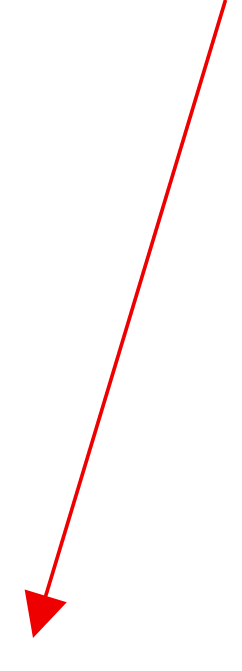
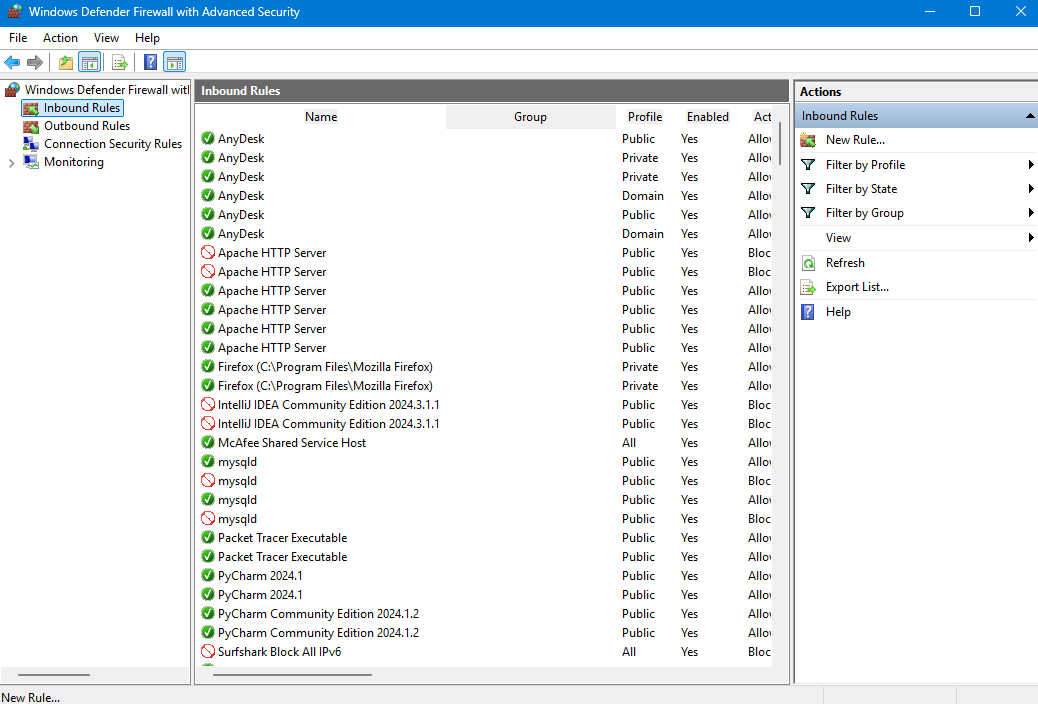
**PC0> ping 192.168.2.10**

**Task 9: Document how to block and allow specific traffic using a firewall.**

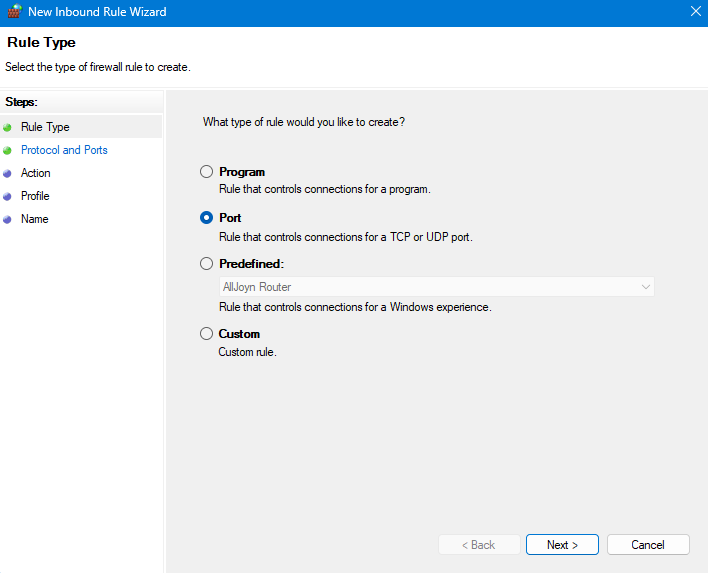
### **Allow Specific Traffic (e.g., Port 80 – HTTP)**

### **Step 1**: Open Control Panel > Windows Defender Firewall

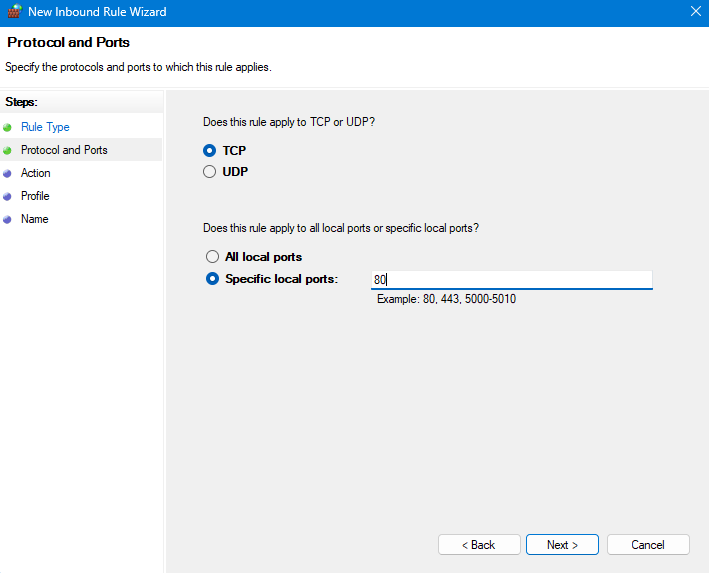


**Step 2: Click Inbound Rules > New Rule.**

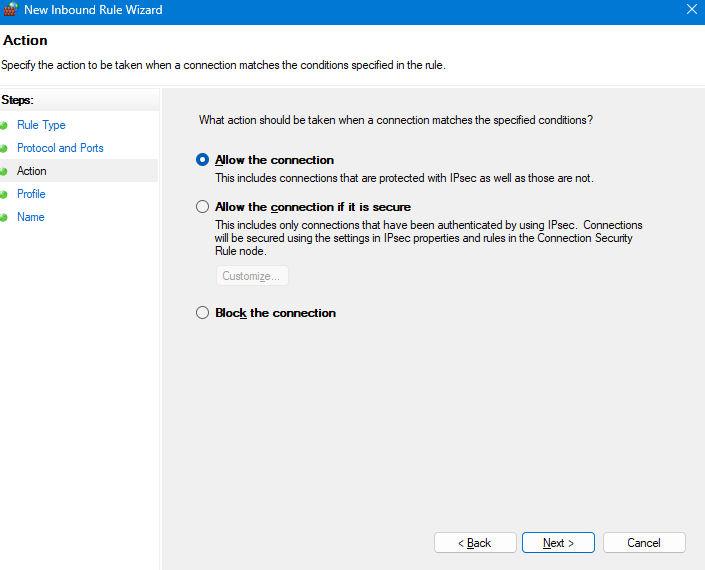
**Step 3: Choose Port and click next.**



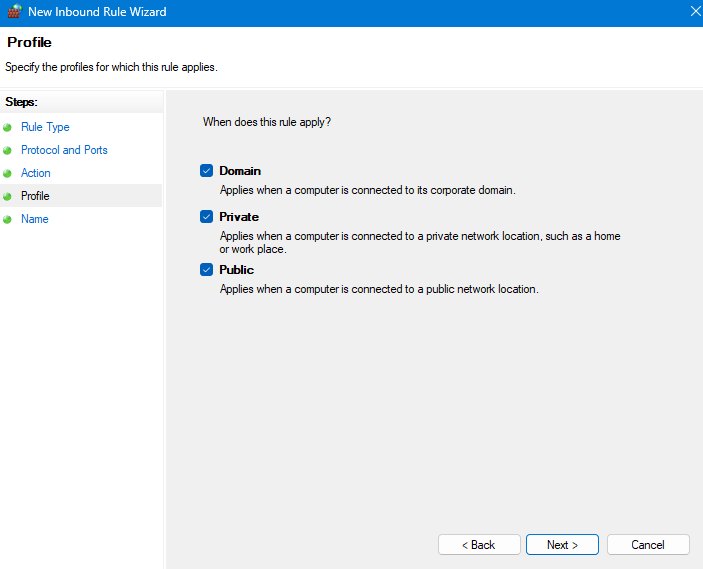
**Step 4: Choose TCP > Specific local ports: 80 and click next.**

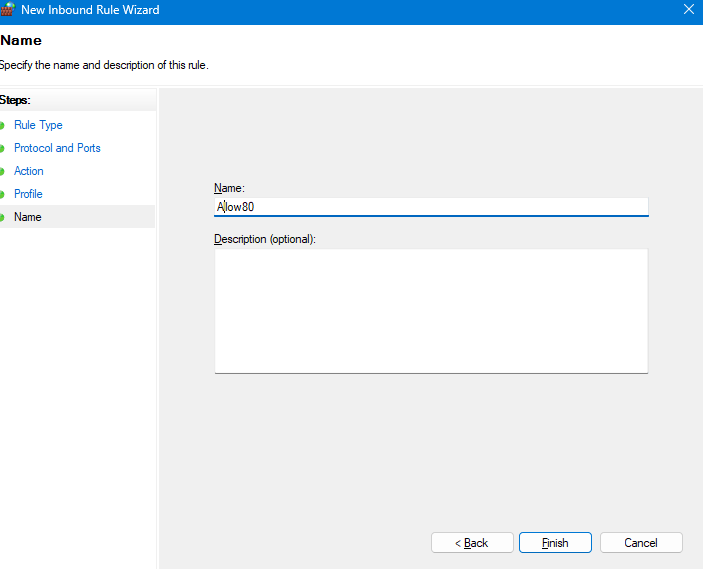


**Step 5: Select Allow the connection.**



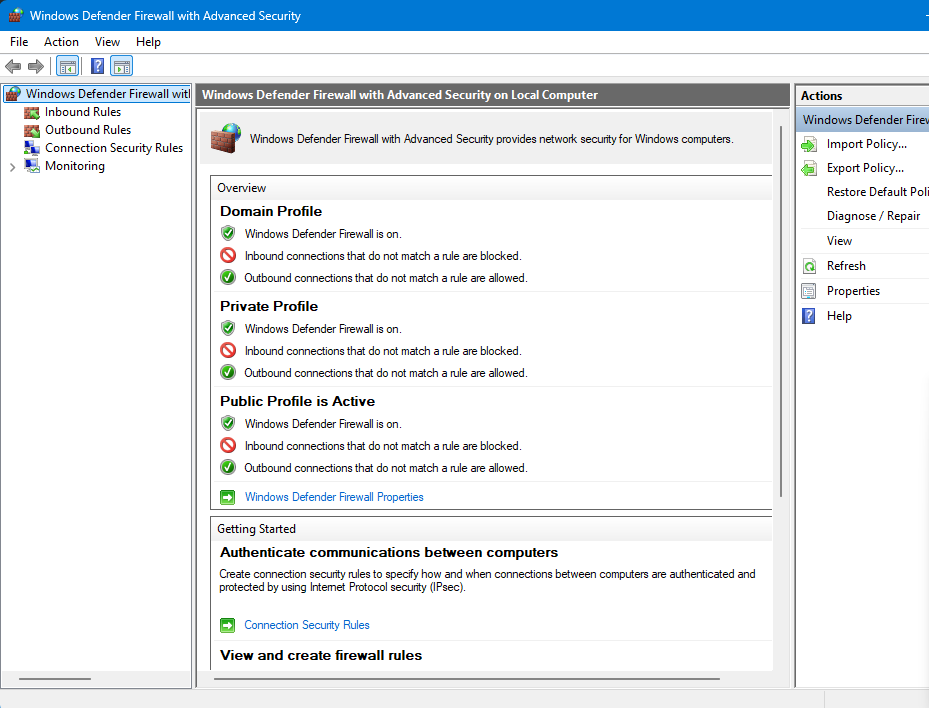
**Step 6: Apply rule to Domain, Private, and Public as needed and click next.**



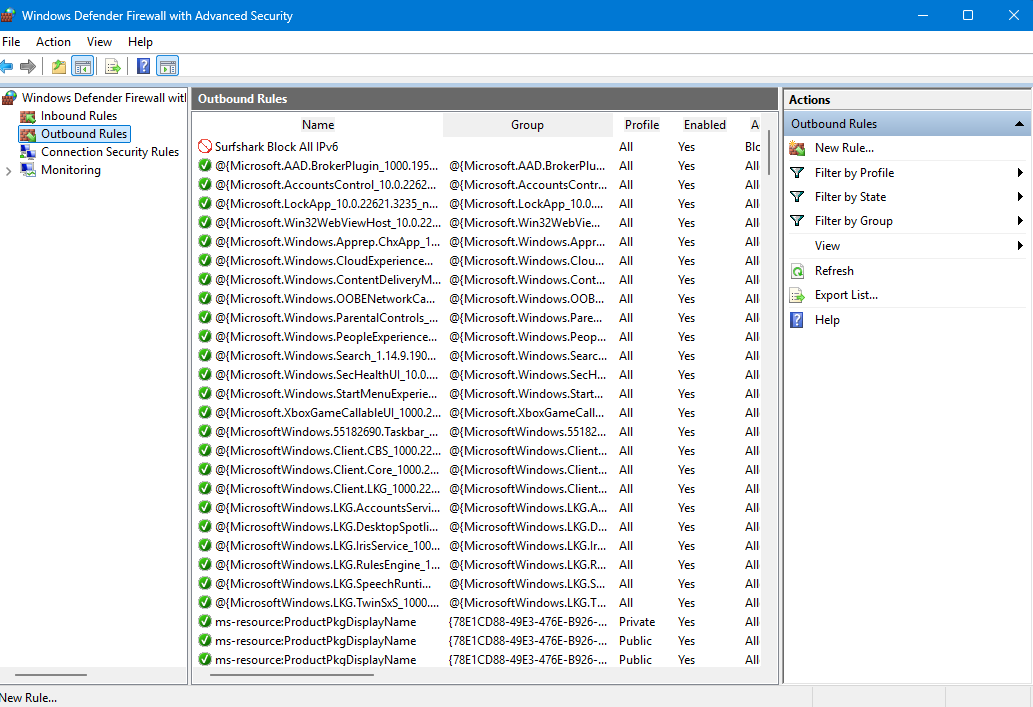
**Step 7: Name the rule and click the finish.**

### **Block All Outgoing Traffic (e.g., Port 443 – HTTPS)**

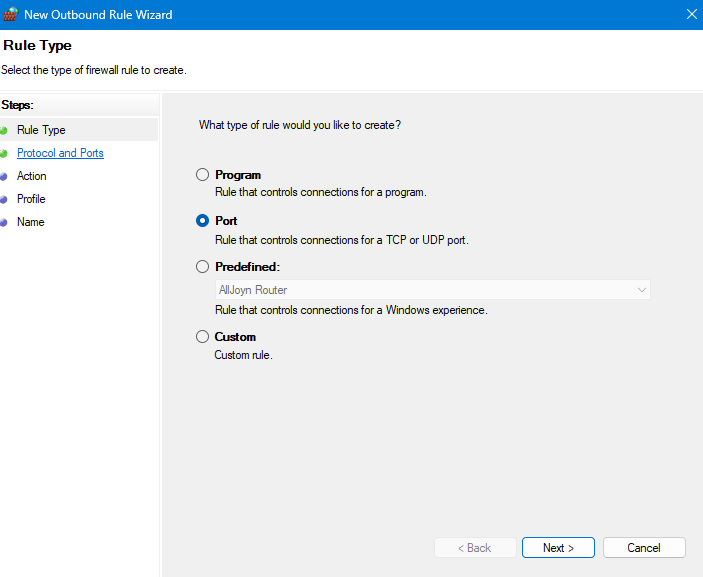
**Step 1**: Open Control Panel > Windows Defender Firewall



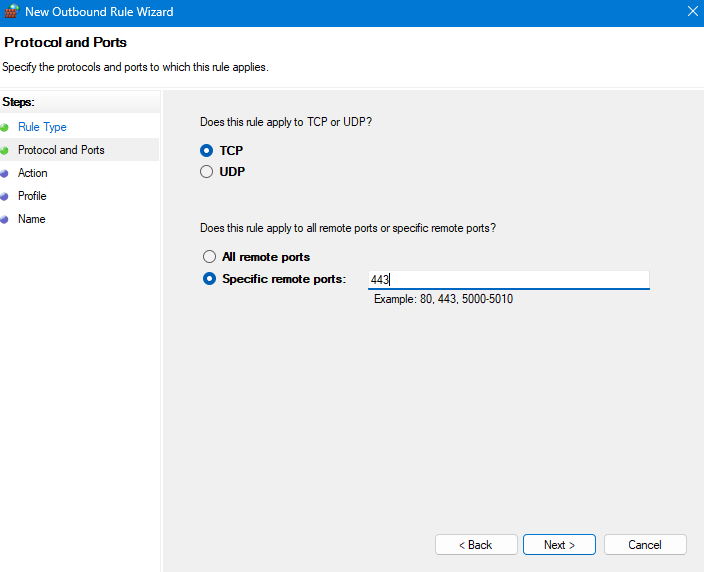
**Step 2**: Click Outbound Rules > New Rule.

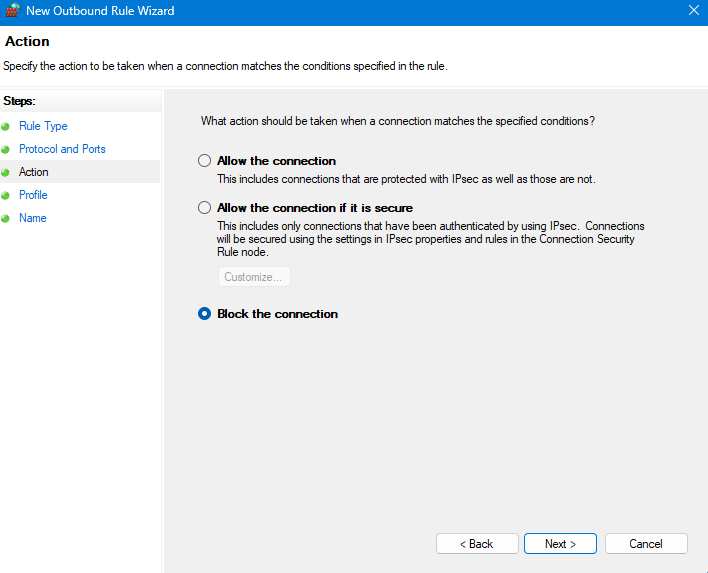


**Step 3**: Choose **Program** or **Port** (depending on what you want to block) and click next.

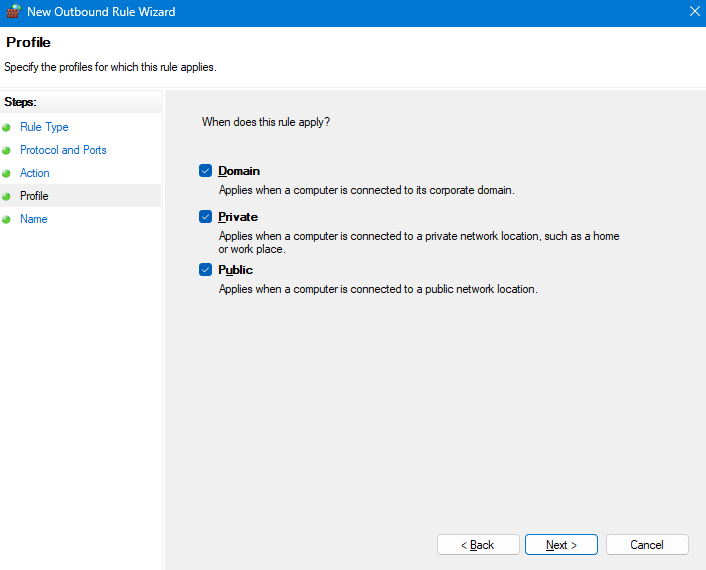


**Step 4**: Choose specific port TCP and specify port (e.g., 443) and click next.

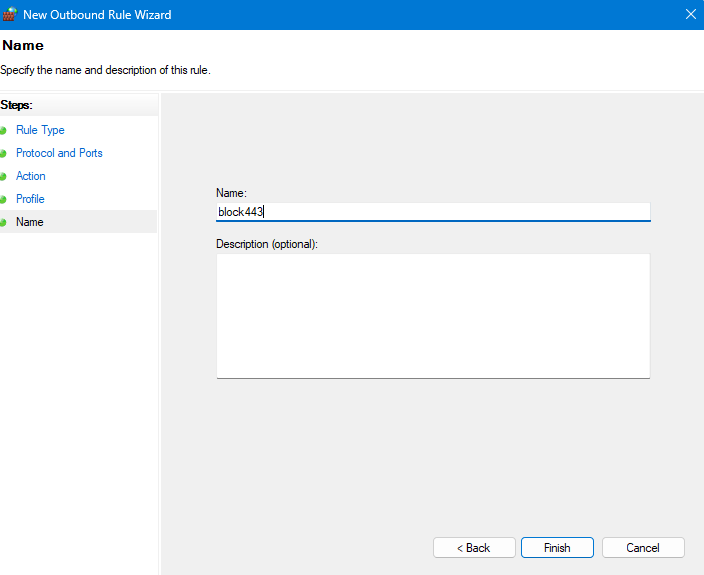


**Step 5:** Select Block the connection and click next.

**Step 6**: Apply to Domain, Private, Public and click next.



Step 7: Name it and click Finish



**Task 10: Document the steps for configuring a small network.**

* **Equipment needed to build a SOHO network**

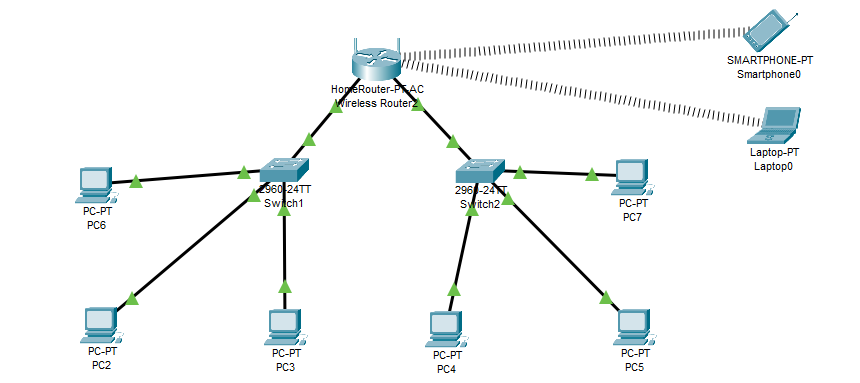
**Wireless home Router**: Ensure you have a wireless router that supports your internet speed.

**Ethernet Cable**: To connect the router to the Switches and PCs.

**Switch**: for more wired devices to connect.

**Laptop**: The device you want to connect wirelessly.

**Smart Phone**: The device you want to connect wirelessly



* **Steps to Set Up a Wireless Network in a SOHO Environment**

**Step 1: Internet Connectivity via Wireless Router**

* The Wireless Router acts as the central networking device.
* It likely connects to an external ISP (not shown) for internet access.
* It provides both wired Ethernet ports and wireless signals.

**Step 2: Switches Connected to the Route**

* Switch1 and Switch2 are connected to the LAN ports of the wireless router using Ethernet cables.
* The router provides IP addressing (via DHCP) and internet access to all connected devices.

**Step 3: Wired Devices Connected to Switches**

* Switch1 connects to three PCs: PC2, PC3, and PC6
* Switch2 connects to four PCs: PC4, PC5, PC7, and one port back to the router
* These switches extend the wired connectivity and help in LAN communication among all devices.

**Step 4: Wireless Devices**

* Laptop0 and Smartphone0 connect to the wireless signals broadcasted by the router.
* They do not need Ethernet cables but must be within range of the Wi-Fi router.
* These devices receive IP addresses from the router and can access the internet and other LAN devices.

**Step 5: DHCP and IP Addressing**

* The router acts as the DHCP server, assigning IP addresses dynamically to all devices—wired and wireless.
* All devices are likely part of the same subnet (e.g., 192.168.0.1), allowing communication across the network.

**Step 6: Communication Between Devices**

* Devices connected to the same switch or different switches can communicate via the router's LAN.
* Wireless and wired devices are part of the same LAN, enabling file sharing, printer access, and internet use.

**Network security, Maintenance and Troubleshooting procedures**

**Task 1: Write a report on the role of DNS and HTTP in web communication.**

**Introduction**

When you open a website like www.google.com, you probably don’t think about what happens behind the scenes. But a lot of invisible teamwork is going on between two important technologies: **DNS (Domain Name System)** and **HTTP (Hypertext Transfer Protocol)**. These two act like a **directory** and a **messenger**, helping your device find the right web server and then get the information you asked for.

**What is DNS – Like a Phonebook for the Internet**

You remember names, not numbers, right? That’s exactly what DNS helps with.

Every website lives on a computer somewhere in the world, and that computer has an IP address (like 172.217.194.106). But no one wants to type that. So, when you type www.youtube.com, **DNS converts that name into the correct IP address**, just like looking up a name in your phone to find the number.

**Here’s what happens step-by-step:**

1. You type a website address into your browser.
2. Your device asks a DNS server, “Hey, what’s the IP address for this website?”
3. The DNS server checks its database or asks others until it finds the answer.
4. It replies with the right IP address.
5. Now your browser knows where to go.

So DNS is not about sending data, it’s about helping your browser find the destination.

**What is HTTP – Like a Delivery Truck for Web Content**

Once your browser knows where to go (thanks to DNS), **HTTP comes in to deliver the data.**

Think of HTTP as a polite courier. It knocks on the door of the server (which has the website data), says “Can I please have the homepage?” and then delivers it back to you.

**What happens next:**

1. Your browser uses the IP address to reach the website's server.
2. It sends an **HTTP request** asking for a web page or file.
3. The server receives the request, prepares the page, and sends it back using an **HTTP response**.
4. Your browser then shows you the webpage you asked for.

HTTP is **not permanent or personal**, it doesn’t remember you. Every time you click a link or refresh a page, a brand-new request starts over. That’s why it’s called **stateless**.

**How DNS and HTTP Work Together**

Let’s say you’re ordering pizza online.

* **DNS** helps you find the correct restaurant's phone number (IP address).
* **HTTP** is the call you make to place your order (ask for the web page).

Without DNS, your browser wouldn’t know where to send the request.  
Without HTTP, you couldn’t ask for the content you want.

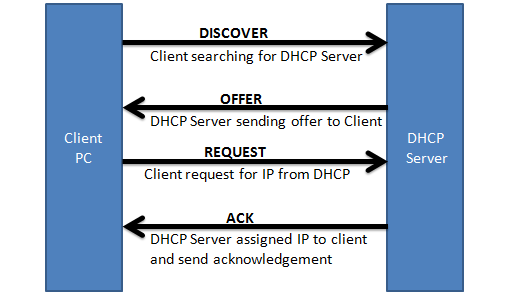
**Real-World Example**

When you visit www.amazon.in:

1. DNS figures out where Amazon’s server is.
2. HTTP requests the homepage.
3. The server sends back images, product listings, prices, etc.
4. You see the page load.

And all of this happens in **milliseconds**, every time you visit a website.

**Task: Create a diagram showing the DHCP process flow.**

****

**Task: Document the configuration and troubleshooting steps.**

To configure a DNS server in Cisco Packet Tracer and verify name resolution from client devices. Also, document how to troubleshoot DNS issues in this simulated environment.

* **DNS Configuration Steps in Cisco Packet Tracer**

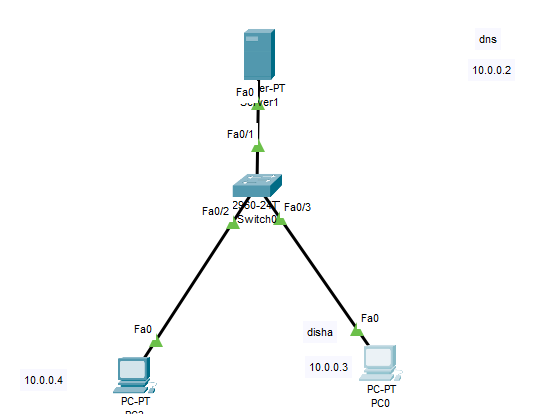
**Step 1: Set Up the Topology**

**Devices Needed:**

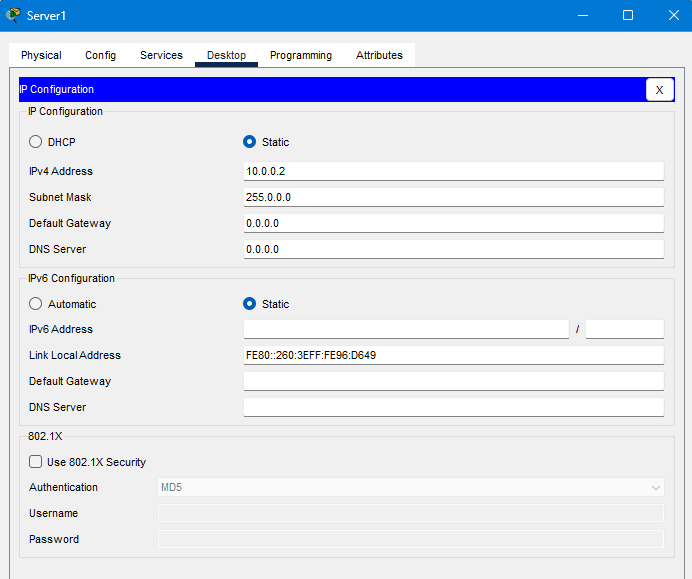
* 1 Server
* 2 or more PCs
* 1 Switch

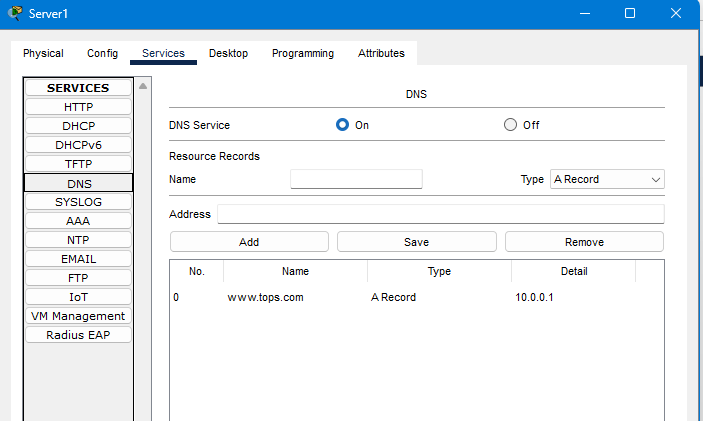
**Connections:**

* Connect all devices to the switch using **copper straight-through cables**.

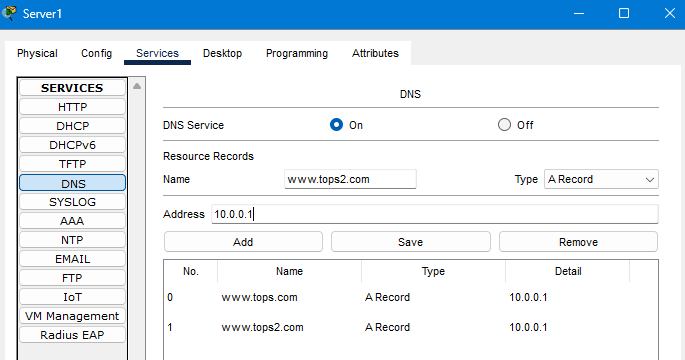


**Step 2: Configure Server as a DNS Server**

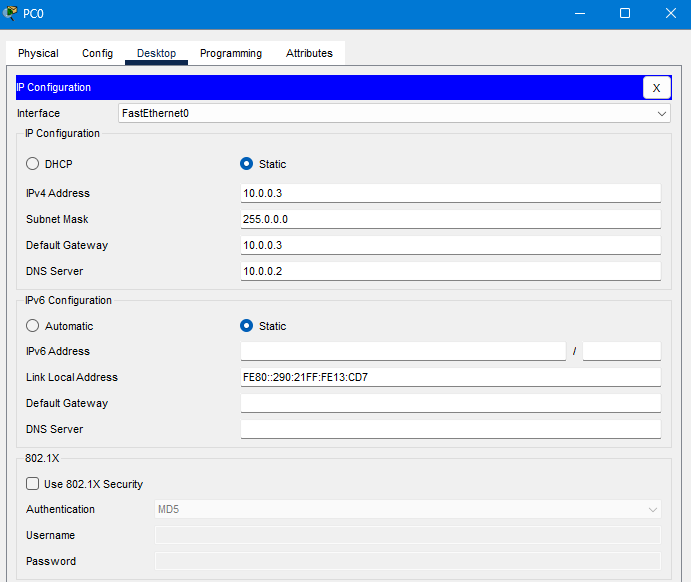
1. **Click on the Server**
2. Go to the **Desktop tab**
3. Open **IP Configuration**
   * Set a static IP address (e.g., 10.0.0.2)
   * Set the **subnet mask** (255.0.0.0)
   * Leave gateway blank or set if a router is used
4. Go to **Services tab**
5. Click on **DNS**
6. **Turn DNS service ON**



1. Add the domain and corresponding IP address:
   * Example:
     + **Name**: www.company.com
     + **Address**: 192.168.1.20 (Assume this is a web server or another PC)
   * Click **Add**



**Step 3: Configure PC Clients**

1. Click on **PC1 (or other clients)**
2. Go to **Desktop > IP Configuration**
   * Set static IP (e.g., 10.0.0.3)
   * Subnet Mask: 255.255.255.0
   * Gateway: (if router is used)
   * **DNS Server**: 192.168.1.10 (IP of your DNS server)

**DNS Troubleshooting Steps in Packet Tracer**

**Step 1: Verify IP Configuration**

* On each PC and the server, go to **IP Configuration** and confirm:
  + IP address and subnet are correct
  + DNS IP is pointing to the server
  + Gateway is set (if cross-network)

**Step 2: Check DNS Service**

* On the server:
  + Go to **Services > DNS**
  + Ensure service is **ON**
  + Make sure the correct hostname and IP mappings exist

**Step 3: Test with IP Directly**

* From the PC, try pinging the **IP address** of the web server directly:

ping 10.0.0.1

* If it works, the network is fine but DNS may be misconfigured.

**Step 4: Try nslookup (Name Resolution Check)**

* In the PC’s **Command Prompt**, run:

nslookup www.tops2.com

* If it fails:
  + Either DNS IP is incorrect
  + Or the domain is not registered in the DNS service on the server

**Step 5: Check Connectivity**

* Ping between devices to check:
  + ping 10.0.0.2 (from PC to DNS server)
  + If this fails: Check cables, switch ports, or IP addresses

**Step 6: Use Simulation Mode**

* Switch Packet Tracer to **Simulation Mode**
* Add a **DNS** filter in the event list
* Try to ping or browse to www.company.com
* Watch the DNS request and response packets
  + You can visually trace where the problem occurs (e.g., request never reaches server)

**Task: Create a table comparing FTP and HTTP.**

| **FTP** | **HTTP** |
| --- | --- |
| Ftp stands for file transfer ptotocol. | HTTP stands for hypertext transefer protocol. |
| Used to transfer file from remote computer after connection is established. | Used to transfer web pages, web services, and big file from remote computer. |
| FTP is slower than HTTP. | HTTP is faster than FTP |
| Usually requires **username & password** for authentication. | Typically no login for public content (can use cookies/sessions) |
| Basic FTP is **not secure** (data sent in plain text) | HTTP is insecure; **HTTPS** encrypts data using SSL/TLS |
| Supports file operations: **rename, delete, list, etc.** | No direct file management capabilities |
| FileZilla, WinSCP, command-line ftp | Web browsers (Chrome, Firefox), curl, Postman |

**Task: Document solutions for common DNS and DHCP issues.**

**Common DNS Issues & Solutions**

| Issue | |  | | --- |  | **Possible Cause** | | --- | | Solution |
| --- | --- | --- | --- | --- |
| DNS name not resolving | - Incorrect DNS IP in client settings - DNS server down | - Verify DNS server IP in client - Ping DNS server - Restart DNS service |
| Slow browsing / delay in name lookup | - DNS cache issues - Server overload | - Flush DNS cache using ipconfig /flushdns or systemd-resolve --flush-caches |
| Incorrect domain resolution | - Wrong entries in DNS zone - Old cached record | - Check DNS zone records - Clear client DNS cache and retry |
| Cannot resolve external websites | - No forwarder configured - Internet not accessible from DNS | - Add a public DNS forwarder (e.g., 8.8.8.8) - Check internet connection |
| Reverse lookup not working | - PTR record missing in reverse zone | - Create or correct reverse lookup (PTR) records in DNS |
| “Server not found” or “No such host” | - Typo in domain name - DNS service not running | - Verify spelling - Restart DNS service and re-test |
| nslookup works but ping does not | - DNS resolves but firewall blocks traffic | - Check firewall settings or host availability |

**Common DHCP Issues & Solutions**

| **Issue** | Possible Cause | Solution |
| --- | --- | --- |
| Client not receiving IP address | - DHCP server not reachable - Cable disconnected - Scope exhausted | | - Check network connection - Verify DHCP is enabled - Ensure IP pool has available addresses | | --- |  |  | | --- | |
| IP Conflict (two devices same IP) | - Static IP within DHCP range - Rogue DHCP server | - Avoid manual IPs in DHCP range - Use DHCP snooping or check logs |
| Client receives APIPA (169.x.x.x) IP | - No DHCP response received | - Restart DHCP client - Check connectivity to DHCP server - Restart DHCP service |
| Incorrect default gateway/subnet mask | - Misconfigured DHCP scope options | - Reconfigure DHCP scope options with correct network settings |
| DHCP lease not renewing | - Lease time too short - Server unreachable during renew | - Increase lease duration - Ensure constant DHCP availability |
| DHCP service not starting | - Port 67 in use - Missing authorization (Windows) | - Restart DHCP service - Check logs for error codes |
| Intermittent IP assignment issues | - Multiple DHCP servers on the same network | - Limit to one DHCP server or use DHCP relay - Use proper VLAN separation |

**Task: Submit a detailed report on the network setup and configurations performed.**

**Network Setup and Configuration Report**

**1. Project Overview**

This report outlines the step-by-step network setup and configurations performed in the given networking environment. The objective was to design a functioning network with appropriate IP addressing, enable DNS and DHCP services, and ensure successful communication between all devices.

**2. Topology Description**

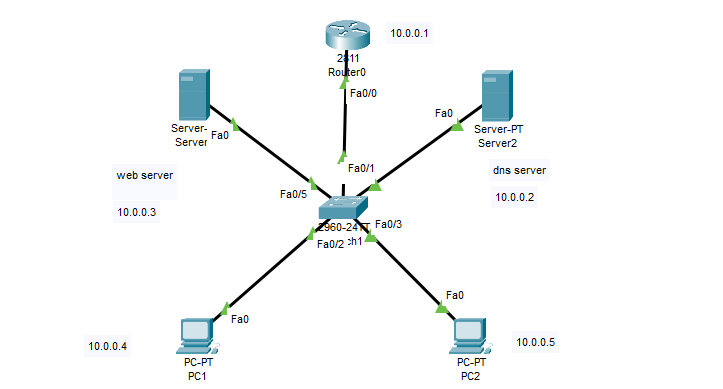
**Devices Used:**

* 1 Router (Cisco 2811)
* 1 Switch (Cisco 2960)
* 1 DNS/DHCP Server
* 2 PCs (Client Devices)
* (Optional) 1 Web Server for testing

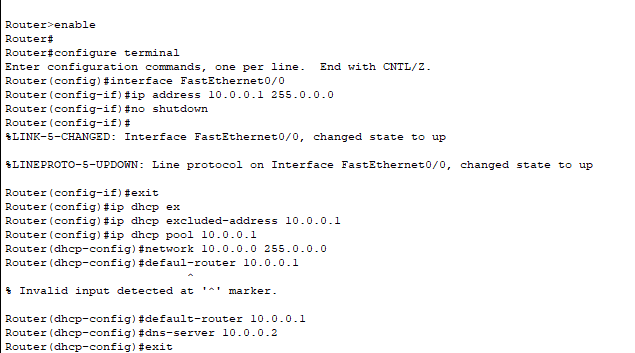
**Network Diagram Summary:**

* All devices are connected through a switch using copper straight-through cables.
* The router is used to provide gateway access if different networks are used.

| Device | IP Address | Subnet Mask | Default Gateway |
| --- | --- | --- | --- |
| Router (G0/0) | 10.0.0.1 | 255.0.0.0 | - |
| DNS/DHCP Server | 10.0.0.2 | 255.0.0.0 | 10.0.0.1 |
| Web server | 10.0.0.3 | 255.0.0.0 | 10.0.0.1 |
| PC1 | DHCP (Dynamic) | Assigned via DHCP | 10.0.0.1 |
| PC2 | DHCP (Dynamic) | Assigned via DHCP | 10.0.0.1 |

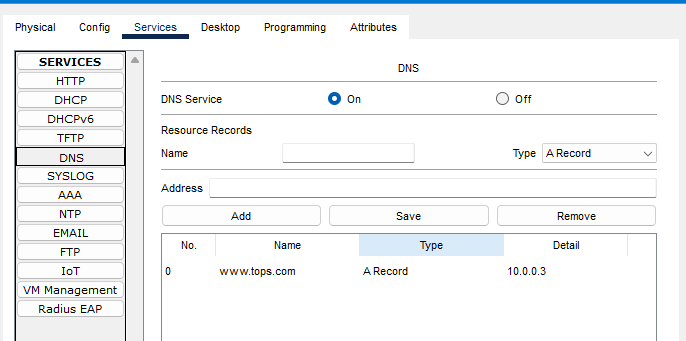


**Router DHCP configuration**



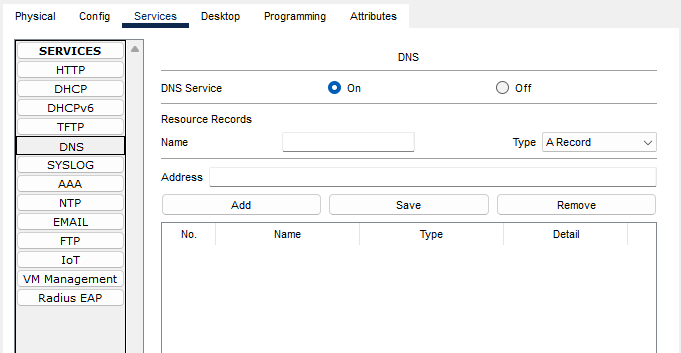
**DNS Server Configuration**

* DNS Service was enabled on the server.
* DNS entries were added using the DNS Service tab in Packet Tracer.
* **Adding record:**
* Domain Name: www.tops.com
* 10.0.0.3 (Web server)

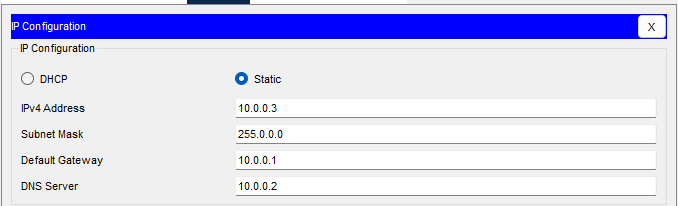


**Web Server Configuration**

* DNS Service was enabled on the server.

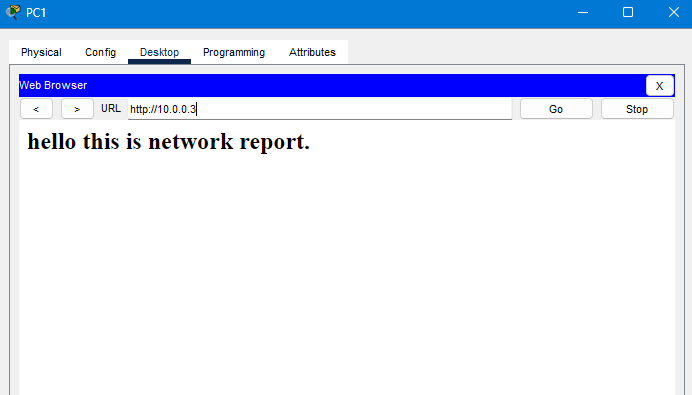


* Default Gateway and DNS server IP addresses added in web server configuration.

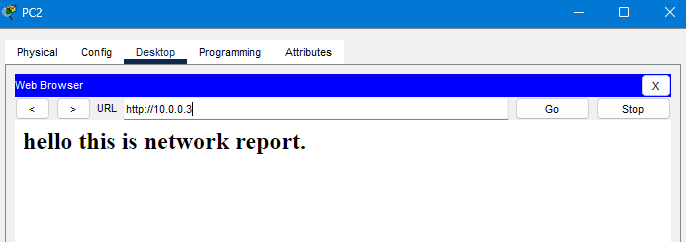


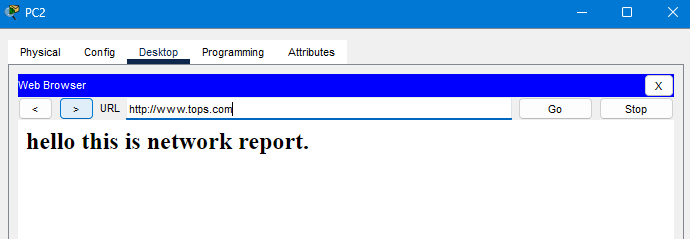
**Verification and testing:**

Verify the dns and dhcp via pc’s web browser.









**PC Configuration**

* **PCs were configured to use DHCP** via the desktop IP configuration.
* After receiving IP addresses, connectivity to the DNS server and external domain was tested.

