Batch: B - 2 Roll No.: 16014022050

Experiment / ~~assignment~~ / ~~tutorial No.:~~ 09

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:
C04:

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:
DHCP (Dynamic Host Configuration Protocol) is a network protocol used to automatically assign IP addresses and other network configuration details to devices on a network, such as PCs, printers, or smartphones. This eliminates the need for network administrators to manually assign static IP addresses to every device.

Here's a breakdown of how DHCP works and the steps involved in setting it up:
How DHCP Works:

1. DHCP Discover: When a device (like a PC) connects to a network, it sends a DHCP Discover message to the network. This message is broadcast to all devices in the network, asking for an IP address.

2. DHCP Offer: The DHCP server (which can be a server or a router) receives the DHCP Discover message. It then responds with a DHCP Offer, which includes an available IP address from a predefined pool of IPs, subnet mask, gateway, and possibly DNS information.
3. DHCP Request: The device that sent the DHCP Discover message sends a DHCP Request message back to the server, requesting the offered IP address.
4. DHCP Acknowledge: The DHCP server sends a DHCP Acknowledge message, confirming the IP address assignment. At this point, the device can use the assigned IP address to communicate on the network.

Components Involved in DHCP:

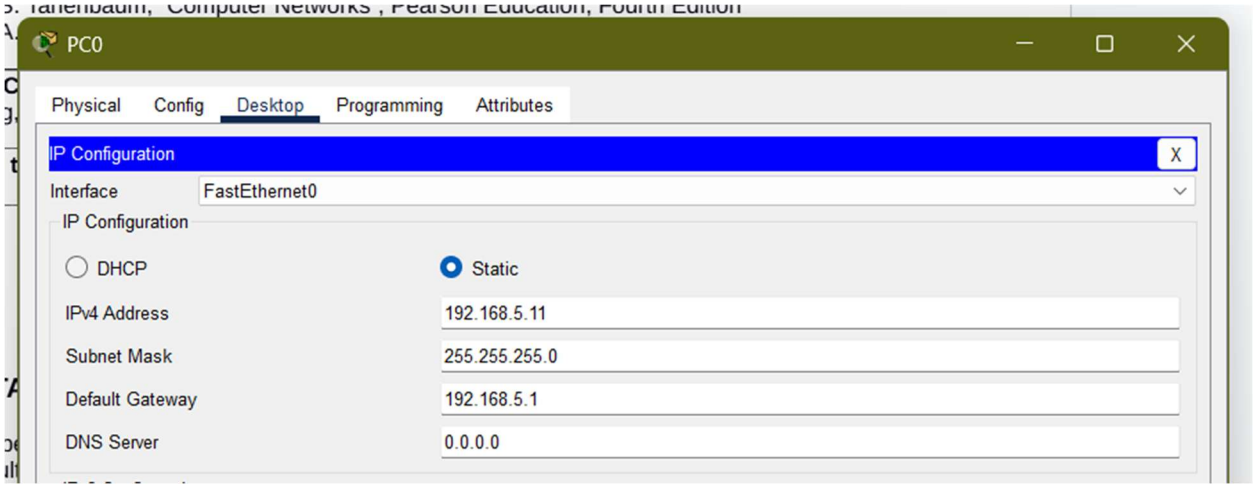
1. DHCP Server: This device has a pool of IP addresses that it can assign to devices on the network. It can also provide other configuration information, such as the default gateway and DNS servers.
2. DHCP Client: This is typically a device (e.g., PC, smartphone, etc.) that sends the DHCP Discover message to obtain an IP address and other network settings automatically.
3. DHCP Lease: The DHCP server assigns an IP address to a client for a specific period. This period is called a lease. The client must renew the lease before it expires if it still requires the IP address.

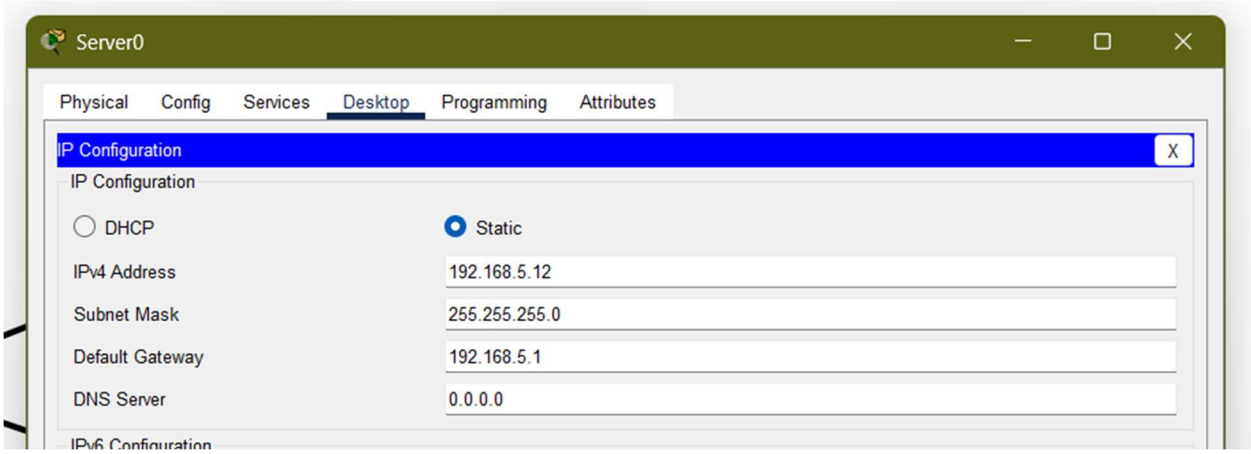
A DNS server's main function is to take a domain name (like www.example.com) and translate it into an IP address (like 192.168.1.2) so that devices can find and communicate with each other on the network.

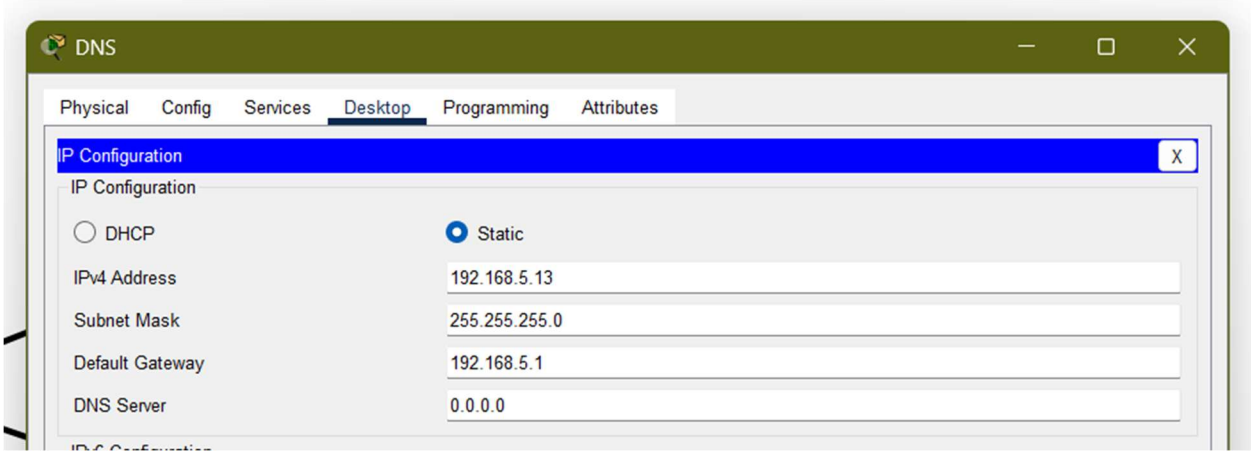
Implementation:

DHCP:

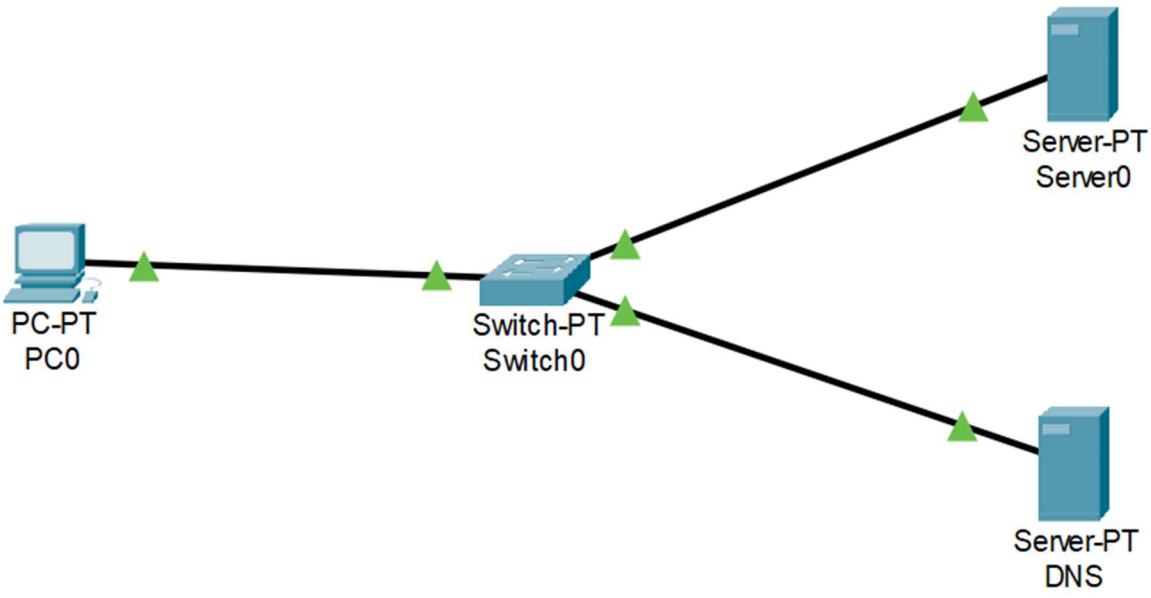
Step 1: First, open the cisco packet tracer desktop and add IP Address for the end device, server0 and DNS with subnet mask and default gateway.





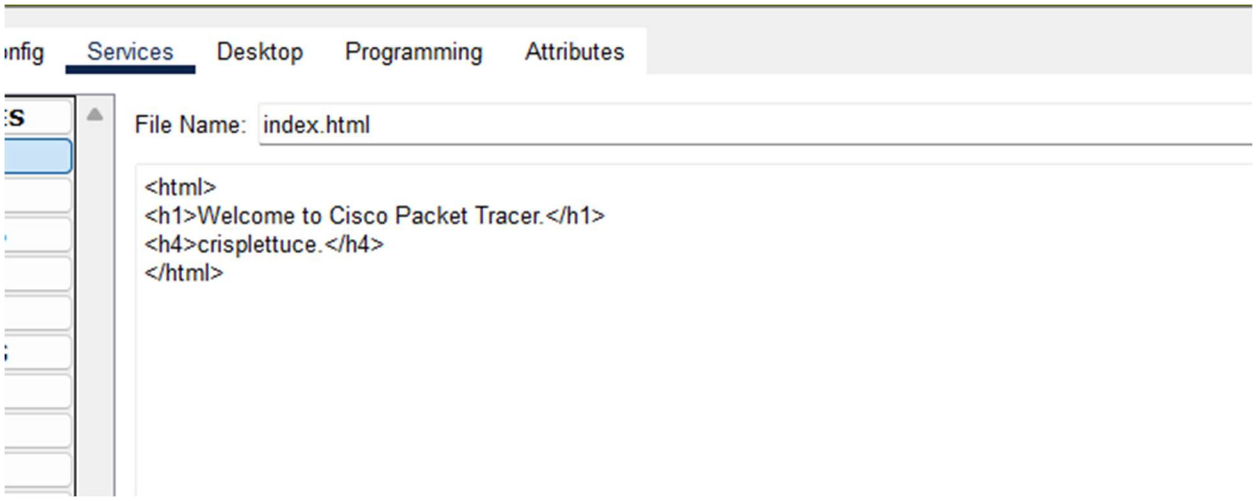


Create a network using them.



Step 2: Configure the HTTP sever0. To configure the HTTP server, go to services then click on HTTP

Then delete all of the files except the index.html and edit it.



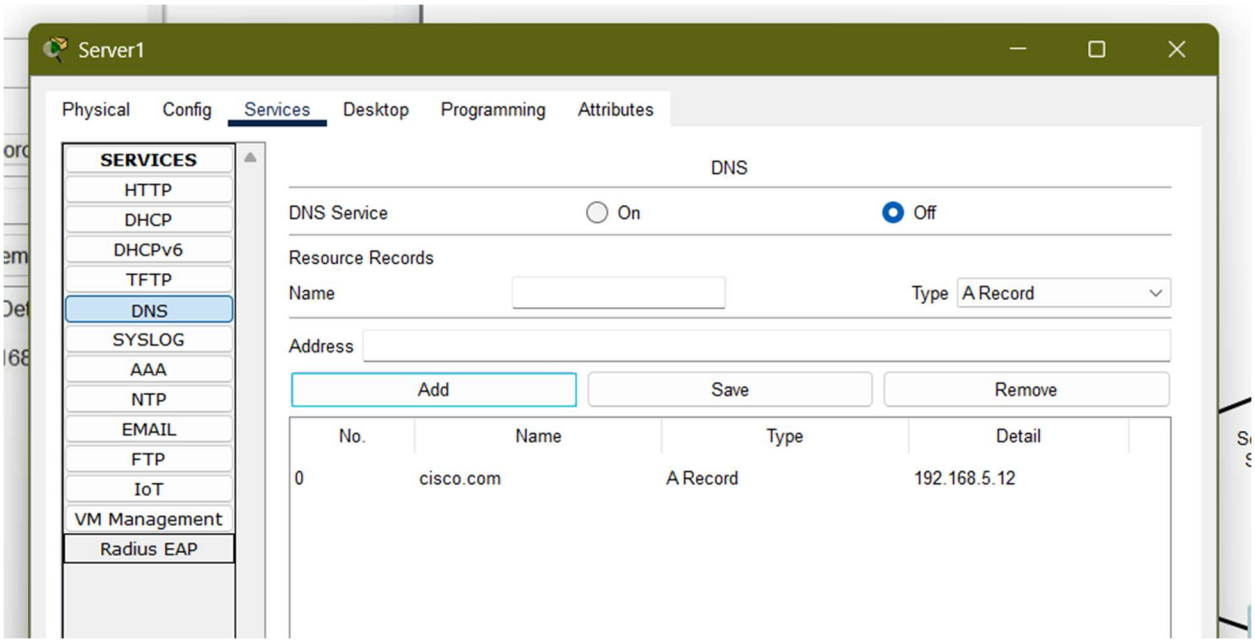
- Go to Services > HTTP: This takes you to the configuration interface for the HTTP server on Server0 in Cisco Packet Tracer.
- Delete All Files Except index.html: You remove any default or unnecessary files that the HTTP server might come with. This makes it simpler to work with and ensures there are no irrelevant files.
- Edit index.html: You now edit the index.html file to create your desired content. For example, you could add a welcome message, images, links, or any content you want to serve to users who connect to the HTTP server.

In DHCP (Dynamic Host Configuration Protocol), the primary goal is to assign IP addresses and other network configuration details automatically to devices (clients) on the network. DNS (Domain Name System), on the other hand, is used to map domain names (like www.example.com) to IP addresses, which are used to locate devices on the network or the internet.

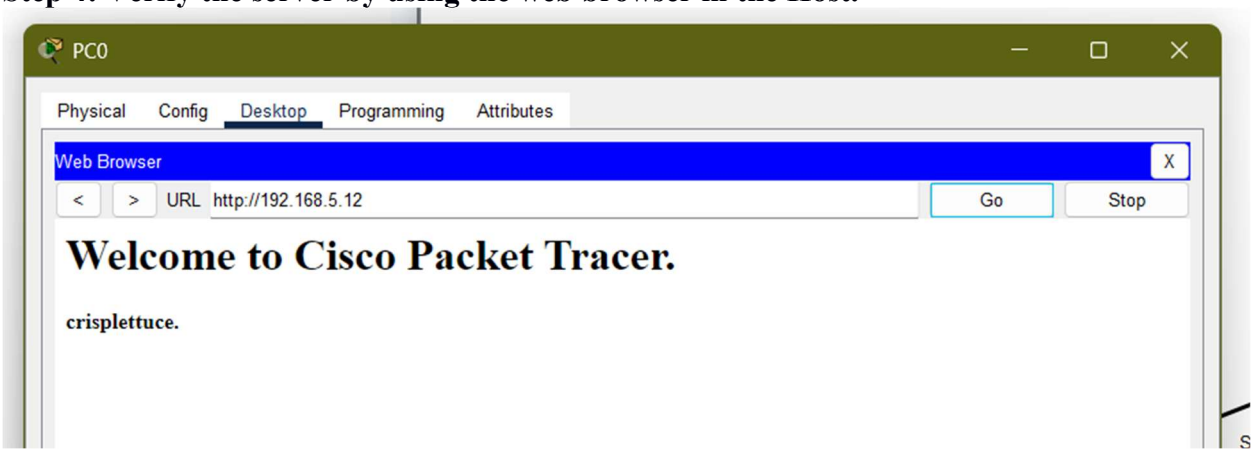
Step 3: Configure the DNS server. To configure the DNS server, go to services then click on DNS.

Then turn on the DNS services. Name the server cisco.com and type address 192.168.5.12. And add the record.

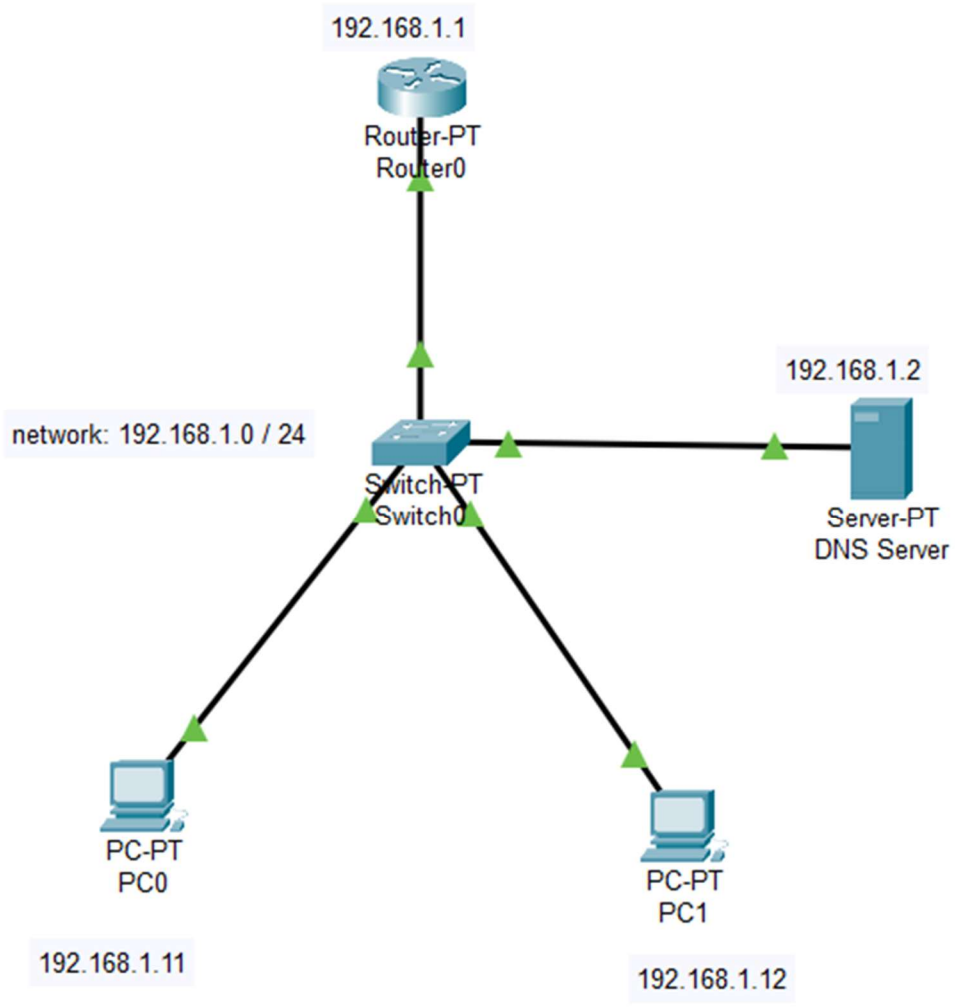
The DNS server ensures that devices can resolve domain names (like cisco.com) to IP addresses (like 192.168.5.12) so that they can access services or websites using names instead of IP addresses.



Step 4: Verify the server by using the web browser in the Host.



DNS:



Step 1: Assign IP Address to the FastEthernet 0/0 interface

You are accessing the router's configuration mode and entering the FastEthernet 0/0 interface configuration.

You're assigning a static IP address (192.168.1.1) to this interface and a subnet mask (255.255.255.0).

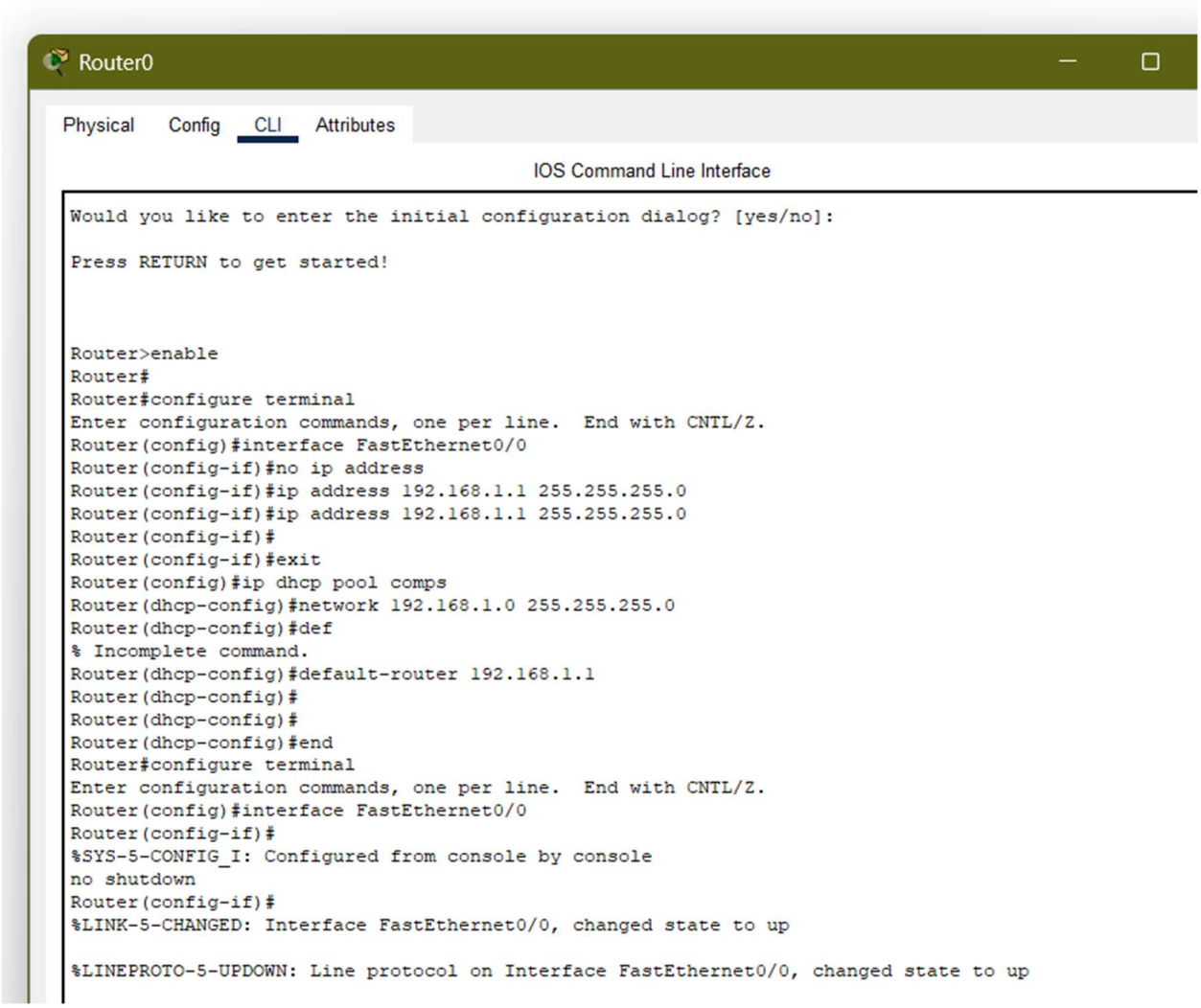
The no shutdown command enables the interface, making it active and operational.

Step 2: Configure network and default gateway

You are creating a DHCP pool named comps. A DHCP pool is a range of IP addresses that the router can assign to devices on the network (like PCs).

The network command defines the network address and subnet mask for the DHCP pool (192.168.1.0/24).

The default-router command sets the default gateway for the devices that will get IPs from this pool, which is the router's IP address (192.168.1.1).

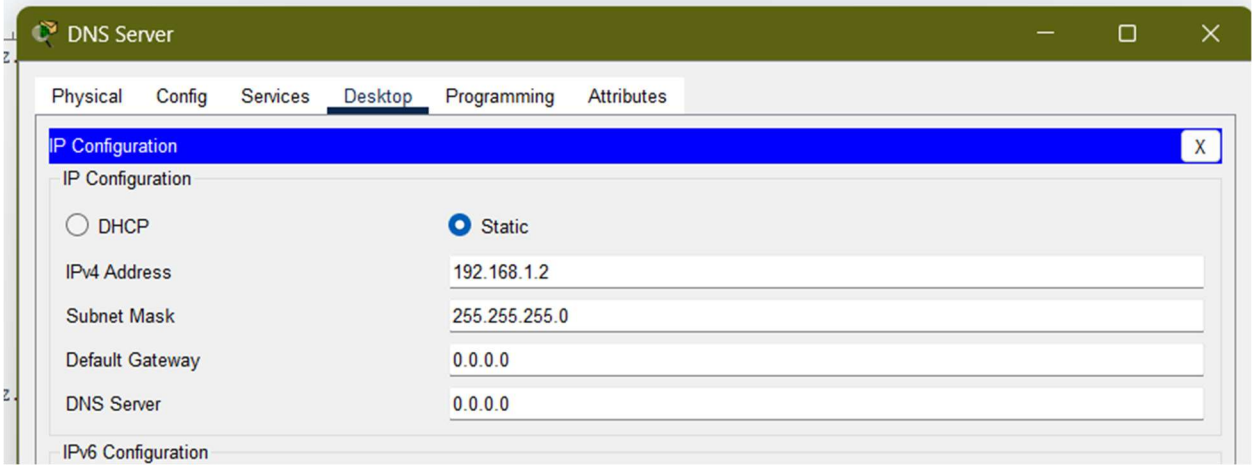


Step 3: Select DHCP in IP configuration of PCs in the network as shown:
On each PC, you will configure the IP settings to use DHCP. This allows them to automatically receive an IP address, subnet mask, default gateway, and DNS server from the router.

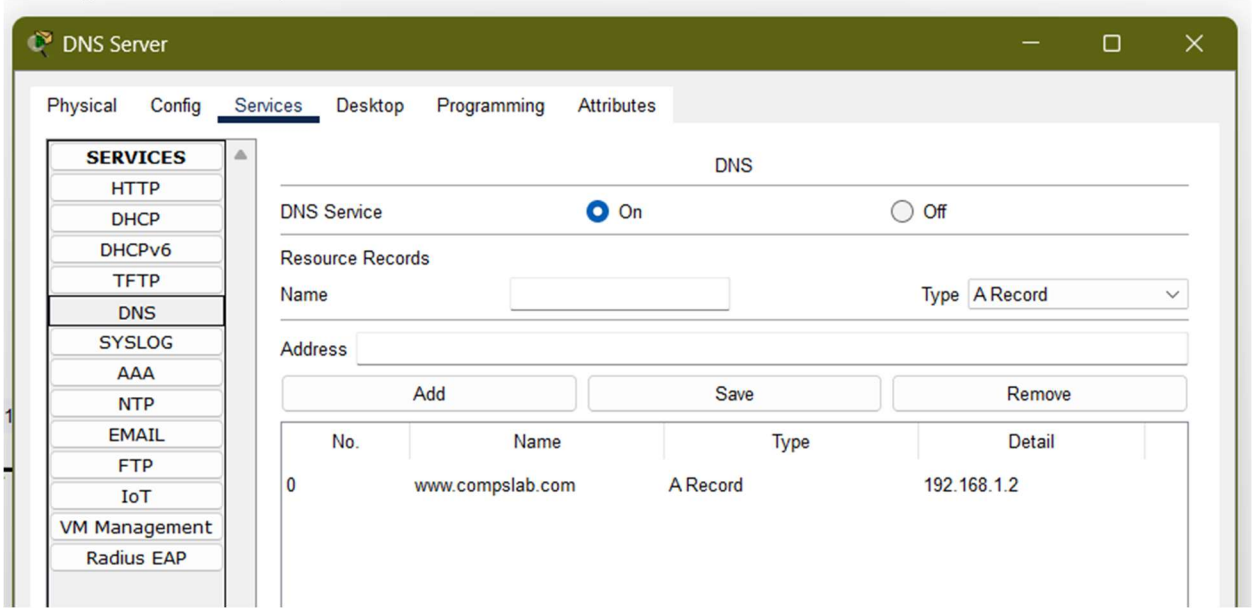
Step 4: Add DNS Server to the network and assign IP address to the server.
First remove dhcp IP configurations from PCs.
Assign static IP address to DNS Server: 192.168.1.2 /24
Assign default gateway and dns server as shown in screenshot.

You're configuring the router's DHCP pool to specify that the DNS server is at 192.168.1.2. This allows the PCs to use this DNS server for resolving domain names.

The excluded-address command is used to prevent the router from assigning IP addresses in a certain range (192.168.1.1 to 192.168.1.10). These addresses are typically reserved for critical devices like the router, DNS server, etc.



Configure DNS entry in DNS server.



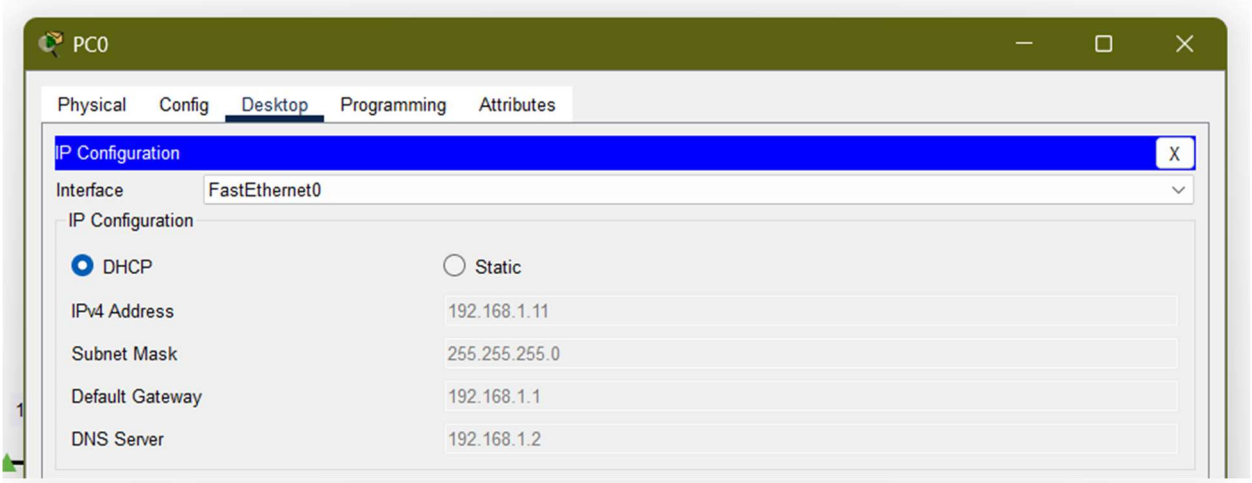
Step 5: Configure dns server & excluded addresses from the pool of IP addresses on router:

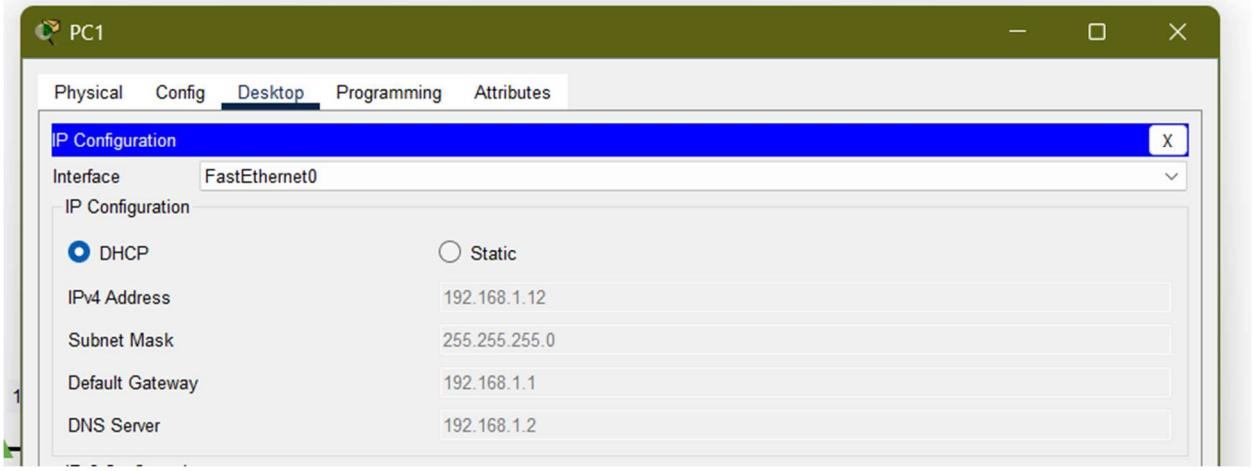
```
Router(config-if)#exit
Router(config)#ip dhcp pool comps
Router(dhcp-config)#dns-server 192.168.1.2
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
Router(config)#do show ip dhcp pool comps
Pool comps :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 2
 Excluded addresses             : 1
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.1.1          192.168.1.1      - 192.168.1.254     2    / 1     / 254
Router(config)#
```

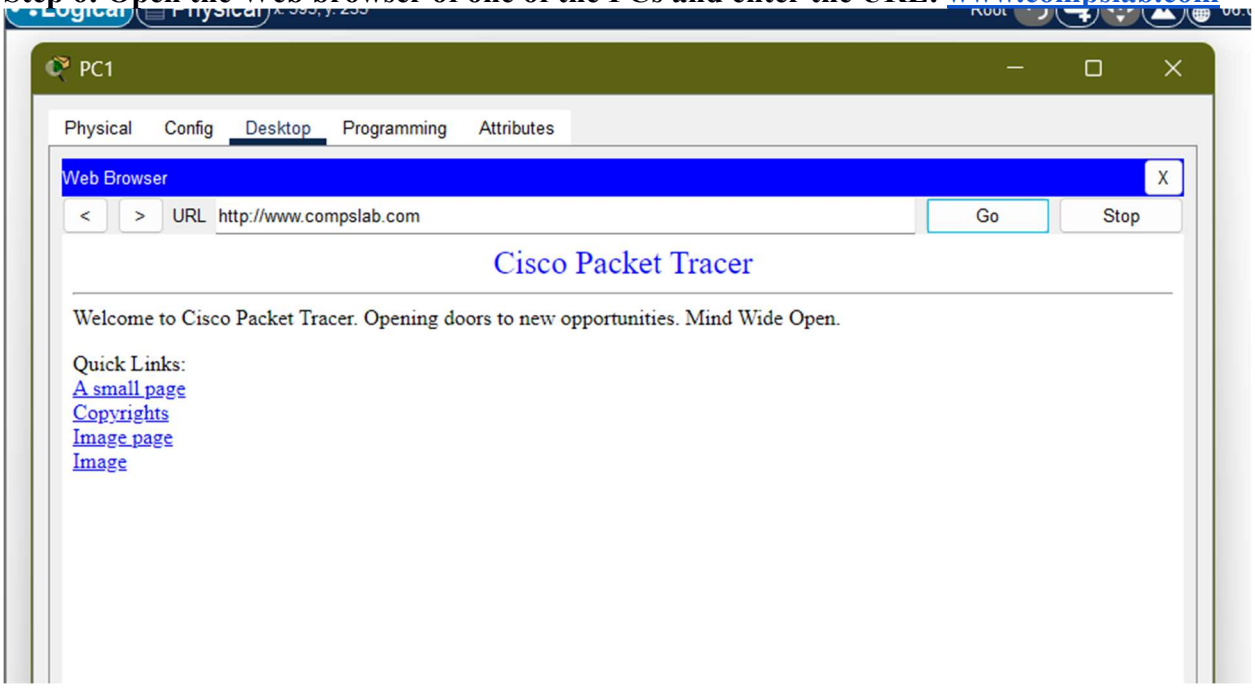
You are verifying the DHCP configuration to ensure that the DHCP pool comps is correctly set up, and you can see how many addresses have been leased out, excluded, and the current status.

Updated IP Configurations of PC0 and PC1 after configuring dns server and excluded addresses:





Step 6: Open the Web browser of one of the PCs and enter the URL: www.compslab.com



After configuring the DNS server (192.168.1.2) and the DHCP settings, you will open a web browser on one of the PCs and type the URL www.compslab.com in the address bar.

If the setup is correct, the DNS server will resolve www.compslab.com to the IP address of the web server (which is likely 192.168.1.12 in your setup).

This should bring up the hosted web page, confirming that the DNS and web server configurations are working properly.

Conclusion:

In this experiment, we successfully studied and configured DHCP (Dynamic Host Configuration Protocol) and DNS (Domain Name System) protocols using Cisco Packet Tracer. By setting up the router to act as a DHCP server, we were able to automatically assign IP addresses to PCs in the network. Additionally, we configured a DNS server to resolve domain names to IP addresses, allowing PCs to access websites using friendly domain names rather than IP addresses. This hands-on setup helped us understand how DHCP and DNS work together to facilitate seamless network communication and domain resolution.

Post Lab Questions:

1. **Describe DHCP and DNS with examples.**

   DHCP (Dynamic Host Configuration Protocol) is a protocol that automatically assigns IP addresses and other network settings (like subnet mask, default gateway, and DNS server) to devices on a network. This eliminates the need for manual IP configuration and makes it easier to manage large networks.
   Example: When you connect your PC to a Wi-Fi network, your router uses DHCP to automatically assign your PC an IP address.

   DNS (Domain Name System) is a system that translates domain names (like www.example.com) into IP addresses (like 192.168.1.2). This allows users to access websites using easy-to-remember names instead of remembering complex IP addresses.
   Example: When you type google.com in your browser, DNS translates that to the IP address of Google's web server, so your computer can access the site.

Date: _____ **Signature of faculty in-charge**