

**UNIVERSITY OF ASIA PACIFIC**

**Department of Computer Science & Engineering**

|  |
| --- |
| DHCP with DNS |

**Course Code :** CSE 320

**Course Title :** Computer Networks Lab

**Submitted by: Submitted To: Name :** Sheikh Nafez Sadnan Md. Akhtaruzzamman Adnan **Reg. No. :** 20101106 Assistant Professor

**Roll No. :** 106 Department of CSE

**Section :** B (2) University of Asia Pacific

**Definition of DHCP**

Dynamic Host Configuration Protocol (DHCP) is an application layer protocol which is used to provide: 

1. Subnet Mask (Option 1 – e.g., 255.255.255.0)
2. Router Address (Option 3 – e.g., 192.168.1.1)
3. DNS Address (Option 6 – e.g., 8.8.8.8)
4. Vendor Class Identifier (Option 43 – e.g., ‘unifi’ = 192.168.1.9 ##where unifi = controller)

DHCP is based on a client-server model and based on discovery, offer, request, and ACK.

DHCP is an under-the-covers mechanism that automates the assignment of IP addresses to fixed and mobile hosts that are connected wired or wirelessly.

When a device wants access to a network that’s using DHCP, it sends a request for an IP address that is picked up by a DHCP server. The server responds be delivering an IP address to the device, then monitors the use of the address and takes it back after a specified time or when the device shuts down. The IP address is then returned to the pool of addresses managed by the DHCP server to be reassigned to another device as it seeks access to the network.

While the delegation of IP addresses is the central function of the protocol, DHCP also assigns a variety of related networking parameters including subnet mask, default gateway address, and domain name server (DNS). DHCP is an IEEE standard built on top of the older BOOTP (bootstrap protocol), which has become obsolete because it only works on IPv4 networks.

**How DHCP works**

DHCP runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP clients. Information includes subnet mask information, default gateway, IP addresses and domain name system addresses.

DHCP is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.

**Components of DHCP**

When working with DHCP, it is important to understand all of the components. Following are the list of components:

* **DHCP Server:** DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
* **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.
* **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
* **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
* **Lease:** Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.
* **DHCP relay:** A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

**Benefits of DHCP**

There are following benefits of DHCP:

**Centralized administration of IP configuration:** DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.

**Dynamic host configuration:** DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.

**Seamless IP host configuration:** The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.

**Flexibility and scalability:** Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.

**Disadvantages of DHCP**

* Tracing internet activity may be difficult as the same machine may have two or more different IP addresses over a period of time.
* Not having a static IP means computers with DHCP cannot be used as servers as their IP will change.

**What is DNS?**

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

**How does DNS work?**

The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a particular home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine-friendly address necessary to locate the example.com webpage.

In order to understand the process behind the DNS resolution, it’s important to learn about the different hardware components a DNS query must pass between. For the web browser, the DNS lookup occurs "behind the scenes" and requires no interaction from the user’s computer apart from the initial request.

**Best DNS Servers**

Here are some of the top DNS servers available:

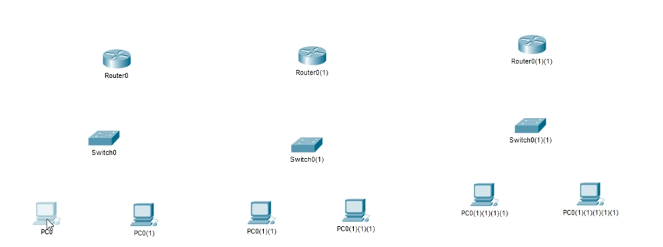
1.         **Cloudflare 1.1.1.1.**This is a simple-to-use DNS service that comes with tutorials for all of the most popular operating systems, such as Mac, Windows, Android, iOS, and Linux. Users can also use Cloudflare’s service to block adult content.

2.         **Google Public DNS.** The Google Public DNS service is different from Cloudflare’s in that it is designed for more technically adept users. But you can find tutorials if needed.

3.         **Quad9.** Quad9’s DNS service is renowned for its fast performance. It also claims to block malicious sites using threat intelligence data.

How to implement **DHCP with DNS (BASIC)**

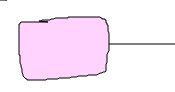
**Step-1:** Open a project in Cisco Packet Tracer.Take a router, switch & PC from the drop down menu. The amount of these equipment’s depends on the architecture of the project.



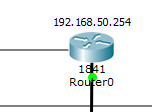
**Step-2:** Rename the equipment’s to avoid confusion.



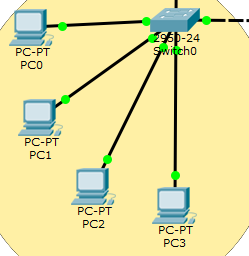
**Step-3:** Draw an ISP area.



**Step-4:** Place the router besides it.



**Step-5:** Assign switch and PC for each department and connect them using straight-though cable (for switch to switch use cross-over cable). Define each department with various color. I’m using 4 pc for IT department, 2 pc for HR department and 3 pc for accounts department. I have 3 switches for those 3 departments.



**Step-6:** Interface between switch and router still not up. Go to switch, then CLI and write down those codes:

*enable*

*configure terminal*

*interface fastEthernet 0/0*

*ip address 192.168.50.254 255.255.255.0*

*no shutdown*

*exit*

Assign DHCP commands:

*ip dhcp pool d*

*network 192.168.50.0 255.255.255.0*

*default-router 192.168.50.254*

*dns-server 8.8.8.8*

*exit*

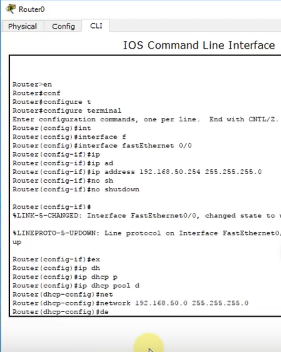
Apply excluded addresses:

*ip dhcp excluded-address 192.168.50.3 192.168.50.20*

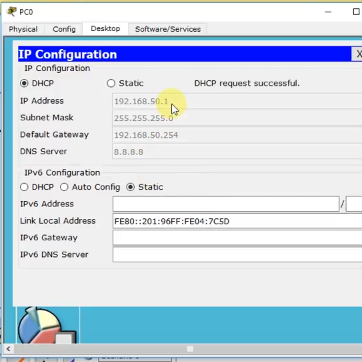
*exit*

Write the configuration:

*wr*



**Step-7:** Go to any pc, then desktop, select DHCP for IP Configuration, It will show DHCP request successful.

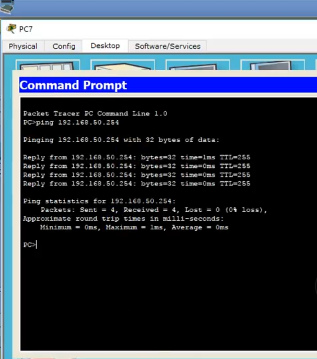


**Step-8:** Go to any pc, and ping. It should succeed with 0% loss.

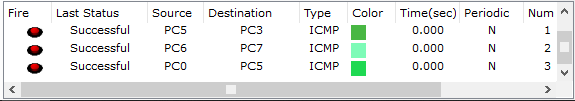
*ping 192.168.50.254*

*or,*

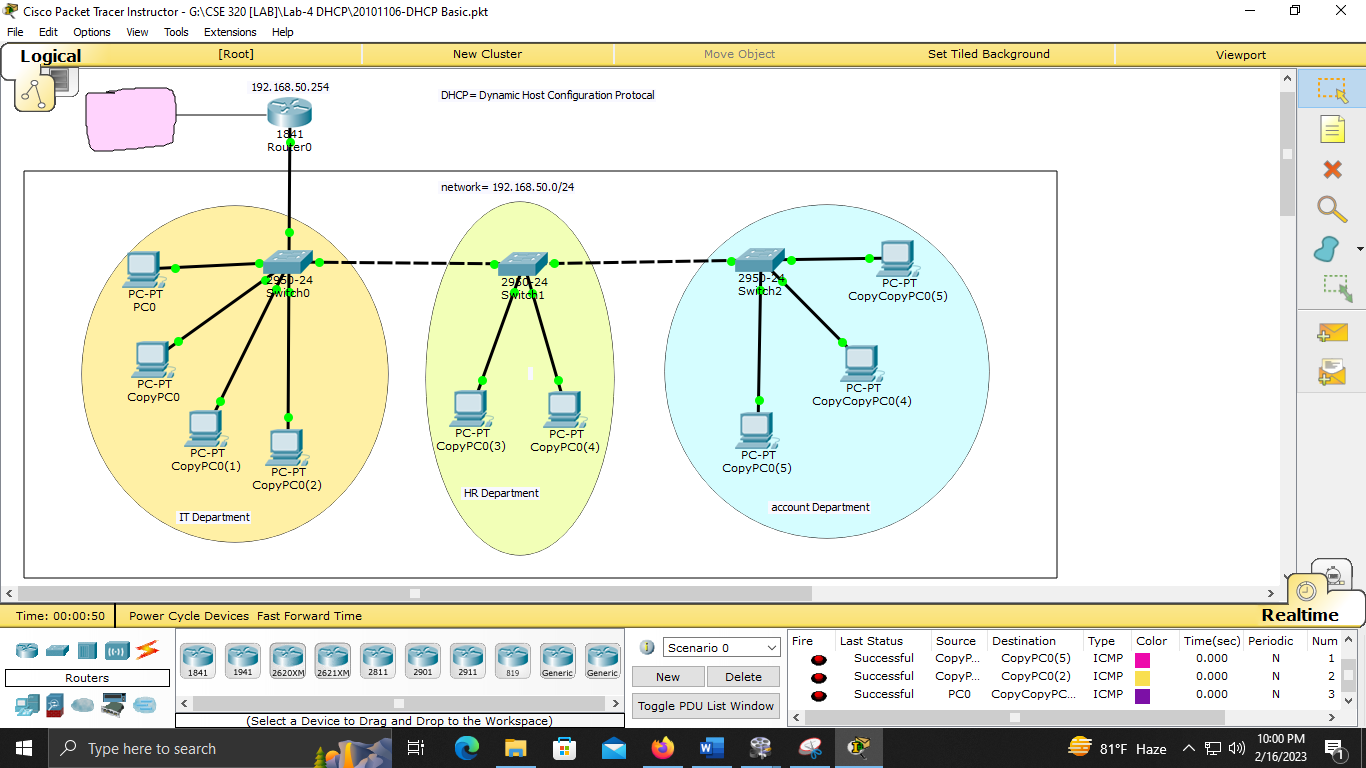
*ping 192.168.50.1*



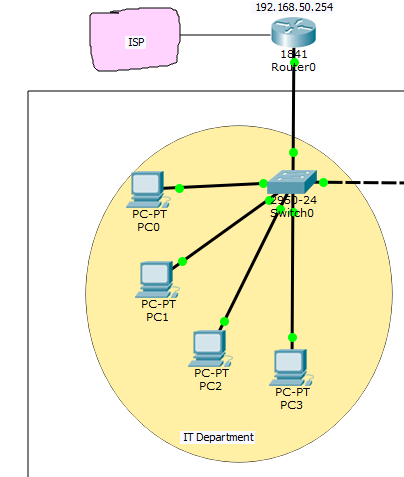
**Step-9:** Try to send packets using different pc’s. It should succeed.

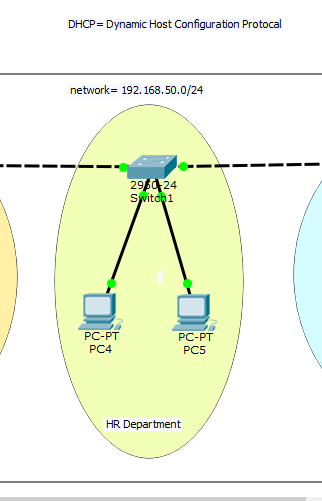


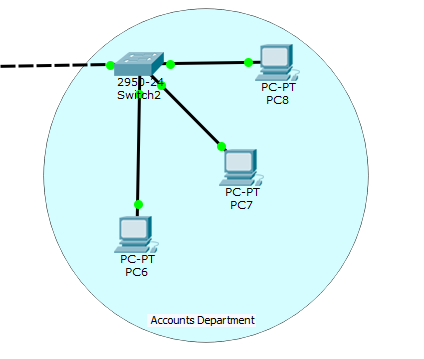
**Overall screenshot of the whole architecture-**



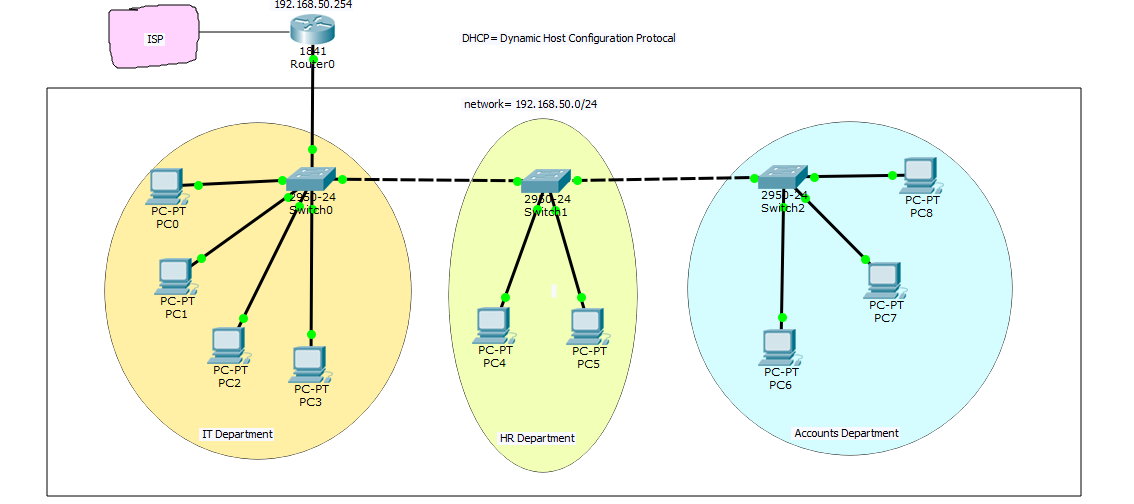
Part by part view-





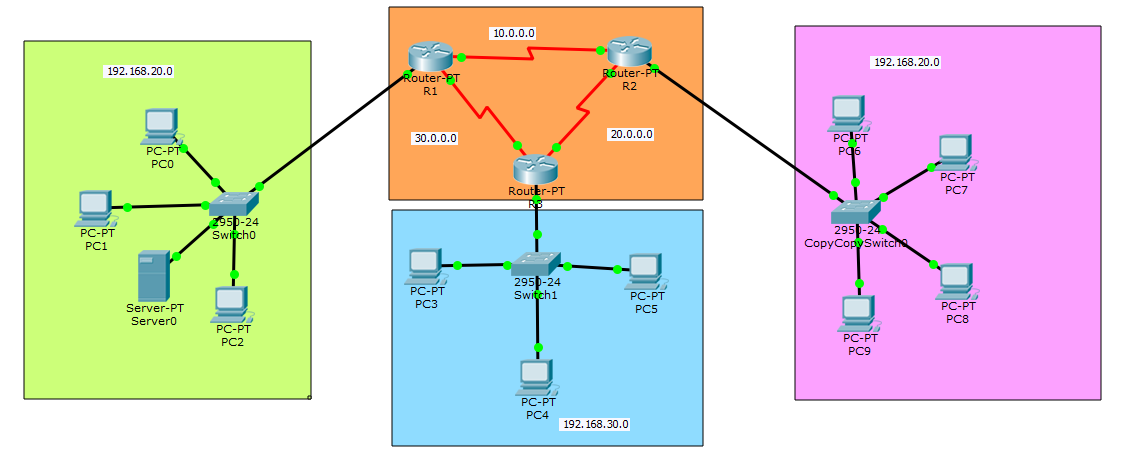


Detailed view-



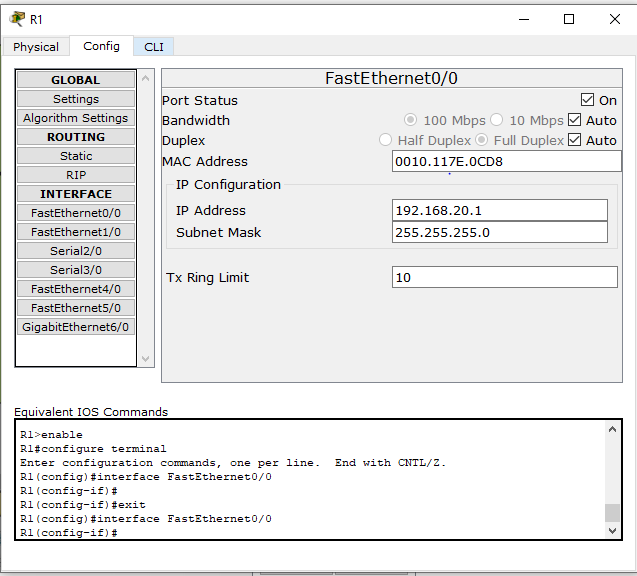
How to implement **DHCP with DNS (ADVANCED)**

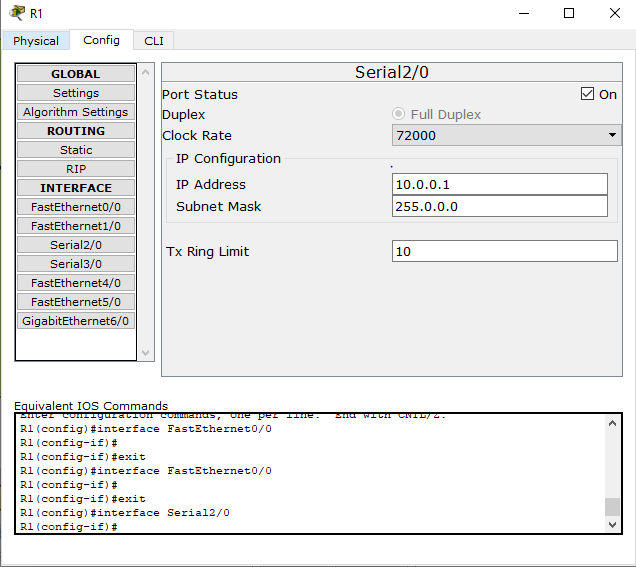
**Step-1:** Create networks with proper labeling of ports and networks.

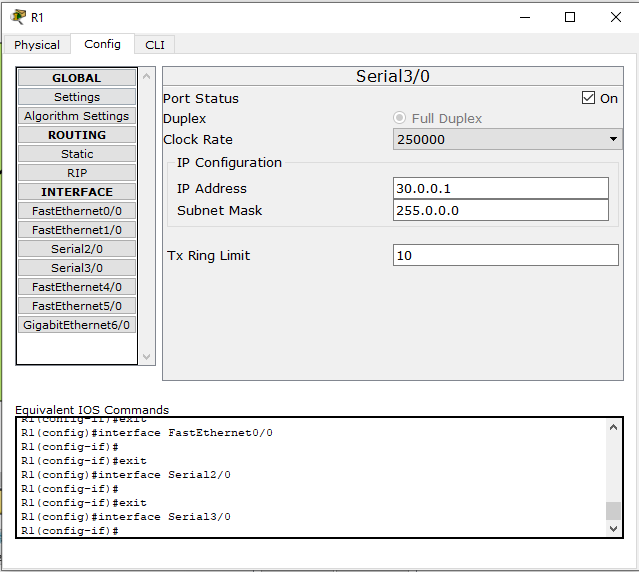


**Step-2:** Configure the ports of the routers.

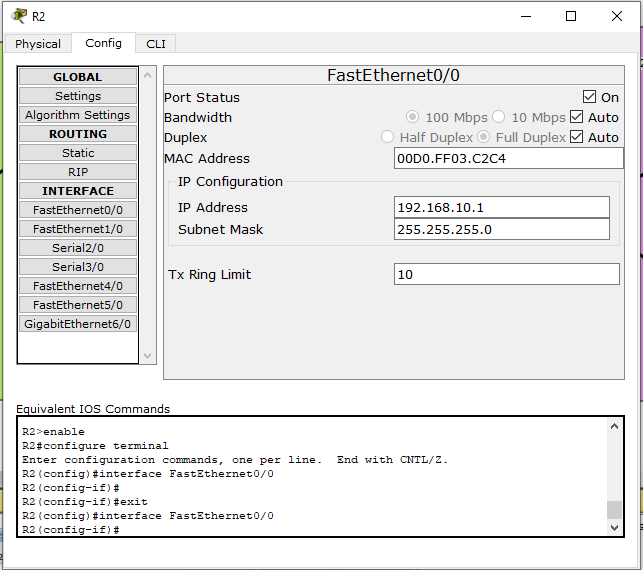
For 1st router and FastEthernet 0/0, Serial2/0 and serial3/0:

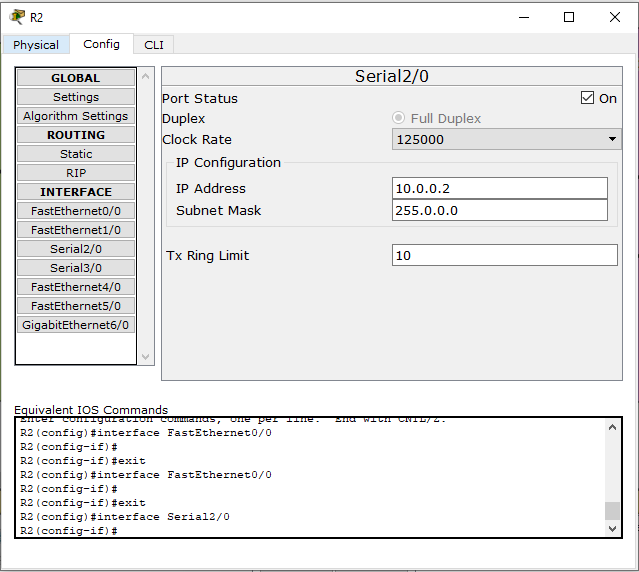


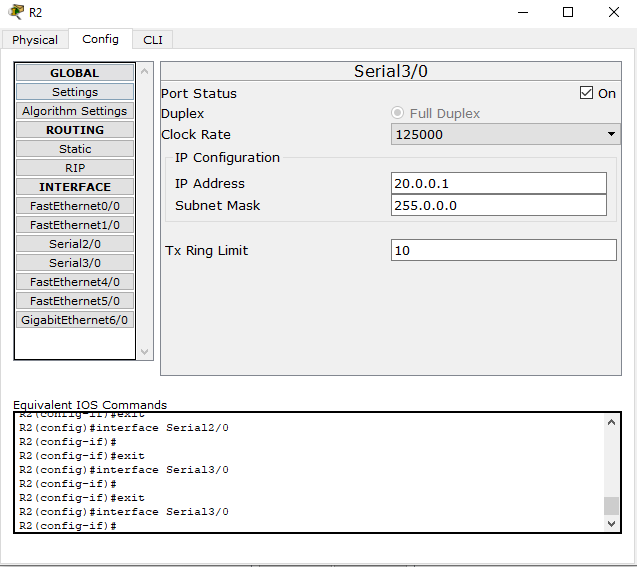




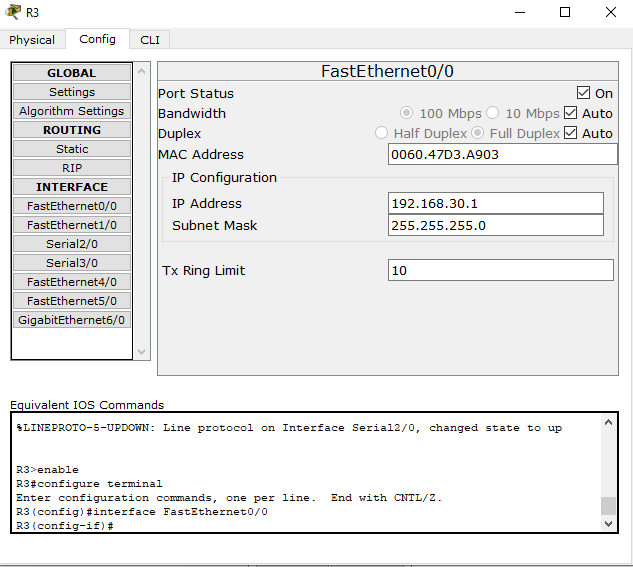
For 2nd router and FastEthernet 0/0, Serial2/0 and serial3/0:

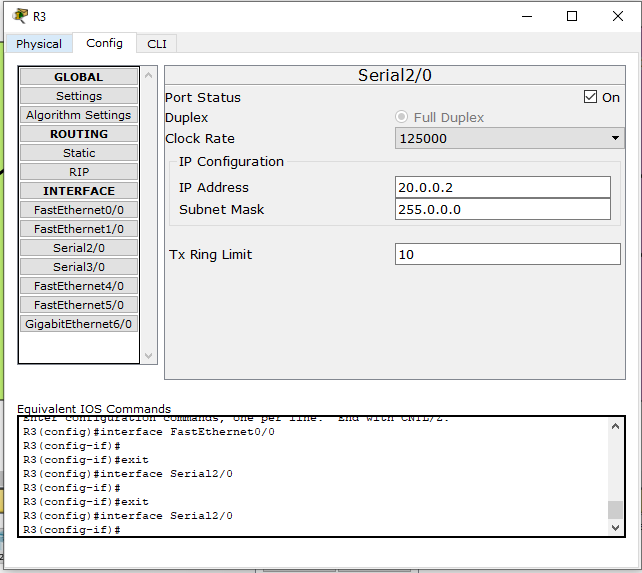


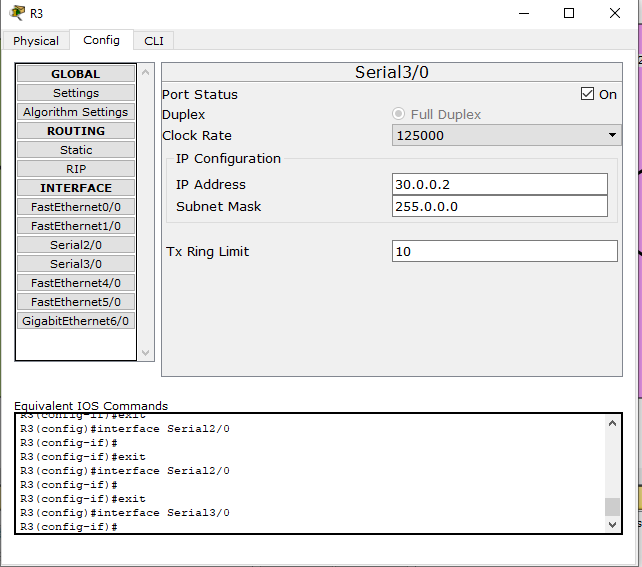




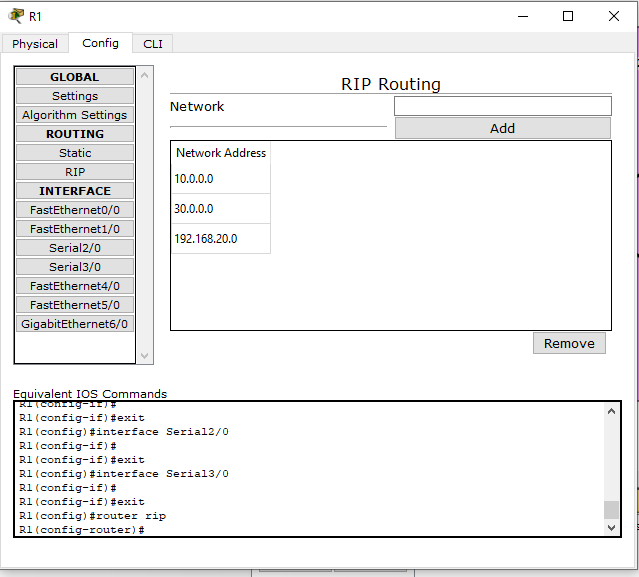
For 3rd router and FastEthernet 0/0, Serial2/0 and serial3/0:

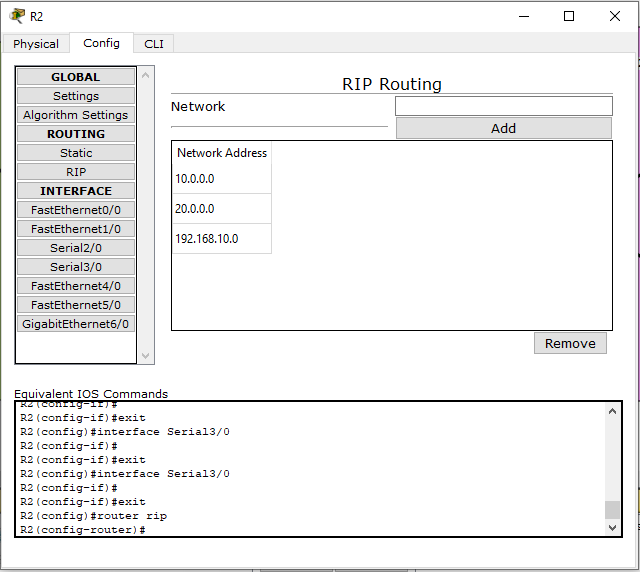


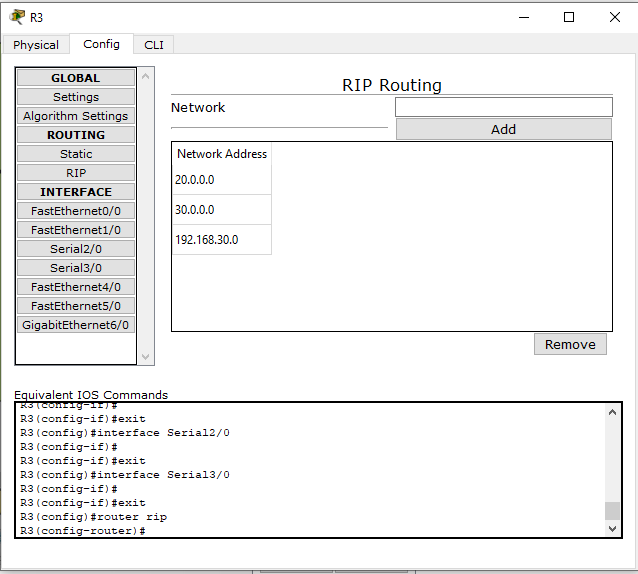




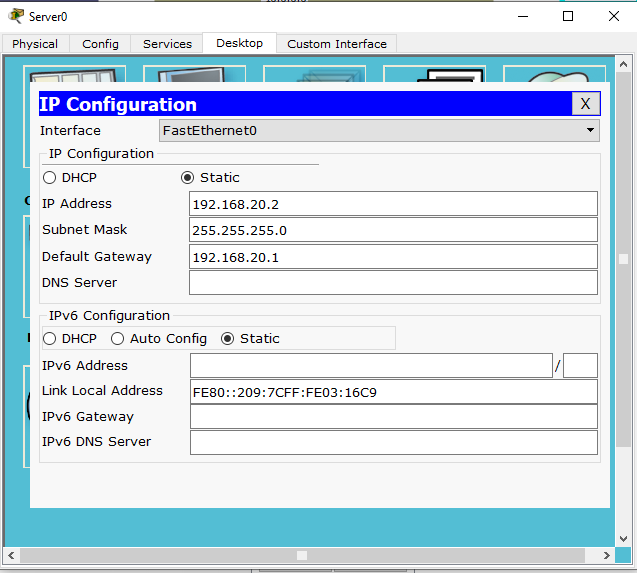
**Step-3:** Put routing information in the routers.

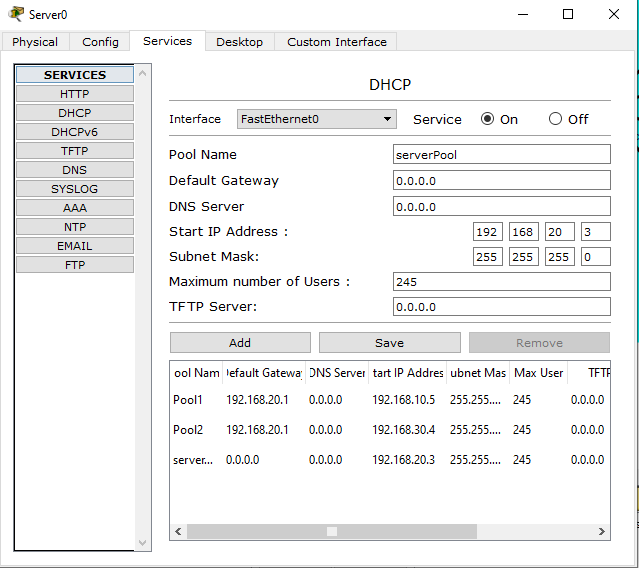






**Step-4:** Configure the DHCP server. Static ip addresses from the range of addresses where we are going to put the DHCP. Put address range of the networks.





**Step-5:** Configure the ports which are gateway of the networks. Go to command line interface (CLI)

*enable*

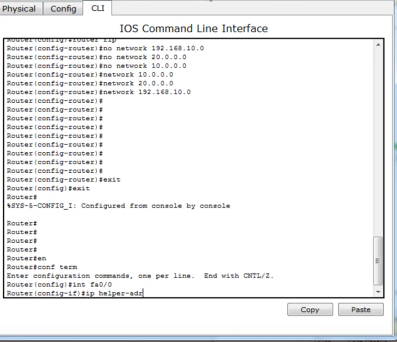
*configure terminal*

*int fa0/0*

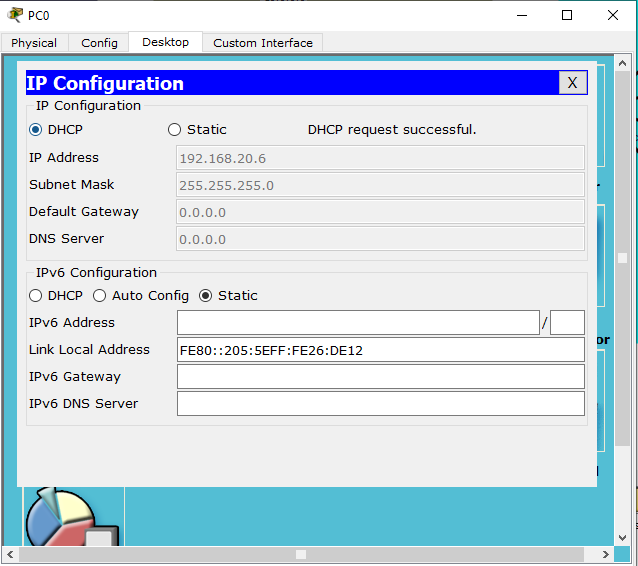
*ip helper-address 192.168.20.2*

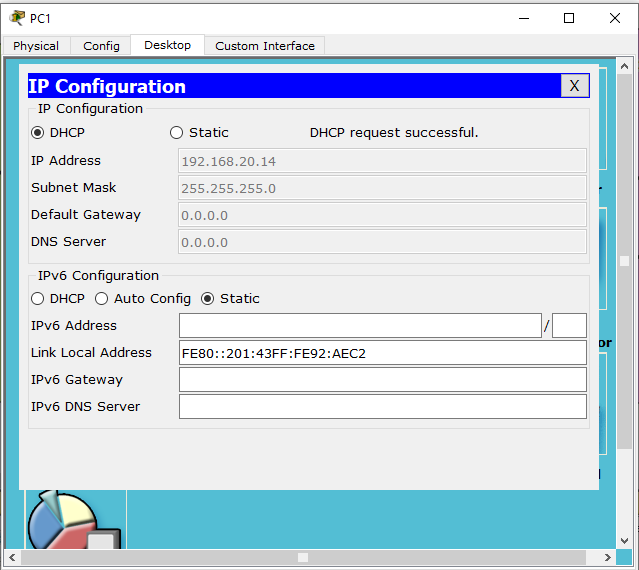
*exit*

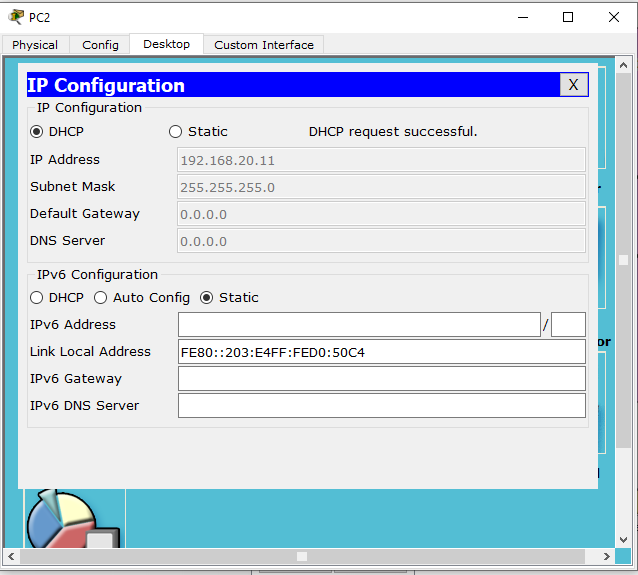
*exit*

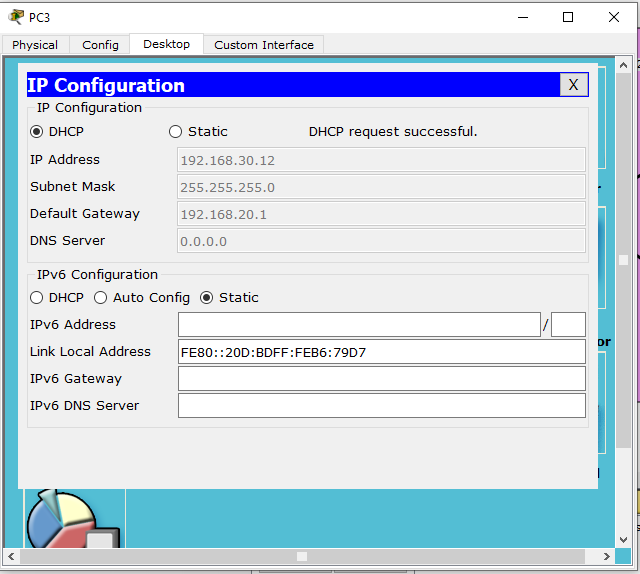


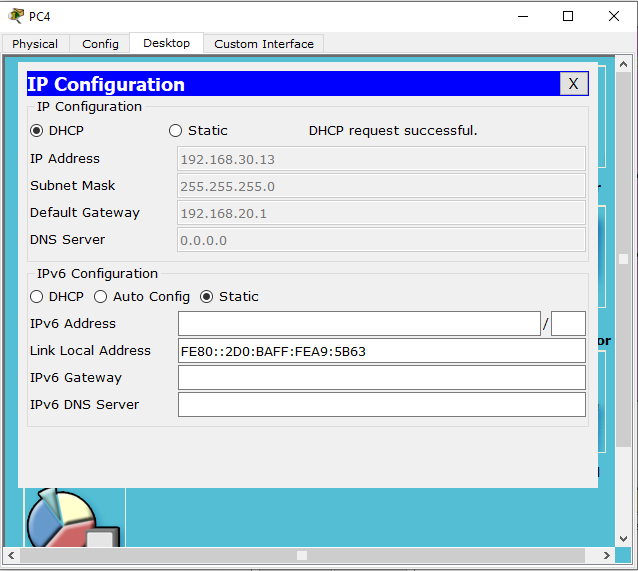
**Step-6:** Request for DHCP, It should succeed

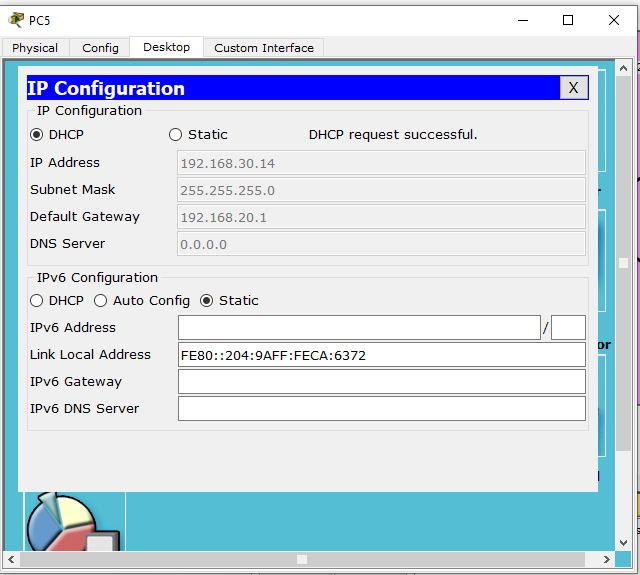


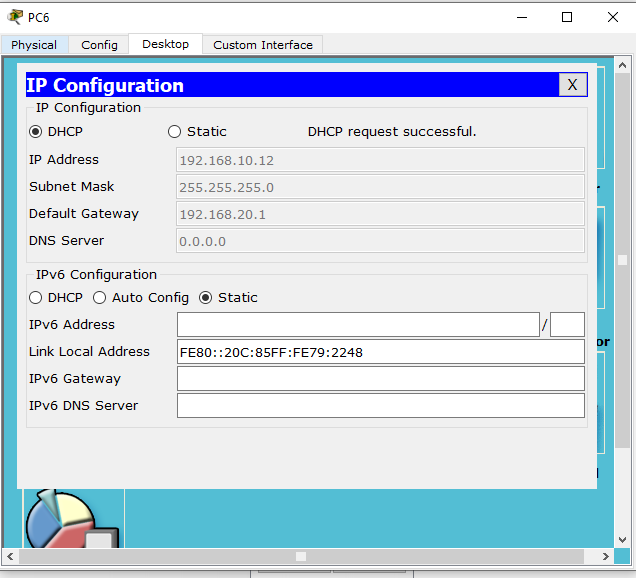


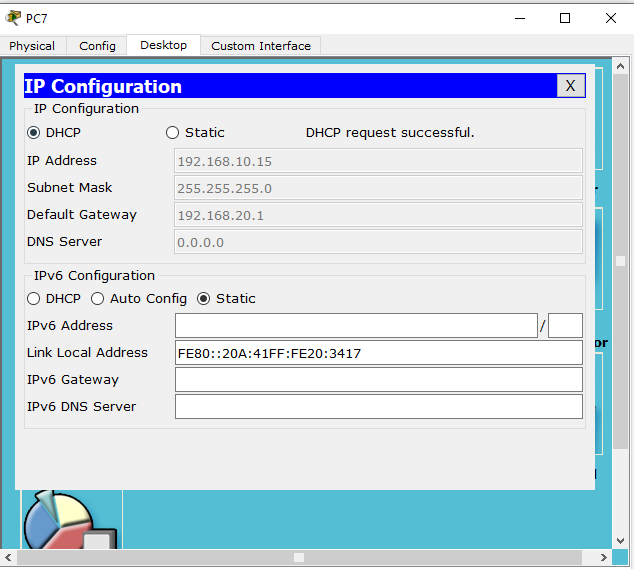


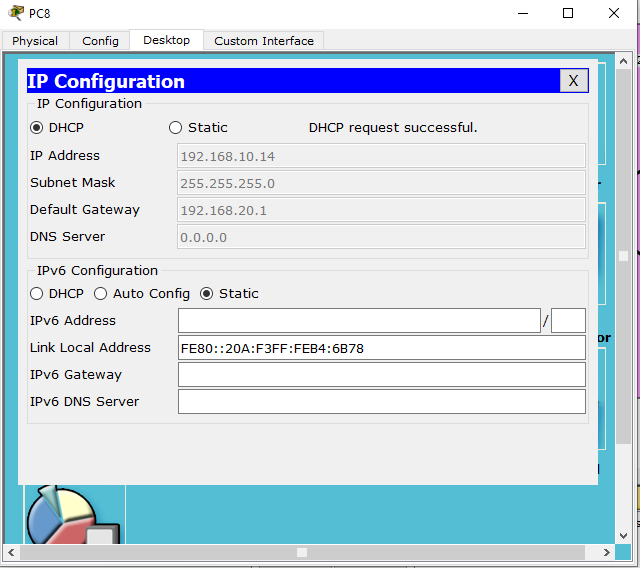


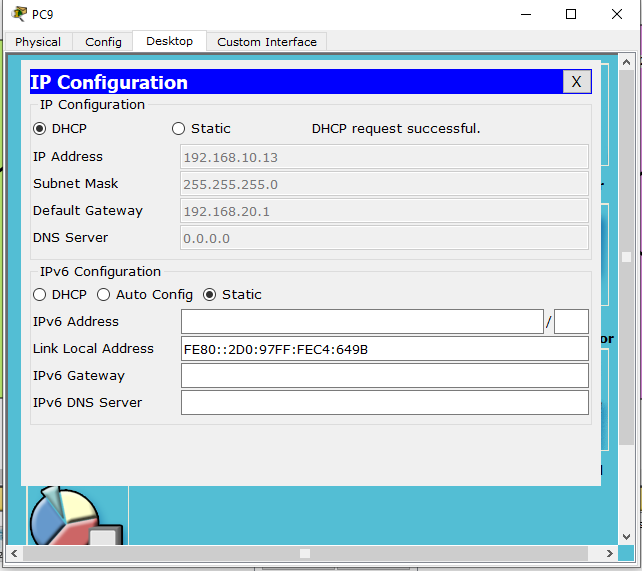




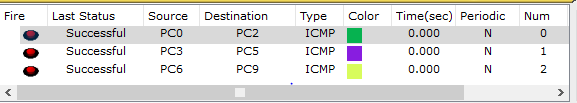




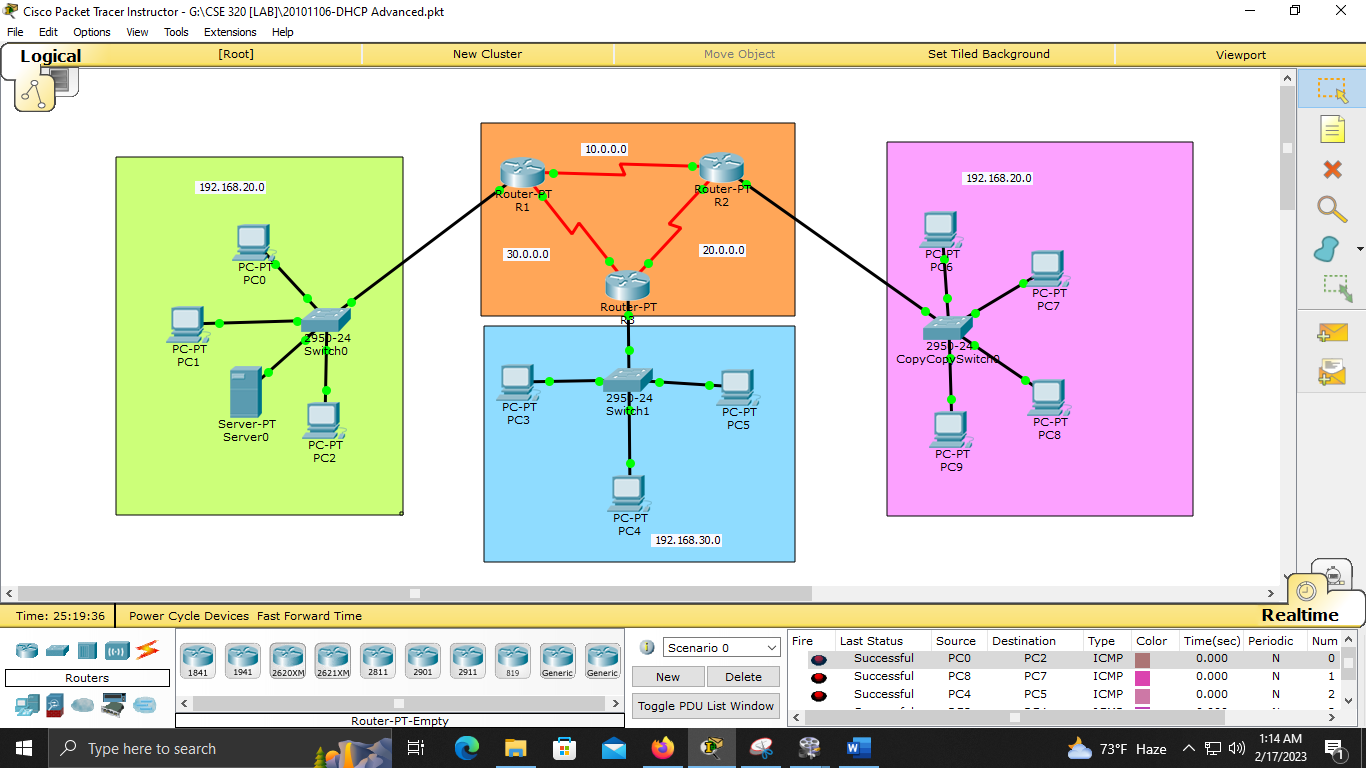




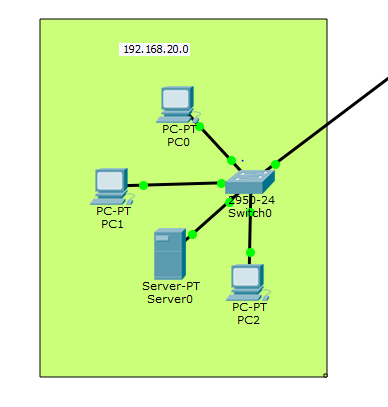
**Step-7:** Try to send packets using different pc’s. It should succeed.

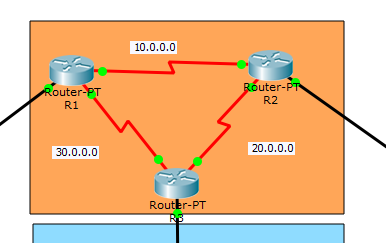


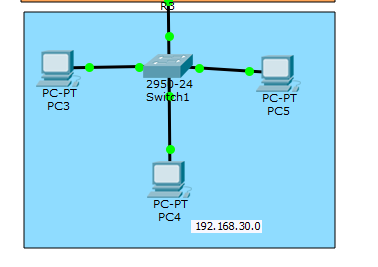
**Overall screenshot of the whole architecture-**

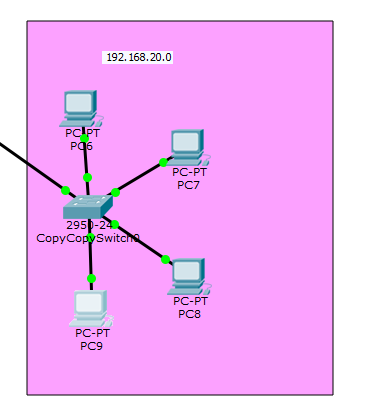


Part by part view-

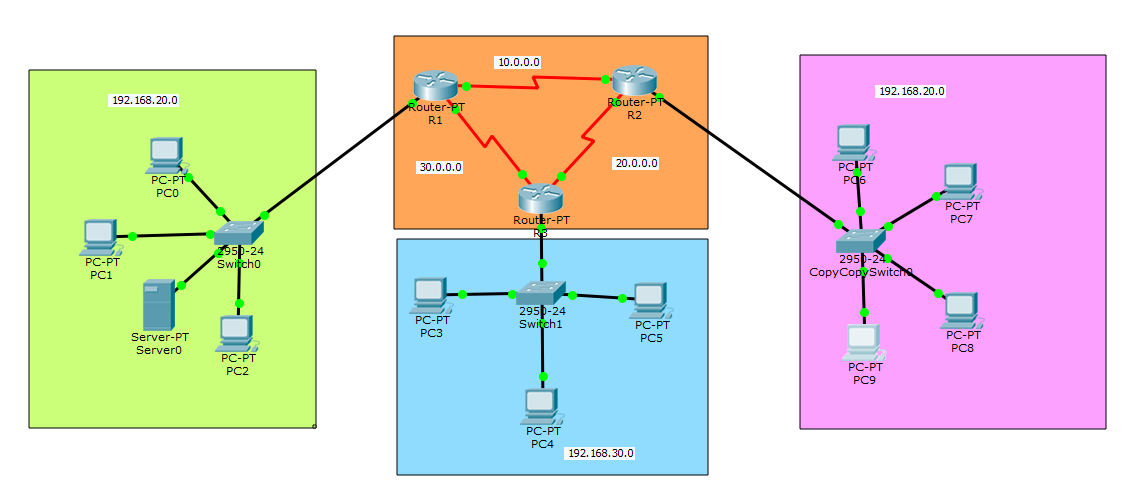








Detailed view-



---------------------------THANK YOU FOR READING--------------------------