**PRACTICAL NO. 4**

**AIM: To configure network with dynamic configuration.**

1. **DHCP**
2. **Access list configuration**
3. **Configure NAT for Static and Dynamic routing**
4. **Configuration of PAT**

**THEORY:**

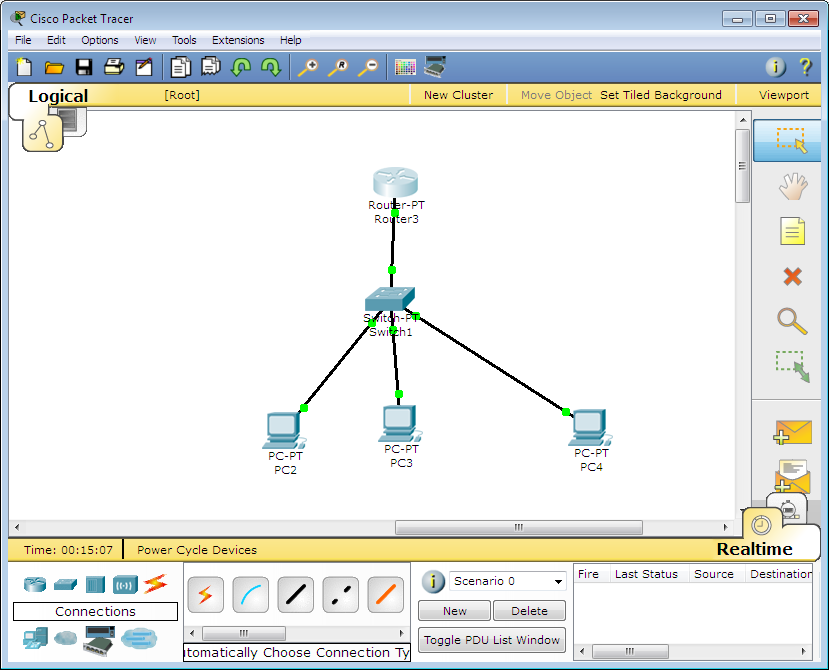
**Configuration of DHCP**

The Dynamic Host Configuration Protocol (DHCP) is a [network management protocol](https://en.wikipedia.org/wiki/Network_protocol) used on [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) networks whereby a DHCP server dynamically assigns an [IP address](https://en.wikipedia.org/wiki/IP_address) and other network configuration parameters to each device on a network so they can communicate with other IP networks.[[1]](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol#cite_note-TechTarget-1) A DHCP server enables computers to request IP addresses and networking parameters automatically from the [Internet service provider](https://en.wikipedia.org/wiki/Internet_service_provider) (ISP), reducing the need for a [network administrator](https://en.wikipedia.org/wiki/Network_administrator) or a user to manually assign IP addresses to all network devices.[[1]](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol#cite_note-TechTarget-1) In the absence of a DHCP server, a computer or other device on the network needs to be manually assigned an IP address, or to assign itself an [APIPA](https://en.wikipedia.org/wiki/APIPA) address, which will not enable it to communicate outside its local subnet.

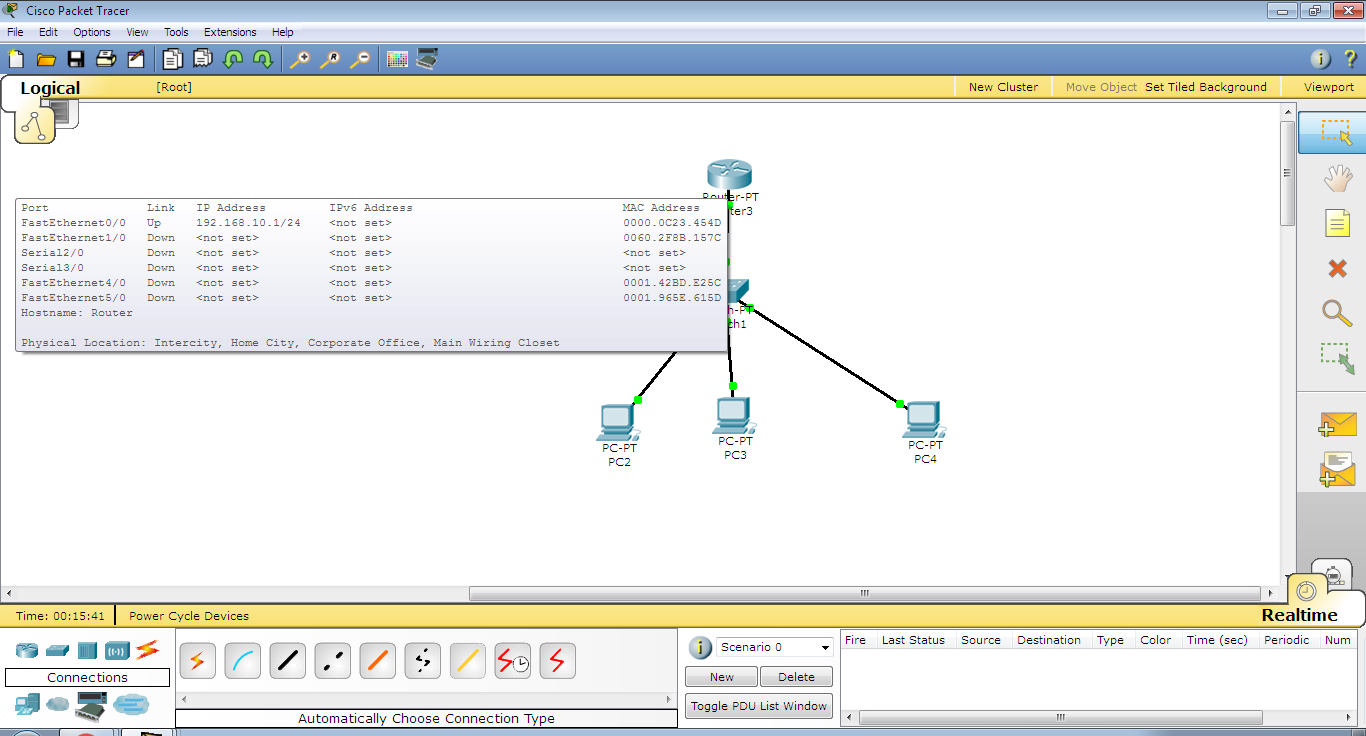
DHCP can be implemented on networks ranging in size from [home networks](https://en.wikipedia.org/wiki/Home_network) to large [campus networks](https://en.wikipedia.org/wiki/Campus_network) and regional [Internet service provider](https://en.wikipedia.org/wiki/Internet_service_provider) networks

Steps to configure DHCP

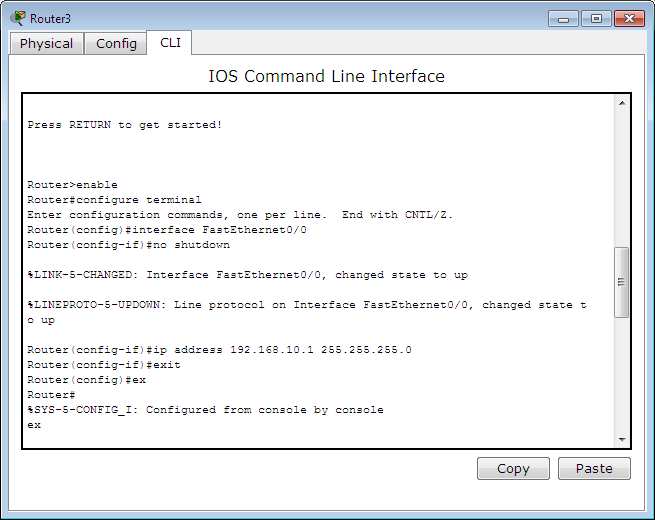
Step 1. Open Packet Tracer and design a network topology as shown in below screenshot.

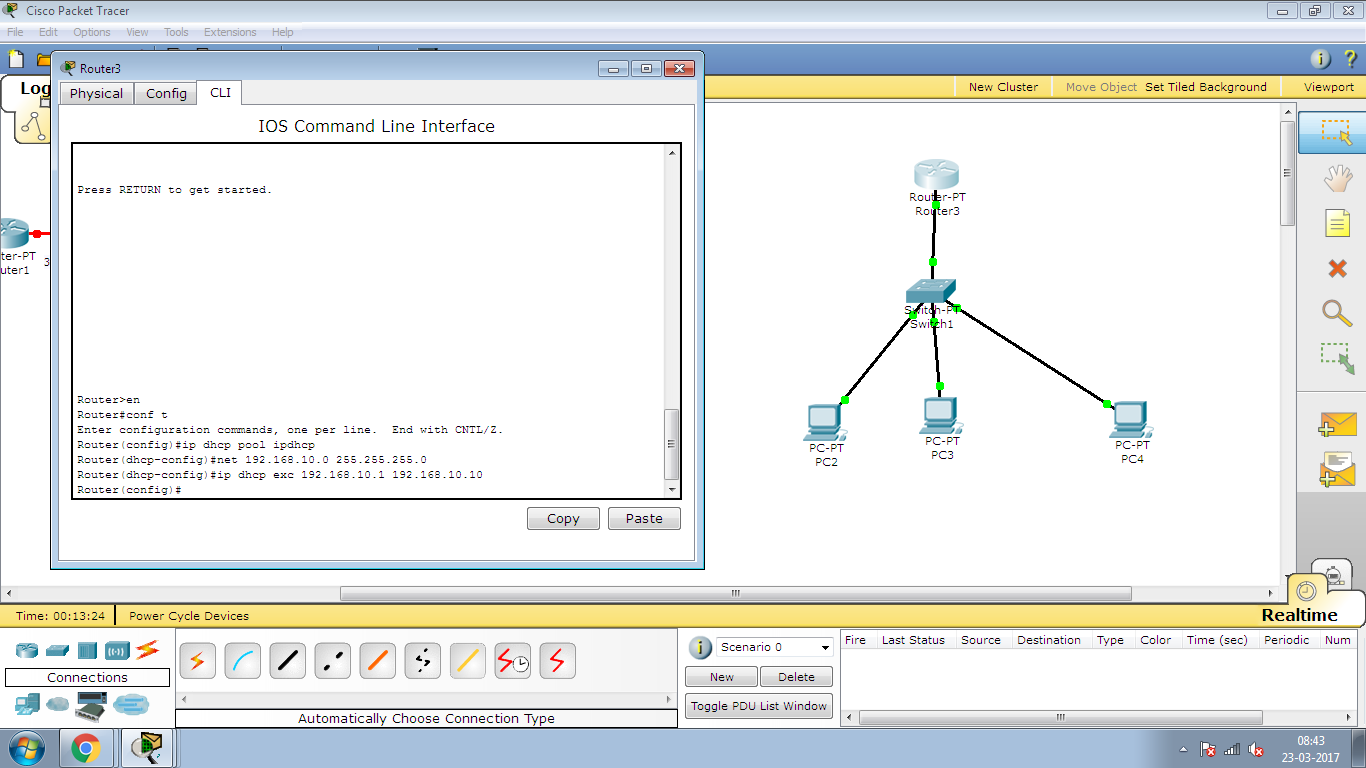


Step 2. Check if all the network topology are connected as shown in below screenshot.

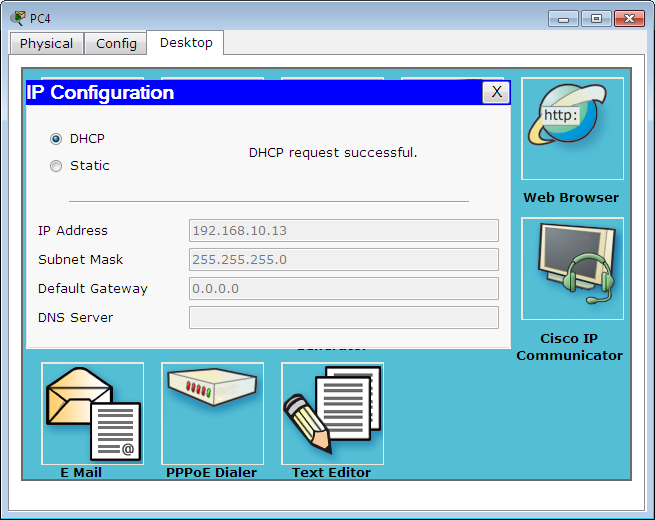


Step 3: Check if all the router are connected through command prompt.





Step 5: Configure dynamic ip configuration for PC4



1. **Access List Configuration**

Access-list (ACL) is a set of rules defined for controlling the network traffic and reducing network attack. ACLs are used to filter traffic based on the set of rules defined for the incoming or out going of the network.

ACL features –

1. The set of rules defined are matched serial wise i.e matching starts with the first line, then 2nd, then 3rd and so on.
2. The packets are matched only until it matches the rule. Once a rule is matched then no further comparison takes place and that rule will be performed.
3. There is an implicit deny at the end of every ACL, i.e., if no condition or rule matches then the packet will be discarded.

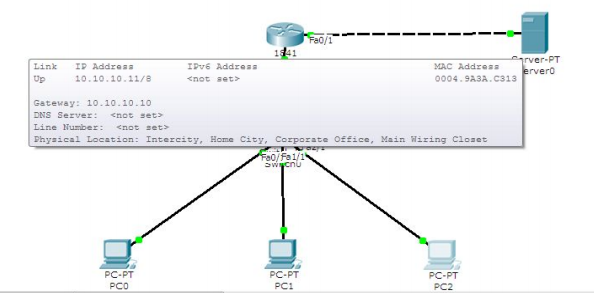
Once the access-list is built, then it should be applied to inbound or outbound of the interface:

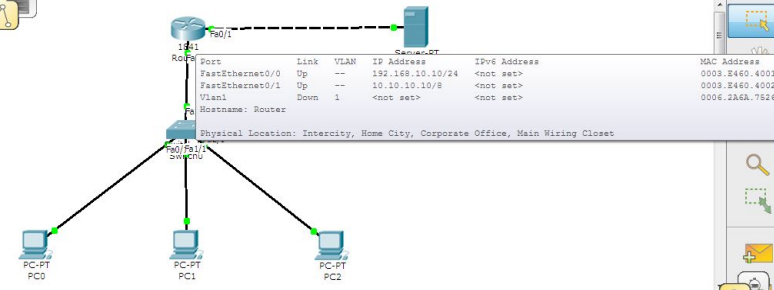
* **nbound access lists –** When an access list is applied on inbound packets of the interface then first the packets will processed according to the access list and then routed to the outbound interface.
* **Outbound access lists –** When an access list is applied on outbound packets of the interface then first the packet will be routed and then processed at the outbound interface.

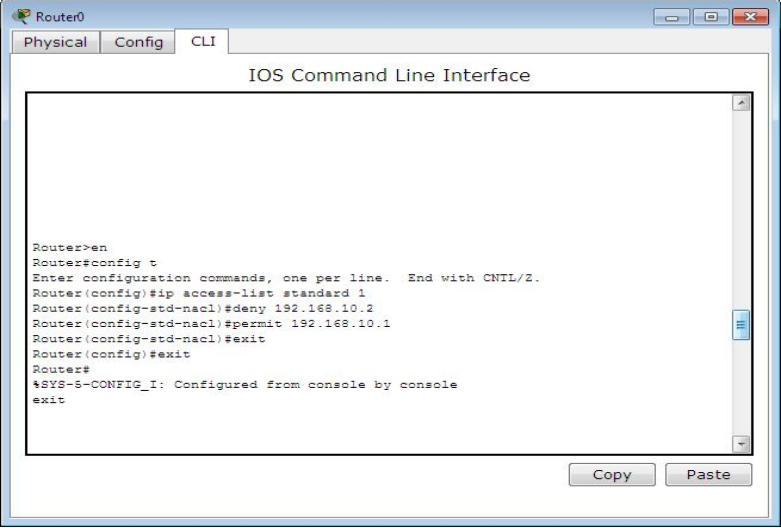
Types of ACL –  
There are two main different types of Access-list namely:

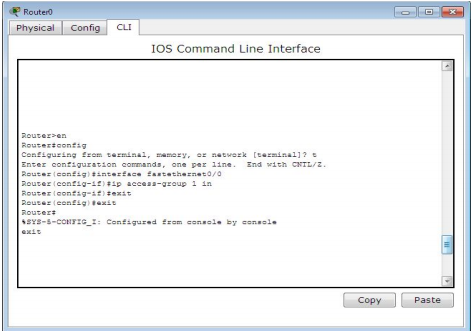
1. **Standard Access-list –** These are the Access-list which are made using the source IP address only. These ACLs permit or deny the entire protocol suite. They don’t distinguish between the IP traffic such as TCP, UDP, Https etc. By using numbers 1-99 or 1300-1999, router will understand it as a standard ACL and the specified address as source IP address.
2. **Extended Access-list –** These are the ACL which uses both source and destination IP address. In these type of ACL, we can also mention which IP traffic should be allowed or denied. These use range 100-199 and 2000-2699.

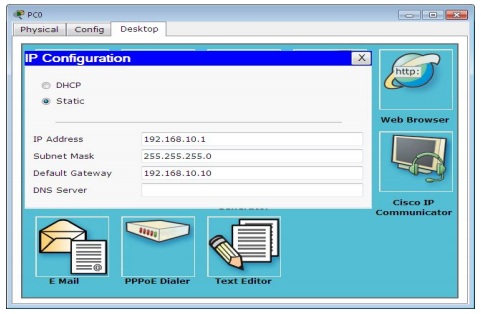
**Configuration of Access List**

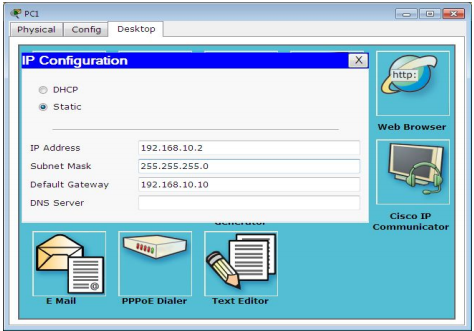


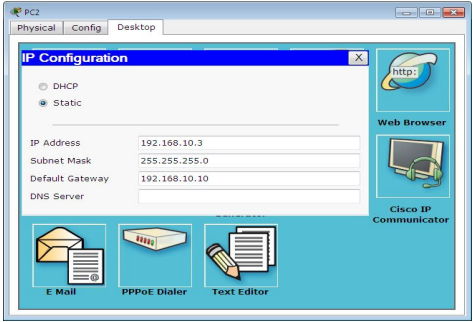


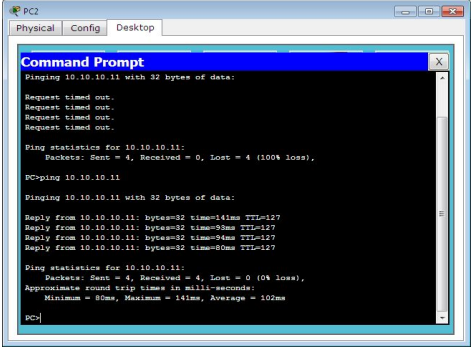












1. **NAT For Static and Dynamic :**

To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of private IP address to a public IP address is required. **Network Address Translation (NAT)** is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on router or firewall.

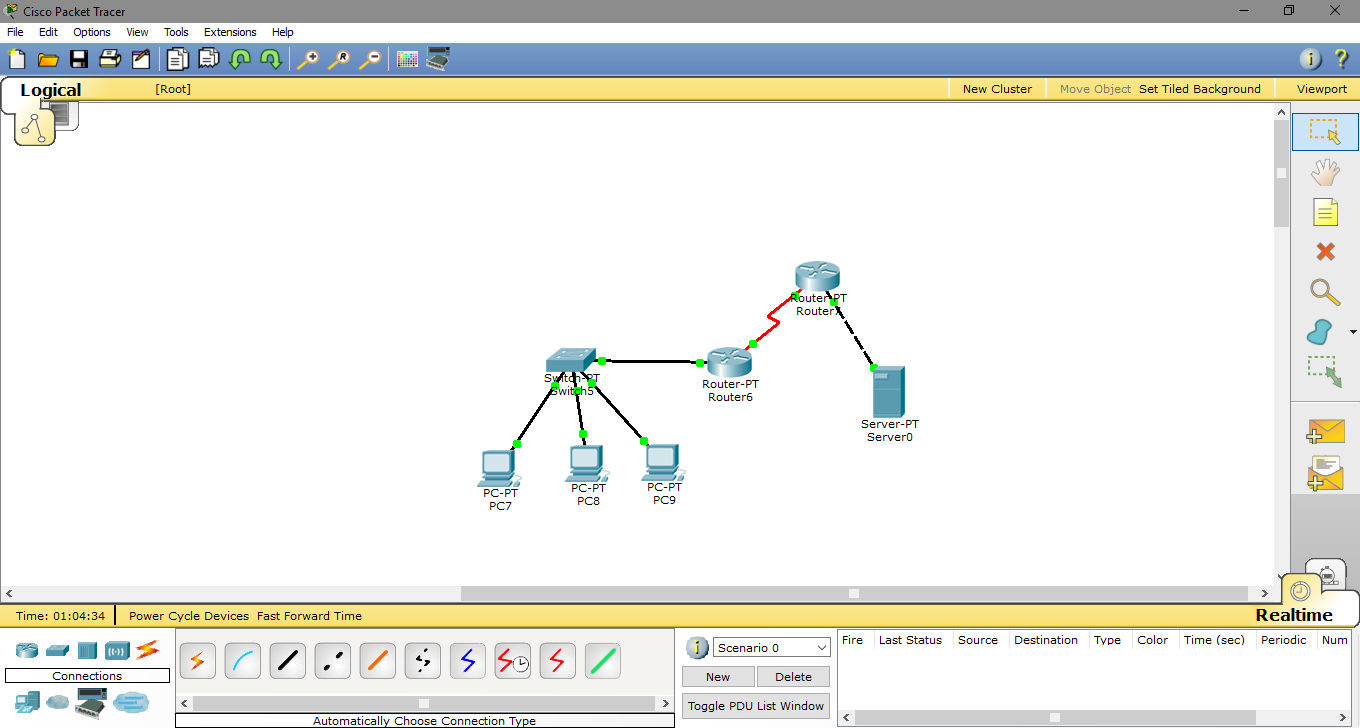
**NAT inside and outside addresses –**  
Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organisation. These are the network Addresses in which the translation of the addresses will be done.

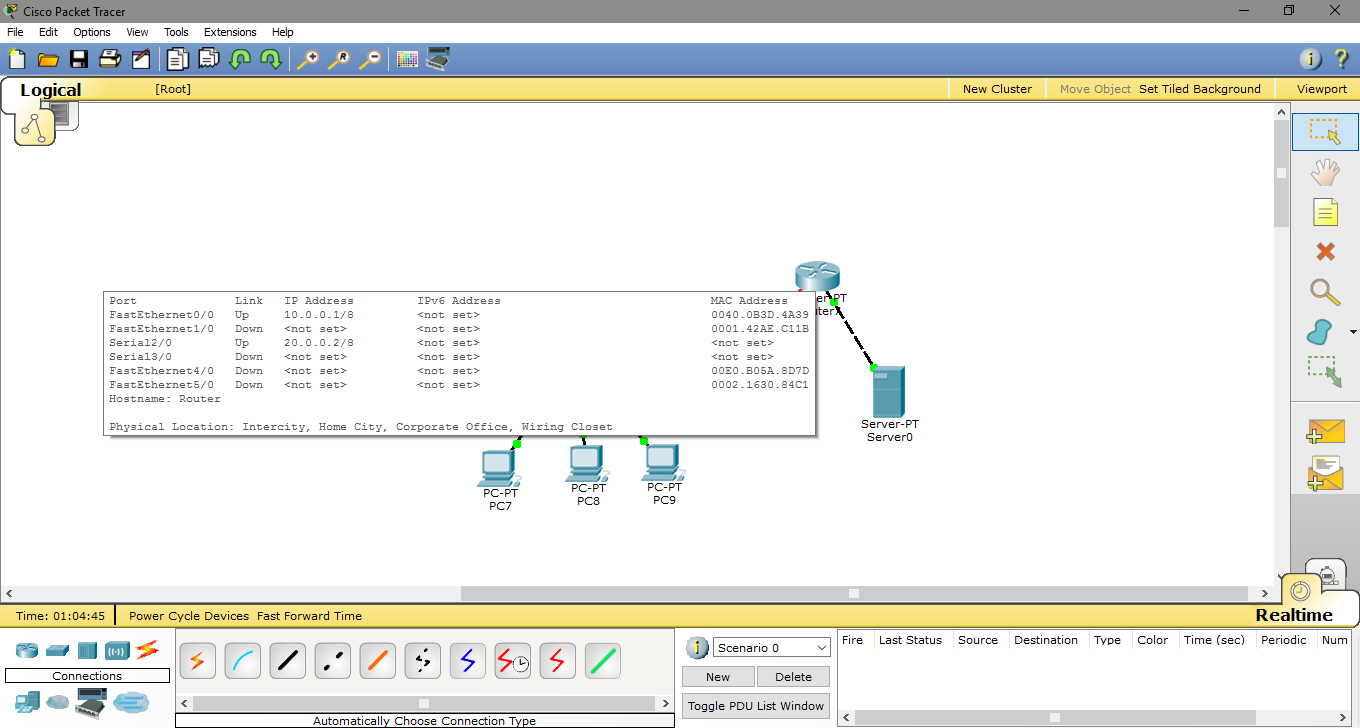
* **Inside local address –** An IP address that is assigned to a host on the Inside (local) network. The address is probably not a IP address assigned by the service provider i.e., these are private IP address. This is the inside host seen from the inside network.
* **Inside global address –** IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.
* **Outside local address –** This is the actual IP address of the destination host in the local network after translation.
* **Outside global address –** This is the outside host as seen form the outside network. It is the IP address of the outside destination host before translation.

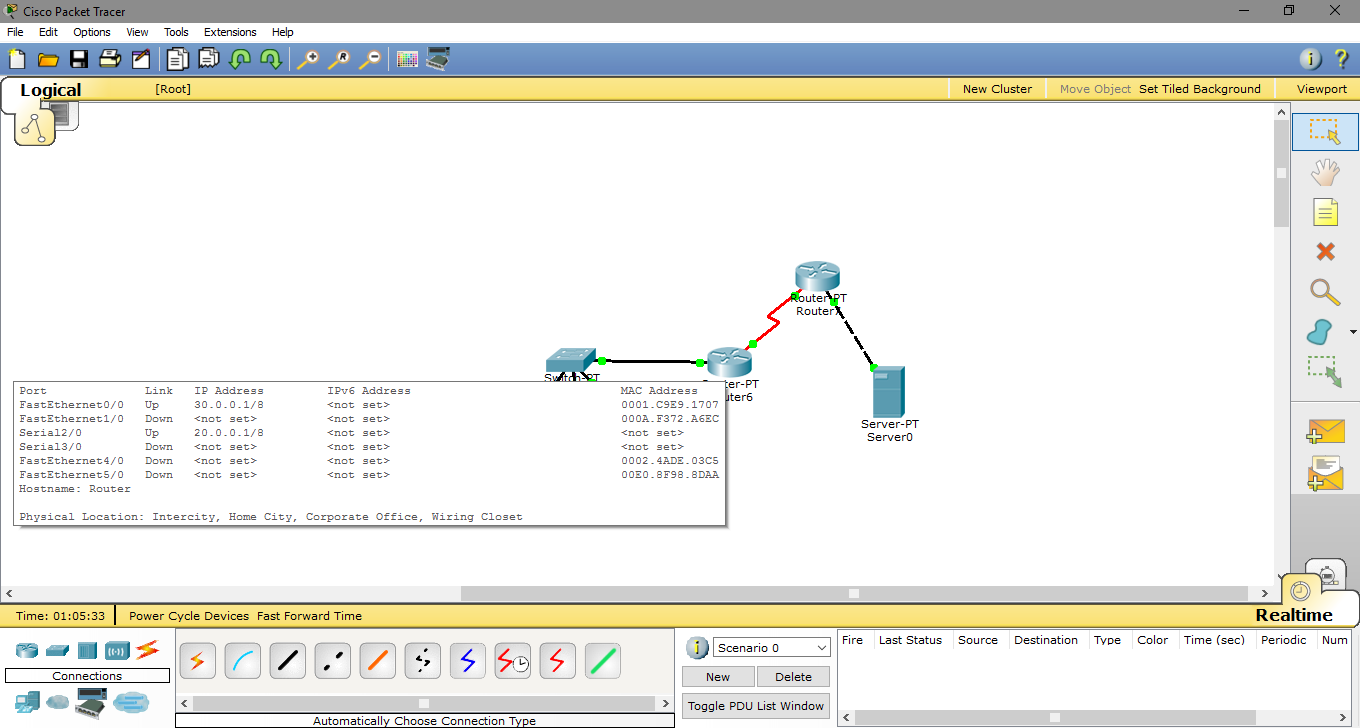
**Network Address Translation (NAT) Types –**  
There are 3 ways to configure NAT:

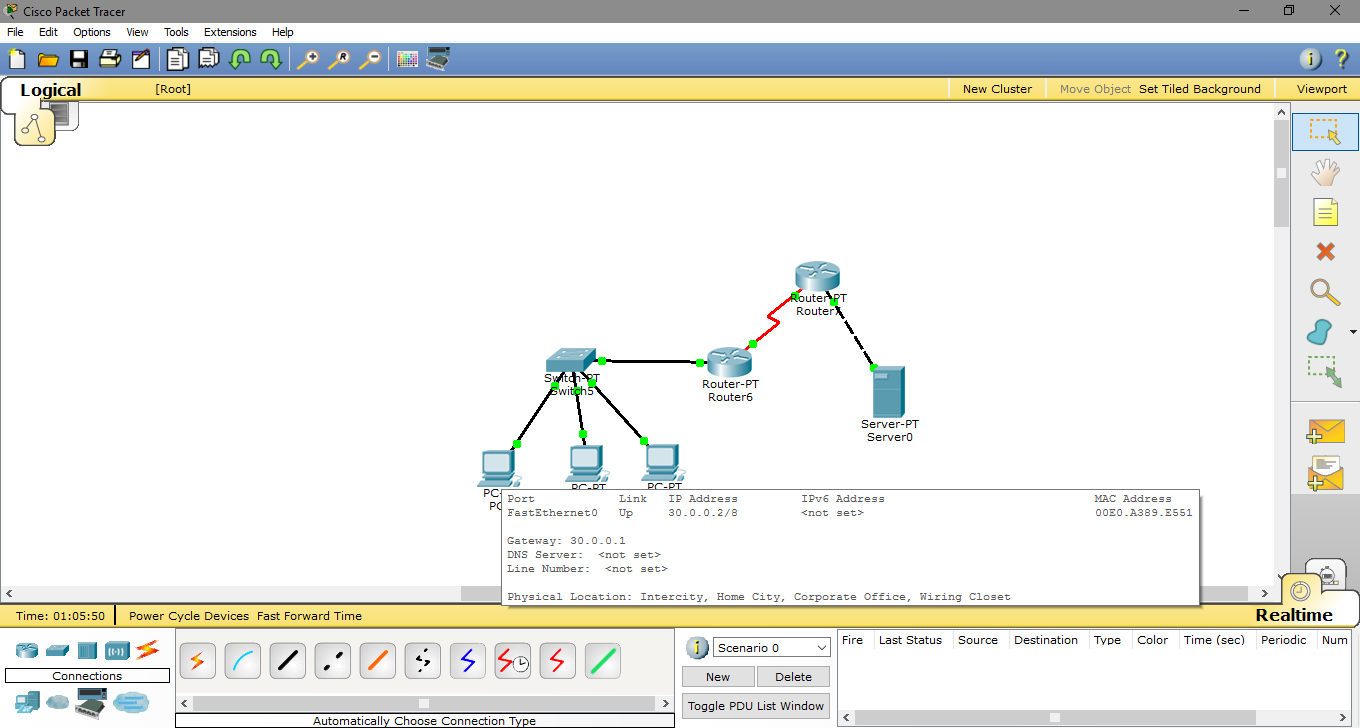
1. **Static NAT –** In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global address. This is generally used for Web hosting. These are not used in organisations as there are many devices who will need Internet access and to provide Internet access, the public IP address is needed.  
     
   Suppose, if there are 3000 devices who need access to the Internet, the organisation have to buy 3000 public addresses that will be very costly.
2. **Dynamic NAT –** In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP address. If the IP address of pool is not free, then the packet will be dropped as an only a fixed number of private IP address can be translated to public addresses.

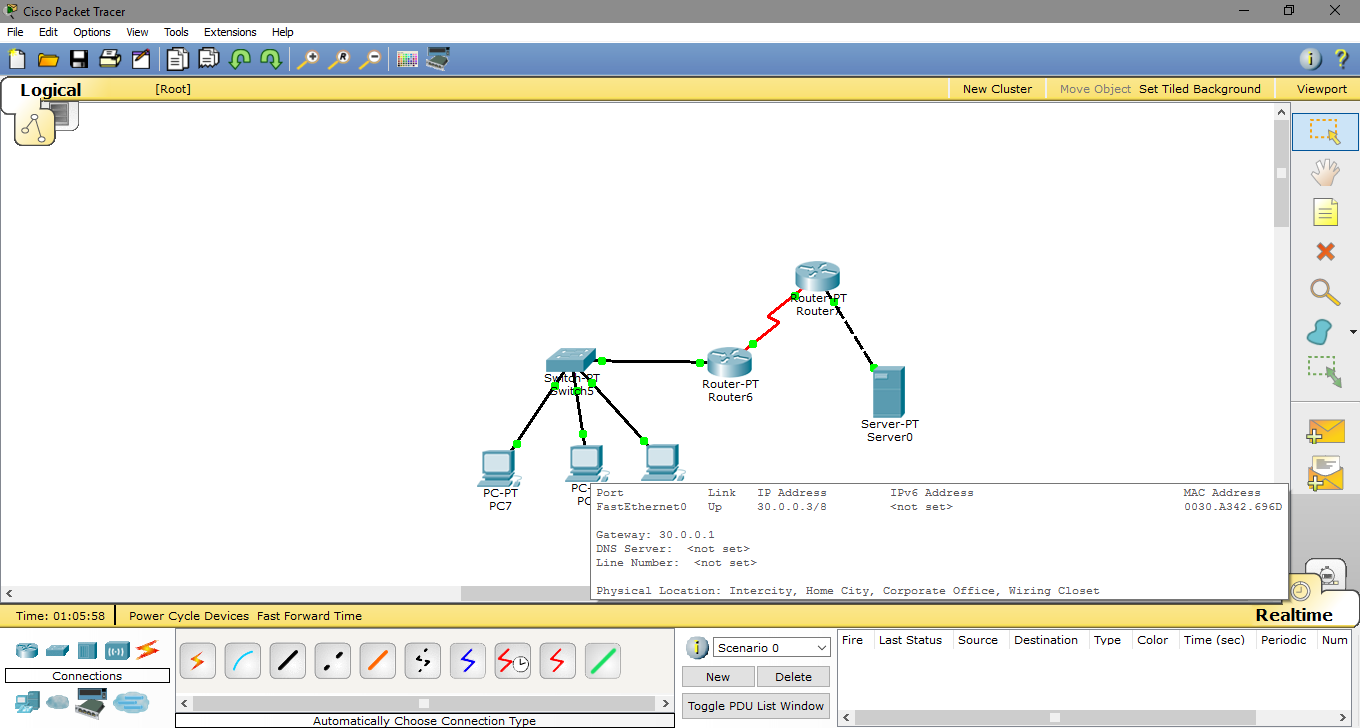
Configuration Of Static NAT

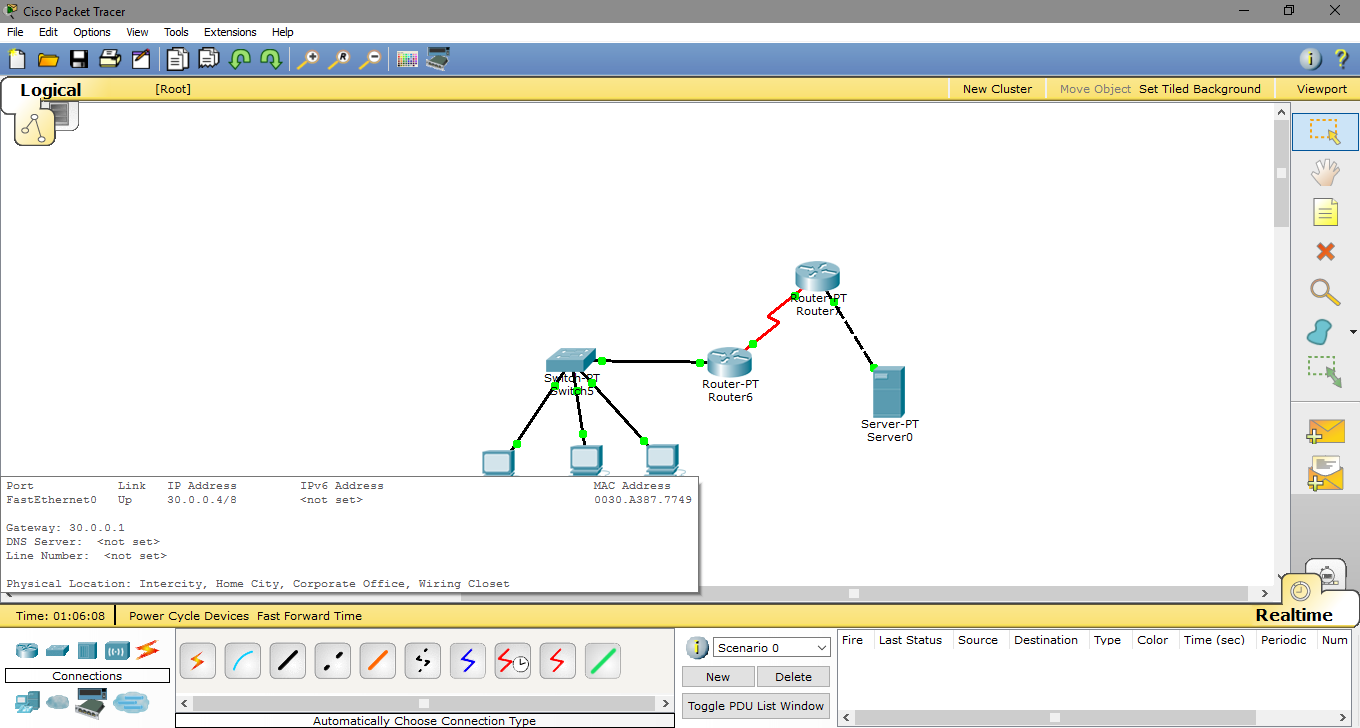


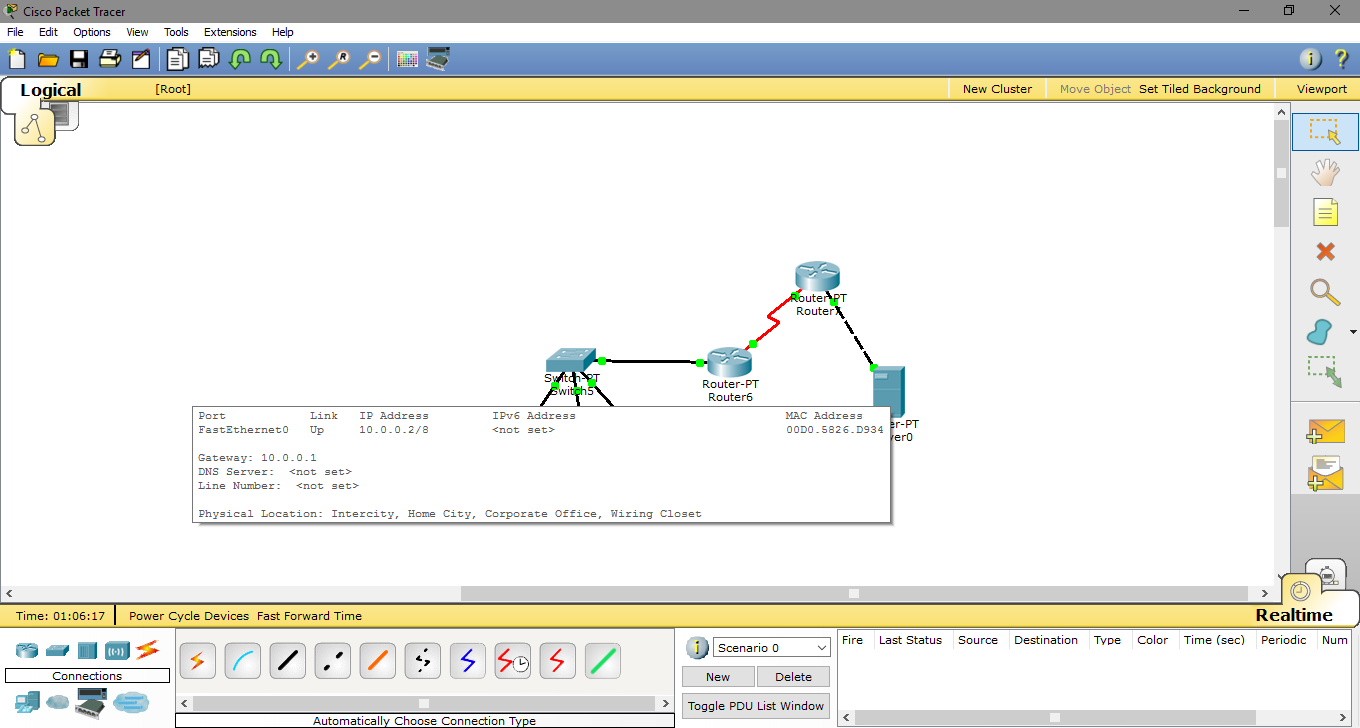


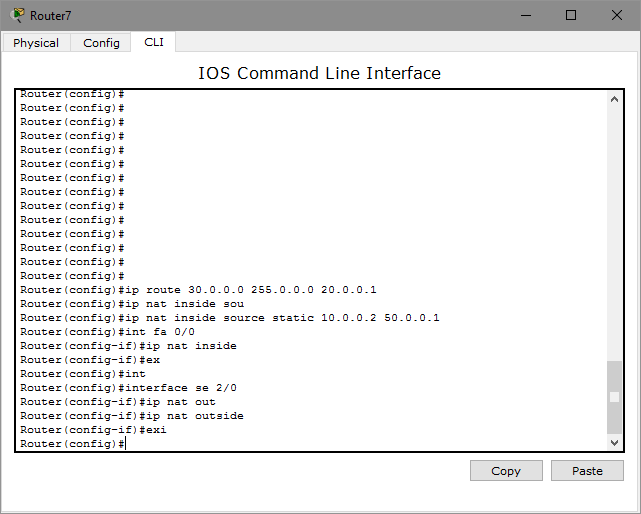


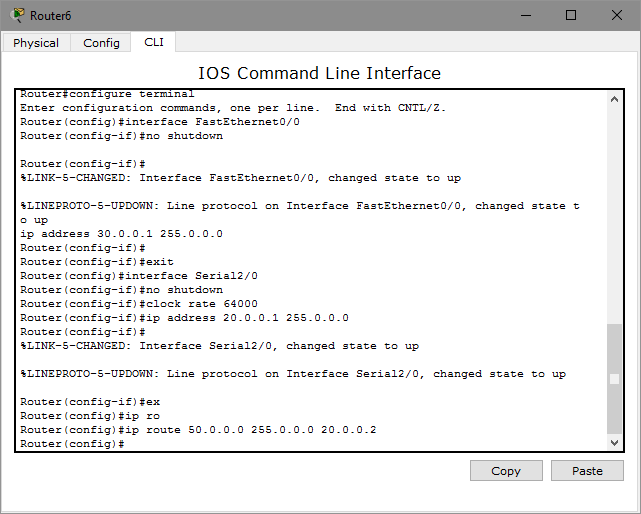




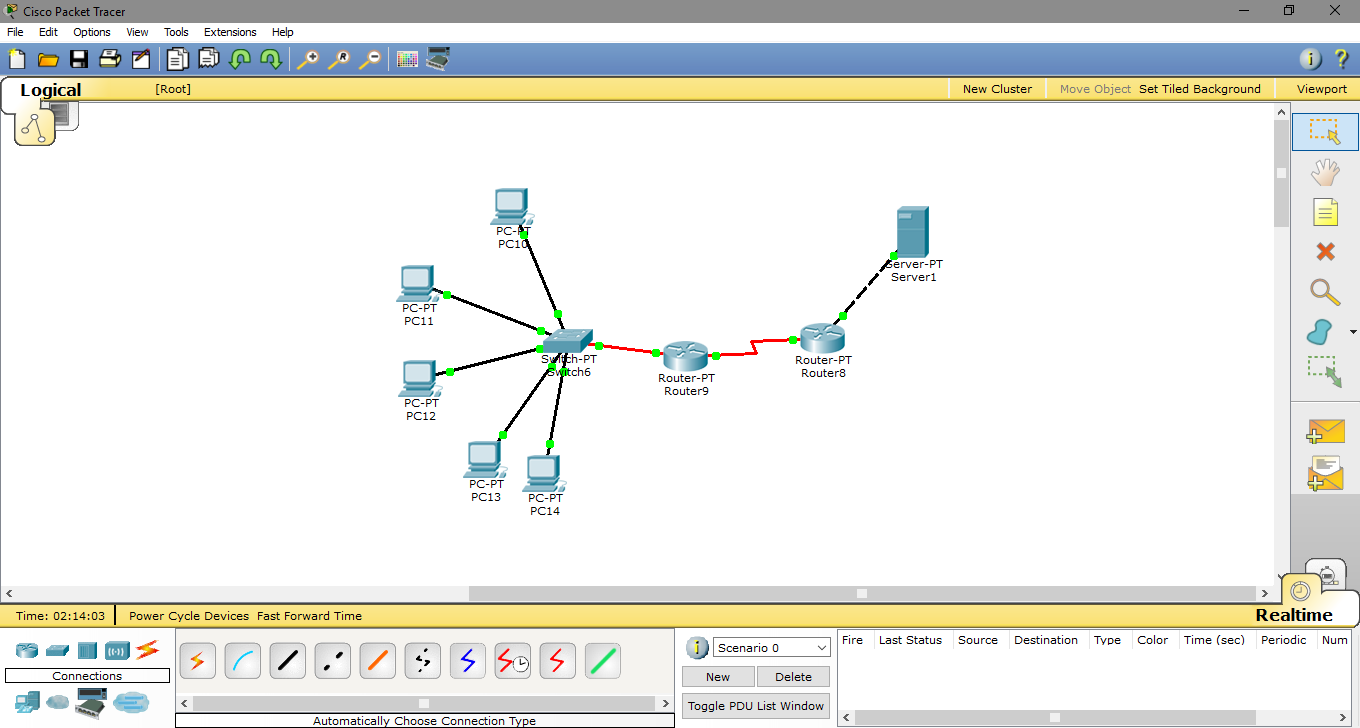


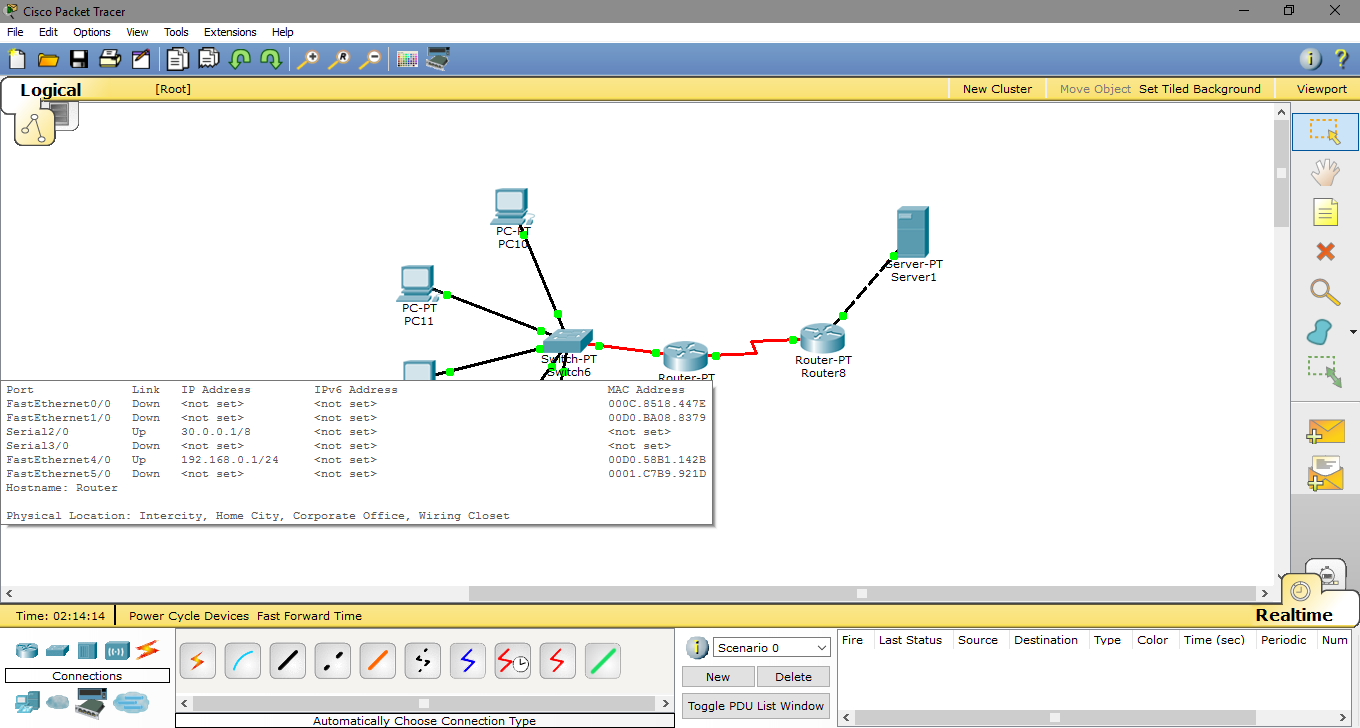


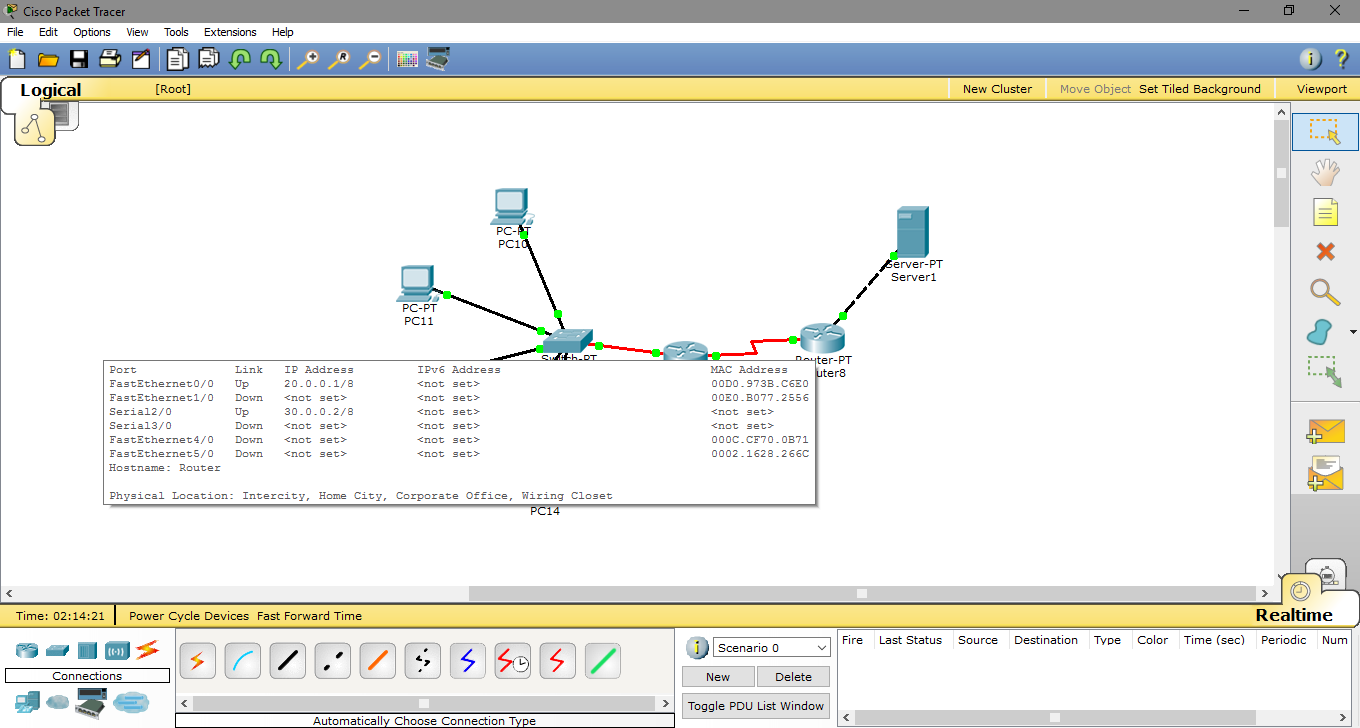


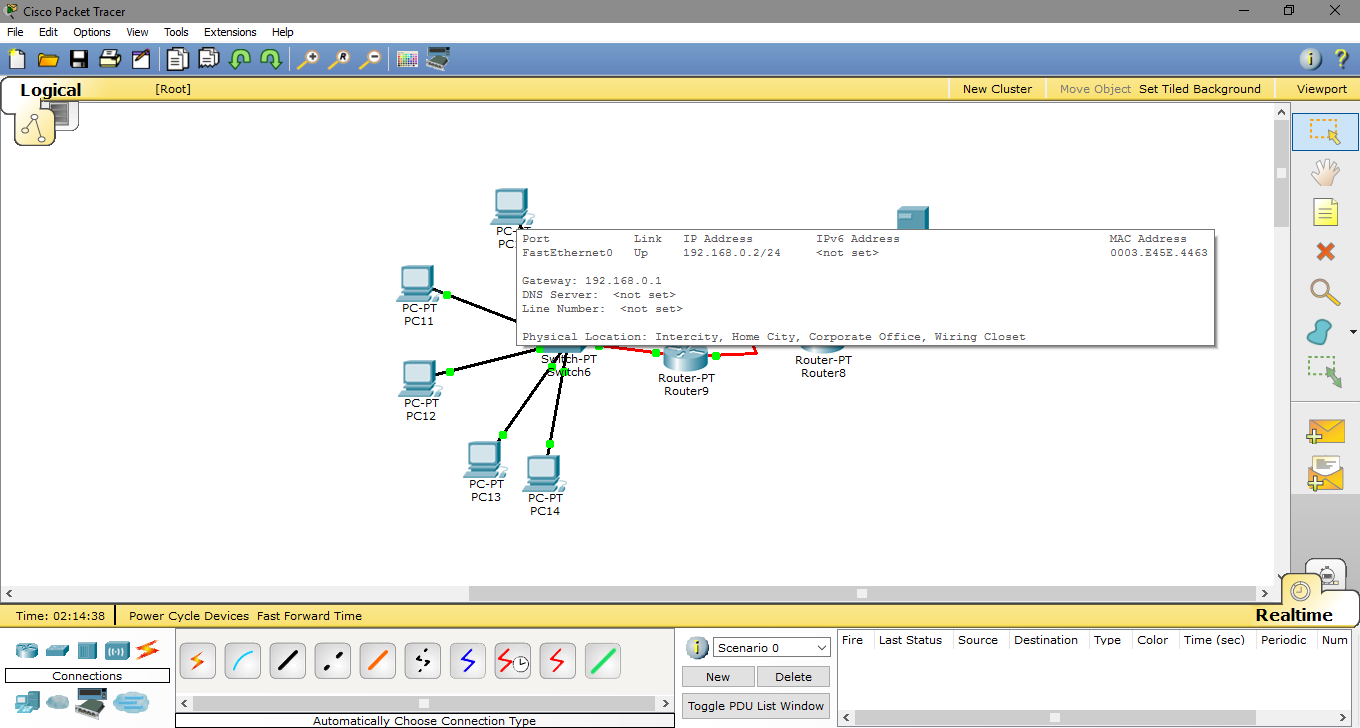


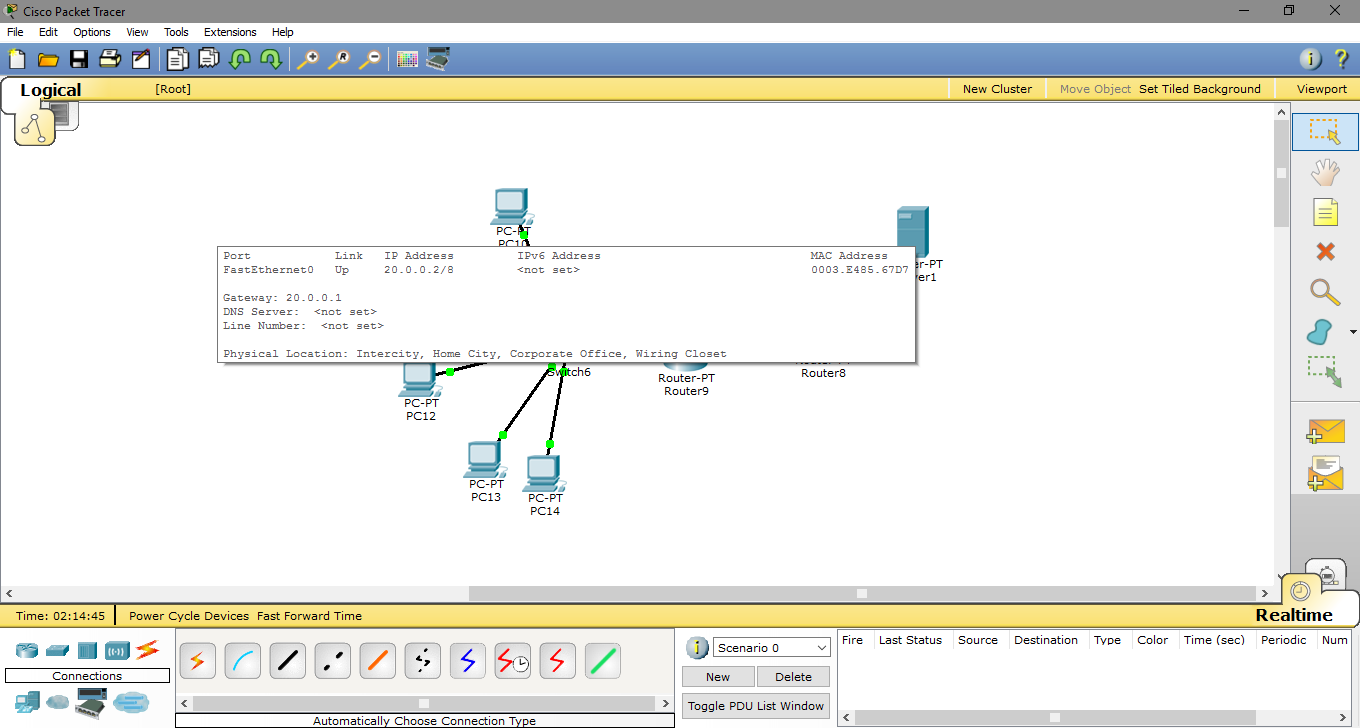
Configuration of Dynamic NAT



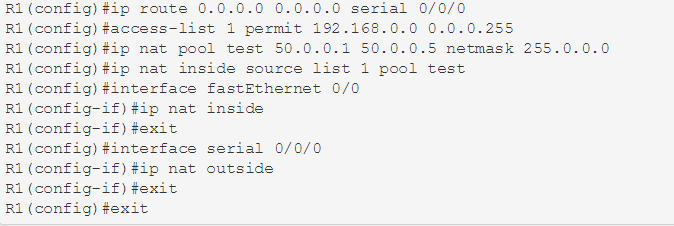


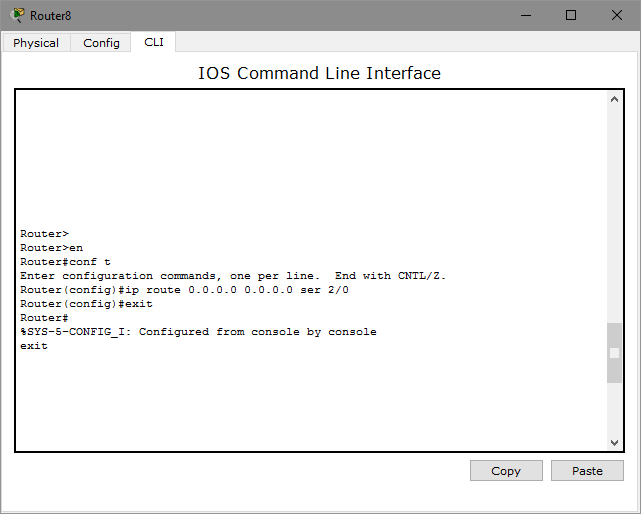


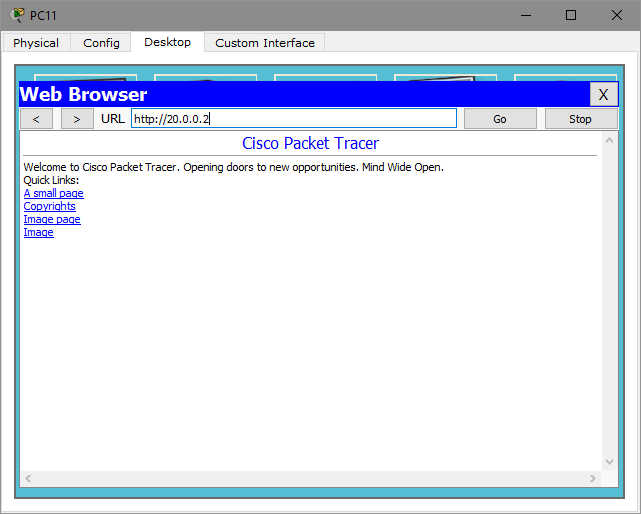


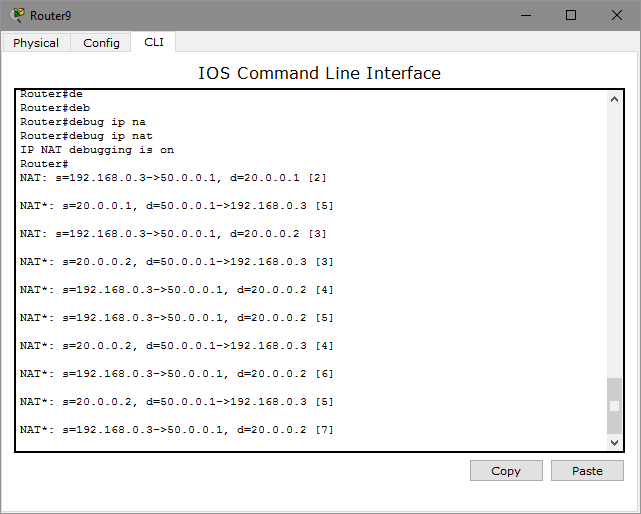


Router Configuration :







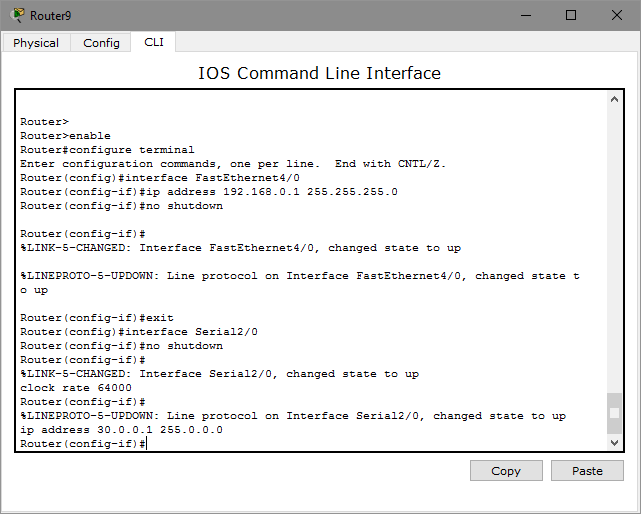


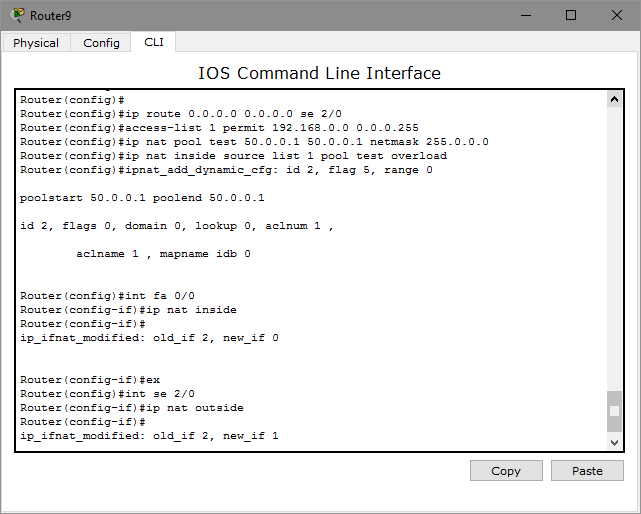
1. **PAT NETWORK**

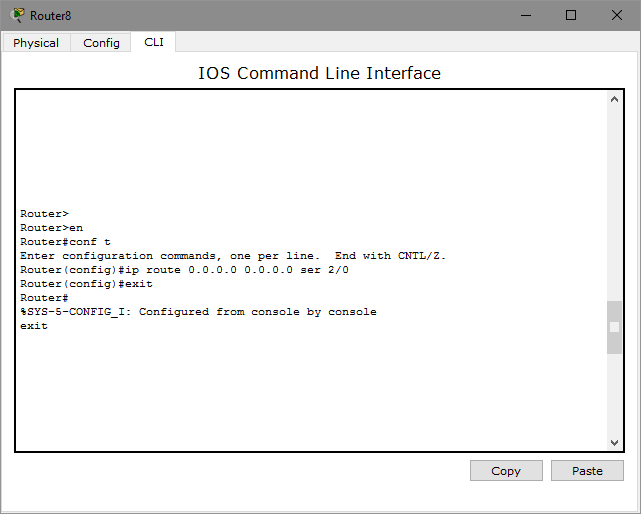
Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public [IP address](https://searchwindevelopment.techtarget.com/definition/IP-address). The goal of PAT is to conserve IP addresses.

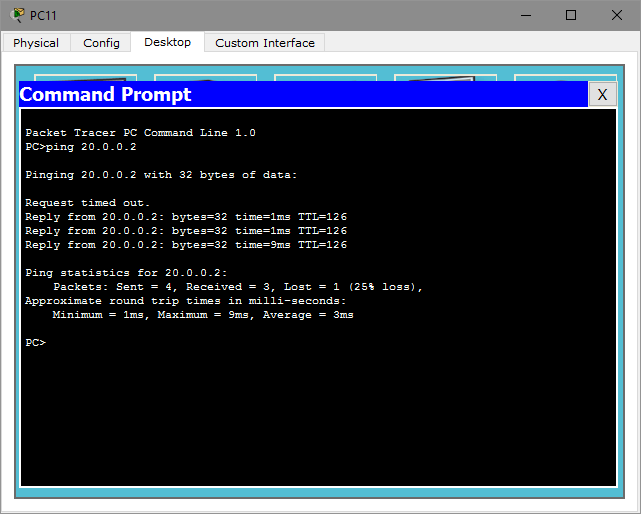
Most home networks use PAT. In such a scenario, the Internet Service Provider ([ISP](https://searchwindevelopment.techtarget.com/definition/ISP)) assigns a single IP address to the home network's [router](https://searchnetworking.techtarget.com/definition/router). When Computer X logs on the Internet, the router assigns the client a [port number](https://searchnetworking.techtarget.com/definition/port-number), which is appended to the internal IP address. This, in effect, gives Computer X a unique address. If Computer Z logs on the Internet at the same time, the router assigns it the same local IP address with a different port number. Although both computers are sharing the same public IP address and accessing the Internet at the same time, the router knows exactly which computer to send specific [packet](https://searchnetworking.techtarget.com/definition/packet)s to because each computer has a unique internal address.

Configuration of PAT









**CONCLUSION:**

We have successfully configured DHCP, Access list configuration, NAT for static and dynamic routing & Pat networks technique.