Devices to be used in labs

1. Routers: 2811
2. Switches: 2960-24TT (or simple 2960)
3. End Devices: Generic (any PC or laptop)
4. Connections:
   a. Copper Crossover: connecting similar devices
   b. Copper Straight-through: connecting non-similar devices
   c. Serial DTE: between routers
5. Network Interface Cards:
   a. WIC-1ENET for one extra ethernet ports
   b. WIC-2T for two serial ports for router connections

*****FOR ROUTER- TO-ROUTER*****

Static Routing:

For directly connected:

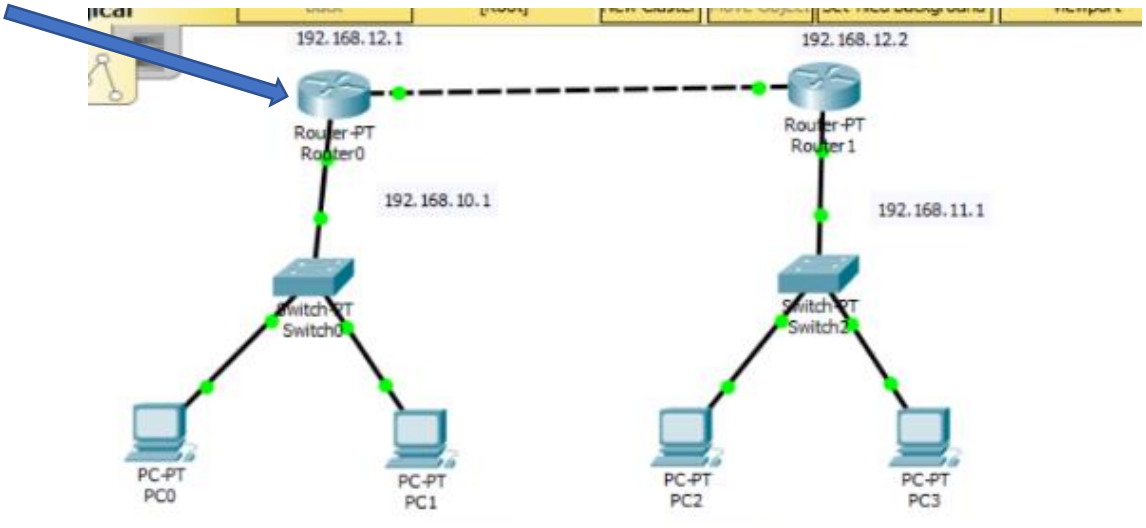
ip add a.b.c.d subnet mask

network access for router1 from right side of router2(i.e not connected):

ip route "giving route to which you want to connected " " subnet mask" " ip of next hop"

example:

ip route 192.168.11.0 255.255.255.0 192.168.12.2



RIP:

router rip

version 2

network a.b.c.d

no auto summary

EIGRP:

router eigrp 10

network x.x.x.x subnet mask

OSPF:

router ospf 1

network x.x.x.x "wildcard mask" area 1

**** DHCP ****

Go to dhcp server and add ip address, subnet mask and default gateway .

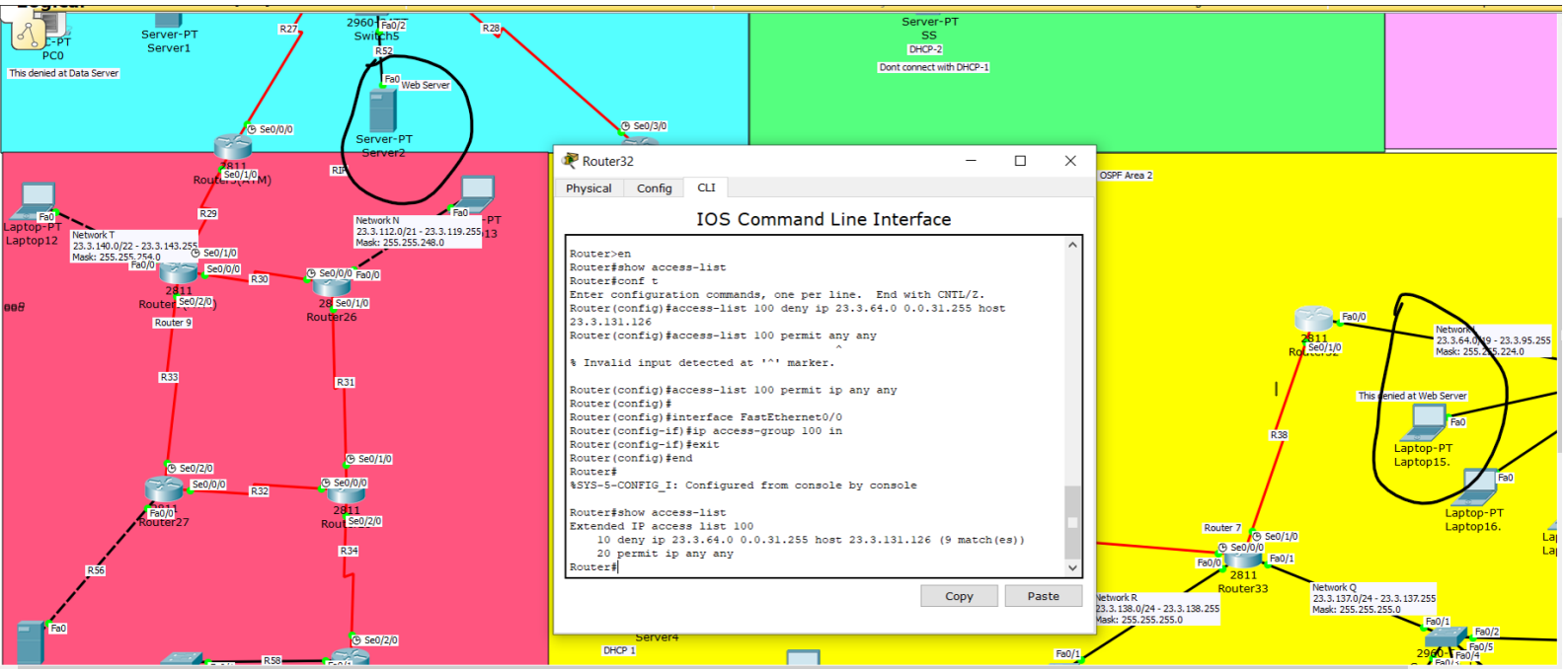
To add a pool:

1. Click DHCP on Services in DHCP Server
2. Switch Service ON
3. Add Pool Name, for Default Gateway(1st usable address in range), DNS Server(0.0.0.0), Start IP Address(next address after Default Gateway) example:
   E: 37.1.3.40 - 37.1.3.47
   Default Gateway: 37.1.3.41
   DNS Server: 0.0.0.0
   Start IP Address: 37.1.3.42
   Subnet Mask: (Calculate)
   Max users: 2^n -2
   TFTP Server: 0.0.0.0

4. Now go to router with which end device is connected, click on connected interface and write : **ip helper-address 192.168.1.10(this is address of server)**
5. Click on Dynamic at end device

**** ACL ****

1. Click on router which has network that Server doesn't want message from.
2. In configure terminal, write:
   access-list 100 deny ip "23.3.64.0" "wildcard mask" host "23.3.131.26"
   23.3.64.0(network which is to be blocked)
   23.3.131.26(Server which doesn't want message)
3. access-list 100 permit ip any any
4. Go to interface on router which is connected to network:
   ip access-group 100 in
5. To check: show access-list

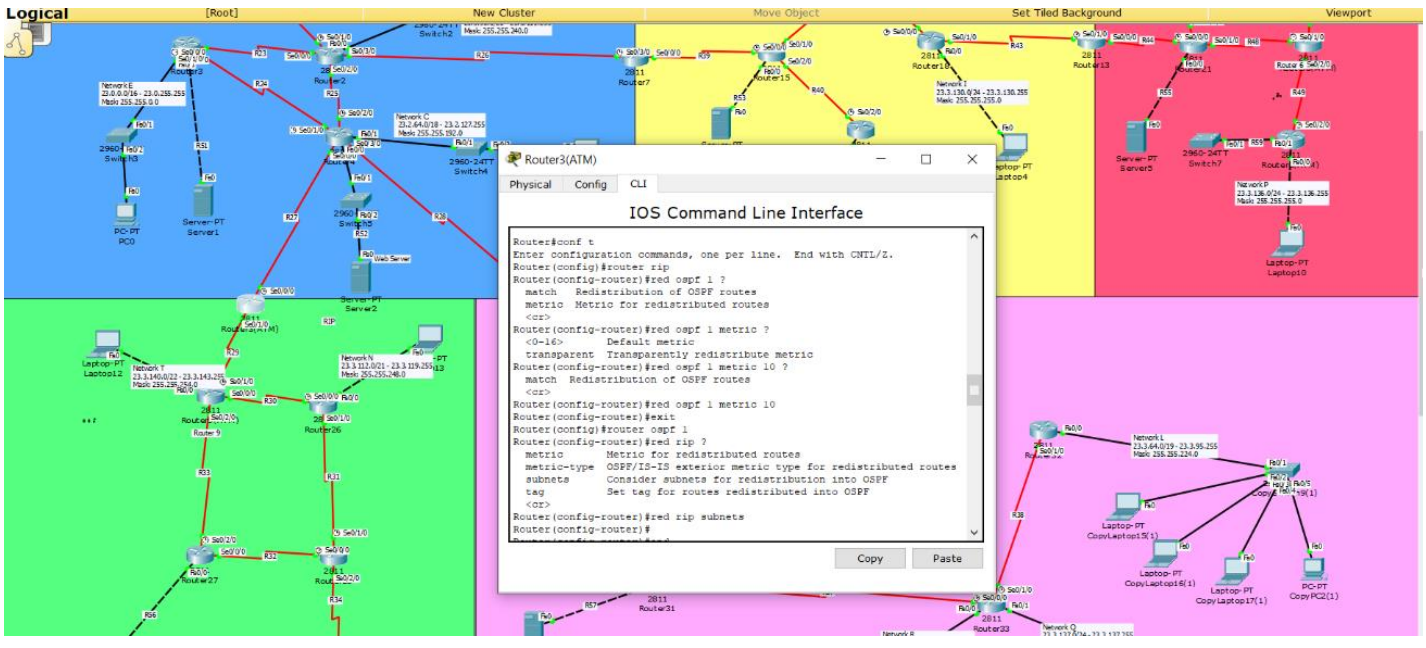


*** NAT ***

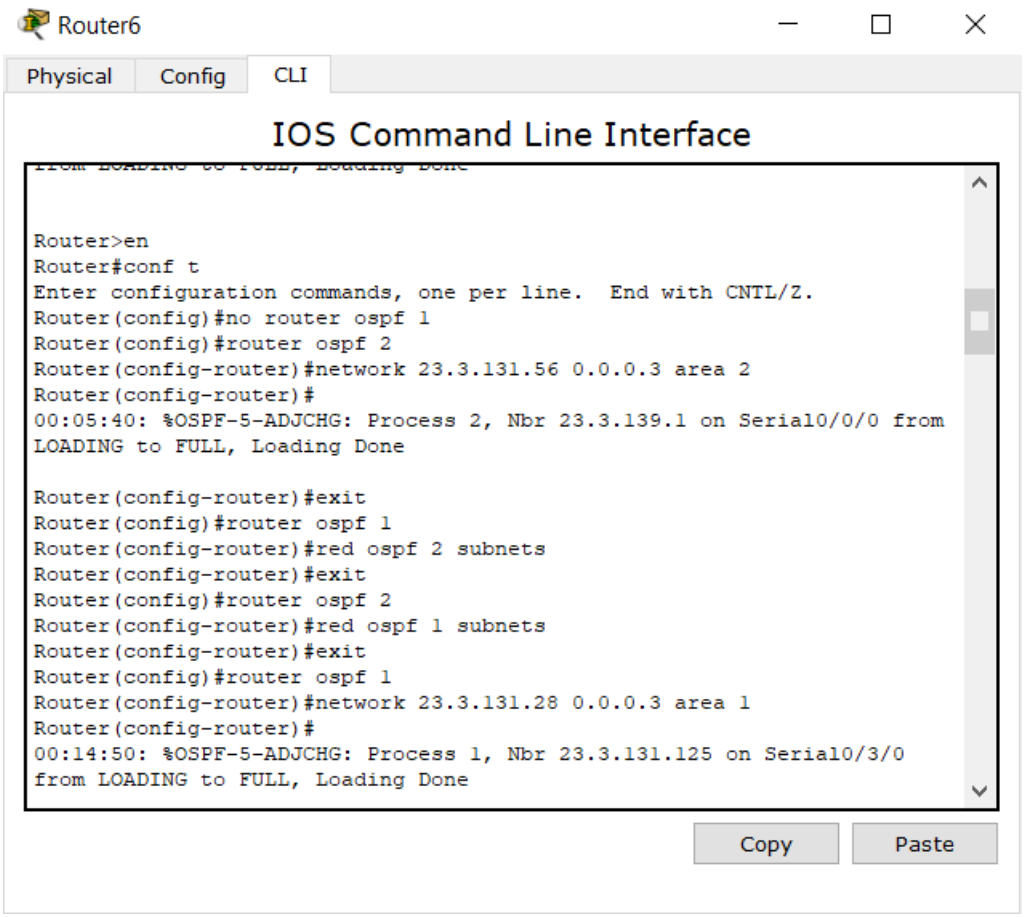
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#
Router(config)#interface FastEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Ethernet0/1/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#access-list 1 permit 23.3.0.0 0.0.63.255
Router(config)#ip nat pool NAT_POOL 92.3.5.13 92.3.5.13 netmask 255.255.255.0
Router(config)#ip nat inside source list 1 pool NAT_POOL overload
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 92.3.5.13:2       23.3.0.2:2         23.2.64.2:2        23.2.64.2:2

Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 92.3.5.13:1       23.3.0.2:1         23.3.138.5:1       23.3.138.5:1
icmp 92.3.5.13:2       23.3.0.2:2         23.2.64.2:2        23.2.64.2:2

Router#
```

*** REDISTRIBUTION ***

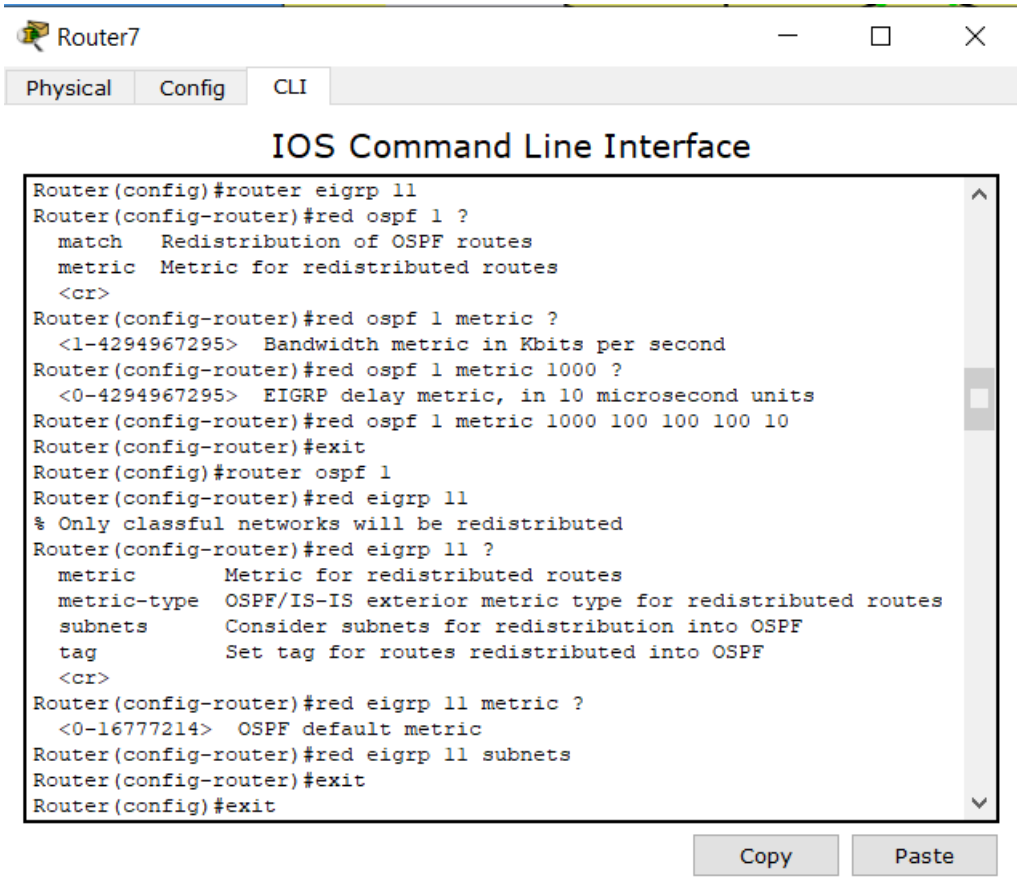
1. Ospf1-RIP(Lower)



2. Ospf1-Ospf2



3. Ospf1 - Eigrp11



4. Eigrp11-RIP(Upper)