|  |  |  |  |
| --- | --- | --- | --- |
| **COURSE** | Network Fundamentals | **ASSIGNMENT NO** |  |
| **MODULE** | Final Assessment | **ASSIGNMENT DATE** | 6/09/2024 |
| **STUDENT NAME** | Konganti Chaithanya Kumar | **SUBMISSION DATE** | 8/09/2024 |

**LAB 2**

**----------------------------------------------------------------------**

* **Use the following network, select a Network ID of your choice and do subnetting to assign the required subnets and host IP’s in each subnet.**
* **Do either static/OSPF routing and establish the connectivity.**
* **Now permit one PC from Subnet 1 to access second subnet and server 1 not server 2, access any PC from second subnet 2 to server 2 through HTTP only and not server 1, deny ping from subnet 2 to both servers.**

**Solution:**

We have chosen the network 192.168.20.0/24 and need to create 5 subnets. To achieve this, we'll subnet the network to accommodate the required subnets.

**Subnetting Steps:**

* **Original Network:** 192.168.20.0/24 (provides 256 IP addresses)
* **Required Subnets:** 5

**Subnet Calculation:**

* **Subnet 1:** 192.168.20.0/27 (Usable IPs: 192.168.20.1 - 192.168.20.30)
* **Subnet 2:** 192.168.20.32/27 (Usable IPs: 192.168.20.33 - 192.168.20.62)
* **Subnet 3:** 192.168.20.64/27 (Usable IPs: 192.168.20.65 - 192.168.20.94)
* **Subnet 4:** 192.168.20.96/27 (Usable IPs: 192.168.20.97 - 192.168.20.126)
* **Subnet 5:** 192.168.20.128/27 (Usable IPs: 192.168.20.129 - 192.168.20.158

**1. Setting Up the Network Topology**

1. **Add Routers to the Workspace:**
2. **Connect the Routers:**
   * + **Router 1** to **Router 2**
     + **Router 2** to **Router 3**

**Router 1:**

* **Interface GigabitEthernet0/0:** 192.168.20.1/27
* **Interface GigabitEthernet0/1:** 192.168.20.97/27

**Router 2:**

* **Interface FastEthernet0/0:** 192.168.20.98/27
* **Interface FastEthernet0/1:** 192.168.20.33/27
* **Interface Ethernet1/0:** 192.168.20.129/27

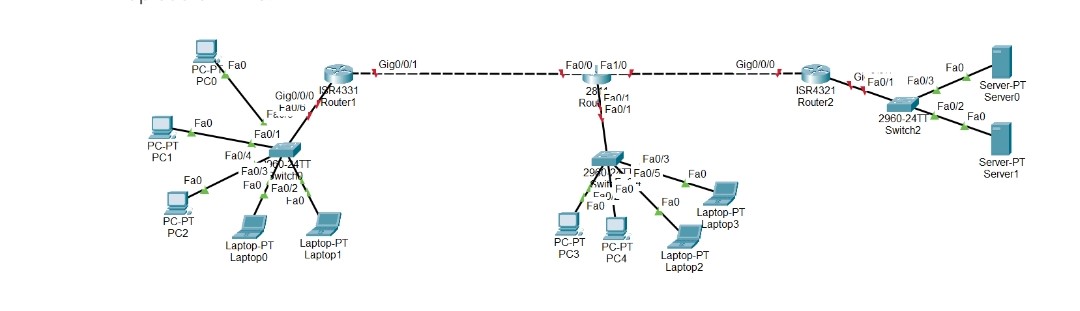
**Router 3:**

* **Interface GigabitEthernet0/0:** 192.168.20.130/27
* **Interface GigabitEthernet0/1:** 192.168.20.65/27

1. **Add PCs/Laptops to the Workspace**

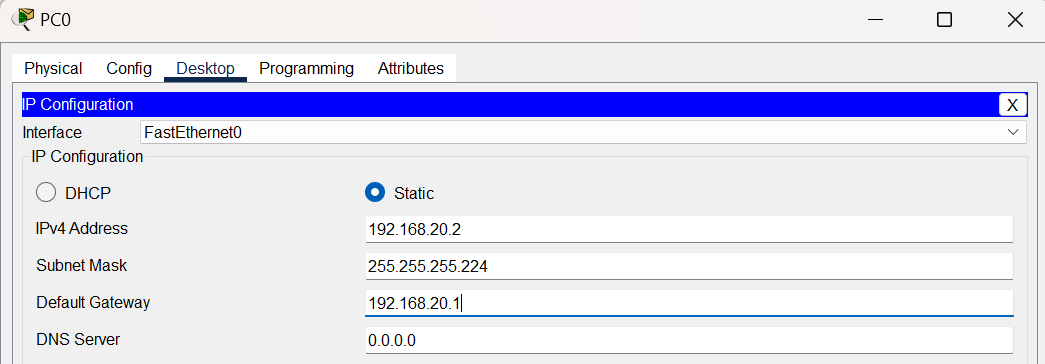
Use appropriate cables (e.g., straight-through or crossover) to connect each PC or laptop to the router or switch in the workspace.

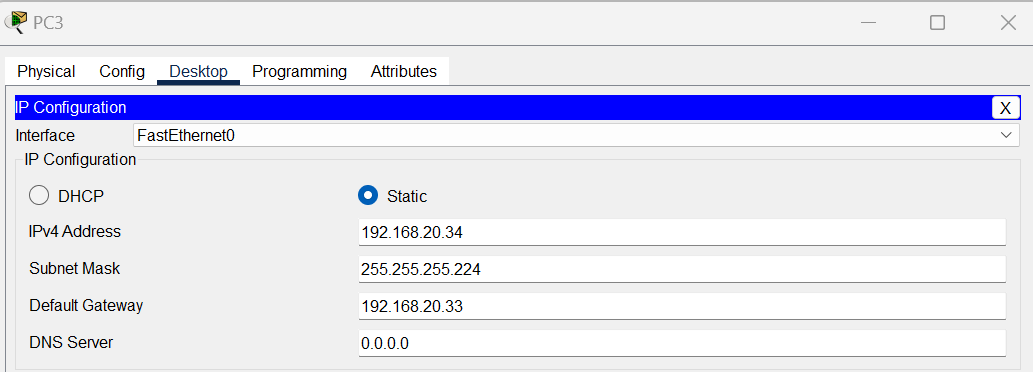
**Topology Diagram:**

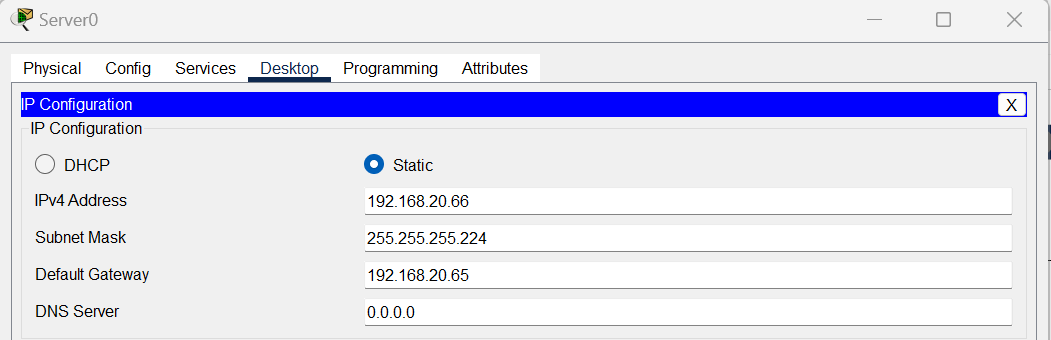


1. **Configuring IP Address, Subnet Mask, and Default Gateway for Devices:**

.

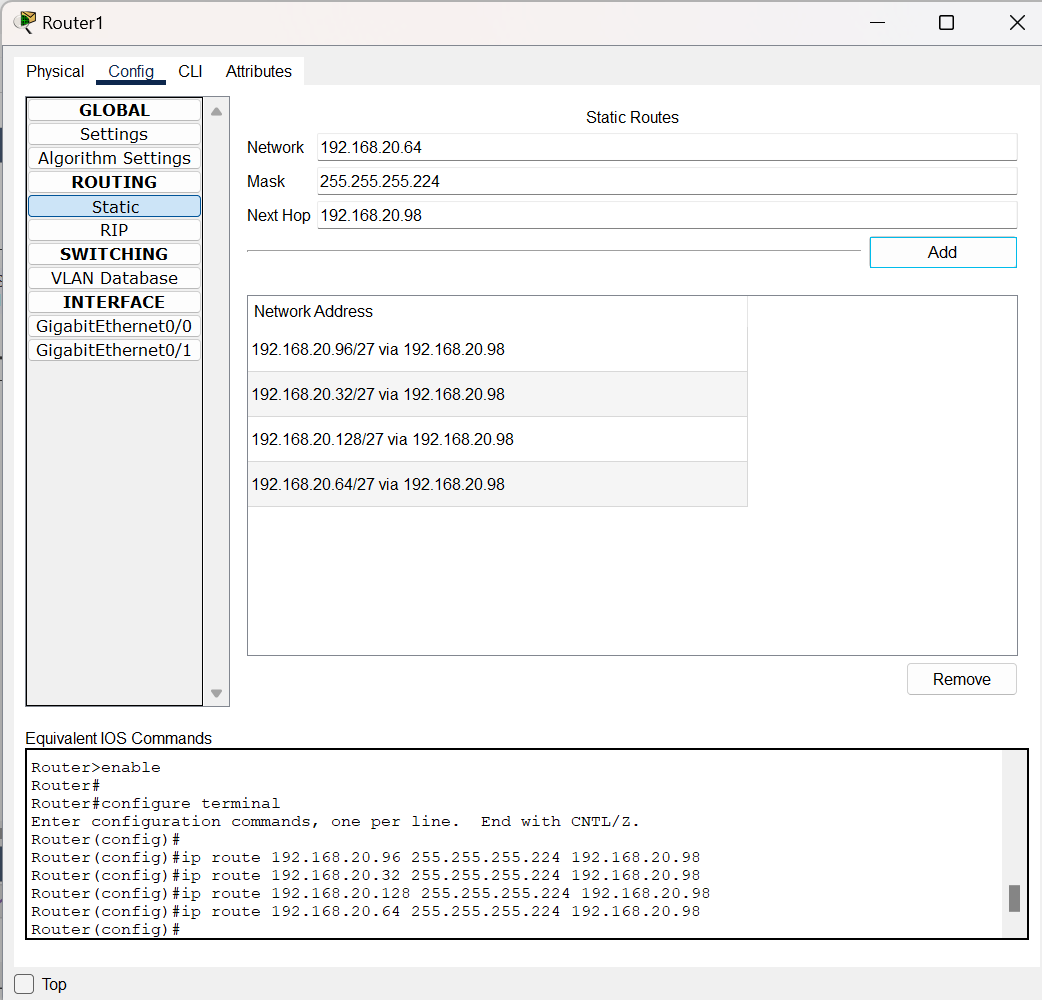
**IP Address for subnet 1:**  


**IP Address for subnet 2:** 

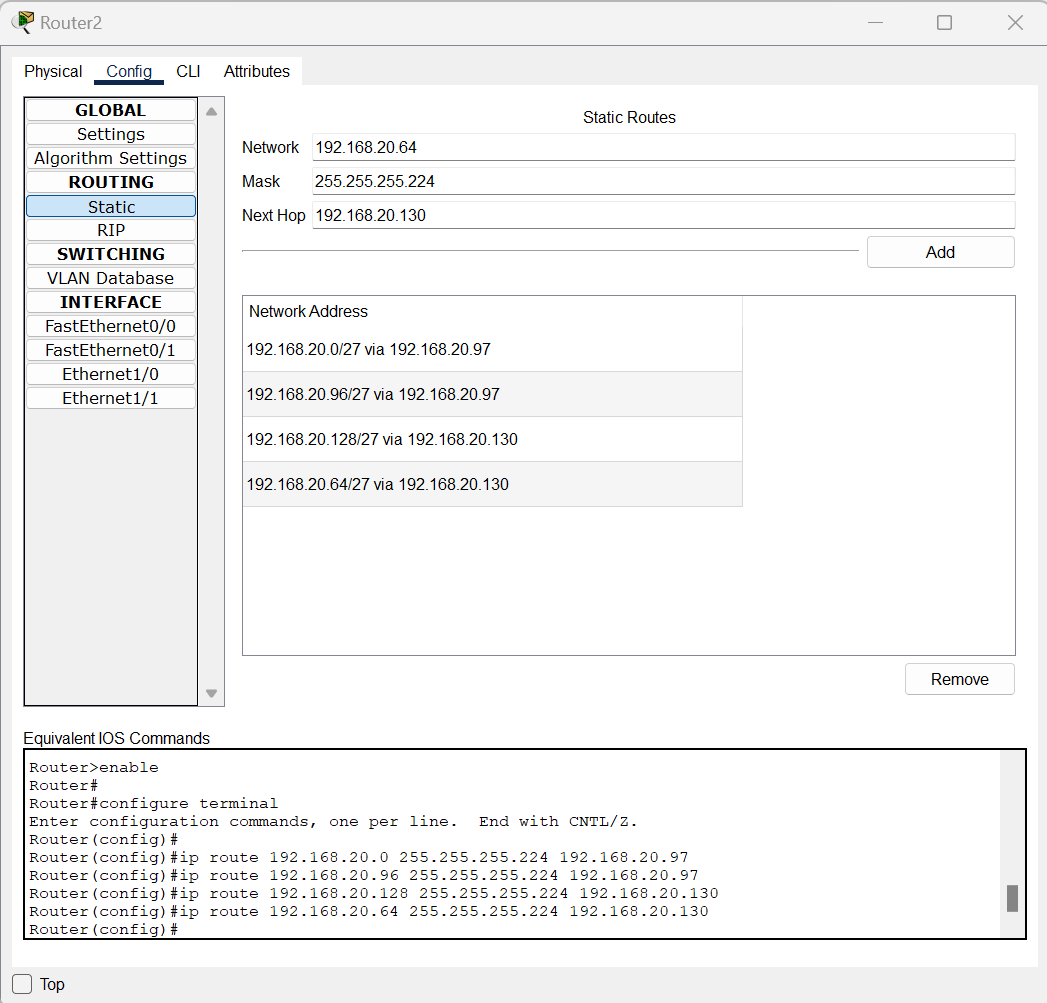
**IP Address for subnet 3:**  


**2. Do static routing and establish the connectivity**.

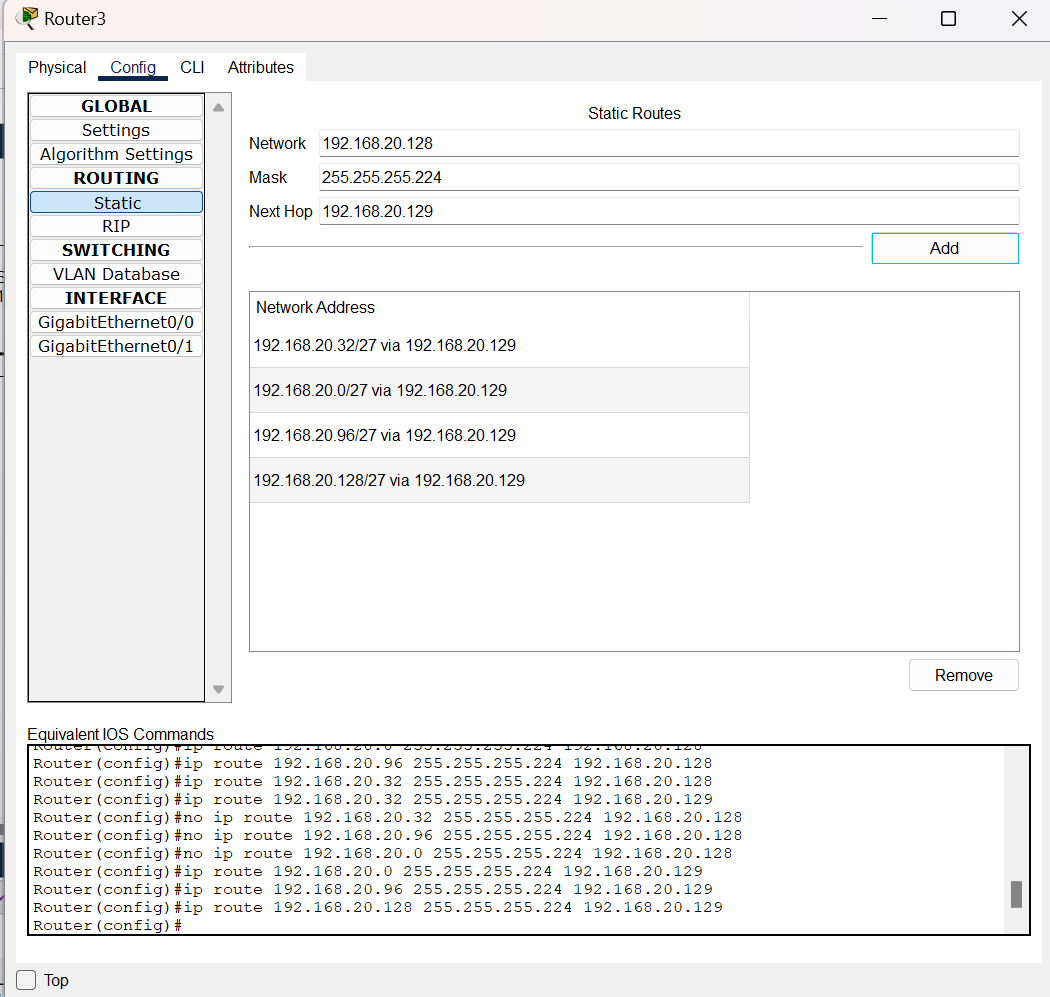
**Router 1 Configuration**



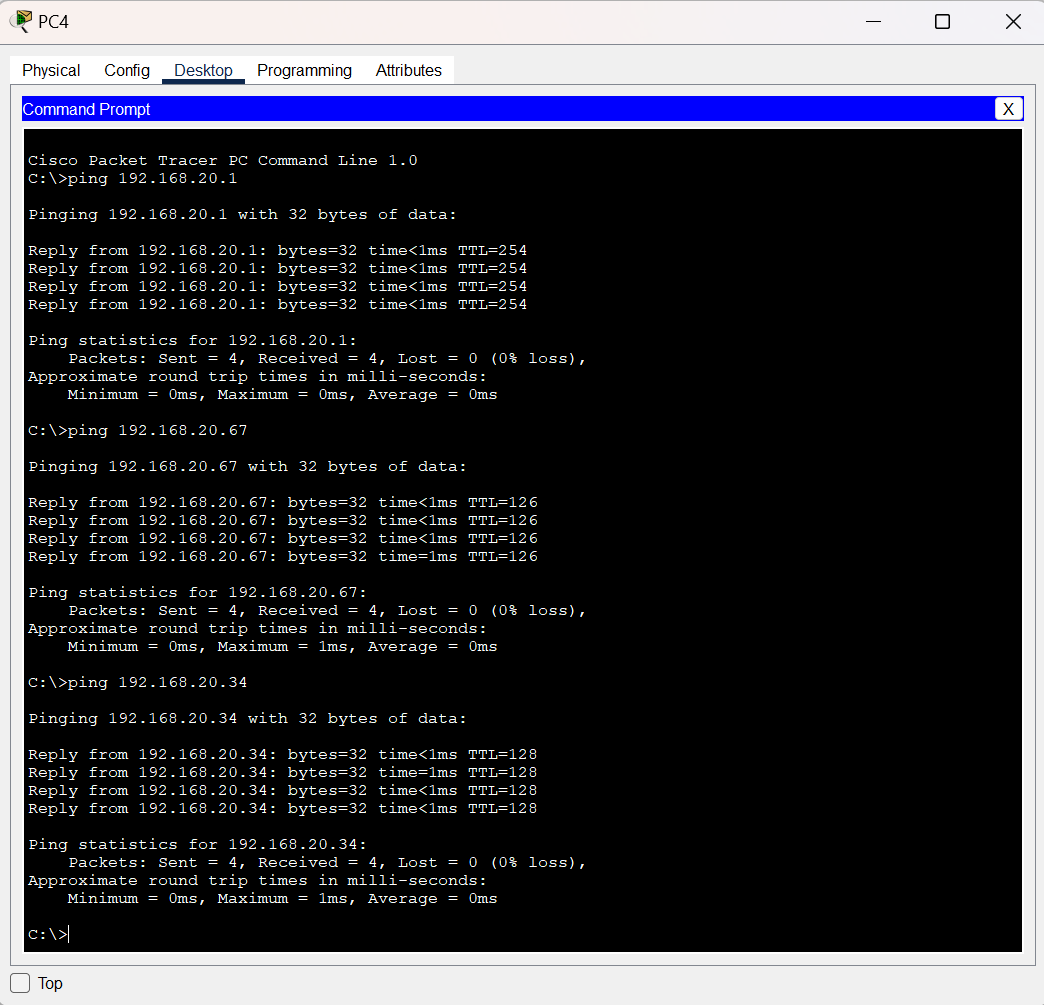
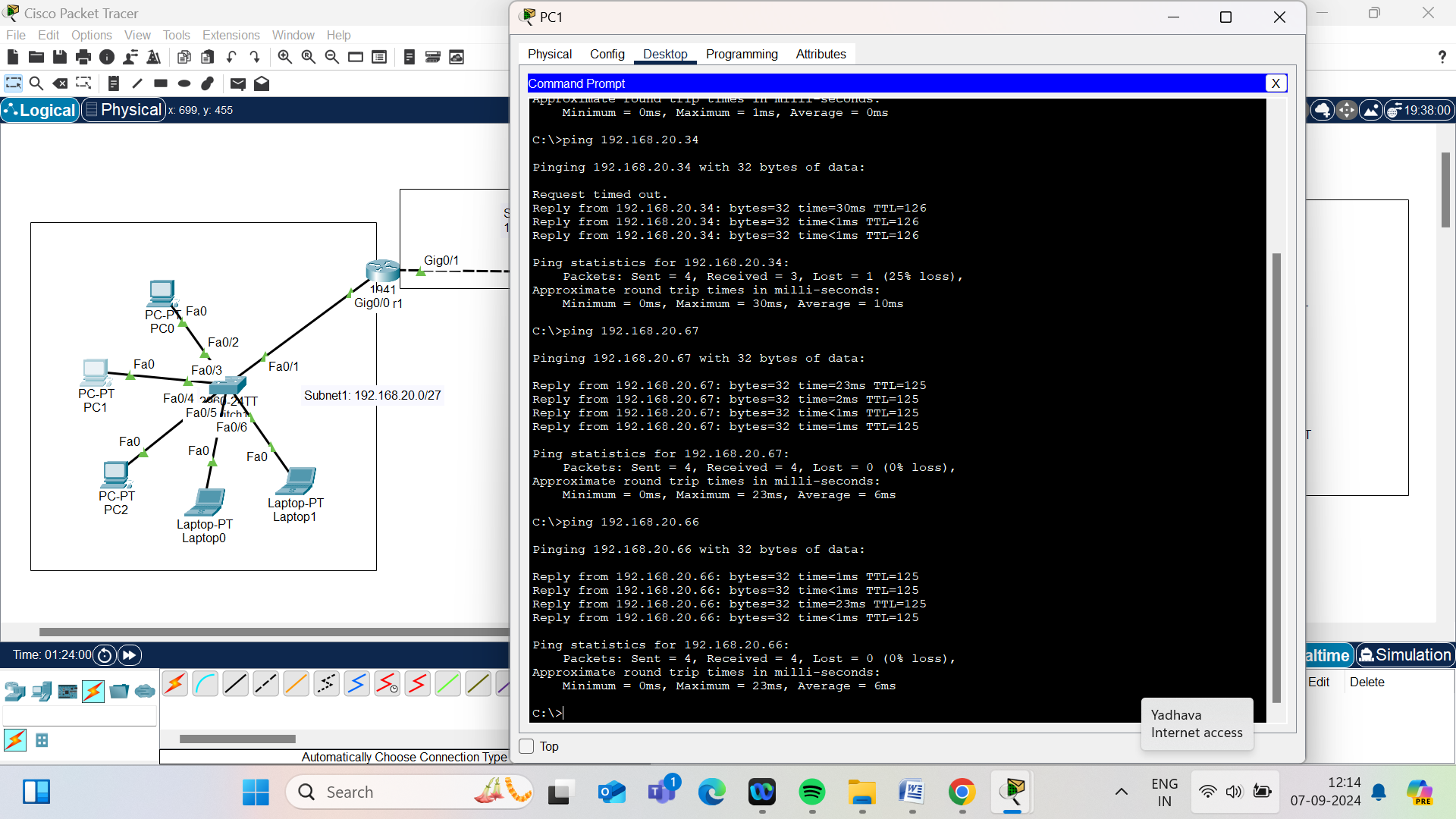
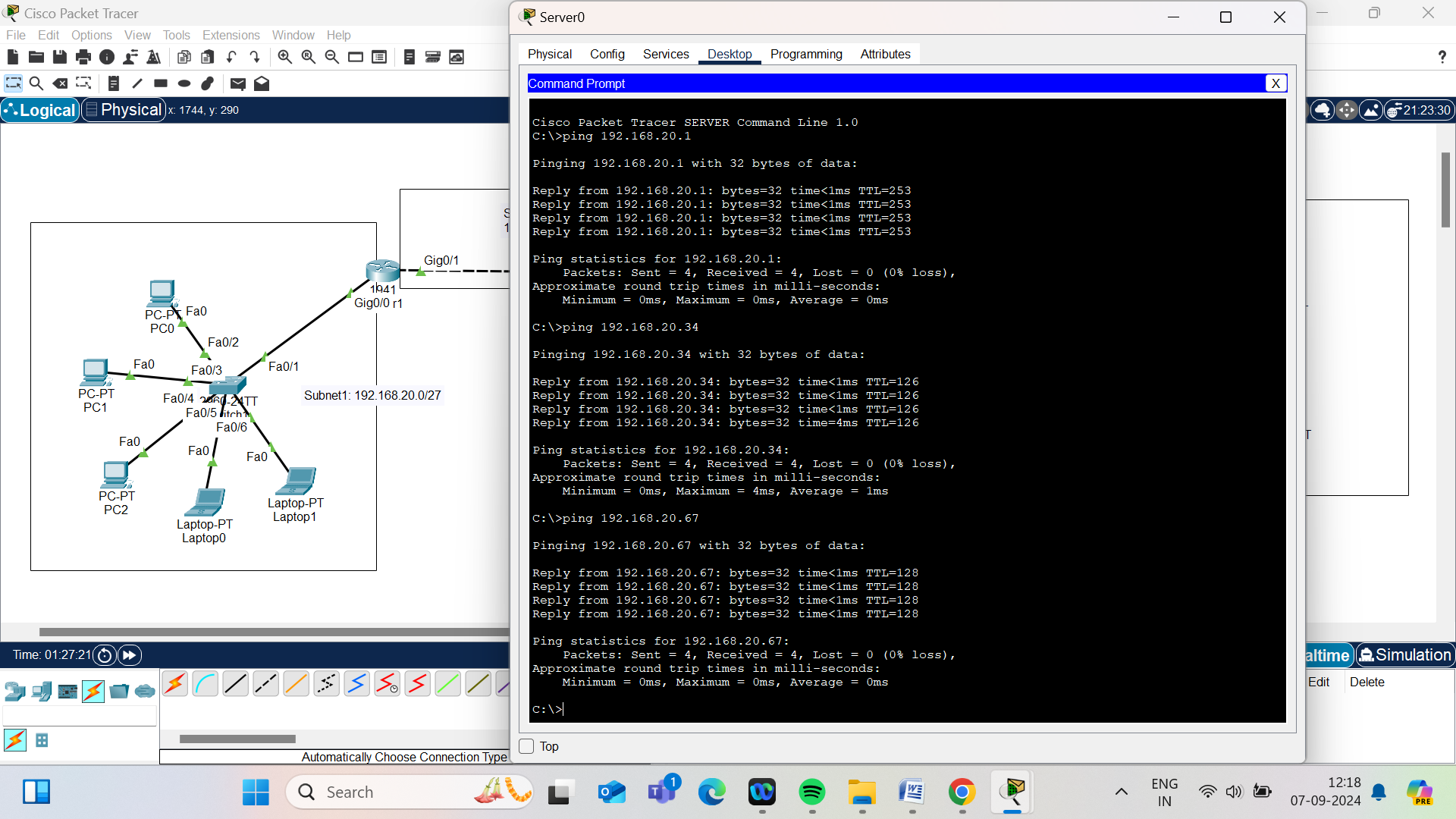
**Router 2 Configuration**



**Router 3 Configuration**



**Ping and check the connectivity between different networks:**

Now permit one PC from Subnet 1 to access second subnet and server 1 not server 2, access any PC from second subnet 2 to server 2 through HTTP only and not server 1, deny ping from subnet 2 to both servers.

**Conditions to Apply**

1. **Permit one PC from Subnet 1 to access Subnet 2 and Server 1 but not Server 2.**
2. **Allow any PC from Subnet 2 to access Server 2 via HTTP only, and not Server 1.**
3. **Deny ping (ICMP) from Subnet 2 to both servers.**

### Steps to Apply Rules on Each Router :

#### Router 1 (R1)

**Objective:** Allow traffic from Subnet 1 to Subnet 2 and Server 1 but not to Server 2.

1. **Create and Apply Access Control List (ACL) on Router 1:**
   * **Create ACL to Allow Access for any one PC to Subnet 2.**

R3(config)#ip access-list extended 100

R3(config-ext-nacl)# permit ip host 192.168.20.3 192.168.20.32 0.0.0.31

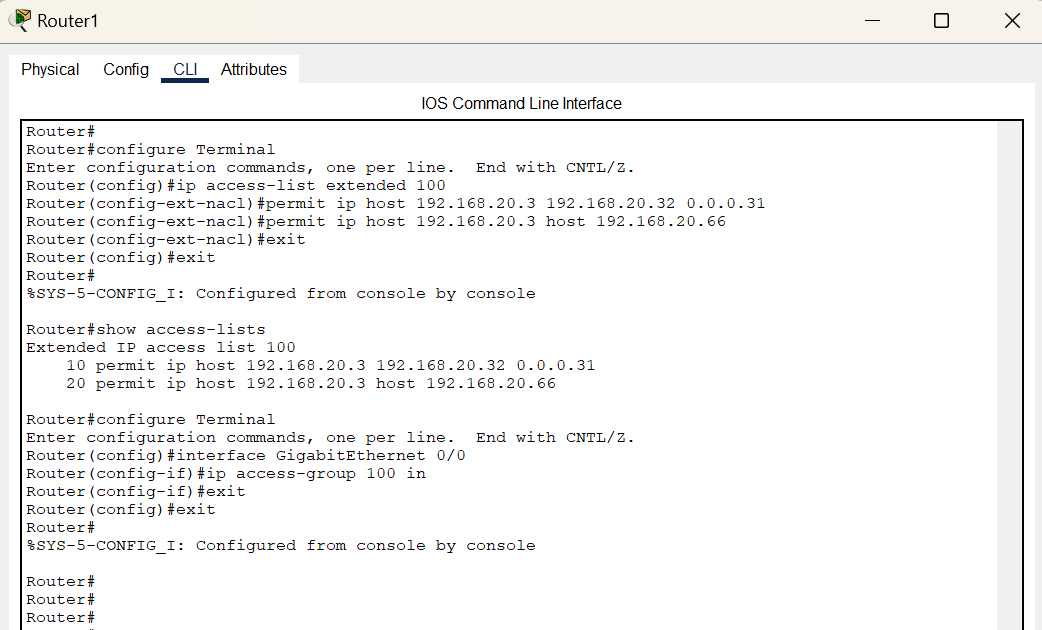
R3(config-ext-nacl)# permit ip host 192.168.20.3 host 192.168.20.66

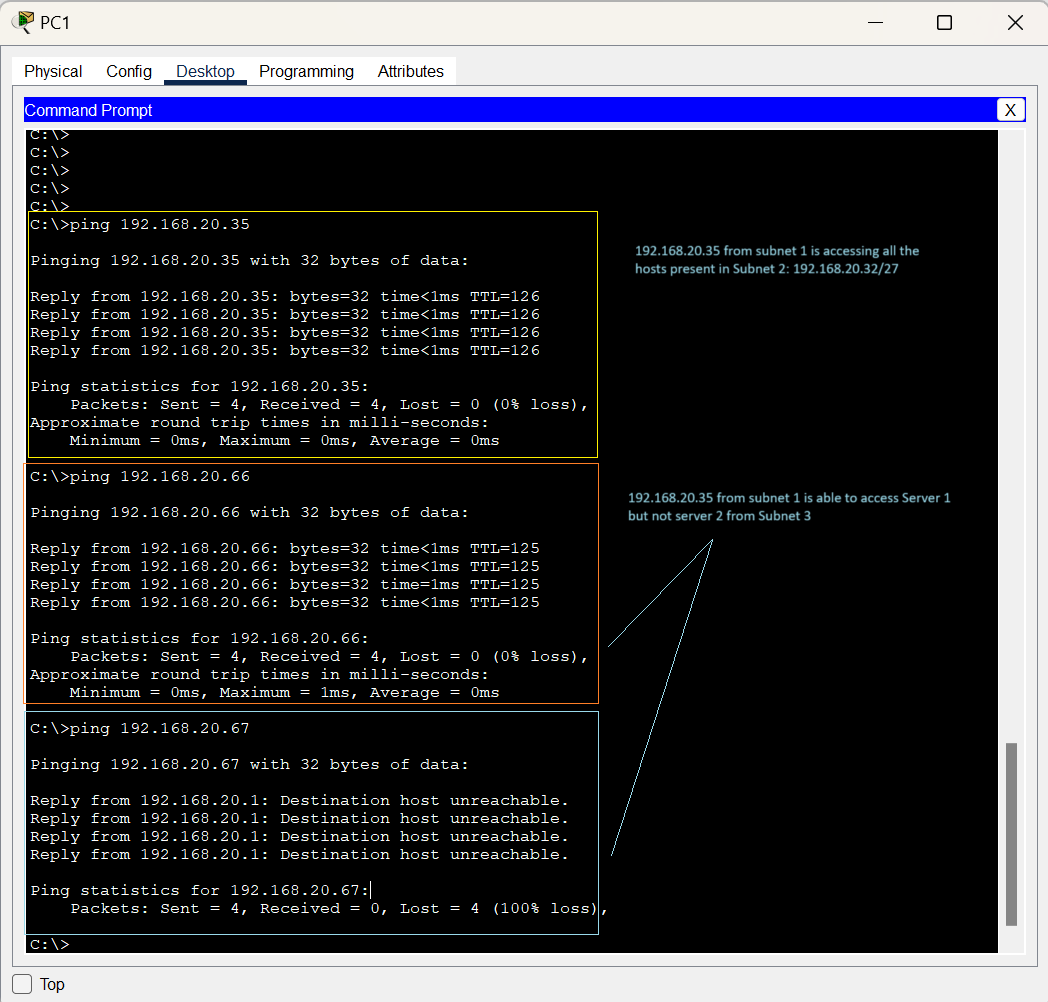
This ACL allows the PC with IP address 192.168.20.3 in Subnet 1 to access devices in Subnet 2 and Server 1(in Subnet3) while blocking access to Server 2.

* + Apply the ACL to the interface connecting to Subnet 1:

R2(config)#interface GigabitEthernet0/0

R2(config-if)#ip access-group 100 in





#### Router 2 (R2)

**Objective:** Allow any PC from Subnet 2 to access Server 2 via HTTP only, and deny ICMP traffic from Subnet 2 to both servers.

1. **Create and Apply Access Control List (ACL) on Router 2:**

R3(config)#ip access-list extended 100

R3(config-ext-nacl)# permit ip host 192.168.20.32 0.0.0.31 host 192.168.20.67 eq www

R3(config-ext-nacl)# deny icmp 192.168.20.32 0.0.0.31 host 192.168.20.66

R3(config-ext-nacl)# deny icmp 192.168.20.32 0.0.0.31 host 192.168.20.67

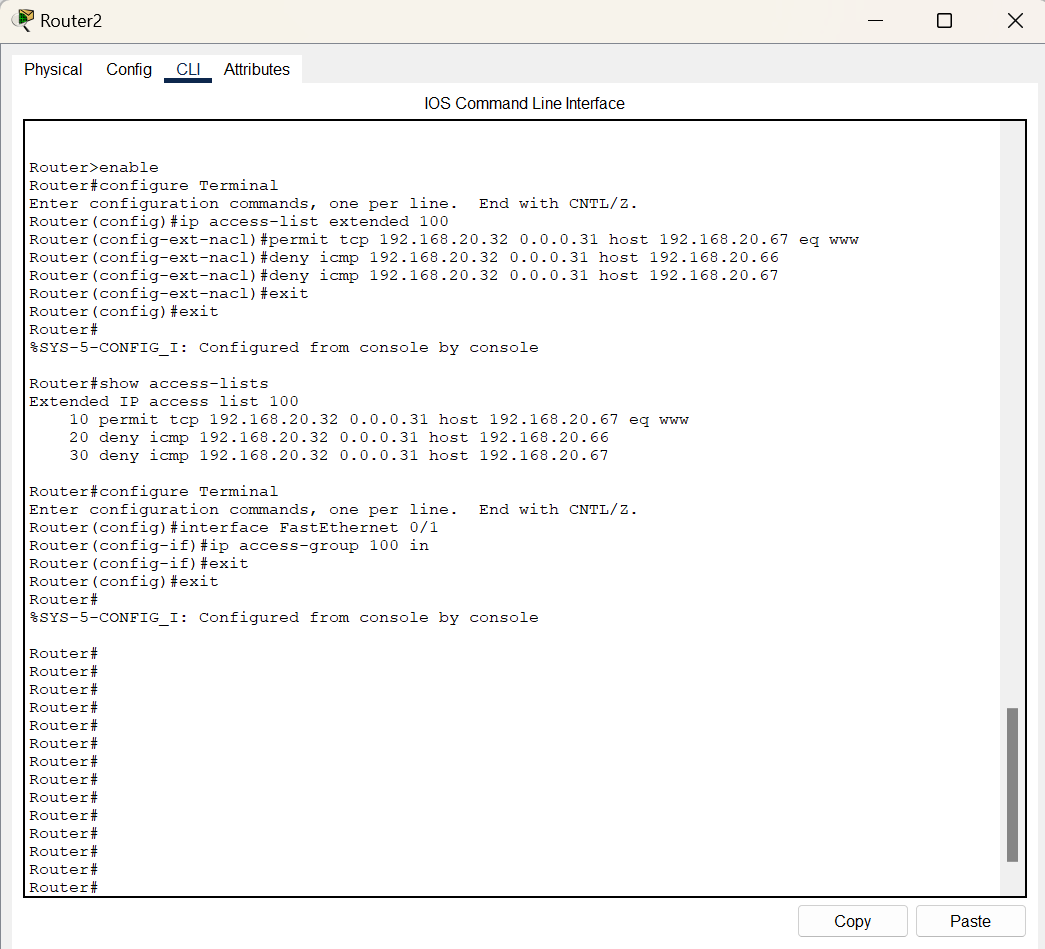
The configuration allows any PC from Subnet 2 to access Server 2 via HTTP only, while ICMP traffic from Subnet 2 to both servers is denied.

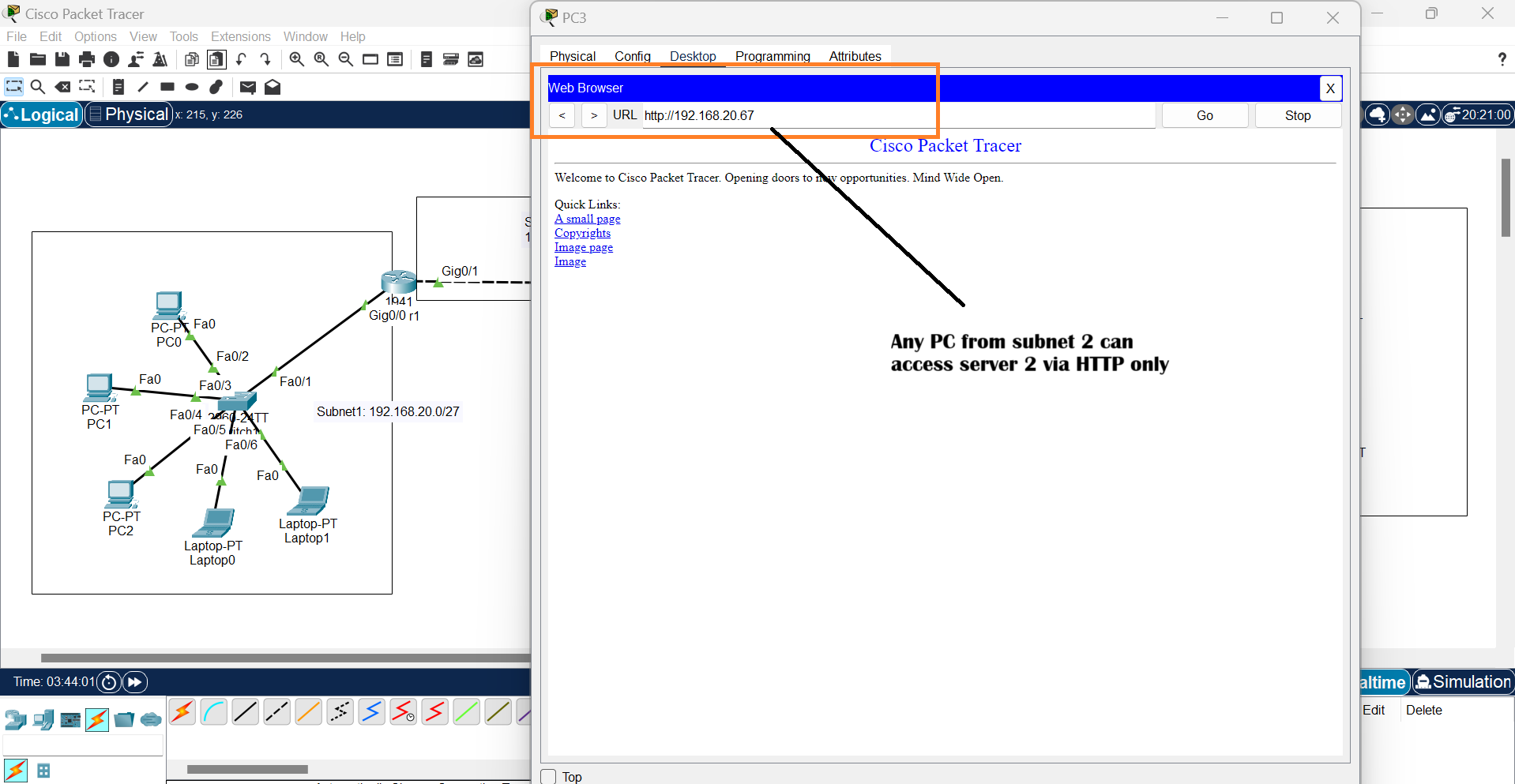
1. Apply the ACL to the interface connecting to Subnet 2:

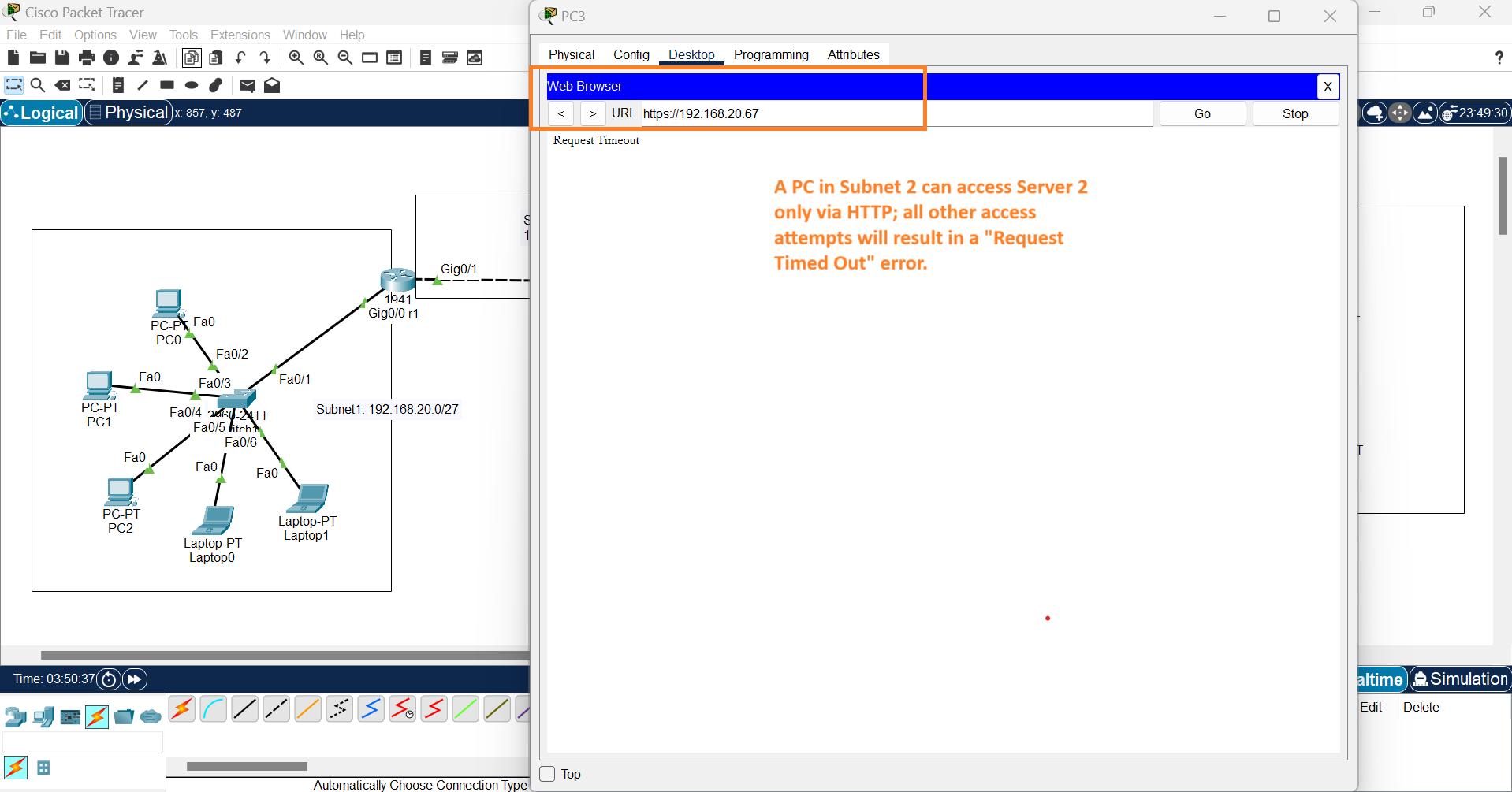
R2(config)#interface FastEthernet 0/1

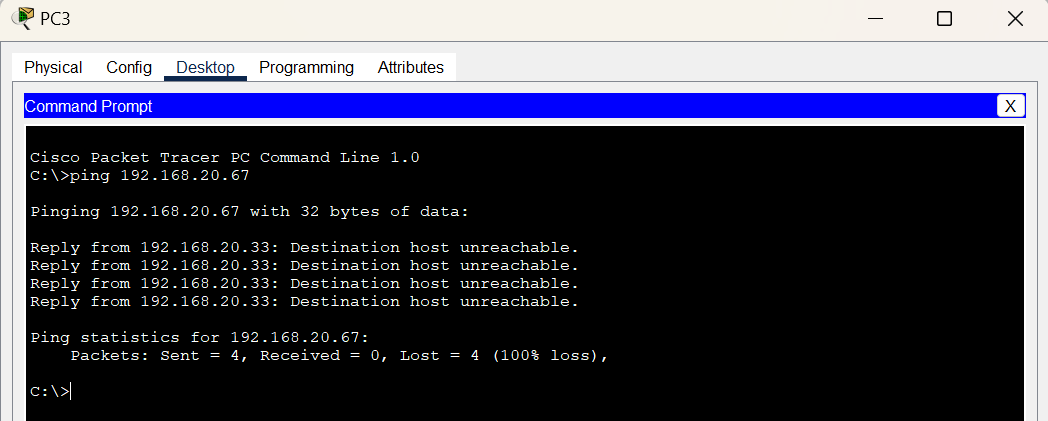
R2(config-if)#ip access-group 100 in

**ACL Configuration Results showing ACL configuration correctly permits only HTTP access to Server 2**









**The result showing ACL configuration correctly denies ping requests from Subnet 2 to both servers.**

