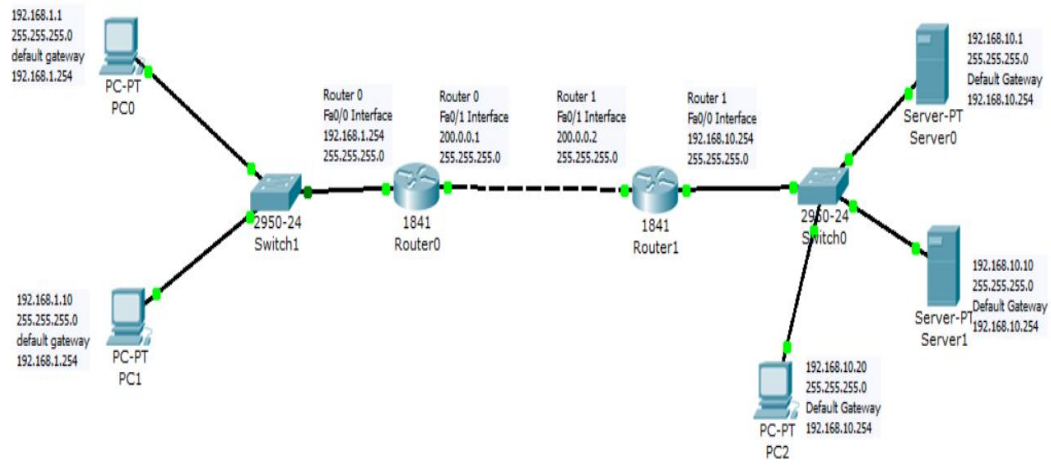
Configuring Simple access-list on Cisco Router

This documents provides details about configuring simple access-list on Cisco routers.

The network is configured as shown below.
As the routing is enabled on the routers, all network computers are allowed to communicate with any computer in other side network.
However it is a violation of organization's security policy. It is required to restrict user access only to other certain computers of other network. Access lists on routers help you achieve this goal.
There are two types of access lists supported - Standard and Extended. The standard access list allows filtering only based source IP. It does not allow you to specify other options like - destination IP, protocol, destination port, source port etc. Thus standard access list will allow entire traffic from an IP or block entire traffic from that IP. If you specify a number between 1 to 99, the router will create a standard access list.

The extended access list allows you to specify source IP, destination IP, protocol, destination port, source port etc. Thus you can block or allow specific trafic between the computers. If you specify a number for an access list between 100 to 199 then the router creates an extended access list.



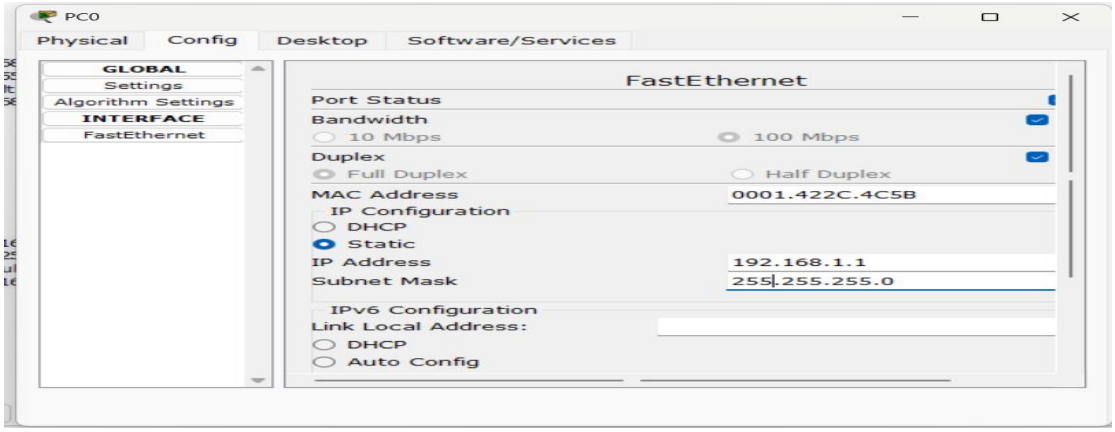
Goal to achieve:-
1. PC0 can access website on Server 0.
2. PC0 can not access website on Server 1.
3. PC1 can access website on Server 1
4. PC1 can not access website on Server 0.
5. PC0 can ping to PC2 and Server 1.

Configuration: -
Use cross cable to connect Router 0 Ethernet port to Router 1 Ethernet port. Here Router 0 FastEthernet0/1 interface is connected to FastEthernet0/1 interface.

1. **First configure PC0 and PC1.**

Click on PC0. Following window opens. Here in Gateway field enter the Gateway IP as shown below.

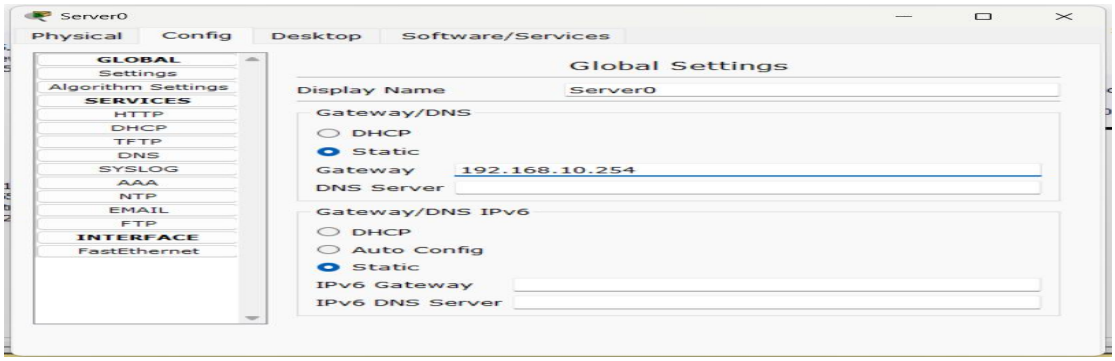
Then click FastEthernet below INTERFACE and assign the IP address as shown below. Make sure you click the subnet mask field.



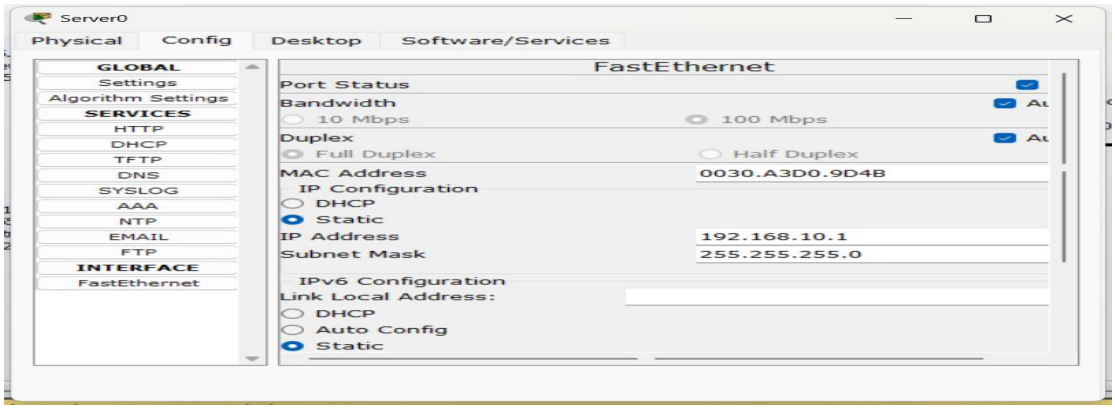
Close the window.
Similarly configure Gateway and IP Address for the PC1. Make sure you assign an IP address as mentioned in the main network diagram.

2. **Configure Server 0, Server 1 and PC 2**

Click on Server 0. On the window that opens, specify the Gateway address as shown below.

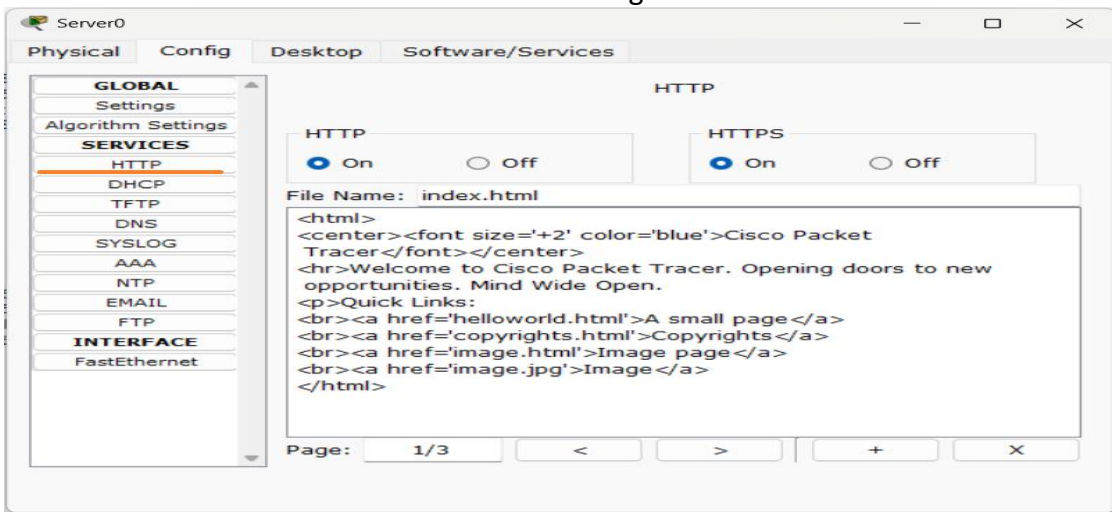


Then click FastEthernet below INTERFACE. Provide IP address as shown below. Click in the Subnet Mask field.

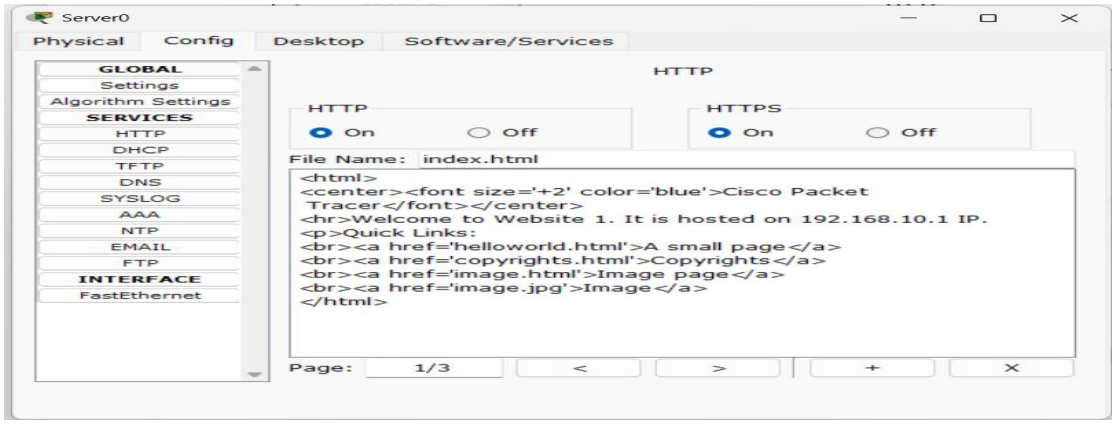


As the HTTP server content is same on both servers, it will be difficult to know which server is accessed from clients. Thus we will change the HTTP content on both the servers.

For this Click HTTP tab on the left side. Following is the default content.

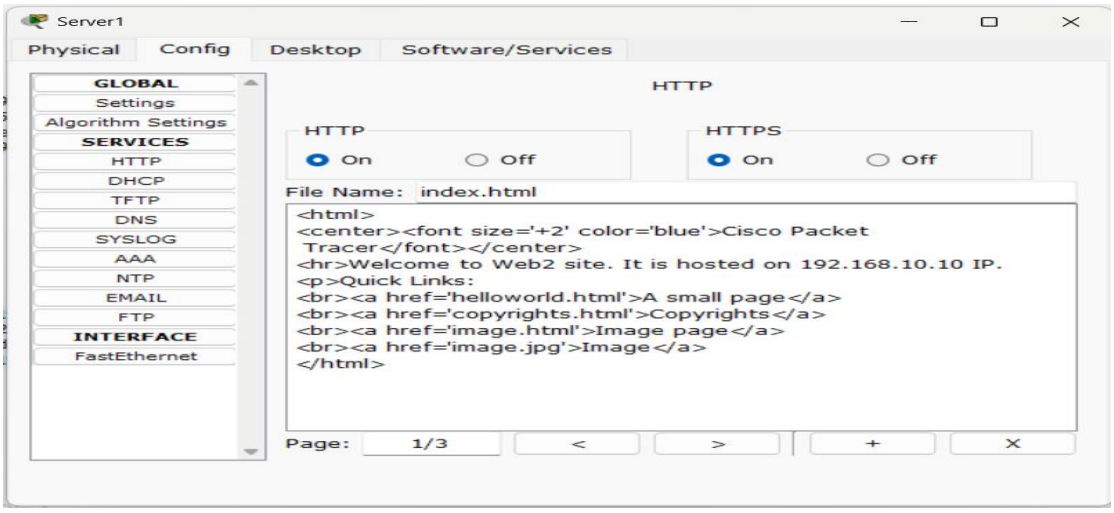


Modify the content as shown below. Change the line Welcome to Cisco Packet Tracer.



Close the window.

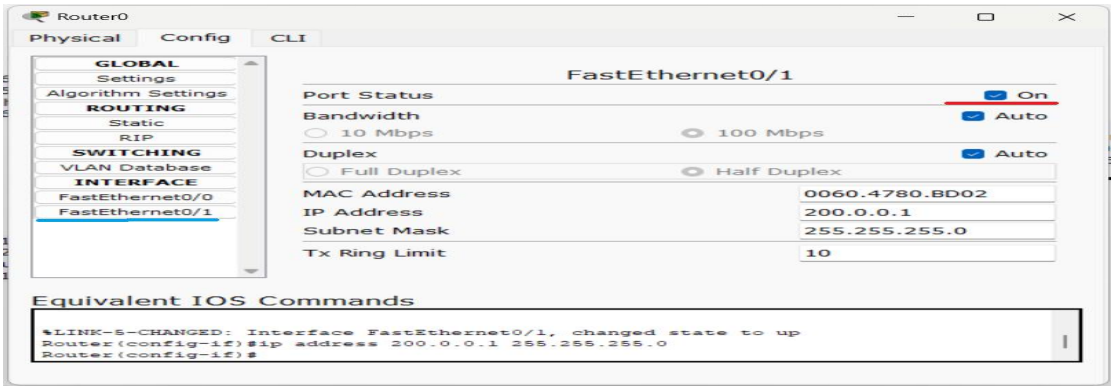
Follow the same steps to configure Gateway and IP address for Server 1. Similarly modify the HTTP content on Server 1 as shown below.



3. **Configure Router 0.**

This is the router on which PAT or NAT overload will be configured.
Click on the Router 0.
Click on the FastEthernet0/0. Enter IP address as shown below. This is the LAN side IP.

Now click on FastEthernet0/1. Enter IP address as shown below. This is the WAN side IP of the Router 0.

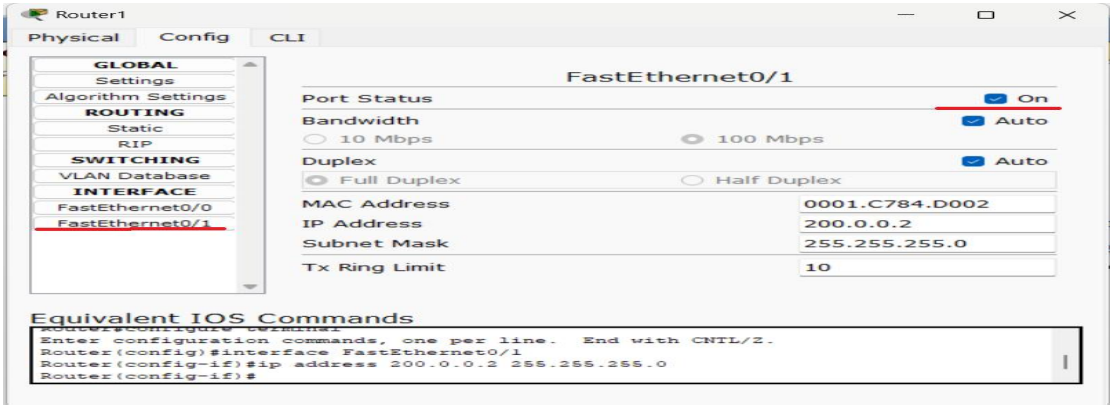


4. **Configure Router 1.**

This is the router on which Static NAT will be configured.
Click on the Router 1.

Click on the FastEthernet0/0. Enter IP address as shown below. This is the LAN side IP.

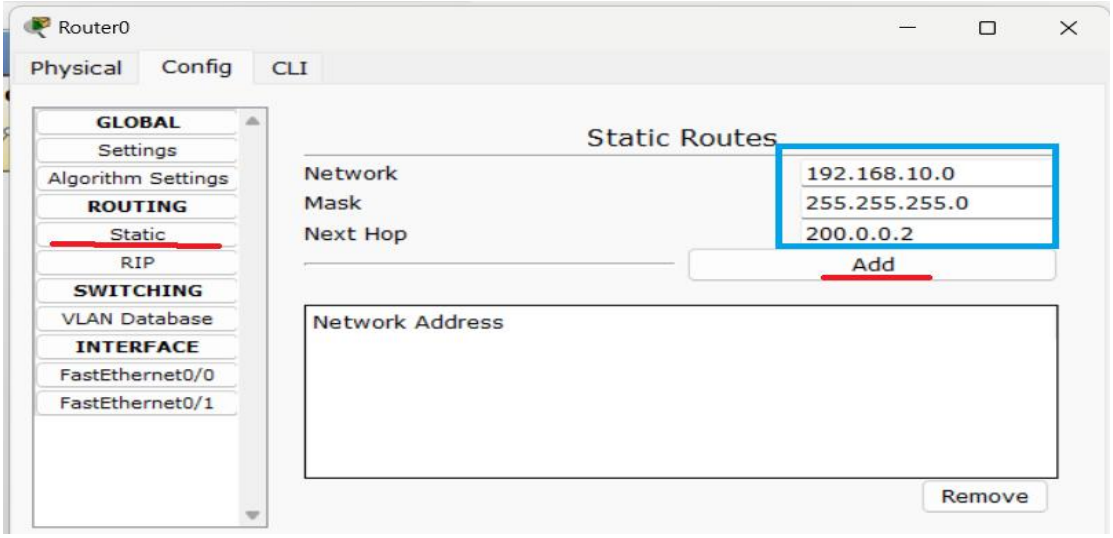
Now click on FastEthernet0/1. Enter IP address as shown below. This is the WAN side IP of the Router 1.



5. **Configure routing on Router 0**

In this step we inform Router 0 about how it can reach to the other network.

Click on Router 0. Below ROUTING click static. Then fill the other end network address and subnet mask. As the Router 0 can reach network 192.168.10.0 through Router 1, the next hop is the WAN address of Router 1.

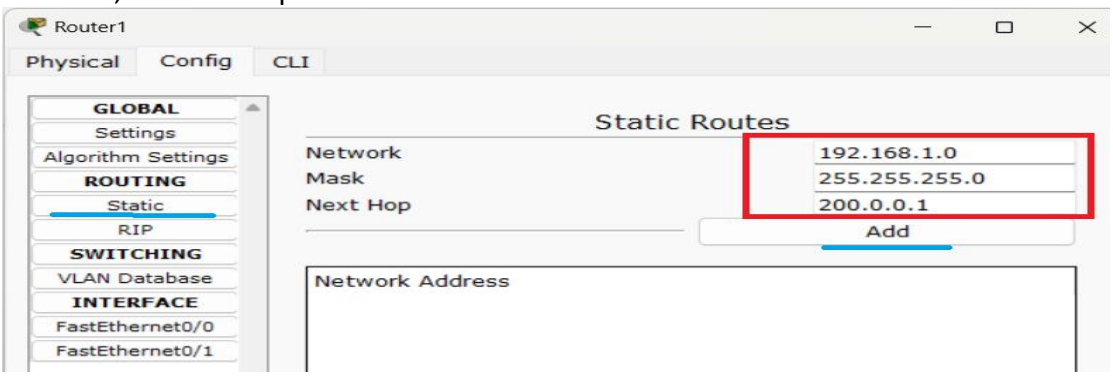


Click Add.

6. **Configure routing on Router 1**

In this step we inform Router 1 about how it can reach to the other network.

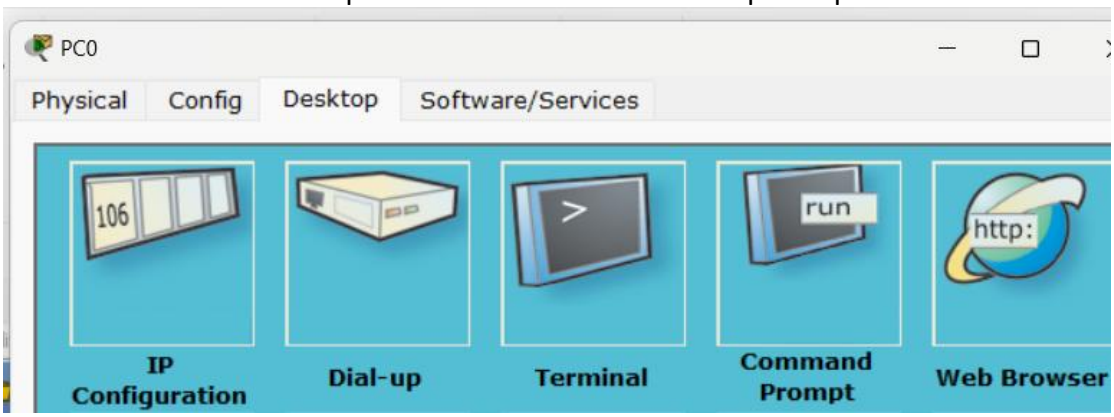
Click on Router 1. Below ROUTING click static. Then fill the other end network address and subnet mask. As the Router 0 can reach network 192.168.1.0 through Router 0, the next hop is the WAN address of Router 0.



Click Add.

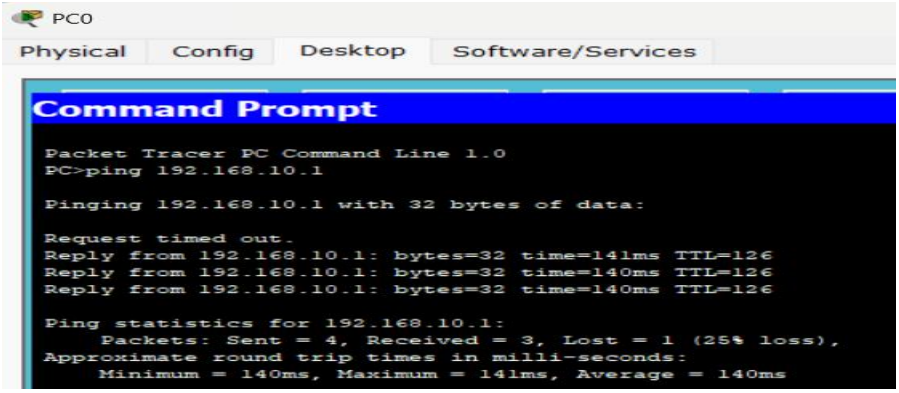
7. Check if routing configuration is successful.

Click on PC0. Go to Desktop tab. Click on Command Prompt to open.



From the PC0 command prompt ping to Server 0.

Ping to Server 0 from PC0 is successful.



Similarly try to ping to Server 1 and PC2 IP addresses. Check if you get reply as shown above. Also try accessing Server 0 and Server 1 websites from PC0 and PC1.

Thus the connectivity between 2 networks is established.

8. **Configure access list on Router 0.**

As the requirement is to control access for PC0 and PC1, we are configuring the access list on Router 0.

We can configure access-list on Router 1 also. But then the packets will travel through Router 0 and on WAN link and then get dropped on Router 1. This will unnecessarily increase overhead on Router 0 and also unwanted traffic on WAN link.

Here we create extended access list. The default behaviour of access list is to block the traffic. Thus we will add only the allow rules in the access list.

1. PC0 can access website on Server 0. (add)
2. PC0 can not access website on Server 1.
3. PC1 can access website on Server 1 (add)
4. PC1 can not access website on Server 0.
5. PC0 can ping to PC2 and Server 1. (add)

Click on Router 0. Click the CLI tab.

If you get **router>** prompt, type **enable** and press Enter. This will give you router# prompt. Type **conf t.** this will give you **router(config)#** prompt. (If you get any other prompt like **router(config-if)#** then type exit to come back to **router(config)#** prompt.)

Following command will allow PC0 to access website on Server 0.

access-list 100 permit tcp host 192.168.1.1 host 192.168.10.1 eq www

In the above command **100** is the access list number. As we are specifying a single IP address in the source and destination we need to type **host** before IP address. If you specify network address then typing **host** is not required. The **eq www**, matches the tcp port 80 which is http port.

Following command will allow PC1 to access website on Server 1.

access-list 100 permit tcp host 192.168.1.10 host 192.168.10.10 eq www

Following command will allow PC0 to ping to Server 1. But only ping ICMP traffic is allowed. No other ICMP traffic is allowed.

access-list 100 permit icmp host 192.168.1.1 host 192.168.1.10 echo

Following command will allow PC0 to ping to PC2. But only ping ICMP traffic is allowed. No other ICMP traffic is allowed.

access-list 100 permit icmp host 192.168.1.1 host 192.168.1.20 echo

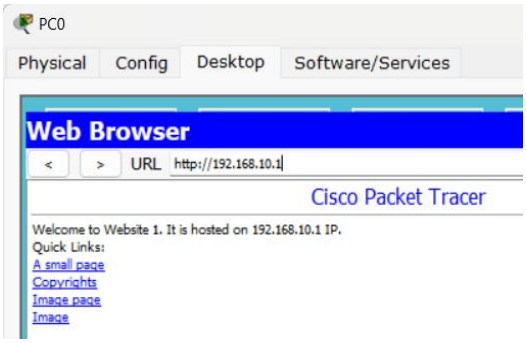
Now apply the access list to the interface. The IP address mentioned first in the above command are source IP's. These IP's will be in the source field of IP packet when the packet comes in from the FastEthernet0/0 interface of the Router 0. Thus the access list needs to be applied to that interfae.

int fa0/0
ip access-group 100 in
This is shown in the following screen shot.

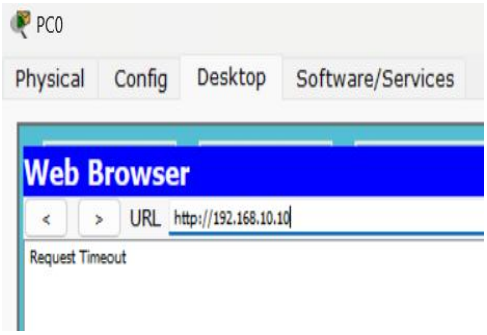
```
Router(config)#int fa0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#
```

9. Verify the access-list configuration
Click PC0. Go to Desktop. Open Browser and access websites on Server 0 and Server1.

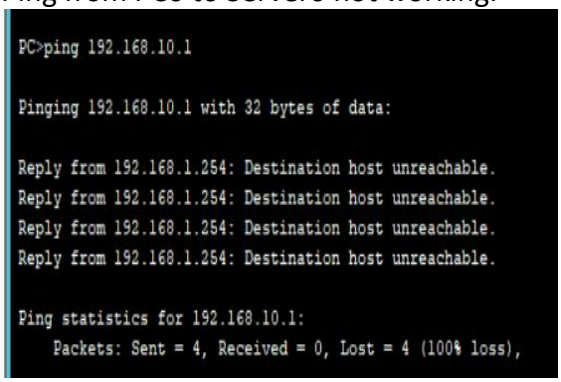
PC0 is able to access Server0 website.



PC0 not able to access Server1 website.



Ping from PC0 to Server0 not working.



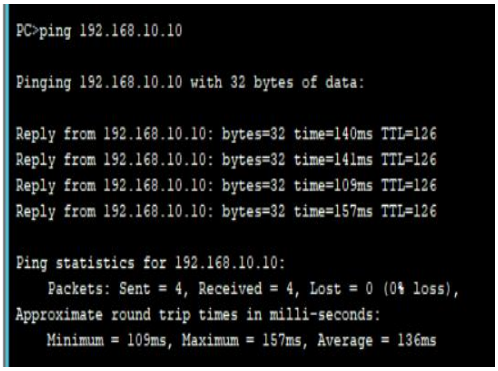
```
PC>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.
Reply from 192.168.1.254: Destination host unreachable.

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ping from PC0 to Server1 working



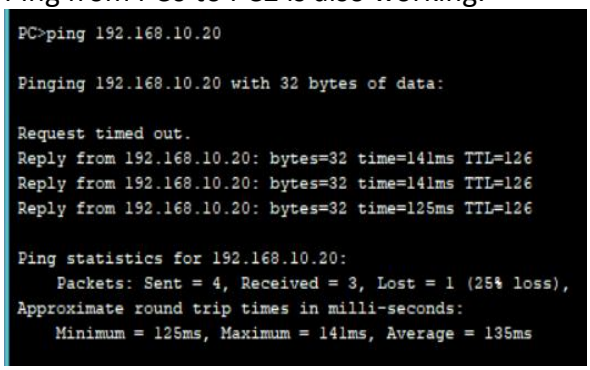
```
PC>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.10.10: bytes=32 time=140ms TTL=126
Reply from 192.168.10.10: bytes=32 time=141ms TTL=126
Reply from 192.168.10.10: bytes=32 time=109ms TTL=126
Reply from 192.168.10.10: bytes=32 time=157ms TTL=126

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 109ms, Maximum = 157ms, Average = 136ms
```

Ping from PC0 to PC2 is also working.



```
PC>ping 192.168.10.20

Pinging 192.168.10.20 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.20: bytes=32 time=141ms TTL=126
Reply from 192.168.10.20: bytes=32 time=141ms TTL=126
Reply from 192.168.10.20: bytes=32 time=125ms TTL=126

Ping statistics for 192.168.10.20:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 125ms, Maximum = 141ms, Average = 135ms
```

Similarly test from PC1 that the required access is working.

<u>This is how you have successfully configured a simple access list on the Cisco Router.</u>