LAB 8

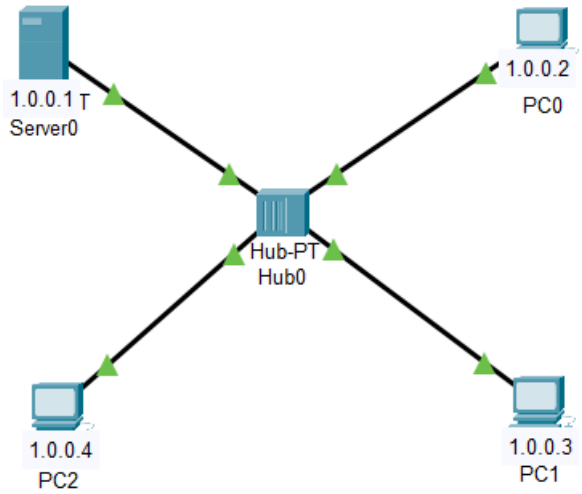
Firewall Implementation, Router Access Control List (ACL)

Objective:

- To understand the router firewall and Access Control Lists (ACLs).

Firewall Configuration:

To configure Firewall three PCs and a server is connected to a hub as shown in the figure below:

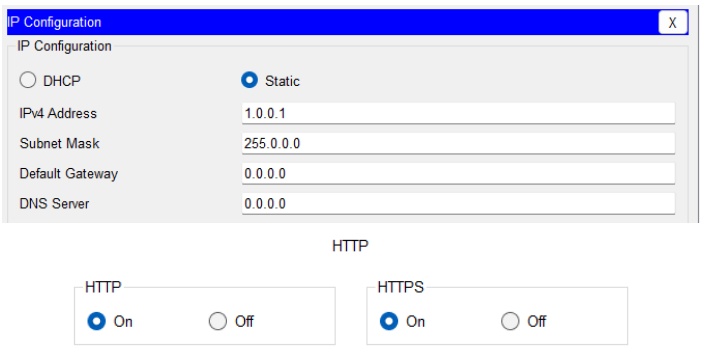


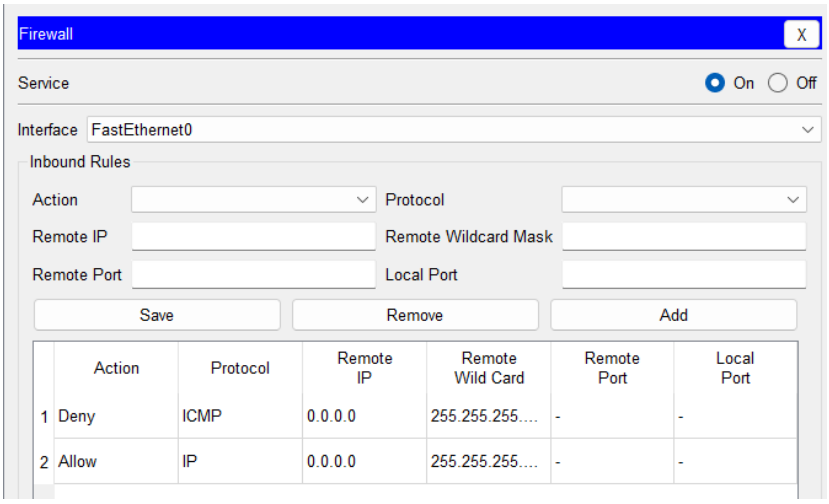
Configuration:

Connect the PCs and server to the hub.

For server:

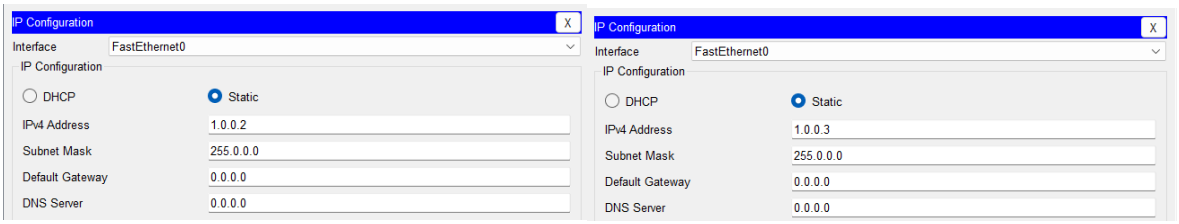
- Double click on the server and go to desktop.
- Then set 1.0.0.1 as the IP Address for the server.
- Go to services and turn on HTTP and HTTPS.
- Click on firewall in the desktop and turn it on.
- Specify the rules as desired. Here IP is allowed whereas ICMP is Blocked.





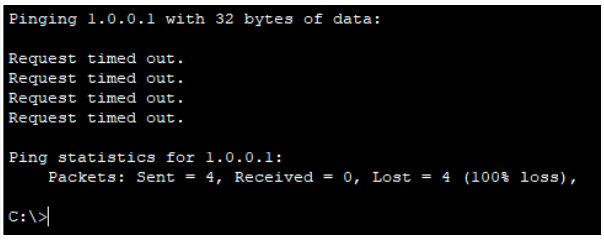
For PCs:

- Double click on the Pc and go to desktop.
- Then set the IP Address for the PC.
    - 1.0.0.2 For PC 0
    - 1.0.0.3 For PC 1
    - 1.0.0.4 For PC 2



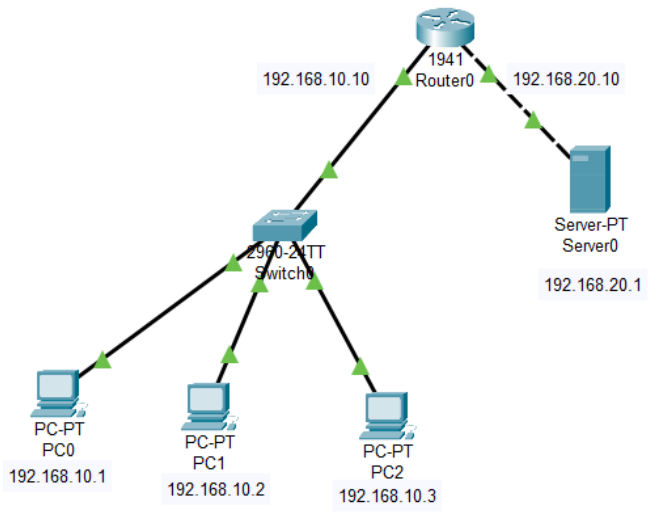
To test for proper configuration:

- Double click on any of the PC and go to desktop.
- Open Command prompt.
- Ping the server from any other PC in the network. If firewall is configured successfully Request will time out.
- Then open browser in any Pc and put the IP of the server the webpage will load.



ACL Configuration:

To configure Firewall three PCs and a server is connected to a hub as shown in the figure below:

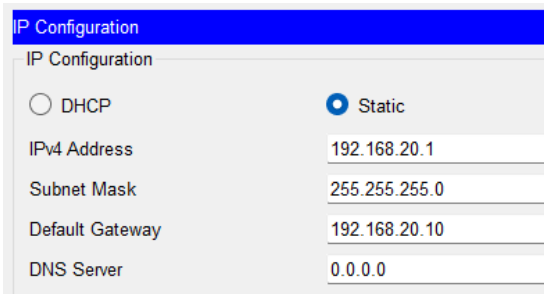


Configuration:

Connect the PCs to the switch and the connect it with the router. Then router is connected to the server.

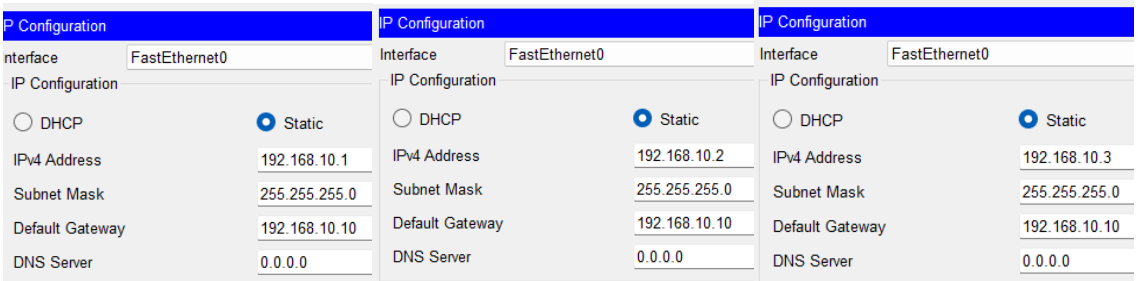
For server:

- Double click on the server and go to desktop.
- Set the IP address as 192.166.20.1 and the Gateway as 192.168.20.10.



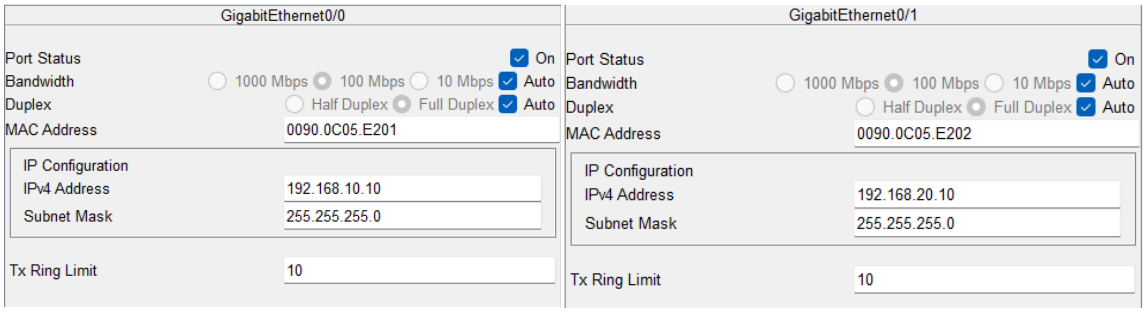
For PCs:

- Double click on PC and go to Desktop.
- Then set the IP address for the PC. The IP Address are:
  - 192.168.10.1 for PC0.
  - 192.168.10.2 for PC1.
  - 192.168.10.3 for PC2.



For Router:

- Double click on router and go to configure then Interfaces.
- Turn on GigabitEthernet 0/0 and set the IP as 192.168.10.10.
- Turn on GigabitEthernet 0/1 and set the IP as 192.168.20.10.
- Go to CLI and type the following:
    1. Ip access-list standard 10
    2. Deny host 192.168.10.2
    3. Permit any
    4. Exit




```
Router(config)#ip access-list standard 10
Router(config-std-nacl)#deny host192.168.10.2
                                 ^
% Invalid input detected at '^' marker.

Router(config-std-nacl)#deny host 192.168.10.2
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
```

```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip access-group 10 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ac
Standard IP access list 10
    10 deny host 192.168.10.2
    20 permit any
```

To test for proper configuration:

- Double click on any of the PC and go to desktop.
- Open Command prompt.
- Ping the server form the PC. If the Configuration is successful then host will be unreachable when pinging form PC 1. Other PCs will get proper reply.