Practical 8
Configure basic security features for networks

Aim: Understanding and Configuring basic security features for networks

Theory:

Basic security features for networks are foundational measures that are essential for securing a network and its data. These features help protect against common threats and vulnerabilities.
Here are some key basic security features for networks:

1. Firewalls: Firewalls act as a barrier between a trusted internal network and untrusted external networks (like the internet). They control incoming and outgoing network traffic based on an organization's previously established security policies. Firewalls can be hardware-based or software-based.

2. Network Segmentation: Divide the network into segments or VLANs (Virtual LANs) to isolate different parts of the network from each other. This prevents lateral movement of threats within the network.

3. Strong Authentication: Require strong and unique passwords or passphrases for all devices and user accounts. Implement multi-factor authentication (MFA) whenever possible to add an extra layer of security.

4. Encryption: Use encryption protocols like HTTPS, SSL/TLS, and VPNs to protect data in transit. Also, encrypt sensitive data at rest to safeguard it from unauthorized access.

5. Intrusion Detection and Prevention Systems (IDPS): Deploy IDPS to monitor network traffic for signs of suspicious or malicious activity and take action to prevent or mitigate threats.

6. Patch Management: Regularly update and patch network devices, operating systems, and software to address known vulnerabilities. Vulnerability management is a critical component of network security.

7. Security Policies: Establish and enforce security policies and procedures. These policies should cover access control, data handling, incident response, and more.

8. Network Monitoring and Logging: Continuously monitor network traffic and maintain logs of network activities. Analyze logs to detect and respond to security incidents.

9. User Education and Awareness: Educate users about security best practices, including how to recognize phishing attempts, avoid downloading malicious attachments, and report suspicious activity.

10. Backup and Recovery: Regularly back up critical data and test the restoration process. Having reliable backups is crucial for recovering from data breaches or system failures.

11. Access Control: Implement role-based access control (RBAC) to ensure that users have the minimum necessary privileges to perform their tasks. Restrict access to sensitive data and systems.

12. Security Updates: Stay informed about security threats and vulnerabilities by subscribing to security bulletins and alerts. Promptly apply security updates and patches to address new threats.

13. Denial of Service (DoS) Protection: Implement DoS protection mechanisms to mitigate or prevent attacks that can overwhelm network resources.

14. Perimeter Security: Secure the network perimeter by configuring routers and switches to filter traffic and block unauthorized access attempts.

These basic security features provide a strong foundation for network security. Organizations often build upon these foundational measures with more advanced security technologies and practices to address specific threats and risks relevant to their environment.

Topology:

For the present case we use the Access Control Lists, to demonstrate one of the basic security features
Consider the following topology

	Interface	IP address	Subnet Mask	Gateway	Wildcard Mask
PC0	FastEthernet0	192.168.1.2	255.255.255.0	192.168.1.1	0.0.0.255
PC1	FastEthernet0	192.168.1.3			
PC2	FastEthernet0	192.168.1.4			
PC3	FastEthernet0	192.168.2.2		192.168.2.1	
PC4	FastEthernet0	192.168.2.3			
PC5	FastEthernet0	192.168.2.4			
Router0	FastEthernet0/0	192.168.1.1			
	FastEthernet0/1	192.168.2.1			
	Ethernet0/1/0	192.168.3.1			
Server	FastEthernet0	192.168.3.2		192.168.3.1	

Note:
We use Router 1840; by default it has 2 interfaces

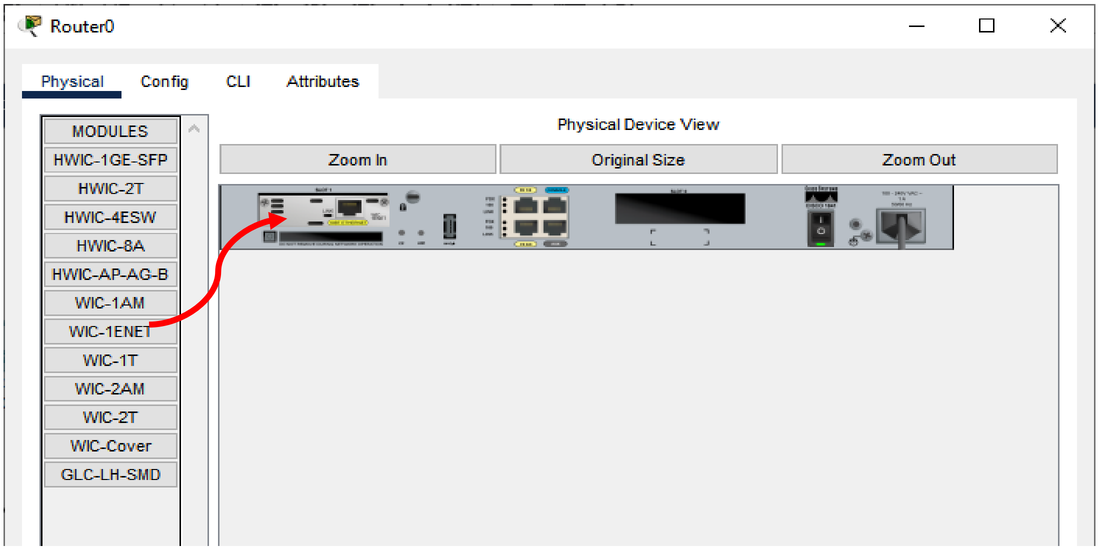
a) FastEthernet0/0 and
b) FastEthernet0/1

And we need to add an extra interface Ethernet0/1/0.

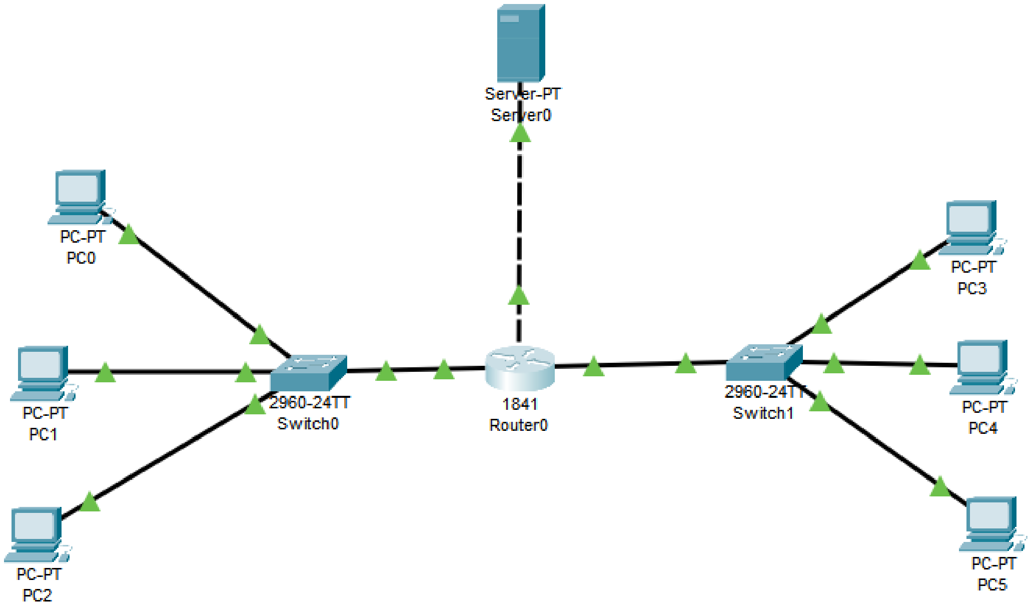
It is done as follows,

a) Click on Router0
b) Turn it OFF
c) Select WC-1ENET interface
d) Drag and drop in the slot and
e) Turn ON the Router

This is how insert the WC-1ENET interface in Router0

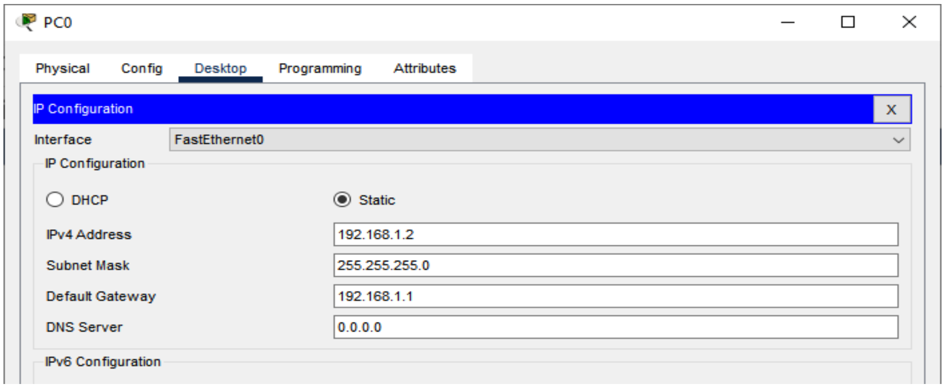


We implement the given topology in Cisco Packet Tracer



Now we configure the components

PC0:



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

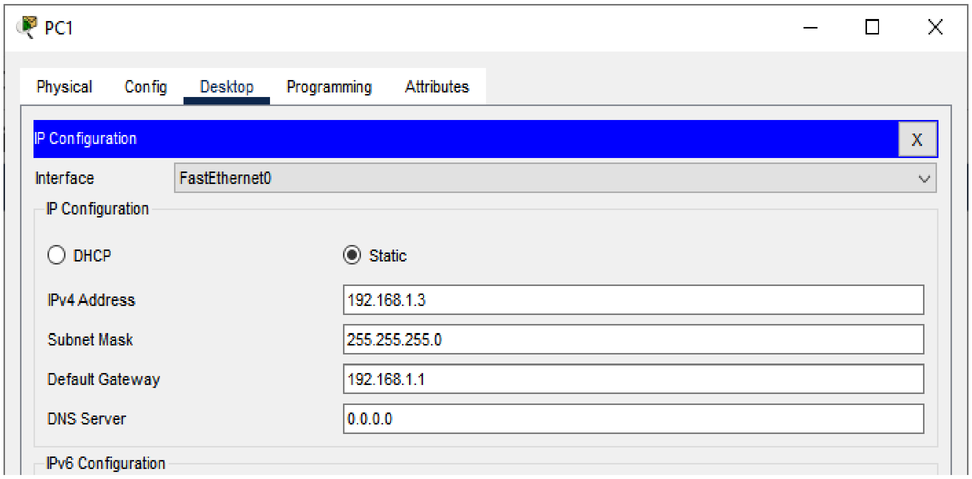
IPv4 Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

PC1:



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

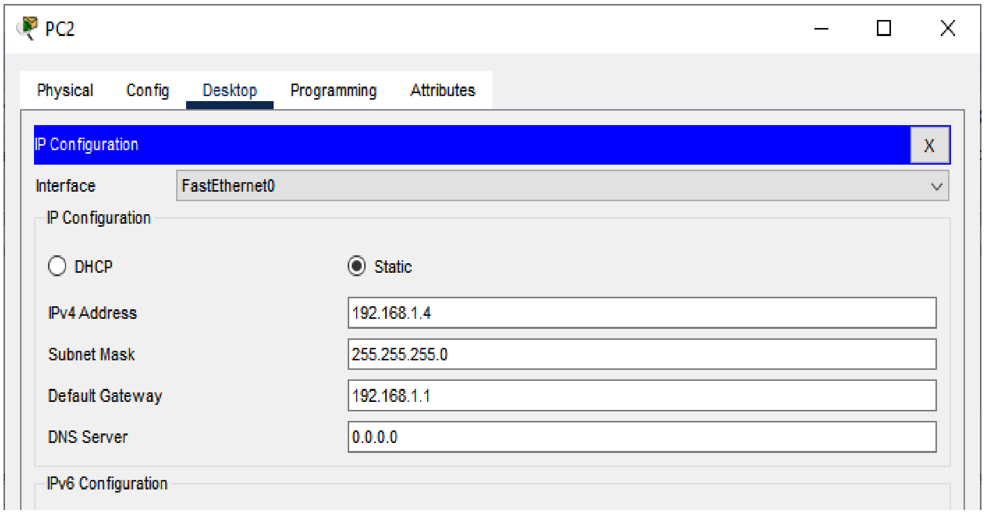
IPv4 Address: 192.168.1.3

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

PC2:



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

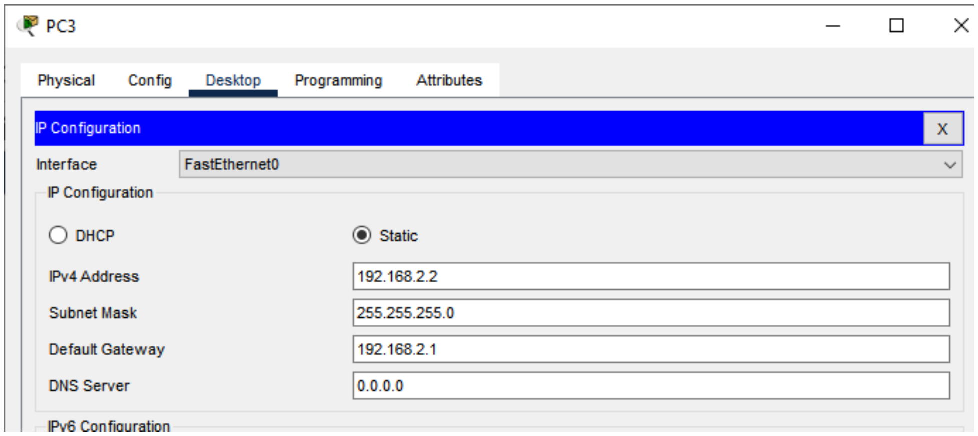
IPv4 Address: 192.168.1.4

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

PC3:



IP Configuration

Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address 192.168.2.2

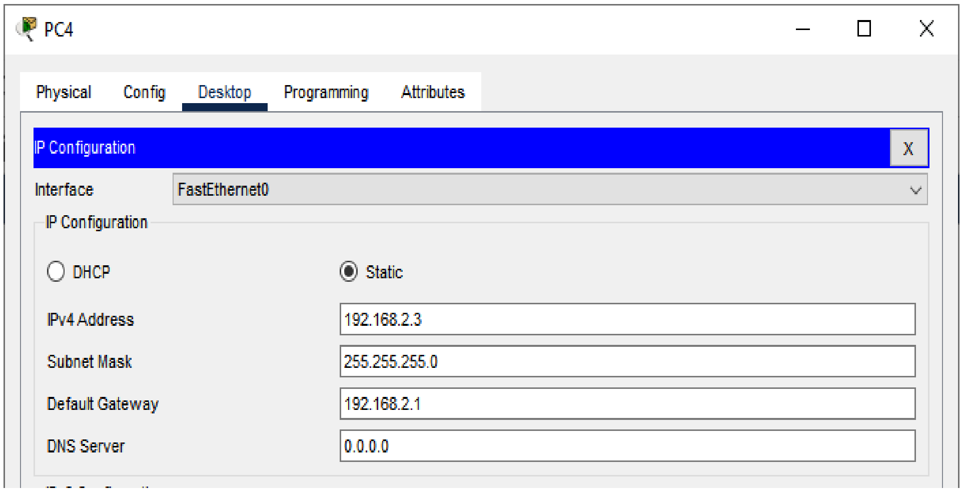
Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server 0.0.0.0

IPv6 Configuration

PC4:



IP Configuration

Interface FastEthernet0

IP Configuration

○ DHCP ● Static

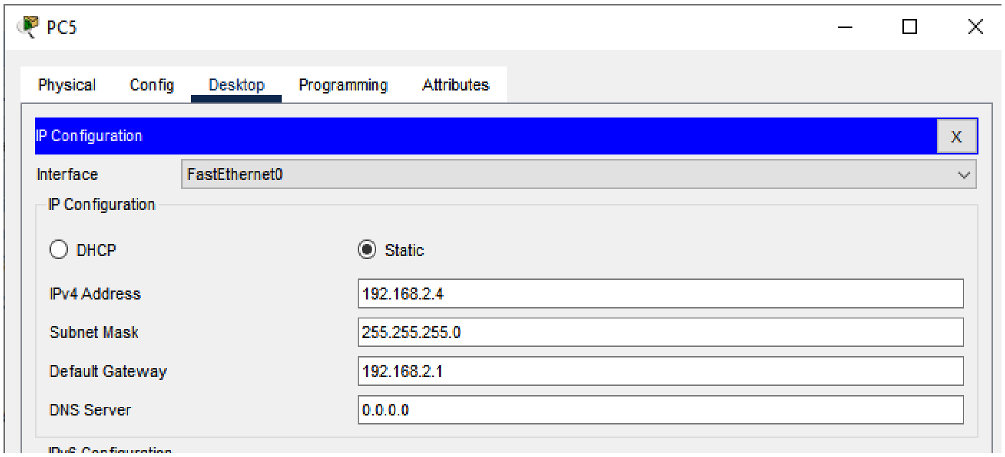
IPv4 Address 192.168.2.3

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server 0.0.0.0

PC5:



IP Configuration

Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address 192.168.2.4

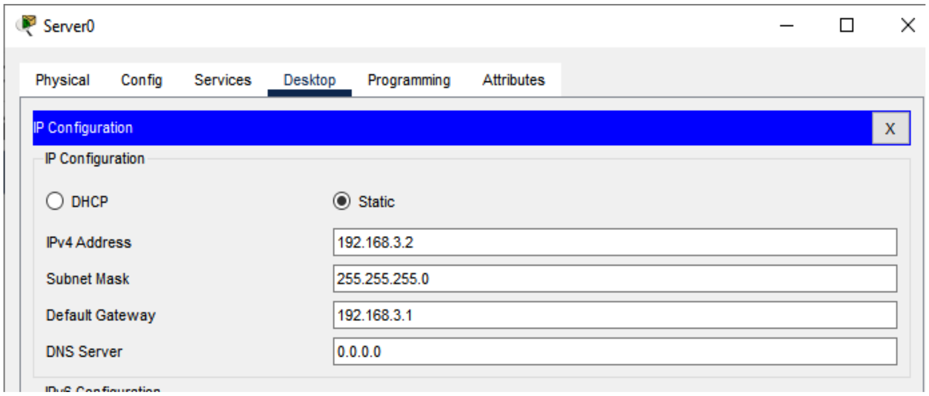
Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server 0.0.0.0

IPv6 Configuration

Server0:



IP Configuration

○ DHCP ● Static

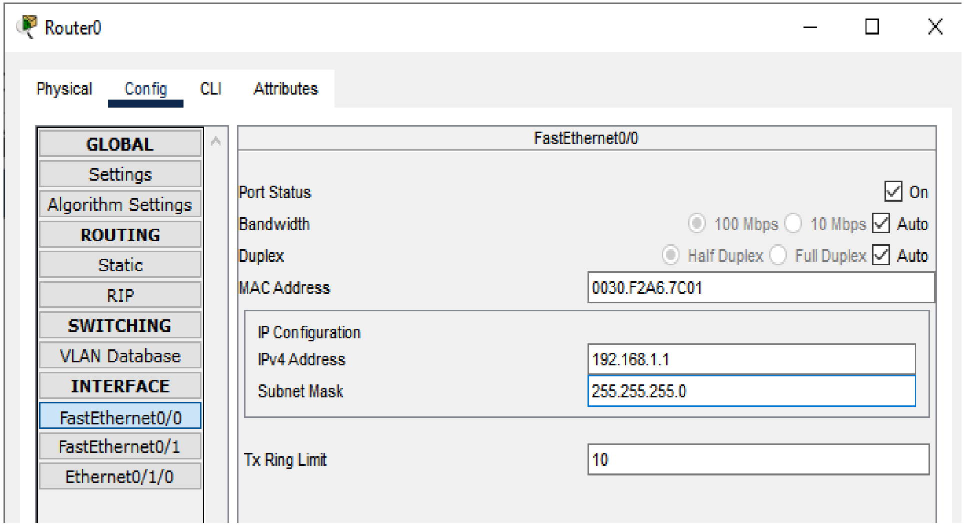
IPv4 Address: 192.168.3.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.3.1

DNS Server: 0.0.0.0

Router0: Interface FastEthernet0/0



FastEthernet0/0

Port Status ☑ On

Bandwidth ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ○ Full Duplex ☑ Auto

MAC Address: 0030.F2A6.7C01

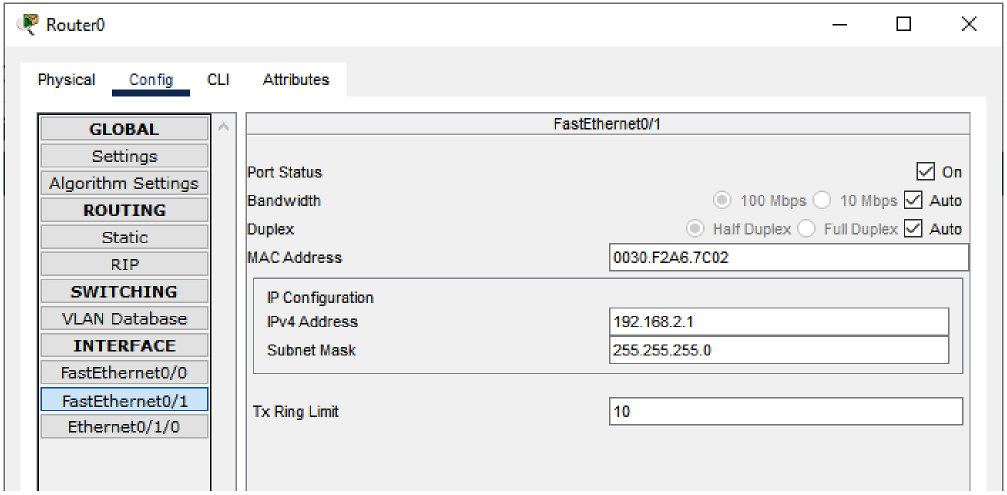
IP Configuration

IPv4 Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Router0: Interface FastEthernet0/1



FastEthernet0/1

Port Status ☑ On

Bandwidth ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ○ Full Duplex ☑ Auto

MAC Address: 0030.F2A6.7C02

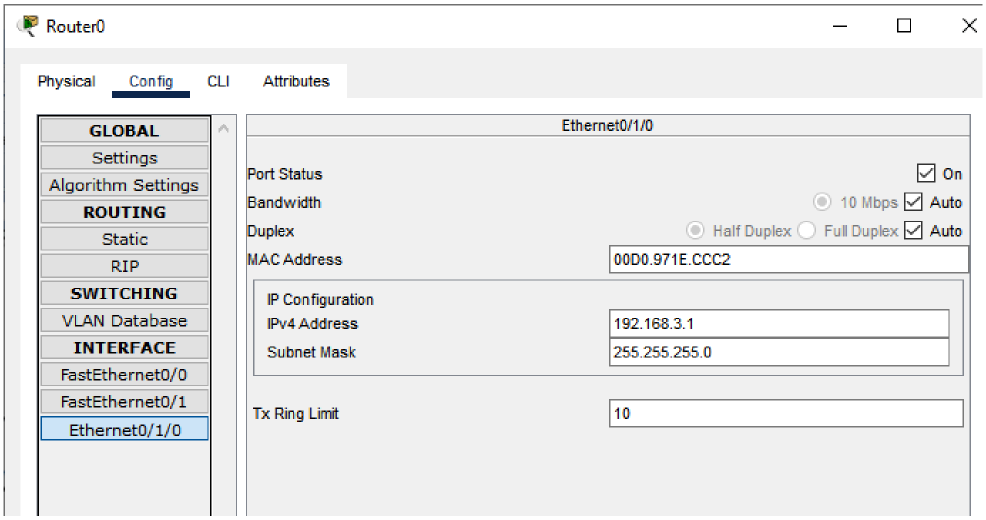
IP Configuration

IPv4 Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Router0: Interface Ethernet0/1/0



Router0

Physical Config CLI Attributes

GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Ethernet0/1/0

Ethernet0/1/0

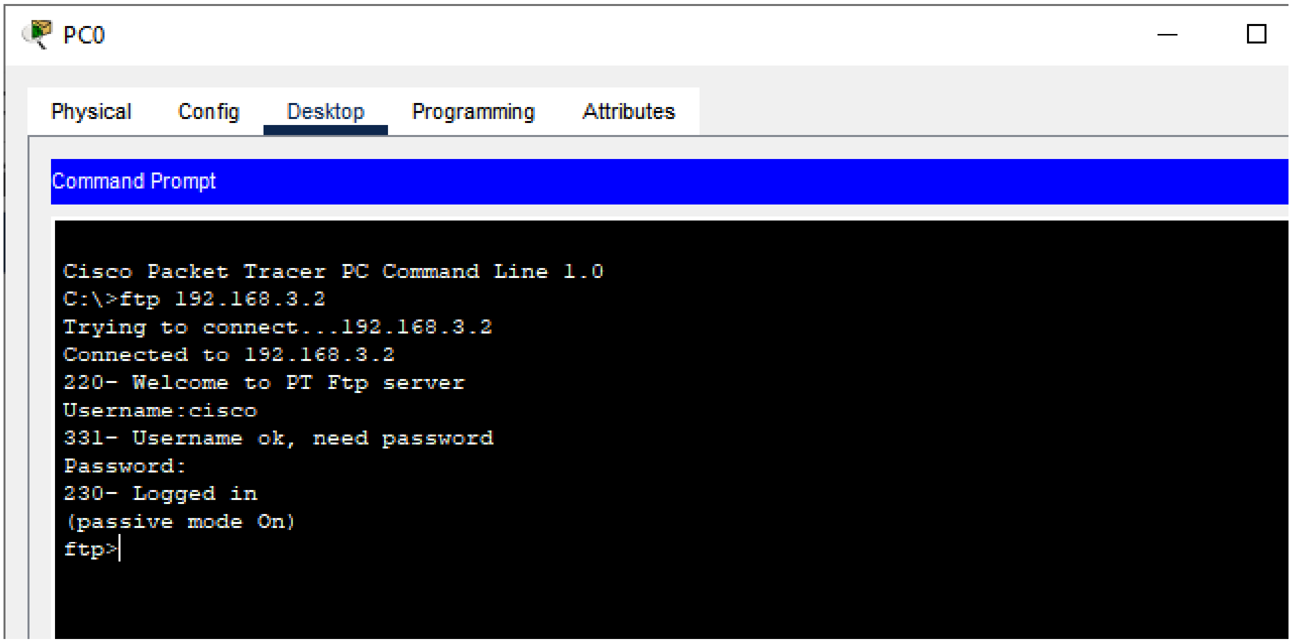
Port Status ☑ On
Bandwidth ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ○ Full Duplex ☑ Auto
MAC Address 00D0.971E.CCC2

IP Configuration
IPv4 Address 192.168.3.1
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Checking the ftp Service:

From PC0: (Username: cisco: Password: cisco)



PC0

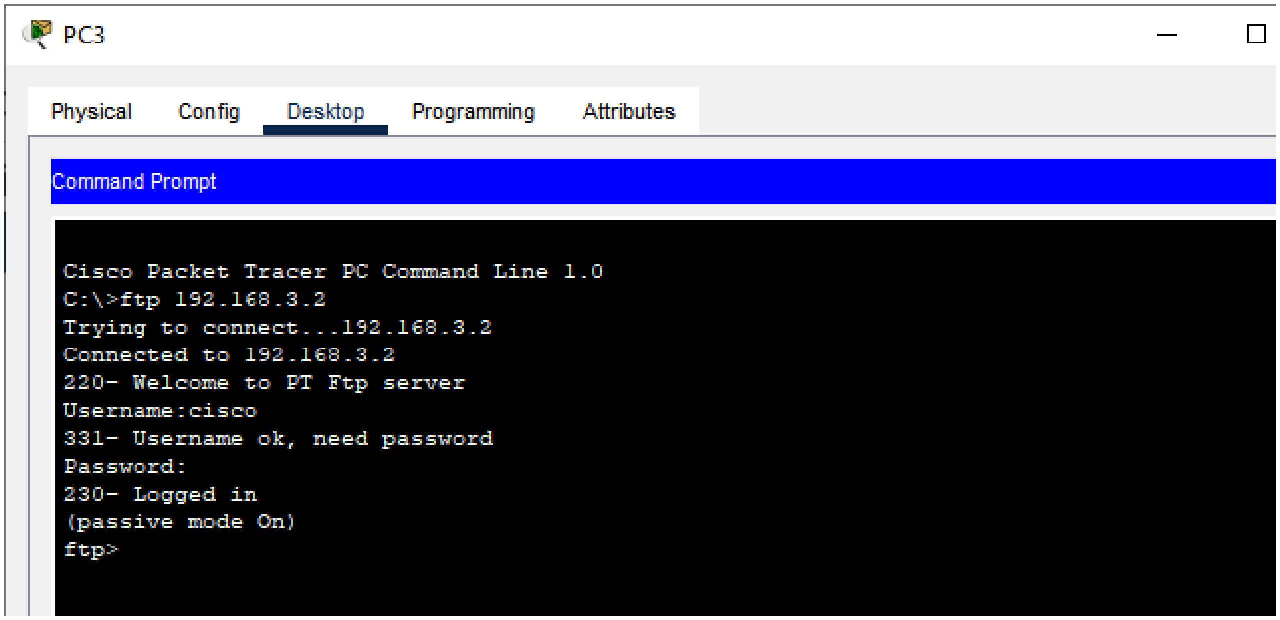
Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.3.2
Trying to connect...192.168.3.2
Connected to 192.168.3.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

We see that ftp service is accessible to PC0 and all the PCs in its network

From PC3: (Username: cisco: Password: cisco)



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.3.2
Trying to connect...192.168.3.2
Connected to 192.168.3.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

We see that ftp service is accessible to PC3 and all the PCs in its network

Configuring ACLs: Now we configure the ACLs so that ftp service is available to all PCs in one network and is not available to the PCs in the other network

We configure so that PC0 – PC2 get the ftp Service while PC3-PC5 do not get the service

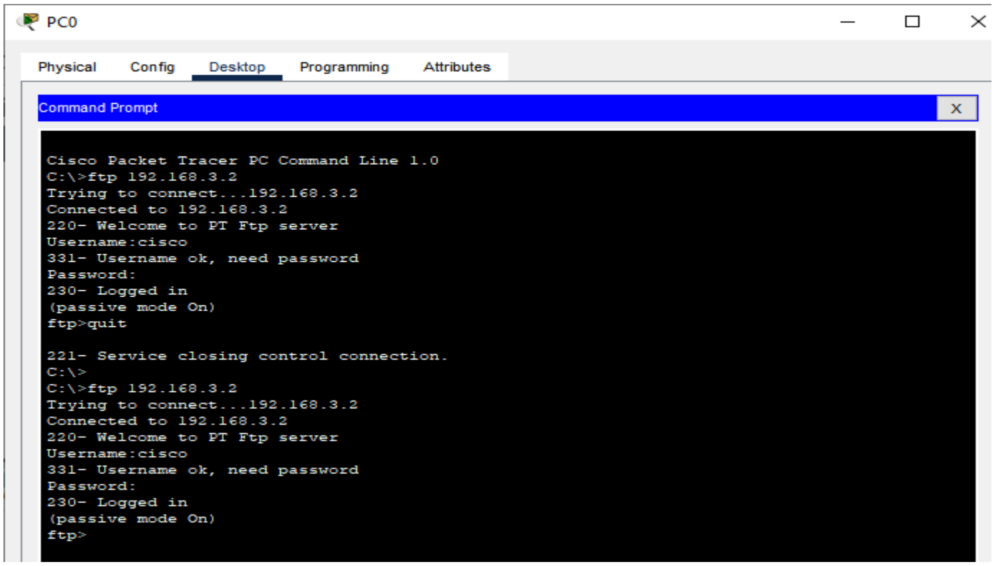
Configuring Router0 for ACLs:

We enter the following commands in the CLI mode of Router0

```
Router>
Router>enable
Router#
Router#configure terminal
Router(config)#access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq ftp
Router(config)#access-list 100 deny tcp 192.168.2.0 0.0.0.255 any eq ftp
Router(config)#interface ethernet 0/1/0
Router(config-if)#
Router(config-if)#ip access-group 100 out
Router(config-if)#
```

After configuring the Router0 for ACL, we check the ftp service on PC0 (network 1) and PC3(network 2)

PC0:

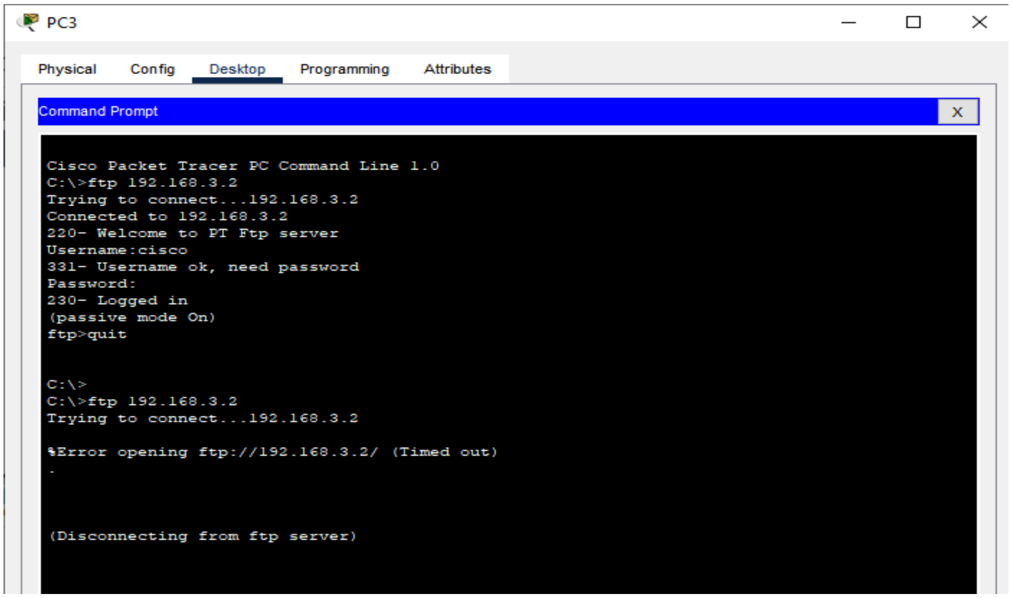


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.3.2
Trying to connect...192.168.3.2
Connected to 192.168.3.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit

221- Service closing control connection.
C:\>
C:\>ftp 192.168.3.2
Trying to connect...192.168.3.2
Connected to 192.168.3.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

As expected PC0 and all PCs in the network will be ALLOWED access to ftp service

PC3:



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.3.2
Trying to connect...192.168.3.2
Connected to 192.168.3.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit


C:\>
C:\>ftp 192.168.3.2
Trying to connect...192.168.3.2

%Error opening ftp://192.168.3.2/ (Timed out)
.



(Disconnecting from ftp server)
```

As expected PC3 and all PCs in the network will be DENIED access to ftp service

Video demonstration of the given Practical, scan the QR code

https://youtu.be/OdV7dYVr-Ug