

Secure the Management Plane

Aim: To Secure the management plane using various strategies

Theory: The management plane is responsible for managing a network device — such as configuring settings, monitoring status, and maintaining security. It allows administrators to communicate with the router or switch through command-line interfaces (CLI) or graphical interfaces.

Examples of management plane protocols:

- Telnet (insecure, plaintext)
- SSH (secure)
- SNMP
- HTTP/HTTPS
- Console/VTY access

The management plane is a critical attack surface. If compromised, attackers can:

- View or change device configurations
- Shut down interfaces
- Redirect traffic
- Launch attacks on other devices

Hence, securing it is essential for protecting the entire network infrastructure.

Methods to Secure the Management Plane

1. Use Secure Access Protocols

Replace insecure protocols like Telnet with SSH, which provides encrypted access to the CLI.

2. Implement User Authentication

Configure local usernames and passwords, and set privilege levels to limit what users can do.

3. Use Access Control Lists (ACLs)

Limit access to management interfaces by allowing only authorized IP addresses to connect.

4. Configure Strong Passwords & Encryption

Use `'enable secret'`, `'service password-encryption'`, and avoid weak or default credentials.

5. Disable Unused Services

Turn off services like CDP, HTTP, FTP, and bootp that are not in use to reduce the attack surface.

6. Display Banner Warnings

Configure `'banner motd'` and `'banner login'` to display legal notices or warnings to deter unauthorized users.

7. Verify and Test the Setup

Always test your configuration using commands like ``show running-config``, ``show ip ssh``, ``show access-lists``, and attempt authorized and unauthorized access.

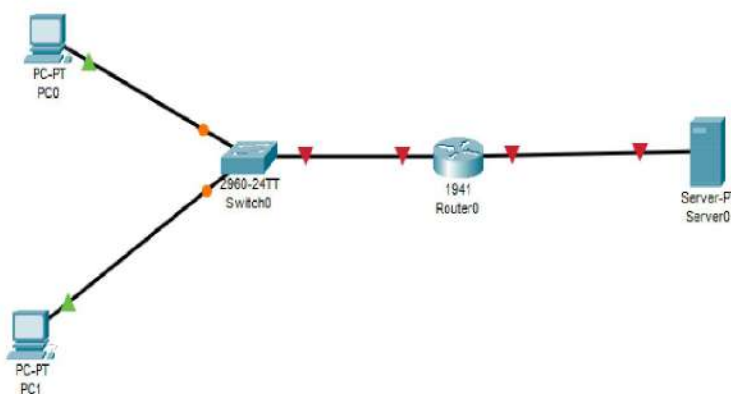
Real-World Importance

In enterprise networks, securing the management plane ensures:

- Only authorized personnel can make changes
- Devices are not compromised remotely
- Regulatory compliance with security standards (like ISO, NIST, etc.)
- Reduced risk of configuration tampering, insider threats, and cyber attacks

Topology:

We use the following topology

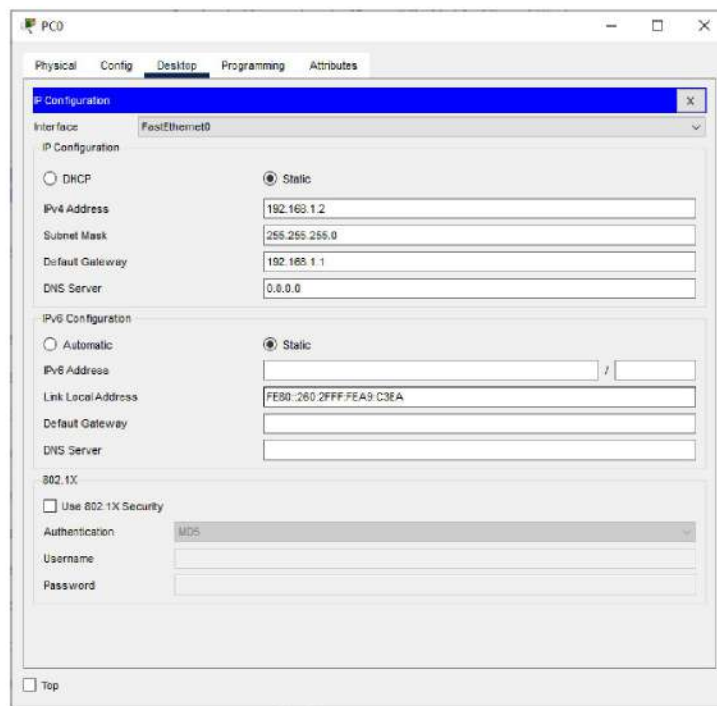


IP Addressing Table:

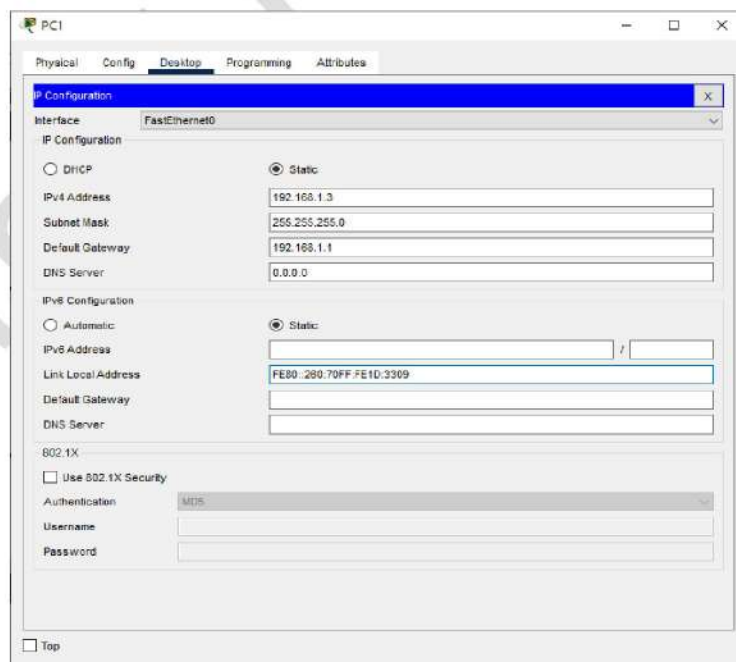
Device	Interface	IP Address	Subnet Mask	Gateway
PC0	FastEthernet0	192.168.1.2	255.255.255.0	192.168.1.1
PC1	FastEthernet0	192.168.1.3	255.255.255.0	192.168.1.1
Router	GigabitEthernet0/0	192.168.1.1	255.255.255.0	
Router	GigabitEthernet0/1	192.168.2.1	255.255.255.0	
Server	FastEthernet0	192.168.2.2	255.255.255.0	192.168.2.1

We Configure the IP addresses as follows

PC0 :



PC1 :



Server:

The screenshot shows the 'Server0' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is expanded, showing the following settings:

- 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:**
 - ☐ Automatic
 - ☒ Static
 - IPv6 Address: (empty)
 - Link Local Address: FE80::201:C7FF:FE48:BEDB
 - Default Gateway: (empty)
 - DNS Server: (empty)
- 802.1X:**
 - ☐ Use 802.1X Security
 - Authentication: MD5
 - Username: (empty)
 - Password: (empty)

At the bottom left, there is a 'Top' button.

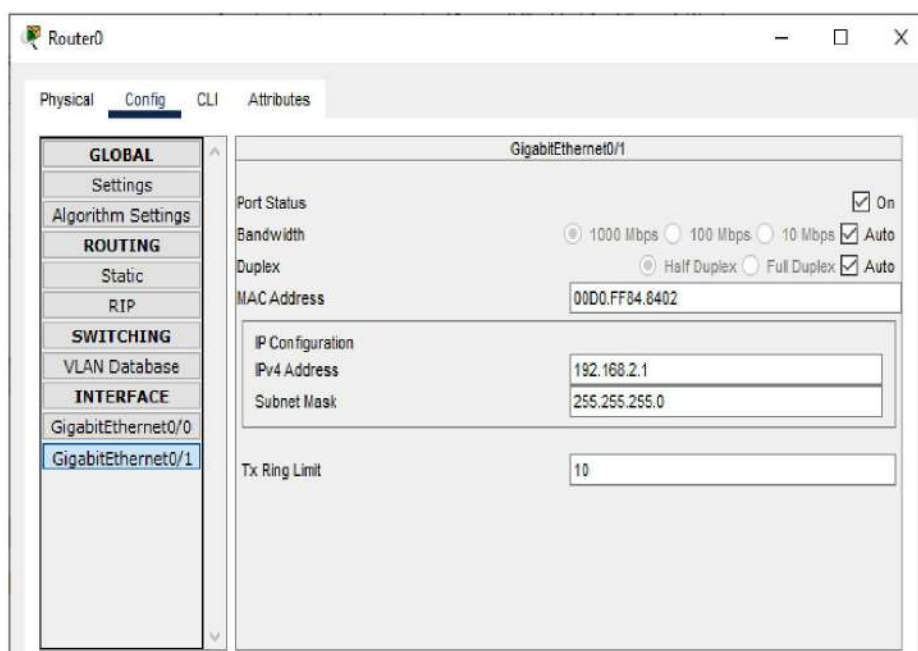
Router0: interface GigabitEthernet0/0

The screenshot shows the 'Router0' configuration window with the 'Config' tab selected. The 'GigabitEthernet0/0' interface is selected in the left sidebar. The configuration for this interface is shown on the right:

- Port Status:** ☒ On
- Bandwidth:** ☒ 1000 Mbps, ☐ 100 Mbps, ☐ 10 Mbps, ☒ Auto
- Duplex:** ☒ Half Duplex, ☐ Full Duplex, ☒ Auto
- MAC Address:** 00D0.FF84.8401
- IP Configuration:**
 - IPv4 Address: 192.168.1.1
 - Subnet Mask: 255.255.255.0
- Tx Ring Limit:** 10

The left sidebar shows a tree view with categories: GLOBAL, ROUTING, SWITCHING, and INTERFACE. Under INTERFACE, 'GigabitEthernet0/0' is selected.

Router0: interface GigabitEthernet0/1



Now we secure the management plane using the following steps

Step 1: Secure access to Router0 via SSH

```
Router>enable
Router#
Router#configure terminal
Router(config)#
Router(config)#hostname R1
R1(config)#
R1(config)#ip domain-name ismileacademy.com
R1(config)#
R1(config)#crypto key generate rsa
```

The name for the keys will be: R1.ismileacademy.com

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 2048

% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

```
R1(config)#ip ssh version 2
```

```
*Mar 1 0:25:48.611: %SSH-5-ENABLED: SSH 1.99 has been enabled
```



```
R1(config)#
R1(config)#ip ssh time-out 60
R1(config)#ip ssh authentication-retries 2
R1(config)#username admin privilege 15 secret smilehp
R1(config)#line vty 0 4
R1(config-line)#
R1(config-line)#transport input ssh
R1(config-line)#
R1(config-line)#login local
R1(config-line)#exit
R1(config)#
```

Step 2: Restrict Access to Router using access control list

```
R1(config)#access-list 10 permit 192.168.1.2
R1(config)#access-list 10 deny any
R1(config)#line vty 0 4
R1(config-line)#
R1(config-line)#access-class 10 in
R1(config-line)#exit
R1(config)#
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#
R1(config-if)#ip access-group 10 in
R1(config-if)#exit
R1(config)#
```

Step 3: Disable unused services in the Server

```
R1(config)#
R1(config)#ip access-list extended smile
R1(config-ext-nacl)#
R1(config-ext-nacl)#permit icmp host 192.168.1.2 host 192.168.2.2
R1(config-ext-nacl)#permit tcp host 192.168.1.2 host 192.168.2.2 eq 21
R1(config-ext-nacl)#permit tcp host 192.168.1.2 host 192.168.2.2 eq 22
R1(config-ext-nacl)#deny ip any host 192.168.2.2
R1(config-ext-nacl)#exit
R1(config)#
R1(config)#interface gigabitEthernet 0/1
R1(config-if)#
R1(config-if)#ip access-group smile out
R1(config-if)#exit
R1(config)#
```

Step 4: Configure Banner messages

```
R1(config)#banner motd b
```

Enter TEXT message. End with the character 'b'.

```
*****
```

```
* Unauthorized access is prohibited. Disconnect now! *
```

```
R1(config)#
```

```
R1(config)#banner login b
```

Enter TEXT message. End with the character 'b'.

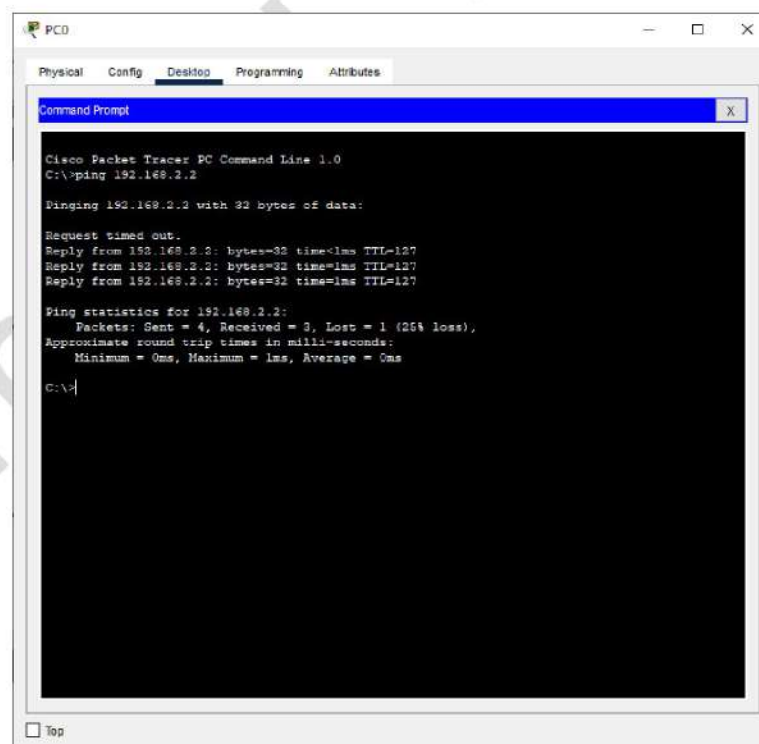
```
*****
```

```
* Authorized personnel only. Unauthorized users beware!*
```

The above steps complete the configuration part of Secure management plane, now we verify it as follows

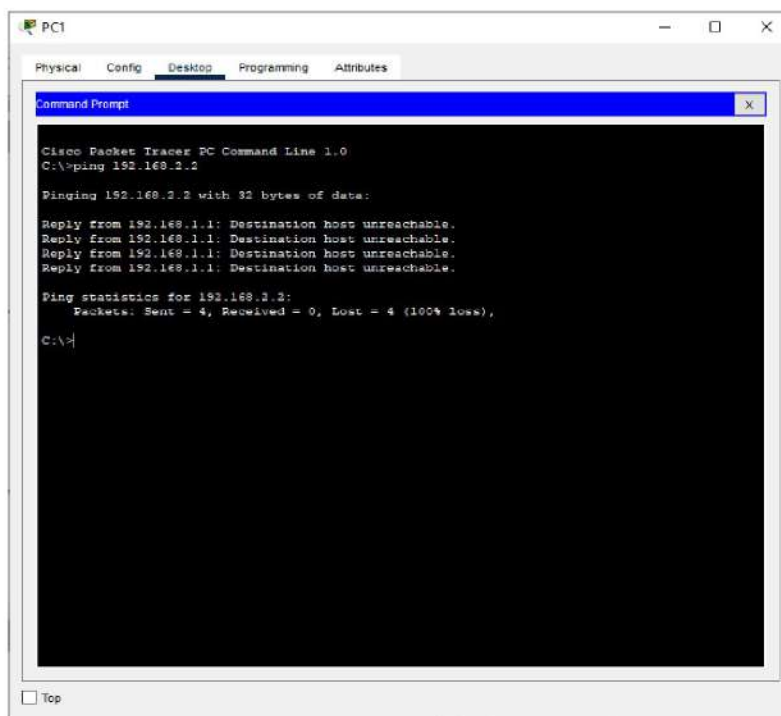
Output:

- 1) Checking for PING message
PC0: Checking for ping message from PC0 to Server



It is successful

PC1: Checking for ping message from PC1 to Server



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

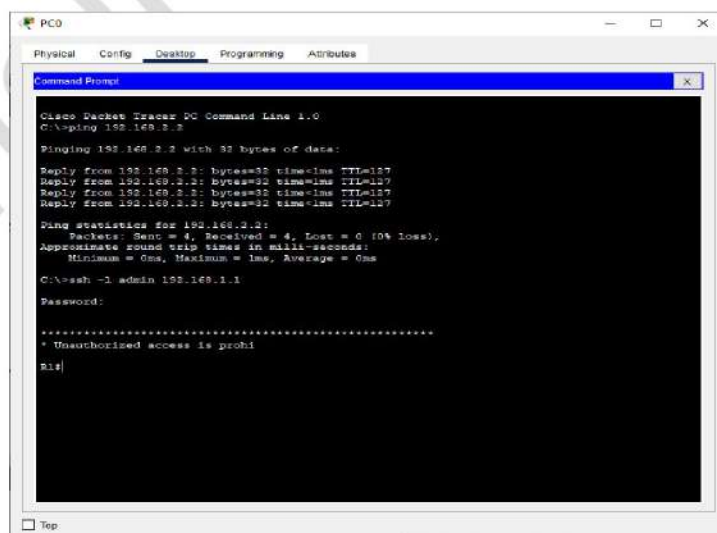
Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

It is failure

2) Checking for remote login using ssh

PC0:



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ssh -l admin 192.168.1.1

Password:
.....
* Unauthorized access is prohi
R1#
```

It is success

PC1:

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ssh -l admin 192.168.1.1

% Connection timed out; remote host not responding
C:\>
    
```

It is failure

3) Checking for ftp

PC0:

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=1ms TTL=127
Reply from 192.168.2.2: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ssh -l admin 192.168.1.1

Password:
*****
* Unauthorized access is prohibited.
*

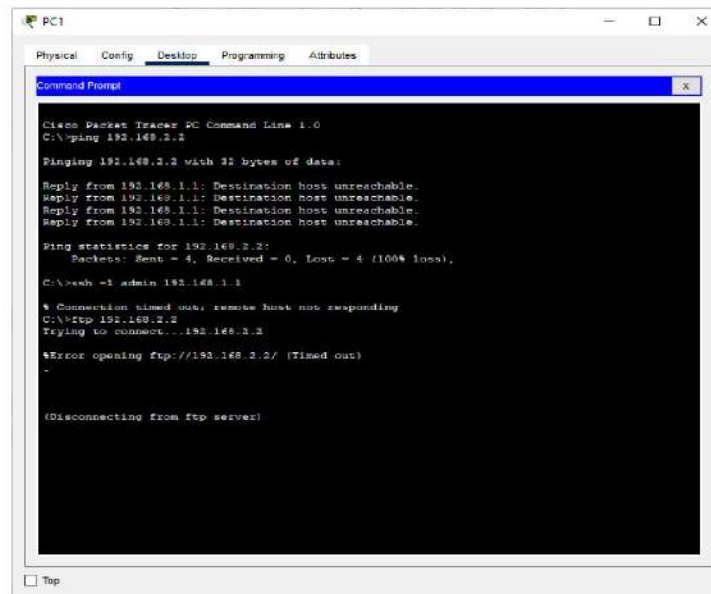
Hitquit
Translating "quit"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Hitquit

[Connection to 192.168.1.1 closed by foreign host]
C:\>ftp 192.168.2.2
Trying to connect...192.168.2.2
Connected to 192.168.2.2
220- Welcome to FT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
    
```

It is success

PC1:



```

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>push -i admin 192.168.1.1

* Connection timed out; remote host not responding
C:\>ftp 192.168.2.2
Trying to connect...192.168.2.2

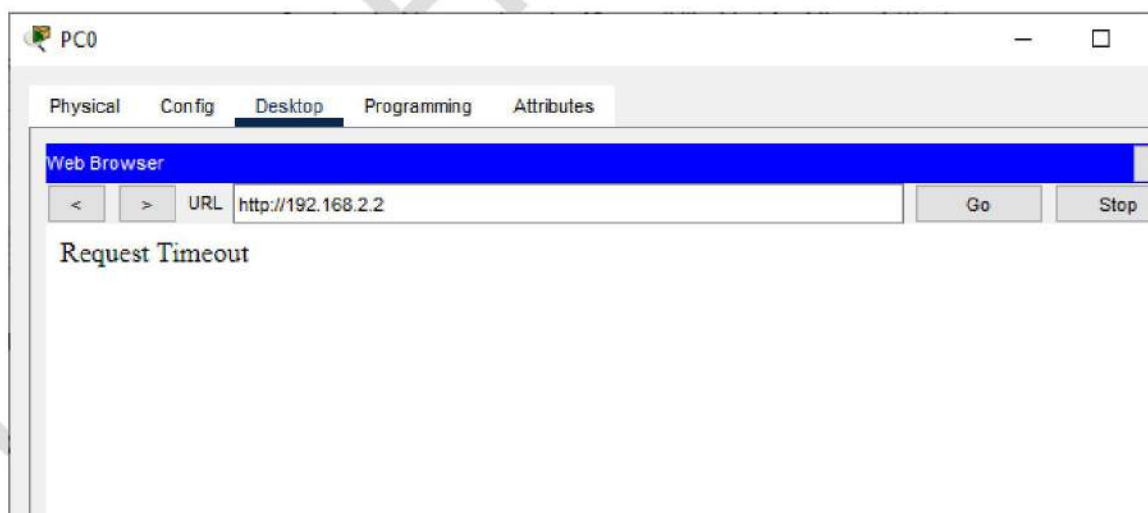
*Error opening ftp://192.168.2.2/ (Timed out)

(Disconnecting from ftp server)
    
```

It is failure

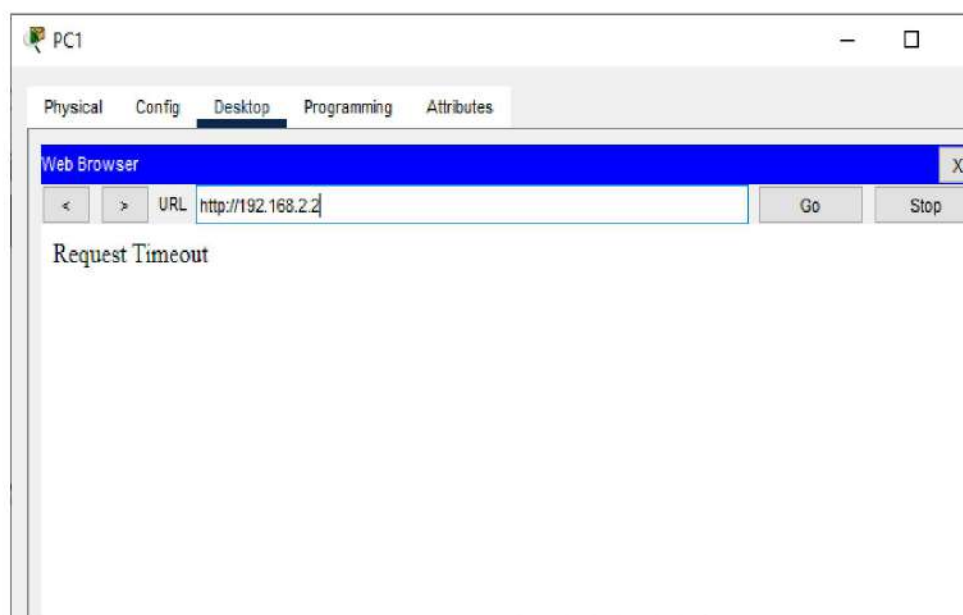
4) Checking for http:

PC0:



It does not connect and times out

PC1:



It does not connect and times out

The following things are configured while performing the Secure management plane and also verified

Test	PC1 (192.168.1.2)	PC2 (192.168.1.3)
Ping server	✓ Allowed	✗ Blocked
FTP to server	✓ Allowed	✗ Blocked
SSH to server	✓ Allowed	✗ Blocked
HTTP/HTTPS/DNS etc.	✗ Blocked	✗ Blocked

For Video demonstration of the given practical click on the link or scan the QR-code

<https://youtu.be/OL8lwe0sRLs>

