

Task: Homework 7

The screenshot displays a Cisco Packet Tracer simulation environment. The network topology consists of three 2600 RTT switches. The left switch is connected to PC-PT PC1 and PC-PT PC2. The middle switch is connected to PC-PT TFTP_SERVER and PC-PT WEB_SERVER. The right switch is connected to PC-PT TFTP_SERVER and PC-PT WEB_SERVER. The network is connected to the Internet via a 2600 RTT Switch. Two command prompt windows are open: one on PC1 showing a successful ping to 10.1.4.20, and one on the WEB_SERVER showing the IP configuration for FastEthernet0. A yellow sticky note is placed over the bottom right of the network diagram.

PC1 Command Prompt:

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 10.1.4.20

Pinging 10.1.4.20 with 32 bytes of data:
Reply from 10.1.4.20: bytes=32 time=1ms TTL=125
Reply from 10.1.4.20: bytes=32 time=1ms TTL=125
Reply from 10.1.4.20: bytes=32 time=1ms TTL=125
Reply from 10.1.4.20: bytes=32 time=1ms TTL=125

Ping statistics for 10.1.4.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

WEB_SERVER Command Prompt:

```
C:\>ipconfig

FastEthernet0 Connection (default port)

    Connection-specific DNS Suffix...: 
    Link-local IPv6 Address . . . . .: FE80::201:97FF:FE7C:6B37
    IPv6 Address . . . . . : 
    IPv4 Address . . . . . : 10.1.4.20
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.1.4.1

C:\>ipconfig

FastEthernet0 Connection (default port)

    Connection-specific DNS Suffix...: 
    Link-local IPv6 Address . . . . .: FE80::201:97FF:FE7C:6B37
    IPv6 Address . . . . . : 
    IPv4 Address . . . . . : 10.1.4.20
    Subnet Mask . . . . . : 255.255.255.0
    Default gateway . . . . . : 10.1.4.1

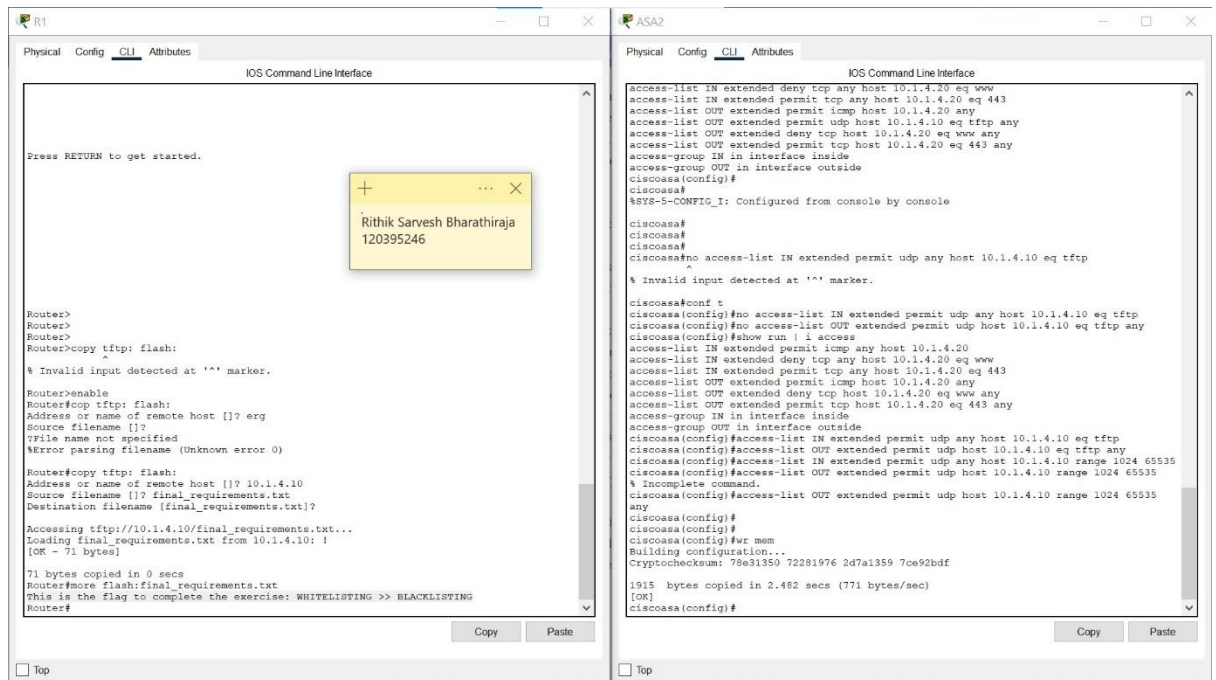
C:\>
```

Yellow Sticky Note:

Rithik Sarvesh Bharathiraja
120395246

[illegible]

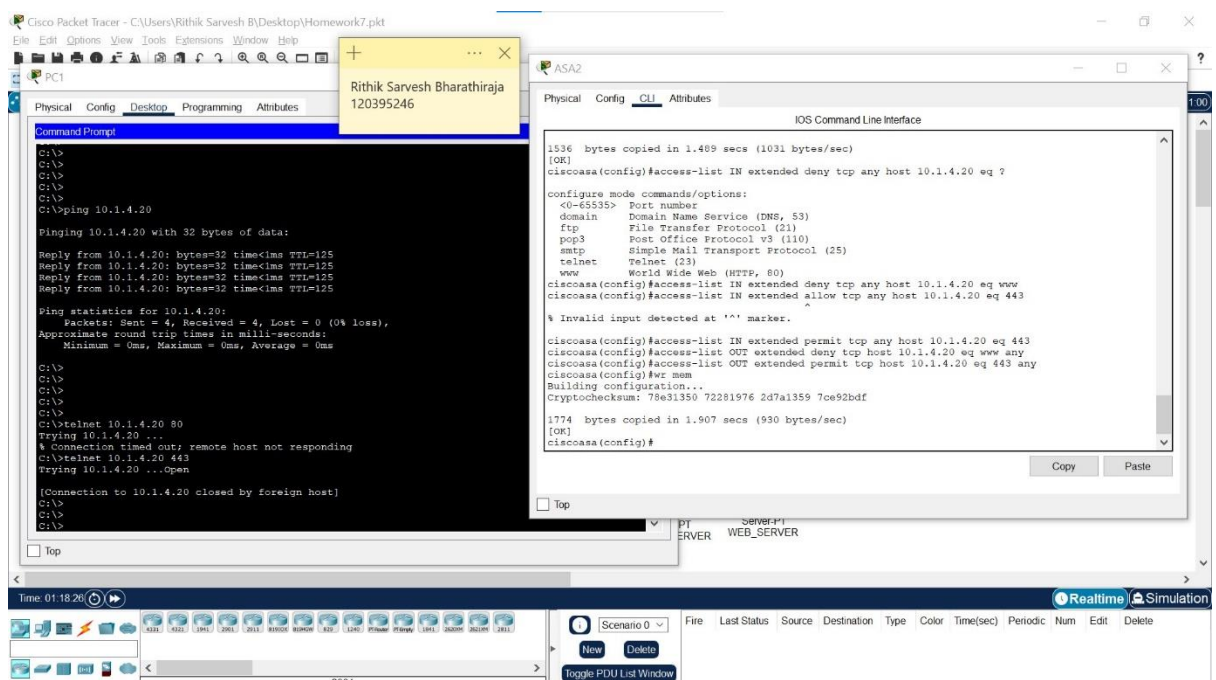
2)



TFTP uses port 69 for requests. Subsequently, communication is established via individually assigned port numbers (between 1024 and 65535), which the TFTP server sends to the requesting client in the form of TIDs (Transfer Identifiers). Thus, we have to add another rule including the range of port numbers from 1024 to 65535.

Access list is established to allow to-and-fro traffic between the client and the server. But the content of the data is not monitored by the firewall. Thus, malicious files can be sent in this way. As TFTP does not provide any authentication or encryption, which means anyone can access or modify the files during the transfer. Thus, implementing the rule doesn't do anything effective here.

3)



Positioning deny rules ahead of permit rules to ensure that traffic intended to be explicitly blocked is denied early in the evaluation process. This prevents any later permit rules from allowing potentially harmful traffic through. Placing permit rules after the deny rules to allow legitimate traffic through after unwanted traffic has been blocked. Thus, Traffic in Port 80 is denied first and then the traffic in port 443 is allowed.