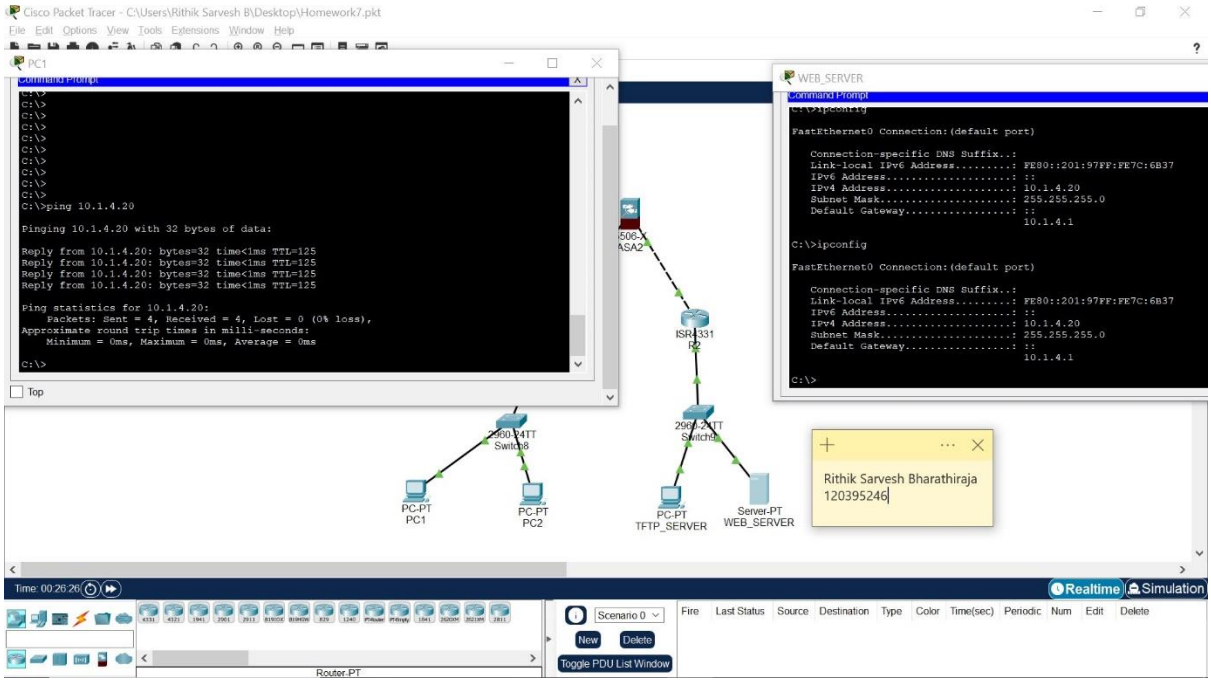
Name: Rithik Sarvesh Bharathiraja

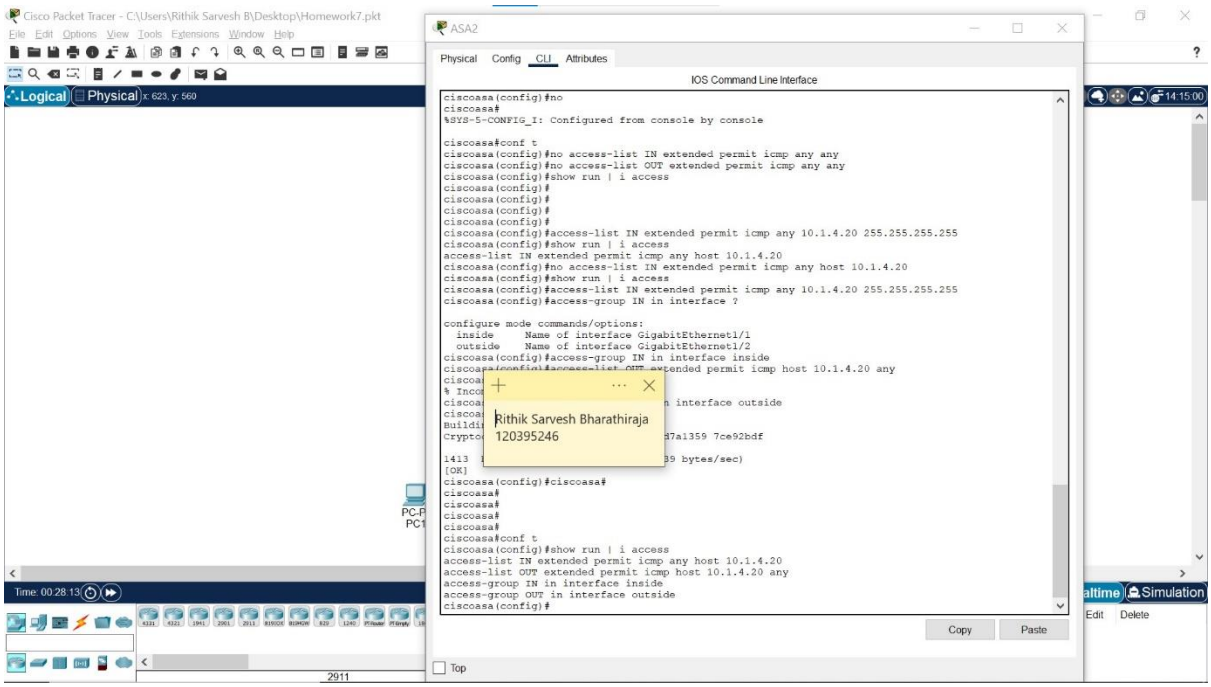
UID: 120395246

Course: ENPM693

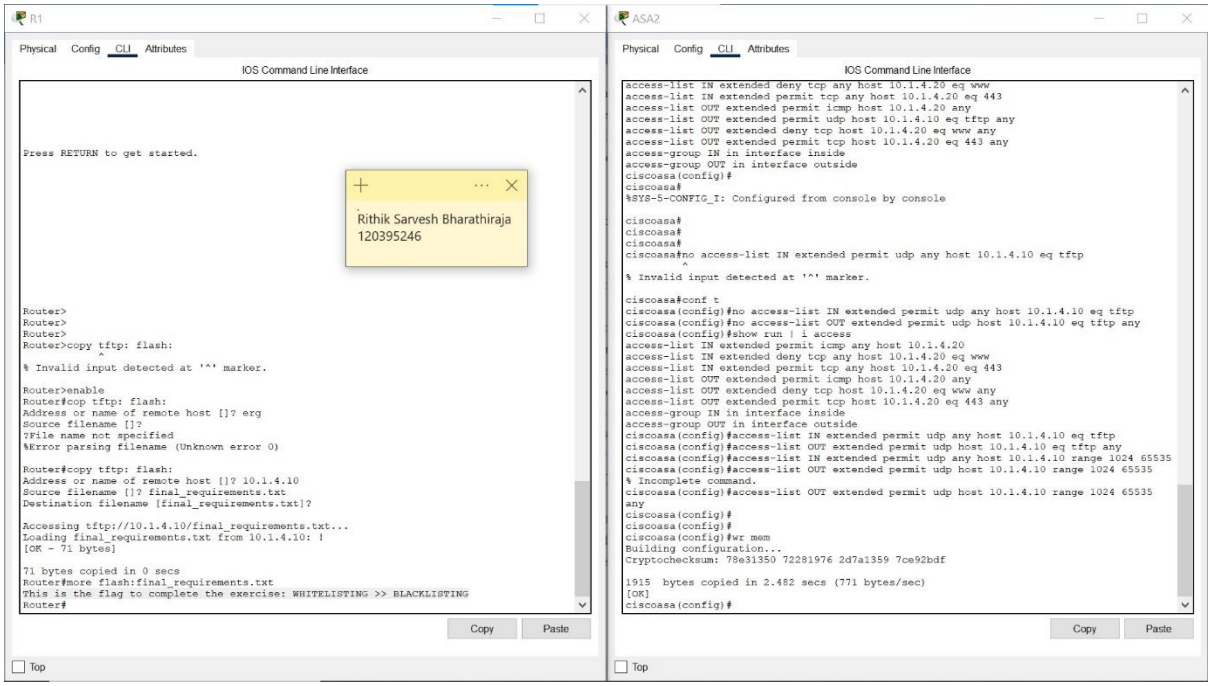
Task: Homework 7

1)





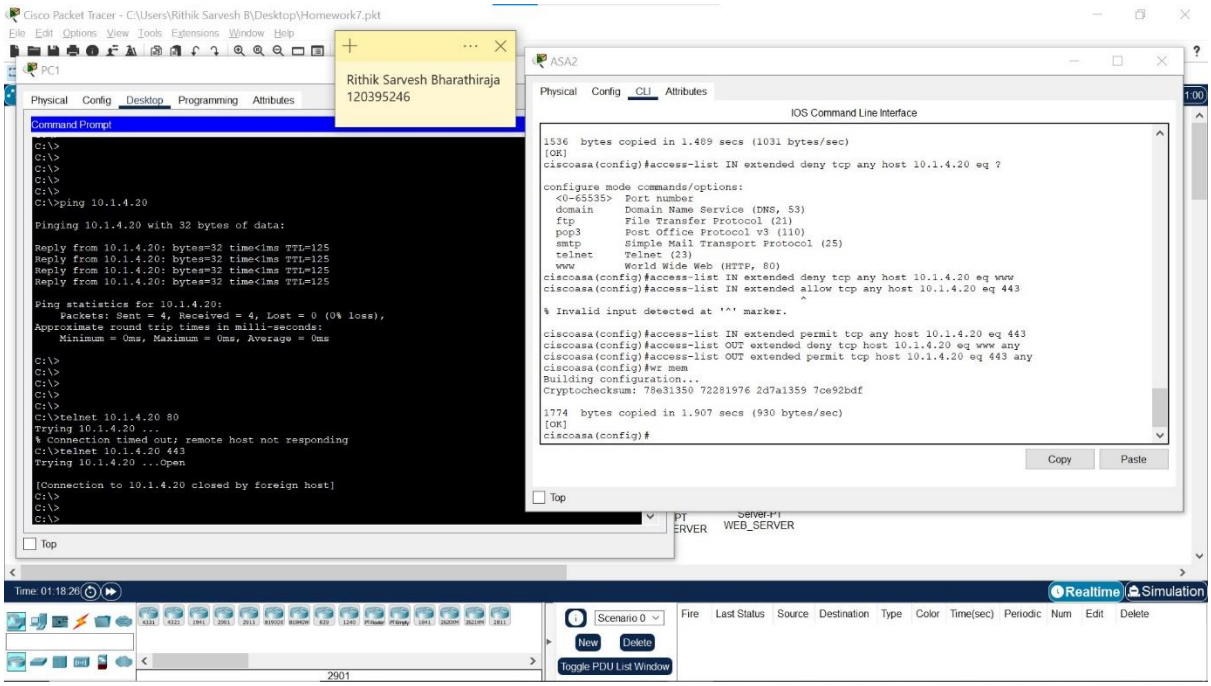
2)



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.