Terna Engineering College
Computer Engineering Department

Class: TE **Sem.: VI**

Course: System Security Lab

PART A

(PART A : TO BE REFFERED BY STUDENTS)

Experiment No.06

A.1 Aim: Design a network and implement packet sniffing on telnet traffic using wireshark.

A.2 Prerequisite:

1. Basic Knowledge of IP addresses, Port numbers, TCP and UDP Protocols.

A.3 Outcome:

After successful completion of this experiment students will be able to

Apply basic network command to gather basic network information.

A.4 Theory:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color-coding and other features that let you dig deep into network traffic and inspect individual packets.

Features of Wireshark :

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- Export some or all packets in a number of capture file formats.

SNO.	NAME OF THE DEVICE	INTERFACE	IP ADDRESS	Subnet Mask	Default Gateway

- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.
- Create various statistics.

Capturing Packets

After downloading and installing wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface. You can configure advanced features by clicking Capture Options.

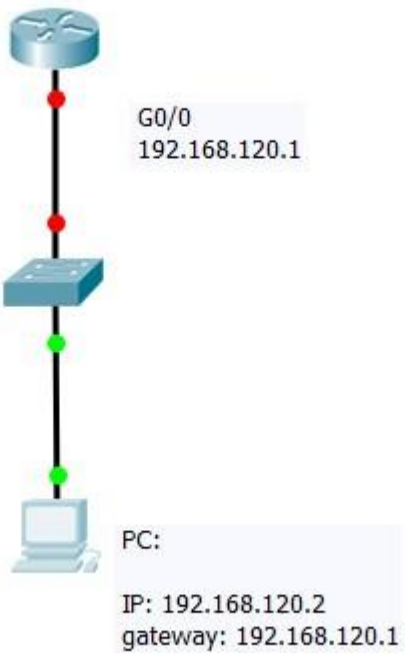
Filtering Packets

If you‘re trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you‘ll likely have a large amount of packets to sift through. That‘s where Wireshark‘s filters come in. The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type ―dns‖ and you‘ll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.

A5. Interface Configuration table

1.	Router 0	g0/0	192.168.120.1	255.255.255.0	--------
2.	PC	Fast Ethernet	192.168.120.2	255.255.255.0	192.168.120.1

A6. Design



PART B

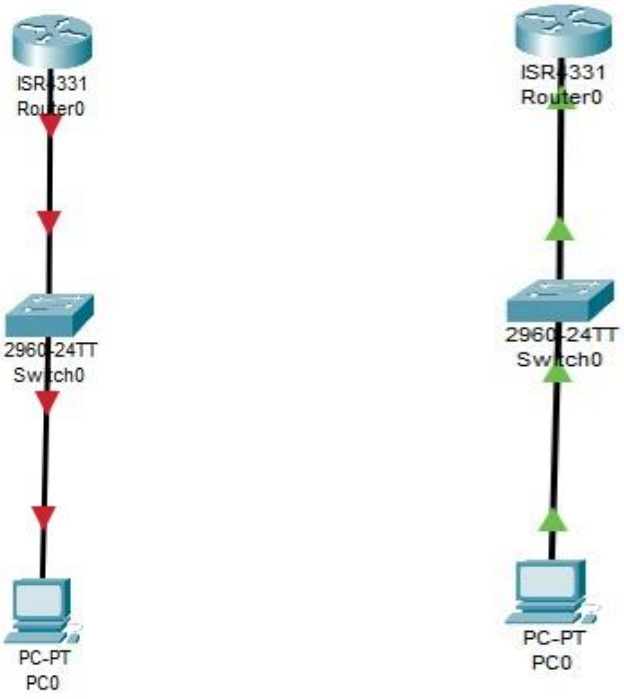
(PART B : TO BE COMPLETED BY STUDENTS)

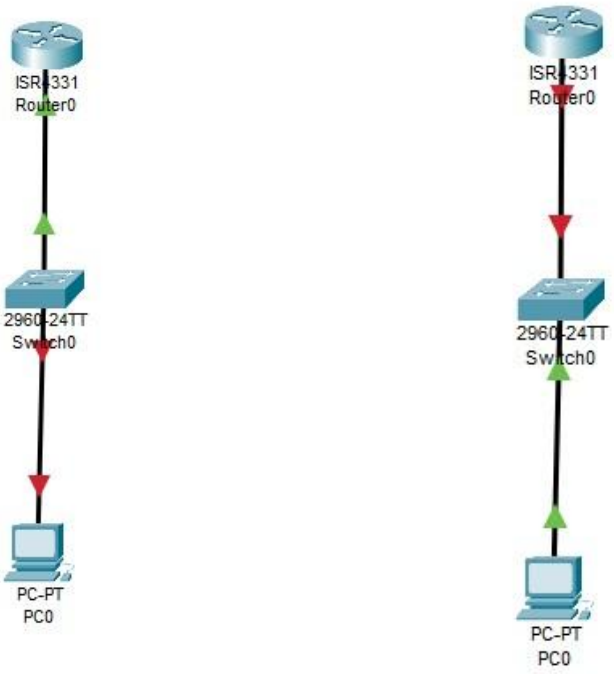
(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)

Roll No.: B26	Name: Dhruv Shirsat
Class : TE COMPS B	Batch : B2
Date of Experiment:	Date of Submission
Grade :	

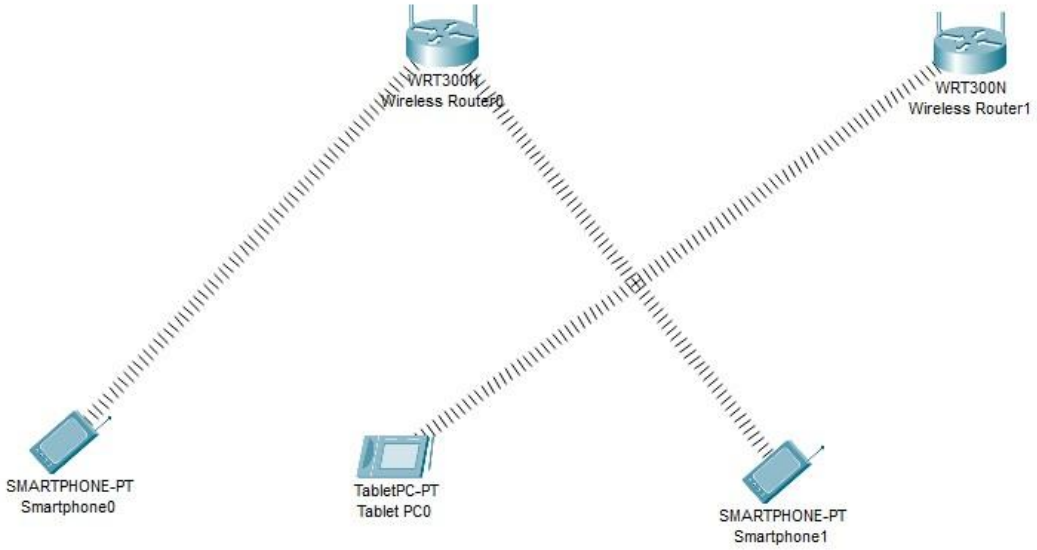
B.1 Output

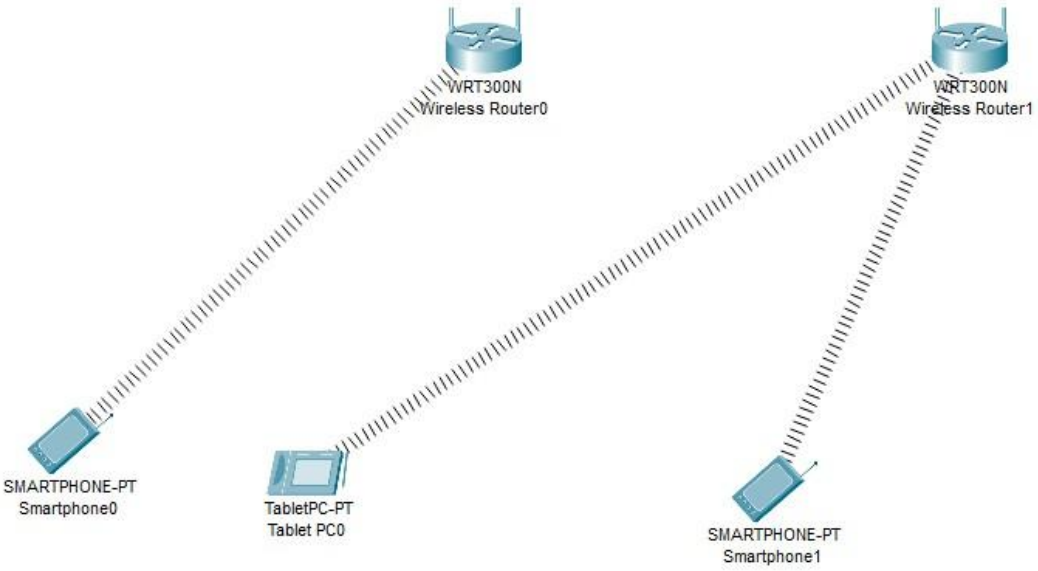
Wired Connection:

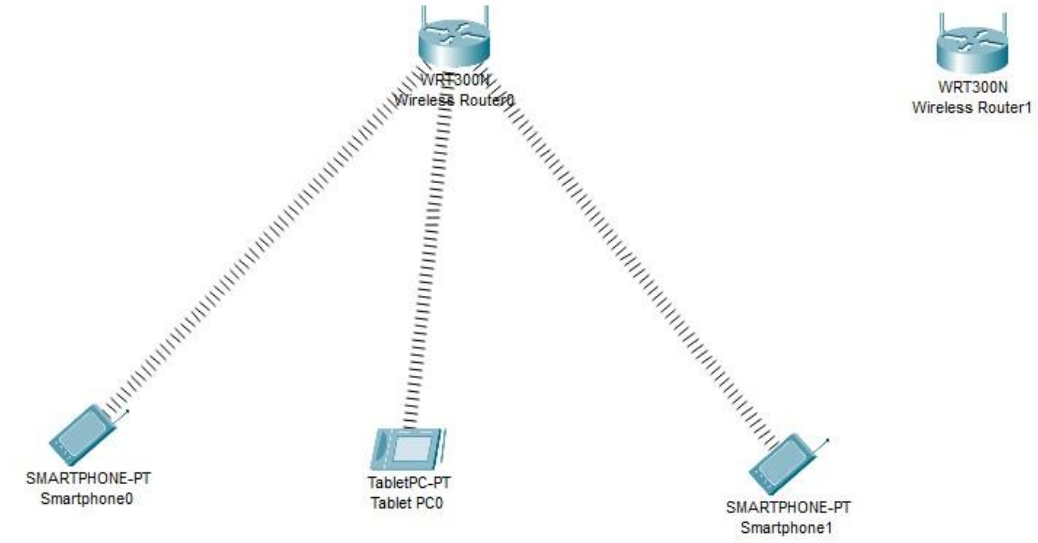


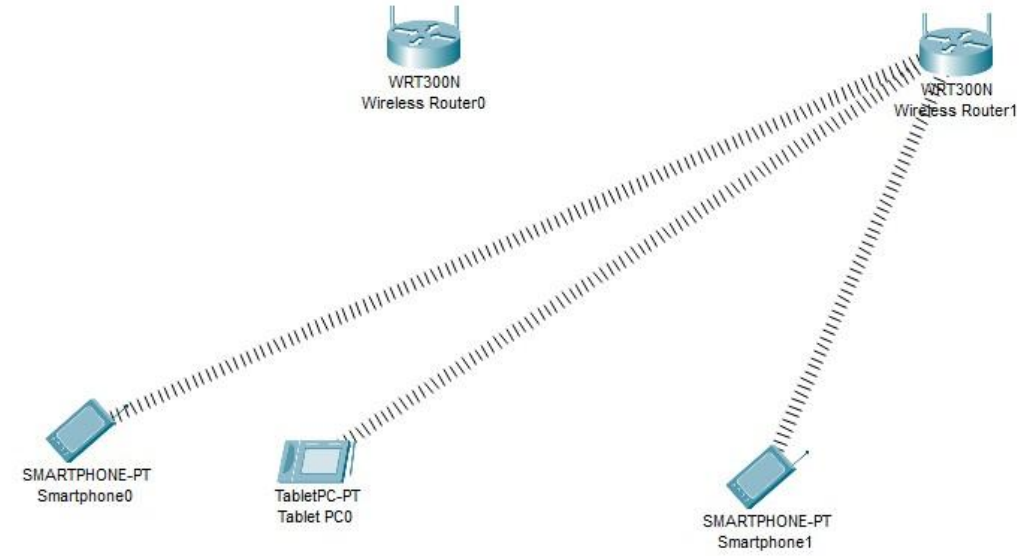


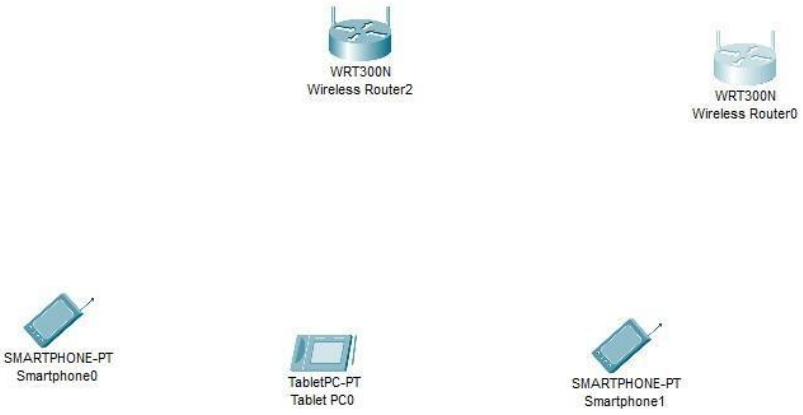
Wireless Connection:



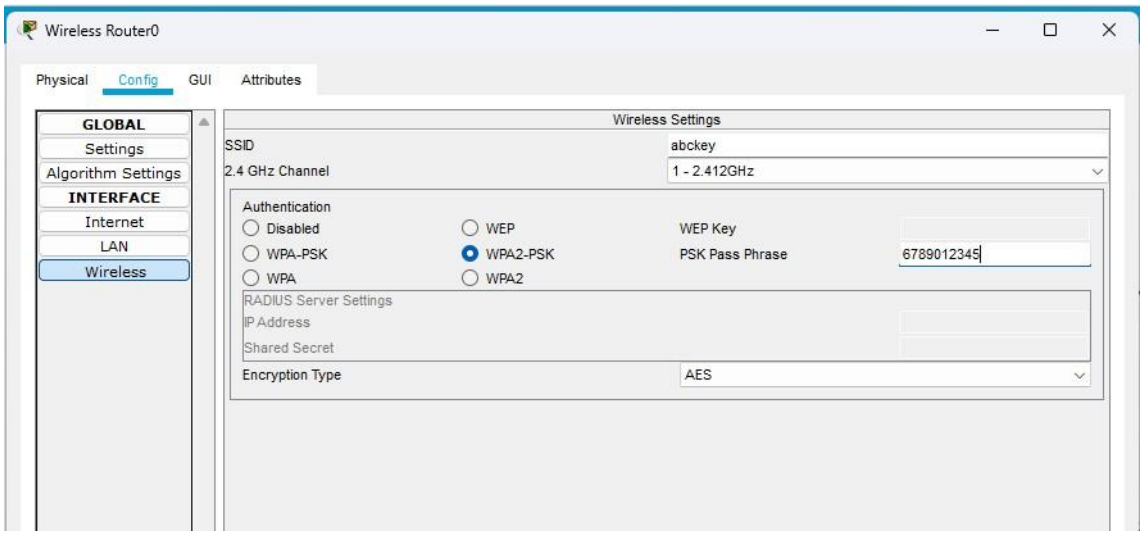

WRT300N
Wireless Router0
WRT300N
Wireless Router1
SMARTPHONE-PT
Smartphone0
TabletPC-PT
Tablet PC0
SMARTPHONE-PT
Smartphone1


WRT300N
Wireless Router0
WRT300N
Wireless Router1
SMARTPHONE-PT
Smartphone0
TabletPC-PT
Tablet PC0
SMARTPHONE-PT
Smartphone1


WRT300N
Wireless Router0
WRT300N
Wireless Router1
SMARTPHONE-PT
Smartphone0
TabletPC-PT
Tablet PC0
SMARTPHONE-PT
Smartphone1


WRT300N
Wireless Router2
WRT300N
Wireless Router0
SMARTPHONE-PT
Smartphone0
TabletPC-PT
Tablet PC0
SMARTPHONE-PT
Smartphone1

Router Configuration:

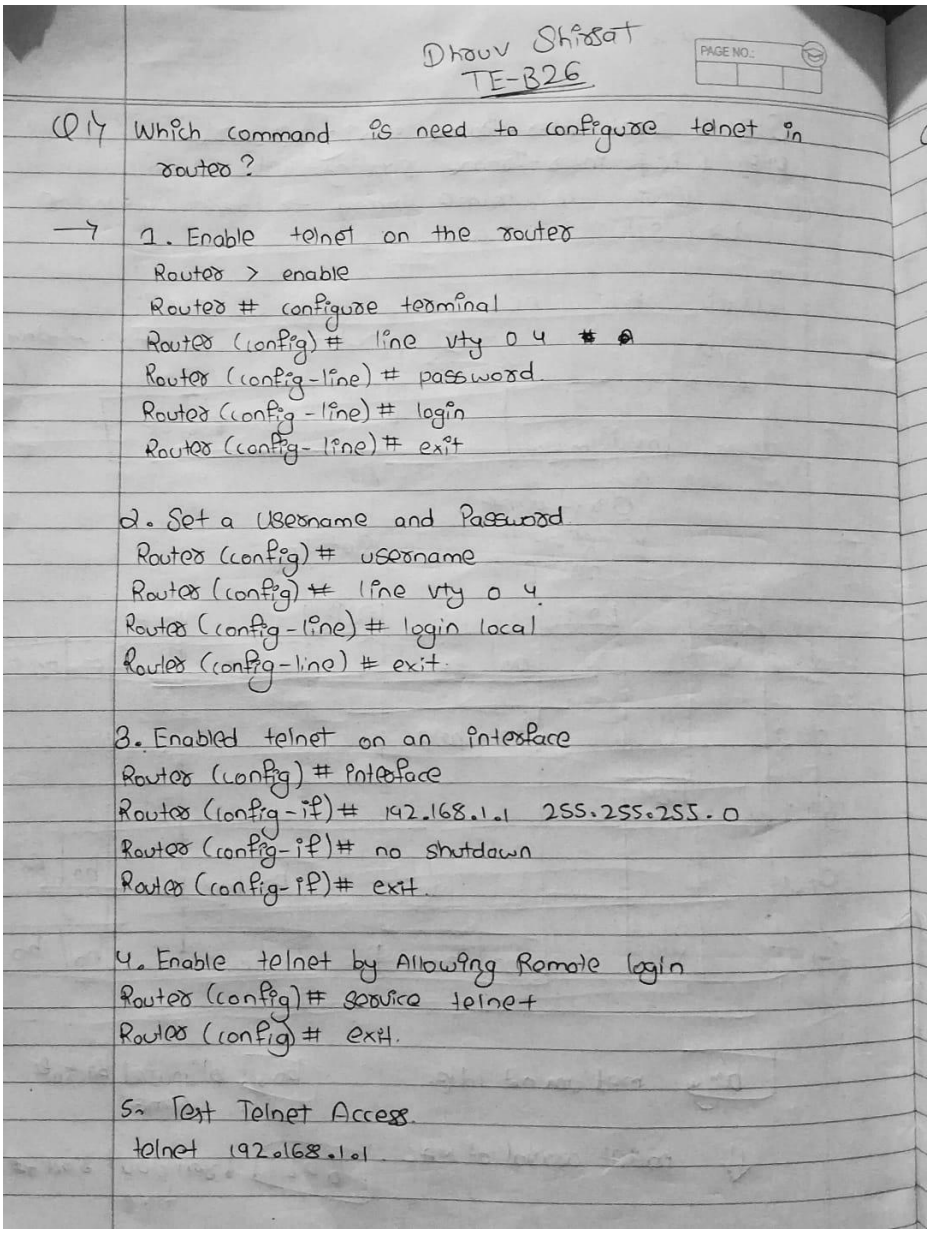


B.2. Commands / tools used with syntax:

Tool used-Cisco Packet Tracer

B.3 Question of Curiosity:

1. Which command is need to configure telnet in router?



Dhruv Shirsat
TE-B26

PAGE NO:

Q1) Which command is need to configure telnet in router?

→ 1. Enable telnet on the router
Router > enable
Router # configure terminal
Router (config) # line vty 0 4
Router (config-line) # password
Router (config-line) # login
Router (config-line) # exit

2. Set a username and Password
Router (config) # username
Router (config) # line vty 0 4
Router (config-line) # login local
Router (config-line) # exit

3. Enabled telnet on an interface
Router (config) # interface
Router (config-if) # 192.168.1.1 255.255.255.0
Router (config-if) # no shutdown
Router (config-if) # exit

4. Enable telnet by Allowing Remote login
Router (config) # service telnet
Router (config) # exit

5. Test Telnet Access.
telnet 192.168.1.1

2. What are the steps needed to extract data from sniffed traffic?

Set Up a Packet Sniffer – Use tools like Wireshark or tcpdump in promiscuous mode to capture network traffic.

Capture Network Traffic – Apply filters (e.g., port 23 for Telnet, port 80 for HTTP) to focus on unencrypted data.

Analyze Captured Packets – Inspect packet contents to find usernames, passwords, and session tokens.

Extract Sensitive Information – Use "Follow TCP Stream" in Wireshark to view plaintext data like credentials.

Reconstruct Files/Data – Use export tools to retrieve transferred files or media.

Interpret and Use Data – Analyze the extracted data for security assessment or malicious use (illegal without authorization).

3. What type of packets to be filtered for accessing remote login username and password of a router?

To secure a router from unauthorized remote login access, filter these packets:

1. Block Telnet (Port 23 - Insecure, Plaintext Login)
2. Block SSH (Port 22 - If Not Needed)
3. Block SNMP (Ports 161, 162 - Credential Exposure) Commands:

access-list 101 deny tcp any any eq 23

access-list 101 permit ip any any

interface GigabitEthernet0/1 ip

access-group 101 in

access-list 102 deny tcp any any eq 22 access-list

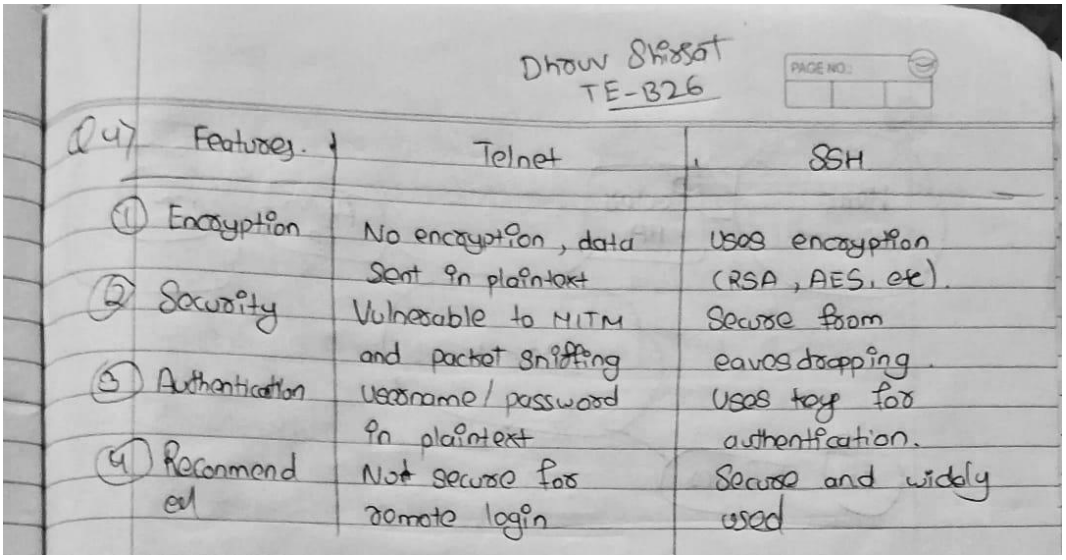
102 permit ip any any

access-list 103 deny udp any any eq 161

access-list 103 deny udp any any eq 162

access-list 103 permit ip any any

4. What are the differences between Telnet and SSH in terms of security?



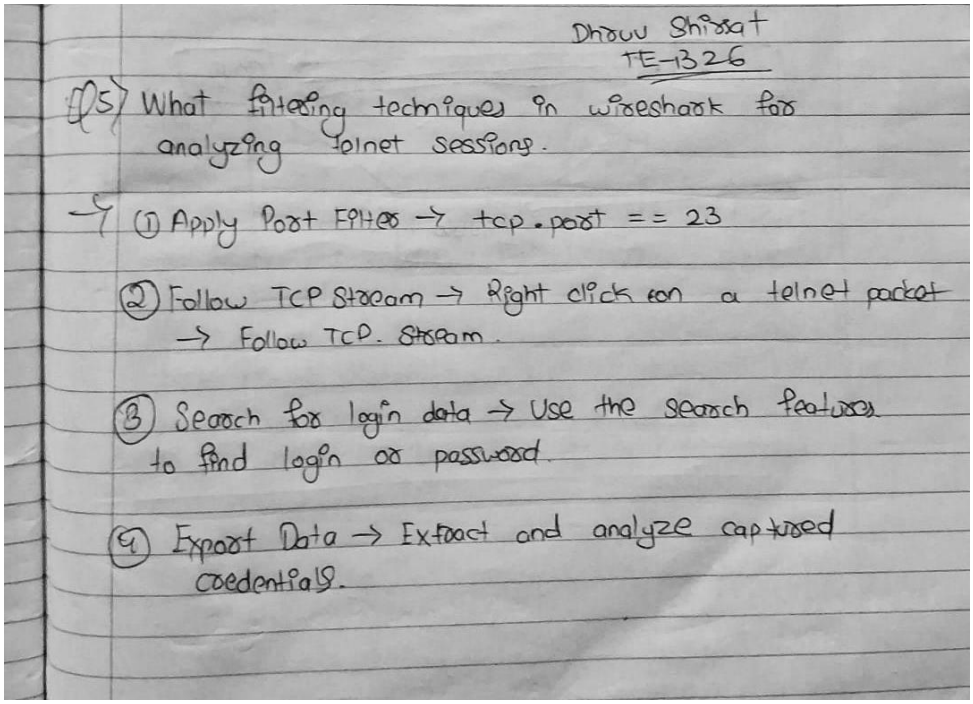
Dhruv Shirsat
TE-B26

PAGE NO.:

Q4)

Features.	Telnet	SSH
(1) Encryption	No encryption, data sent in plaintext	Uses encryption (RSA, AES, etc).
(2) Security	Vulnerable to MITM and packet sniffing	Secure from eavesdropping.
(3) Authentication	Username/password in plaintext	Uses keys for authentication.
(4) Recommended	Not secure for remote login	Secure and widely used

5. What filtering techniques can be used in Wireshark to analyze Telnet sessions?



6.How can encrypted protocols mitigate the risks identified in sniffed Telnet traffic?

1. Secure Shell (SSH) Instead of Telnet

SSH encrypts data using AES, RSA, or ECC encryption, making it unreadable to attackers.

Even if an attacker captures packets, they cannot decrypt the contents without the private key.

2. Use of TLS/SSL for Encrypted Sessions

Protocols like HTTPS, FTPS, and Secure SMTP use TLS/SSL encryption to prevent eavesdropping.

Encryption ensures that data is securely transmitted and cannot be altered by attackers.

3. Implementation of VPNs

A Virtual Private Network (VPN) encrypts all network traffic, making packet sniffing ineffective.

Even if an attacker captures packets, they only see encrypted data, not plaintext credentials

B.4 Conclusion:

The network was successfully designed and configured to enable Telnet communication between devices. Packet sniffing was implemented using a network sniffer in Cisco Packet Tracer, allowing the capture of Telnet traffic. The captured packets clearly showed that Telnet transmits login credentials in plaintext, making it highly vulnerable to attacks. This highlights the security risks associated with using Telnet and emphasizes the importance of secure alternatives like SSH for remote access.