CS321: Computer Networks

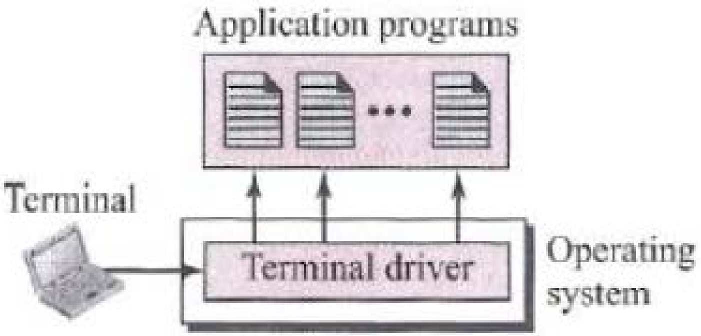
TELNET, SSH

Dr. Manas Khatua
Assistant Professor
Dept. of CSE
IIT Jodhpur
E-mail: manaskhatua@iitj.ac.in

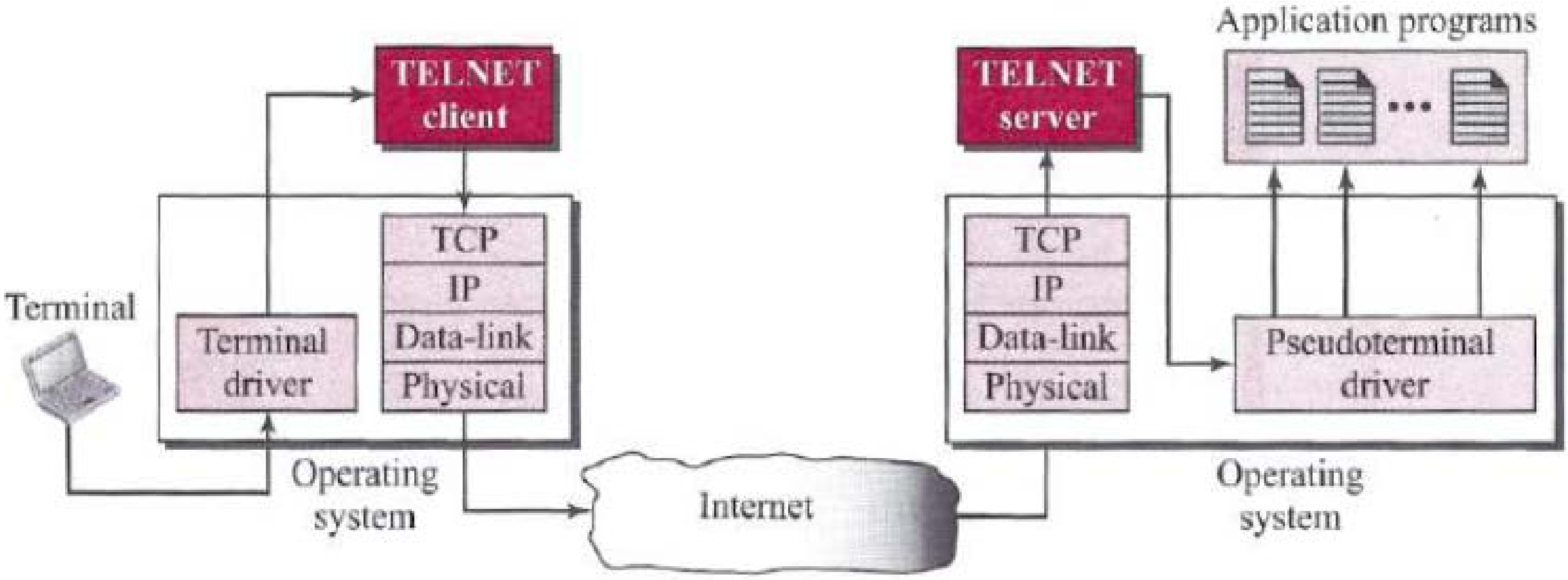
TELNET

- Many cases we need to have some generic client/server programs that allow a user on the client site to log into the computer at the server site and use the services available there.
- E.g., Java Compiler is installed in server. No need in client PC.
- We refer to these generic client/server pairs as *remote logging* applications.
- One of the original remote logging protocols is TELNET, which is an abbreviation for *TErminaL NETwork.*
- It is vulnerable to hacking because it sends all data including the password in plaintext (not encrypted).
- TELNET is almost replaced by SSH because of its vulnerability

Local versus Remote Logging



a. Local logging



b. Remote logging

Cont…

- The user sends the keystrokes to the terminal driver where the local operating system accepts the characters but does not interpret them.
- The characters are sent to the TELNET client, which transforms the characters into a universal character set called *Network Virtual Terminal* (NVT) characters and delivers them to the local TCPIIP stack.
- The commands or text, in NVT form, travel through the Internet and arrive at the TCPIIP stack at the remote machine.

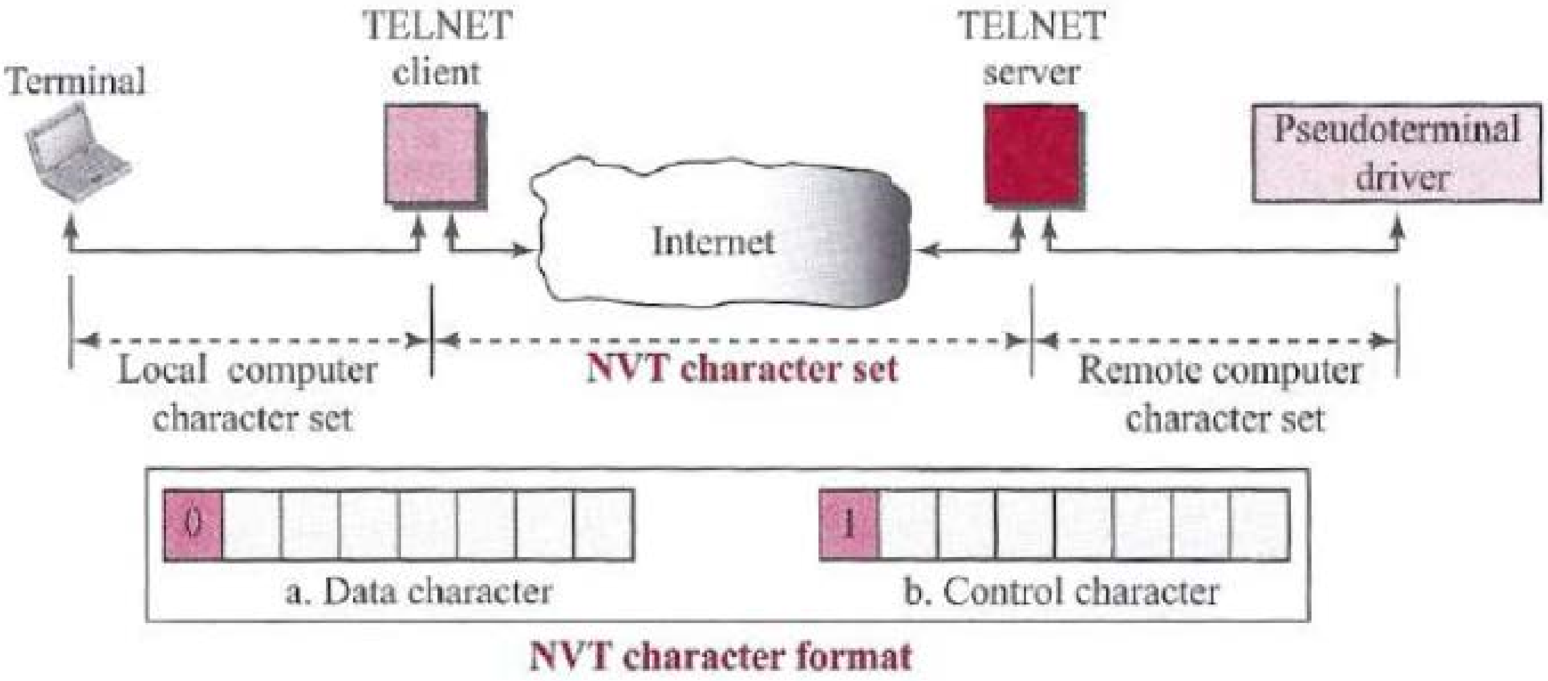
- The commands or text, in NVT form, travel through the Internet and arrive at the TCPIIP stack at the remote machine.

- However, the characters cannot be passed directly to the operating system in the remote machine. The characters are sent to a *pseudoterminal driver (*which pretends that the characters are coming from a terminal to the OS in remote machine).
- The operating system then passes the characters to the appropriate application program.

Cont…

- We are dealing with heterogeneous systems.
- TELNET solves this problem of heterogeneity by defining a universal interface called the *Network Virtual Terminal (NVT)* character set.

- NVT uses two sets of characters, one for data and one for control. Both are 8-bit bytes



Options & Unser Interface

- Options are extra features available to a user with a more sophisticated terminal.

  E.g., -4: IPv4; -6: IPv6; -E: disable escape char

- The operating system (UNIX, for example) defines an interface with user-friendly commands.

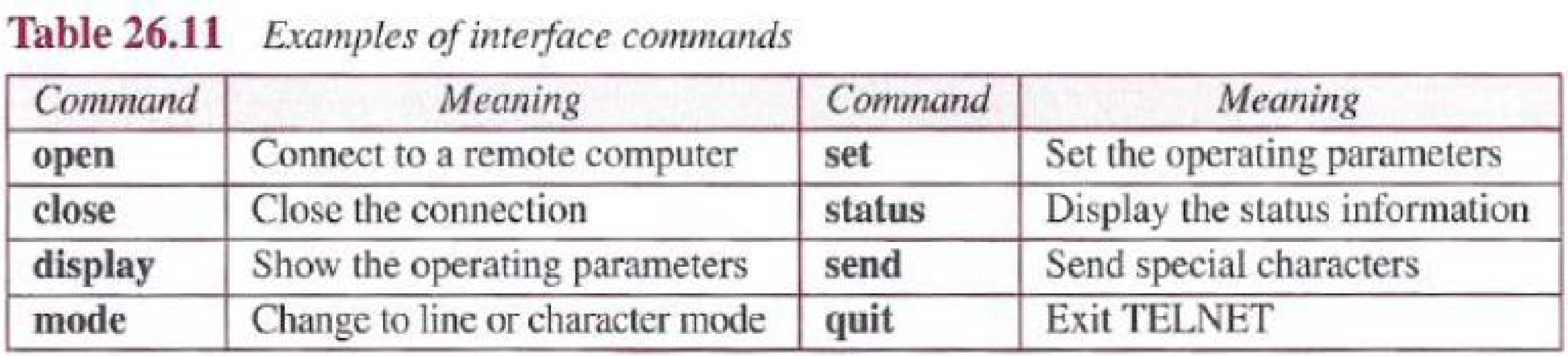


Table 26.11 *Examples of interface commands*

Command	*Meaning*	*Command*	*Meaning*
open	Connect to a remote computer	**set**	Set the operating parameters
close	Close the connection	**status**	Display the status information
display	Show the operating parameters	**send**	Send special characters
mode	Change to line or character mode	**quit**	Exit TELNET

SECURE SHELL (SSH)

- SSH is a secure application program
- Applications
  - SSH for Remote Logging (PuTTy)
  - SSH for File Transfer (sftp)
  - SSH for Secure Copy (scp)

- It has three components:
  - *SSH Transport-Layer Protocol (SSH-TRANS)*
  - *SSH Authentication Protocol (SSH-AUTH)*
  - *SSH Connection Protocol (SSH-CONN)*

SSH-TRANS

- SSH Transport-Layer Protocol
  - It creates a secured channel on top of the TCP
  - the client and server first use the TCP protocol to establish an insecure connection.
  - Then they exchange several security parameters to establish a secure channel on top of the TCP.

- Few services provided by this protocol:
  - Privacy or confidentiality
  - Data integrity
  - Server authentication
  - Compression of the messages

SSH-AUTH

- *SSH Authentication Protocol*
  - Authenticate the client for the server.
  - Authentication starts with the client, which sends a request message to the server.

  - The request includes the user name, server name, the method of authentication, and the required data.
  - The server responds with either a success message, or a failed message,

SSH-CONN

- *SSH Connection Protocol*
  - It provides few more services such as multiplexing
  - SSH-CONN takes the secure channel established by the two previous protocols and lets the client create multiple logical channels over it.
  - Each channel can be used for a different purpose, such as remote logging, file transfer, and so on.

Thanks!