NSCOM01

TCP-based Network Application Protocols

3rd Term– AY2022 – 2023

Instructor: Dr. Marnel Peradilla

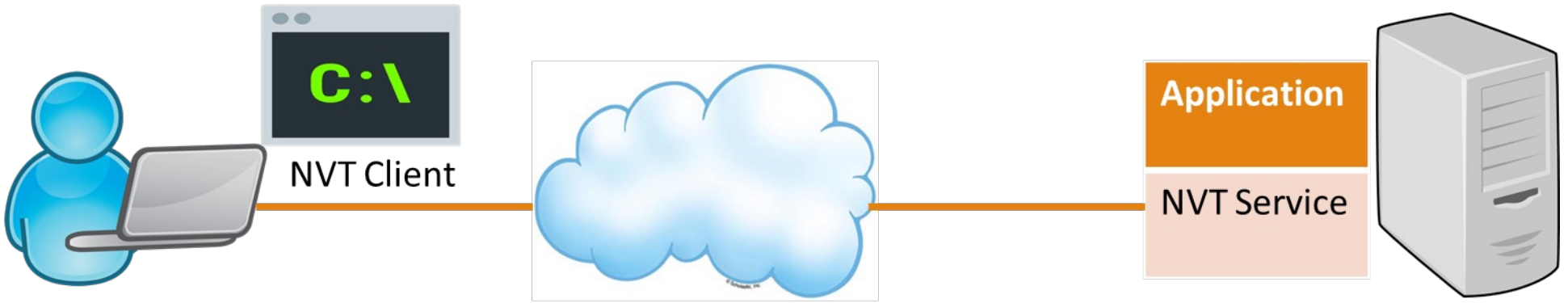
SPIRAL REVIEW: TRANSPORT SERVICES

- **The Transport Control Protocol (TCP) is a connection-oriented transport protocol used in TCP/IP networks**
- **Provides reliable communication between pairs of processes (TCP users) across a variety of reliable and unreliable networks**
  - Features:
  1. Stream-oriented – Data is sent in segments but handled as streams
  2. Connection Oriented – Includes mechanisms to establish, track state and terminate a connection between 2 hosts
  3. Guaranteed delivery – packets are acknowledged by receiving hosts
  4. Flow control - Data transmission adapts to network conditions and host capability
  5. Ordered delivery – Segments may arrive out of-order but are reassembled in the correct sequence

TELNET

NETWORK VIRTUAL TERMINAL APPLICATIONS

- **Network Virtual terminals (NVT) are application services that allow host terminals to interact with another host over a network regardless of terminal type and characteristics**
- **Computers before were commonly proprietary – i.e. different keyboards, different display terminals which use their own formats for input and output**
- **NVTs create a 'common language' for network hosts to interact with each other**
  - peripherals of a host (e.g. keyboard and monitor) can be used to send text-based input to and display output from another host over a network
  - Makes it possible to not require a set of I/O devices per host on the network



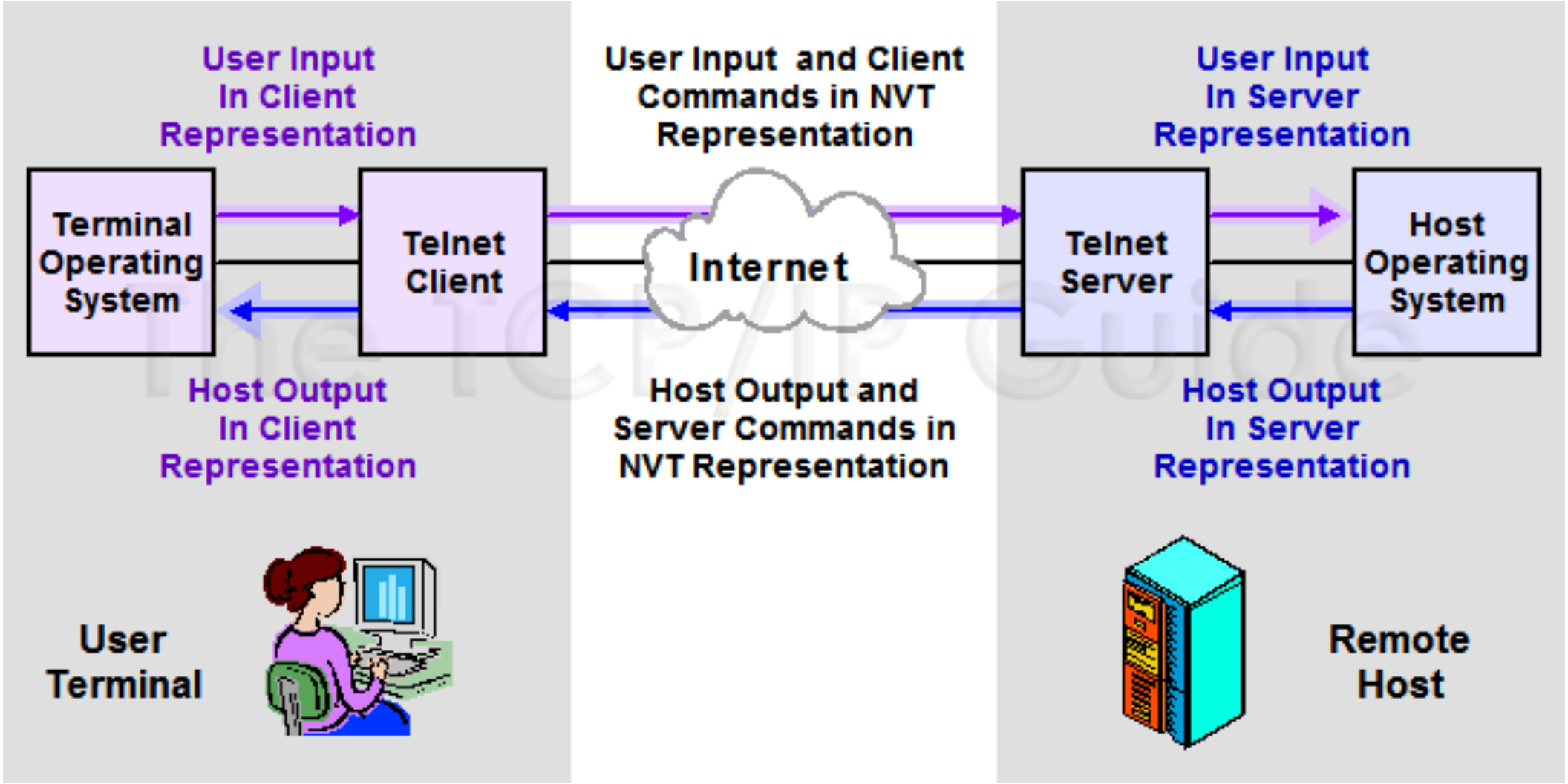
NVT

- **Allows remote log-on to a system and provides a standardized interface, through which a user or client program on one host may access the resources of another host (server) as though the client were a local terminal connected to the server**
  - Connect to routers or switches for monitoring or configuration
  - Connect to servers for management or to perform operations with a command-line based application
- **Network Virtual Terminal Protocols define the standard set of commands that will be used to represent an input from the sender which will be interpreted into the appropriate command on the receiving system**

TELNET

- **Used for the interactive communication of data and commands between client and server**
  - Telnet client - software that acts as an interface to the user to process keystrokes and user commands and present output from the remote machine to the screen
  - Telnet server - a daemon running on a remote computer that has been set up to allow remote sessions.
- **Uses TCP port 23 on the server side to listen for incoming connections**
- **Remote access session appears as if the user is at a terminal directly connected to the remote host**
- **Client and server use the standard Telnet Network Virtual Terminal (NVT) method for encoding data and control commands and sending these using a single connection.**

TELNET


User Input
In Client
Representation
User Input and Client
Commands in NVT
Representation
User Input
In Server
Representation
Terminal
Operating
System
Telnet
Client
Internet
Telnet
Server
Host
Operating
System
Host Output
In Client
Representation
Host Output and
Server Commands in
NVT Representation
Host Output
In Server
Representation
User
Terminal
Remote
Host

TELNET NVT

- **Makes use of the PSH TCP flag in order to send data quickly from client to server transmit keystrokes in realtime to the server**
- **Uses 7-bit codes for characters**
  - Recognizes all standard printable ASCII characters
  - Mandatory control codes: Null, Carriage Return, Line Feed
  - Optional Control codes: Bell, Backspace, Horizontal Tab, Vertical Tab, Form Feed
- **Characters are transmitted as 8 bits each, where most significant bit is set to 0.**
- **Telnet protocol commands are special codes specific to Telnet used for control of the session between hosts and negotiate options between client and server to provide greater functionality for the session**
- **Works using half-duplex communication, but has an option to turn on full-duplex mode**

TELNET PROTOCOL COMMANDS

- **Protocol commands are sent in the same communication stream as regular data**
  - Represented using special byte values in the range from 240 to 254.
  - Preceded by the Interpret As Command (IAC) with a value 0xFF
  - Ex. Interrupt Process Telnet command is represented as has the value 0xF4. This will be sent as 0xFFF4 (IAC, Interrupt)
- **Commonly used Telnet Commands**

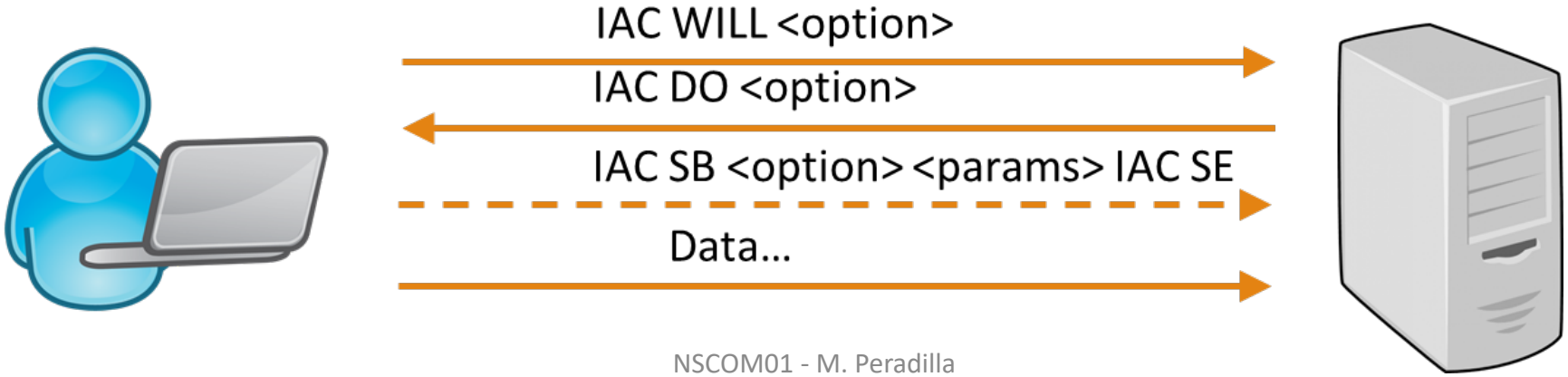
0xF0	SE	Subnegotiation End	Marks the end of a Telnet option subnegotiation
0xF6	AYT	Are You There	Used to check that the remote host is still "alive".
0xF9	GA	Go Ahead	Used in Telnet half-duplex mode to signal the other device that it may transmit.
0xFA	SB	Subnegotiation Begin	Start of a Telnet option subnegotiation for additional parameters
0xFB	WILL	Will Perform	Used in Telnet option negotiation
0xFC	WON'T	Won't Perform	
0xFD	DO	Do Perform	
0XFE	DON'T	Don't Perform	

TELNET OPTIONS

- **Telnet options provide a mechanism by which a telnet client and server can negotiate for more efficient or advanced means of communication.**
- **Either device may choose to initiate the use of an option. Initiating device can specify that it wants to start using an option, or that it wants the other device to start using it.**
- **To enable an option:**
  - WILL: Sent by the initiator to indicate that it wants to start using a particular option. 2 possible replies
    - DO: Sent to indicate agreement that the initiator should use the option; it is then considered enabled.
    - DONT: Sent to specify that the initiator must not use the option.
  - DO: Sent by the initiator to request that the other device start using an option. 2 possible replies
    - WILL: Sent to specify that the responding device will agree to use the option; the option is enabled.
    - WONT: Sent to tell the initiator that the responder will not use the option requested.

TELNET OPTIONS

- **To disable an option:**
  - WONT: Sent by a device to indicate that it is going to stop using an option. The other device must respond with DONT as a confirmation.
  - DONT: Sent by a device to indicate that it wants the other device to stop using an option. The other device must respond with WONT.
- **Subnegotiation is used if an option that both parties agree to have further parameters**
  - Use the SB (subnegotiation begin) and SE (subnegotiation end) commands



TELNET OPTIONS

```
⊞ Frame 4: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
⊞ Ethernet II, Src: 0c:54:15:d7:1a:90 (0c:54:15:d7:1a:90), Dst: 40:b0:76:58:e7:cc (40:b0:76:58:e7:cc)
⊞ Internet Protocol Version 4, Src: 192.168.1.60 (192.168.1.60), Dst: 35.160.169.47 (35.160.169.47)
⊞ Transmission Control Protocol, Src Port: 1844 (1844), Dst Port: 23 (23), Seq: 1, Ack: 1, Len: 21
⊟ Telnet
  ⊞ Will Negotiate About Window Size
  ⊞ Will Terminal Speed
  ⊞ Will Terminal Type
  ⊟ Will New Environment Option
      Command: Will (251)
      Subcommand: New Environment Option
  ⊟ Do Echo
      Command: Do (253)
      Subcommand: Echo
  ⊞ Will Suppress Go Ahead
  ⊞ Do Suppress Go Ahead
```

```
0000  40 b0 76 58 e7 cc 0c 54  15 d7 1a 90 08 00 45 00   @.vX...T ......E.
0010  00 3d 20 a1 40 00 80 06  4b 66 c0 a8 01 3c 23 a0   .= .@... Kf...<#.
0020  a9 2f 07 34 00 17 c9 25  b2 8c e1 f4 d1 88 50 18   ./.4...% ......P.
0030  02 01 b9 49 00 00 ff fb  1f ff fb 20 ff fb 18 ff   ...I.... ... ....
0040  fb 27 ff fd 01 ff fb 03  ff fd 03                  .'...... ...
```

TELNET OPTION NEGOTIATION RULES

- Sender can start option negotiation only if it will change settings, not to advertise its current settings
- Recipient will not acknowledge an option if it is already using the requested settings
- Rejected requests should not be requested again unless something changes
- When both hosts simultaneously request the same option, do not acknowledge because this is taken to mean that both are agreeable to the option
- A receiving host MUST refuse an option being requested if it cannot be support

COMMONLY USED TELNET OPTIONS

0	TRANSMIT-BINARY	Binary Transmission	Allows devices to send data in 8-bit binary form instead of 7-bit ASCII.
1	ECHO	Echo	Allows characters type by the client to be echoed back by the server
3	SUPPRESS-GO-AHEAD	Suppress Go Ahead	Allows devices not operating in half-duplex mode to no longer need to end transmissions using the Telnet Go Ahead command.
32	TERMINAL-SPEED	Terminal Speed	Allows devices to report on the current terminal speed.
31	NAWS	Negotiate About Window Size	Permits communication of the size of the terminal window.
33	TOGGLE-FLOW-CONTROL	Remote Flow Control	Allows flow control between the client and the server to be enabled and disabled.
34	LINEMODE	Linemode	Allows the client to send data one line at a time instead of one character at a time. This improves performance by replacing a large number of tiny TCP transmissions with a smaller number of larger ones.

COMMON TELNET OPTIONS

❑ Echo (Option 1)

- Option allows the server to send back characters inputted from the client side so that these may be displayed back to the client screen (otherwise, user does not see what he/she is tying in)

  Ex: Client: IAC WILL ECHO (0xFF 0xFB 0x01)

  Server: IAC DO ECHO (0xFF 0xFD 0x01)

❑ Suppress-Go-Ahead (Option 3)

- Telnet by default allows only 1 of the communicating hosts to be transmitting at a time
- A host sends a GA (Go ahead) command to signal to the opposite host that it may begin transmitting
- Suppress-Go-Ahead option allows the communicating hosts to forego the GA signal so that they can be both transmitting and receiving simultaneously (full duplex mode)

  Ex: Client: IAC WILL SUPRESS-GO-AHEAD (0xFF 0xFB 0x03)

  Server: IAC DO SUPRESS-GO-AHEAD (0xFF 0xFD 0x03)

COMMON TELNET OPTIONS

❑ Negotiate About Window Size (Option 31)

- Clients normally have to adapt to run terminals in resizable windows on modern window-based operating systems
- Option with subnegotiation is used to set the 2-byte width and 2-byte length of the terminal in terms of number of characters

Ex: To negotiate a terminal that is 80 columns x 24 lines

Server: IAC DO NAWS (0xFF 0xFD 0x1F)

Client: IAC WILL NAWS (0xFF 0xFB 0x1F)

Client: IAC SB NAWS 00 80 00 24 IAC SE (0xFF 0xFA 0x1F 0x00 0x50 0x00 0x18 0xFF 0xF0

COMMON TELNET OPTIONS

❑ Toggle Flow Control (Option 33)

- Telnet data flow may need to be controlled
  - Terminal buffers are close to overflowing
  - Client user may need to slow down the display to read it properly
- Option with subnegotiation is used to set the method to set the flow control method: OFF (0), ON (1), RESTART-ANY (2), RESTART-XON (3)
- Ex: To set the option so that the user can start/pause output using CTRL-C (XON)/CTRL-Q (XOFF)

  Server: IAC DO TOGGLE-FLOW-CONTROL (0xFF 0xFD 0x21)

  Client: IAC WILL TOGGLE-FLOW-CONTROL (0xFF 0xFB 0x21)

  Client: IAC SB TOGGLE-FLOW-CONTROL RESTART-XON IAC SE (0xFF 0xFA 0x21 0x03 0xFF 0xF0

TELNET LIMITATIONS

- **Data is sent in plaintext- hence all keystrokes including potential usernames and password used for logins can be captured from the networked using packet sniffers**
  - Best practices on networks require the use of Secure Shell (SSH) is instead – same functionality but with strong user authentication and encryption
- **Character-based tool so no support for remote access to a graphical and cursor-based interface**
  - For graphical remote logins, Remote Frame Buffer (RFB) or Remote Desktop Protocol (RDP) are commonly used instead
- **Considered to be inefficient because of large overhead. Typically when transmitting data, 1 character is 1 packet – i.e. ethernet+IP+TCP header needed just to transmit 1 byte of data**

REFERENCES

1. Telnet Protocol (The TCP/IP Guide) http://www.tcpipguide.com/free/t_TelnetOverviewHistoryandStandards.htm
2. Telnet and Rlogin (TCP/IP: The Ultimate Protocol Guide) https://books.google.com.ph/books?id=isybabuADPkC&pg=PA5851
3. RFC 854: Telnet protocol Specification https://tools.ietf.org/html/rfc854

MESSAGE FROM DPO

"The information and data contained in the online learning modules, such as the content, audio/visual materials or artwork are considered the intellectual property of the author and shall be treated in accordance with the IP Policies of DLSU. They are considered confidential information and intended only for the person/s or entities to which they are addressed. They are not allowed to be disclosed, distributed, lifted, or in any way reproduced without the written consent of the author/owner of the intellectual property."