TSN2201 COMPUTER NETWORKS

TUTORIAL 6 (Tri 1, 2017/2018)

True/ False

1. Flow control is the regulation of the sender's data rate so that the receiver buffer does not become overwhelmed.

2. Error control only detects errors.

3. In Stop and Wait ARQ, the sender sends a frame and waits for an acknowledgment from the receiver before sending the next frame.

4. Piggybacking couples an acknowledgment with a request.

5. Flow control mechanisms with sliding windows have control variables at both sender and receiver sites.

6. HDLC protocol defines three types of frames: the information frame (I-frame), the supervisory frame (S-frame) and the unnumbered frame (U-frame).

7. HDLC handles data transparency by adding a 1 whenever there are five consecutive 0's following a 1. This is called bit stuffing.

MCQs

1. Flow control is needed to prevent _____.

   a. bit errors   c. overflow of the receiver buffer
   b. overflow of the sender buffer   d. collision between sender and receiver|

2. HDLC is an acronym for:

   a. high-duplex line communication   c. half-duplex digital link combination
   b. high-level data link control   d. host double-level circuit

3. Flow control mechanisms with sliding windows have control variables at:

   a. sender only   c. both sender and receiver
   b. receiver only   d. None of the above

4. An example of piggybacking is when:

    a. packets cross paths
    b. acknowledgment packet is sent with a data frame
    c. packets collide and must be recovered or "piggybacked"
    d. All of the above

**Practical Lab: Capture and Analyse Protocol Data Unit (PDU) using Wireshark**

Wireshark is a software protocol analyser that is used for network analysis, troubleshooting and education. As data travel back and forth over the network, the software is able to capture PDUs, then decode and analyse the content of each PDU. In this lab, student is going to use this software to capture *ping* data.

1. First, launch the Wireshark from your PC.

2. Click on the Interface List, you may select a network interface from the drop down list. Student has to select the Ethernet interface in this lab. Ensure you check on the feature "Capture packets in promiscuous mode".
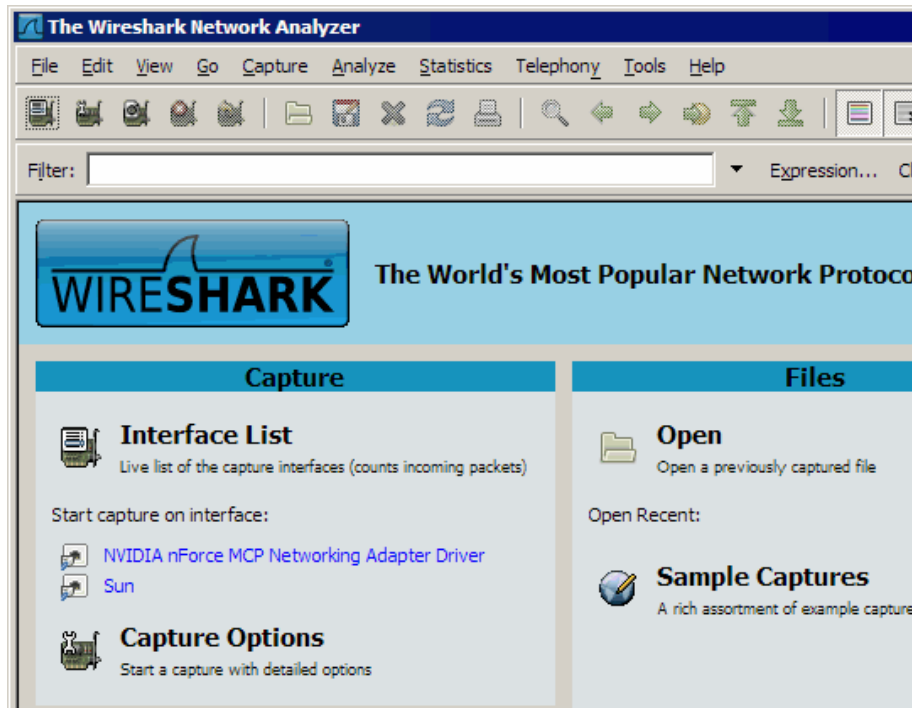
3. Click on the Capture Options, you can see the following window appears. Ensure that you check on the "Use promiscuous mode on all interfaces" checkbox. Explain what is the purpose of enabling promiscuous mode on the interfaces?

4. Capture filter allows you to capture only the packets that you want, this might help you to trace and analyse the data easier. For example: *If you just want to capture ICMP data, then just type icmp in the filter box.*
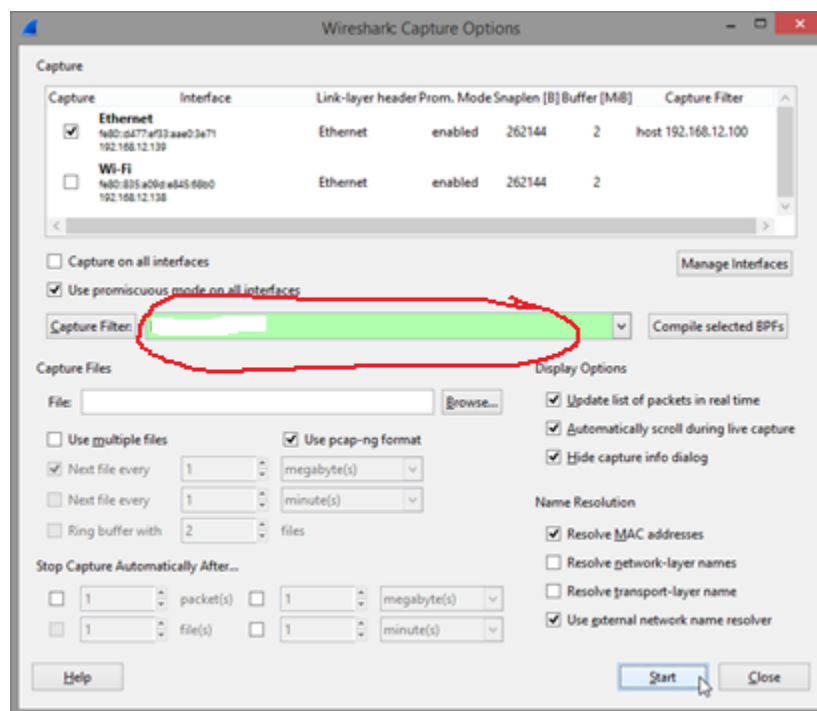
5. Open a command prompt window in your PC.

6. Click on the Start button to begin the data capture process.

7. In the command prompt window, enter the command *ping www.mmu.edu.my*

8. Once the *ping* completed, click the Stop button to terminate the capture process. The main screen is displayed.

9. The main window of the Wireshark has three panes, the top pane is the Packet List Pane, and it displays a summary of each packet captured. The middle pane is the Packet Details Pane, it shows the selected packet in more detail. Packet Bytes Pane is at the bottom pane and it displays the actual data from the selected packet.

10. From the Packet List Pane, identify the protocol used by *ping*. State the full protocol name.

11. What are the listed source and destination IP addresses in the first *ping* packet?

12. What are the listed source and destination MAC addresses in the first *ping* packet?

13. Explore other *ping* packets in the Packet List Pane.

14. From the Packet Bytes Pane, identify the data content sent in the *ping* packet.

15. Can you find the MAC address of the www.mmu.edu.my server? Explain your answer.

16. Exit the Wireshark program without saving, you may save the captured data if you want to.