EXPERIMENT: 10
SLIDING WINDOW PROTOCOL

AIM:

The aim of this experiment is to simulate sliding window flow control protocol.

ALGORITHM (Stop and Wait ARQ)

Server side

Step 1: Start
Step 2: Establish UDP connection with client
Step 3: Receive total number of frames from client
Step 4: Repeat
    Step 4.a: Receive frame P from client.
    Step 4.b: If P = -99, go to step 5
    Step 4.c: Send acknowledgement to client (1 for positive, -1 for Negative)
Step 5: Stop.

Client side

Step 1: Start
Step 2: Establish UDP connection with server.

Scanned with OKEN Scanner

step 3: Send total number of frames N to server.

step 4: for i = 1 to N do

step 4.a: Let ACK = -1

step 4.b: Repeat.

step 4.b.1: send frame to server

step 4.b.2: Receive acknowledgement from server.

step 4.b.3: If ACK == -1, print "Resending"

step 4.b.4: Else, go to step 5

step 5: stop

RESULT

The program executed successfully and the output is obtained.

Scanned with OKEN Scanner

EXPERIMENT: 11
UNDERSTANDING WIRESHARK TOOL

AIM: The aim of this experiment is to understand the working of wireshark tool.

THEORY:

Wireshark: Wireshark is a widely used, open source network analyzer that can capture and display real-time details of network traffic. It is particularly useful for troubleshooting network issues, analyzing network protocols and ensuring network security.

Networks must be monitored to ensure smooth operations and security. Popular with academic institutions, government agencies, corporations and non-profits. Wireshark is one such tool that can offer in-depth view into network activities, diagnose network performance issues or identify potential security Threats.

Scanned with OKEN Scanner

Key features of Wireshark

Wireshark seems to simplify and enhance the process of network traffic analysis. Each function is designed to offer unique insights and control over network activities.

* Packet Capture (PCAP): Converts network traffic into a human-readable format, making it easier to understand and diagnose concerns.
* Real-time Analysis: Provides a live view of network traffic, offering immediate insights into ongoing network activities.
* Filtering Capabilities: Enables users to focus on specific types of network traffic, making analysis more efficient and targeted.
* Graphical User Interface (GUI): Designed for ease of use, ensures that both beginners and experts can navigate and analyze data efficiently.

TCP Packets: Most networks use TCP/IP as the network protocol or set of rules for communication between devices and the rules of TCP/IP require information to be split into packets that contain both a segment of data to be transferred and the address where the data is to be sent.

Flow Graph: The flow graph window shows connections between hosts. It displays the packet time, direction, ports and comments for each captured connection. You can filter all connections by ICMP flows, ICMPV6 flows, VIM flows and TCP flows. Flow graph window is used for showing multiple different topics. Based on it, it offers different controls.

Protocol hiesarchy: This is a tree of all the protocols in the capture. Each row contains the statistical value of one protocol. Two of the columns serve double duty as base graphs. If a display filter is set, it will be shown at the bottom.

Statistics: This section provides a few configurable options for wireshark statistical features.

Problem statement:

Using Wireshark, observe a 3-way handshake establishment, 3-way hand-shaking termination and data transfer in client-server communication using TCP.

3-way handshaking connection Establishment:

1. start Wireshark.
2. Select an interface to use for capturing

packets.

3. Start a network capture by writing down the IP address associated with the selected Ethernet adapter.
4. Open a browser and access a website, then minimize the browser and return to wireshark.
5. Stop the capture.
6. Analyze the captured output in the server capture.
   a) First frame is an ARP broadcast from the source computer to determine the MAC address of the router default gateway.
   b) Second frame is the reply from the router telling the computer the MAC address of its fast Ethernet interface.
   c) Third frame is a DNS query from the computer to the configured DNS server. The computer must have the IP address before it can send the first frame to the Web server.
   d) The fourth frame is the response from the DNS server with the IP address of the website
   e) The fifth frame is the start of the TCP three-way handshake.
7. Filter the capture to view only TCP packets. Look for 3 packets, the first packet - TCP packet is [SYN] packet from the initiating computer. The second is the [SYS, ACK]

response from the Webserver. The third packet is the [ACK] from the source computer which completes the procedure.

8. Inspect the TCP initialization sequence.
   a) The first TCP packet that the relative sequence number is set to 0 and then SYN bit is set to 1 in the flags field.
   b) The second TCP packet of the handshake that the relative sequence number is set to 0, and the SYN bit and the ACK bit are set to 1 in the flags field.
   c) The third and final frame of the handshake, only the ACK bit is set and the sequence number is set to the starting point of 1.
9. The TCP connection is now established and communication between the source computer and the Web server can begin.
10. Close the Wireshark.

RESULT:

Familiarized and understood the use of Wireshark tool.

Scanned with OKEN Scanner