

Introduction to Programming & Networking for Electrical Engineering

Lab 05– Networking

E/21/291

PERERA J.D.T.

[i] List the protocols involved in the communication.

- IP
- HTTP - HYPERTEXT TRANSFER PROTOCOL used by web applications
- TCP - transfer control protocol used by Transport layer
- DNS - domain name system protocol used to resolve web addresses

[ii] Justify the purpose of each protocol used in downloading a web page.

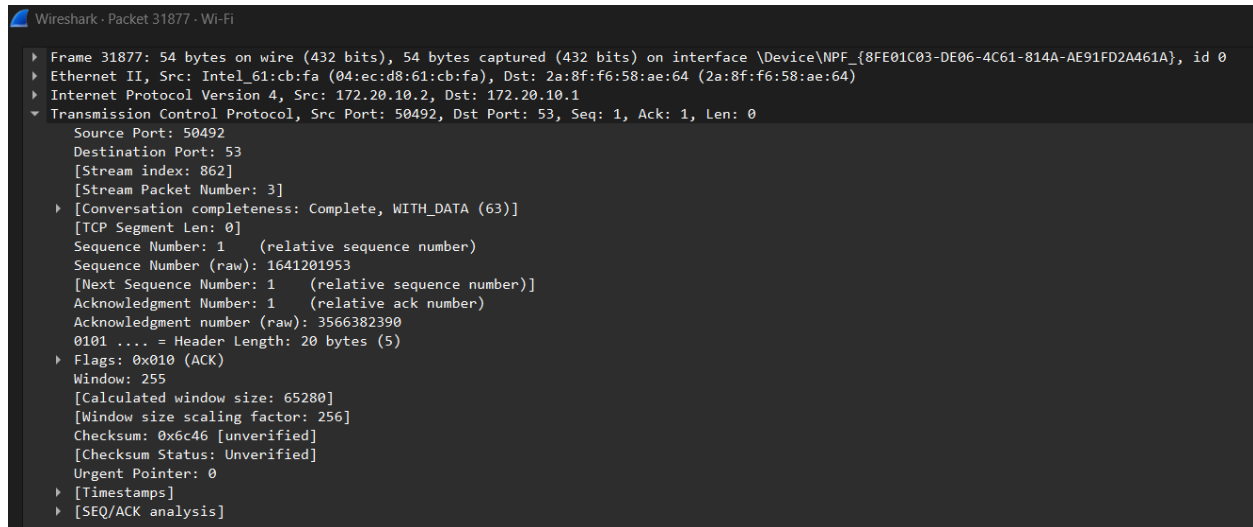
- IP (Internet Protocol): Ensures that data packets are correctly addressed and routed between the web server and the recipient.
- TCP (Transmission Control Protocol): Establishes and maintains a reliable connection, organizes packets in the correct order, and guarantees delivery through acknowledgments.
- DNS (Domain Name System): Converts the domain name entered in the browser into its corresponding numeric IP address.
- HTTP (Hypertext Transfer Protocol): The primary application-layer protocol responsible for sending GET requests to web servers and retrieving HTML content.

[iii] Identify the packets that establish the TCP connection between the client and server (3- way handshake).

The TCP three-way handshake establishes a reliable connection between a client and a server. It consists of the following steps,

1. SYN): The client sends a request to initiate a connection, setting the SYN flag.
2. SYN-ACK : The server responds, acknowledging the request and agreeing to establish the connection, setting both the SYN and ACK flags.
3. ACK : The client confirms the connection by sending a final acknowledgment with the ACK flag set.

[iv] Capture a TCP packet and list its key parameters (e.g., sequence number, acknowledgment number, flags).

A screenshot of the Wireshark network protocol analyzer interface. The top pane shows a list of captured packets, with packet 31877 selected. The middle pane shows the details of this packet, expanded to show the Transmission Control Protocol (TCP) segment. The bottom pane shows the raw packet data in hexadecimal and ASCII. The TCP segment details include: Source Port: 50492, Destination Port: 53, Stream index: 862, Stream Packet Number: 3, Conversation completeness: Complete, WITH_DATA (63), TCP Segment Len: 0, Sequence Number: 1 (relative sequence number), Sequence Number (raw): 1641201953, Next Sequence Number: 1 (relative sequence number), Acknowledgment Number: 1 (relative ack number), Acknowledgment number (raw): 3566382390, 0101 = Header Length: 20 bytes (5), Flags: 0x010 (ACK), Window: 255, [Calculated window size: 65280], [Window size scaling factor: 256], Checksum: 0x6c46 [unverified], [Checksum Status: Unverified], Urgent Pointer: 0, [Timestamps], and [SEQ/ACK analysis].

```
Wireshark - Packet 31877 - Wi-Fi
  ▶ Frame 31877: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{8FE01C03-DE06-4C61-814A-AE91FD2A461A}, id 0
  ▶ Ethernet II, Src: Intel_61:cb:fa (04:ec:d8:61:cb:fa), Dst: 2a:8f:f6:58:ae:64 (2a:8f:f6:58:ae:64)
  ▶ Internet Protocol Version 4, Src: 172.20.10.2, Dst: 172.20.10.1
  ▼ Transmission Control Protocol, Src Port: 50492, Dst Port: 53, Seq: 1, Ack: 1, Len: 0
    Source Port: 50492
    Destination Port: 53
    [Stream index: 862]
    [Stream Packet Number: 3]
    ▶ [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 1 (relative sequence number)
    Sequence Number (raw): 1641201953
    [Next Sequence Number: 1 (relative sequence number)]
    Acknowledgment Number: 1 (relative ack number)
    Acknowledgment number (raw): 3566382390
    0101 .... = Header Length: 20 bytes (5)
    ▶ Flags: 0x010 (ACK)
    Window: 255
    [Calculated window size: 65280]
    [Window size scaling factor: 256]
    Checksum: 0x6c46 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    ▶ [Timestamps]
    ▶ [SEQ/ACK analysis]
```

- Source Port : 50492
- Destination Port : 53
- Stream index : 862
- Steam packet Number: 23
- Conversations Completeness: complete with data (63)
- TCPSegmentLen : 0
- SequenceNumber : 1
- Next Sequence Number: 29
- AcknowledgementNumber : 1
- AcknowledgementNumber(raw) :1641201953
- Flags : 0X010(ACK)
- Window : 255
- Checksum : 0x6c46
- Urgentpointer :0

[v] Identify the parameters used for retransmissions, flow control, and congestion control.

- Retransmissions: Occur when an acknowledgment (ACK) is not received within the expected time frame.
Key parameters: Sequence Number, Acknowledgment Number, Flags.
- Flow Control: Regulates the amount of data that can be transmitted before requiring an acknowledgment, preventing buffer overflow.
Key parameter: Window size.

- Congestion Control: Manages network congestion by dynamically adjusting the window size to prevent excessive data transmission.
Key parameters: Congestion Window, Acknowledgment Number.

[vi] Briefly explain how those parameters work in each case.

- Retransmission - If a sender does not receive an ACK within the timeout period, it retransmits the packet. TCP assumes the packet was lost due to network issues or congestion.
- Flow Control (Sliding Window Protocol) - The receiver advertises the amount of data it can handle using the window size, preventing buffer overflow and ensuring smooth data transmission.
- Congestion Control - TCP dynamically adjusts its sending rate based on detected congestion