IP ADDRESS- 192.268.0.5

**22 0.346996 192.168.0.5 3.33.221.48 TCP 54 50255 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0**

**TCP:**

Transmission Control Protocol, is a fundamental communication protocol used in computer networking that enables reliable, ordered, and error-checked delivery of a stream of data between applications. It's a core part of the Internet Protocol suite and is essential for many internet applications like web browsing, email, and file transfers.

TCP uses a four-step handshake (FIN, ACK, FIN, ACK) to properly close the connection.

TCP uses a  (SYN, SYN-ACK, ACK) to establish a connection between two endpoints.

**1. SYN:**

The client sends a TCP segment with the SYN flag set to signaling the desire to establish a connection with the server.

**2. SYN-ACK:**

The server responds with a TCP segment where both SYN and ACK flags are set to this indicates the server's acknowledgment of the client's SYN and its readiness to synchronize with the client's sequence numbers.

**3. ACK:**

The client, upon receiving the SYN-ACK, sends back a TCP segment with the ACK flag set to confirming the acknowledgment of the server's SYN-ACK and completing the three-way handshake.

**4305 64.116827 192.168.0.5 13.126.138.201 TLSv1.3 85 Application Data**

TLS stands for Transport Layer Security. It's a security protocol that provides privacy and data integrity for communications over the internet. It's the successor to SSL and is used to encrypt various types of internet traffic, including web browsing (HTTPS), email, and messaging.

TLS 1.2 provides enhanced security features, including stronger encryption and improved protection against various attacks.

A screenshot of a computer

AI-generated content may be incorrect.

FRAME-> datalink layer

Packets-> network layer

TCP ->transport layer

**22760 500.951063 192.168.0.5 192.168.0.1 DNS 89 Standard query 0xc48d A v10.events.data.microsoft.com**

Domain Name System (DNS) protocol is a process that allows internet users to navigate the internet using hostnames instead of numeric IP addresses.

recursive DNS servers, root name servers, top level domain name servers and authoritative name servers

Identification, Flags, Number of questions, Number of answers, Number of authority resource records (RRs), and Number of additional RRs.

A screenshot of a computer

AI-generated content may be incorrect.

**8486 145.479704 192.168.0.5 239.255.102.18 UDP 847 52811 → 50002 Len=6725**

UDP stands for User Datagram Protocol. It is a communication protocol used in computer networks, particularly within the TCP/IP

UDP doesn't require a connection to be established before sending data. This means there's no handshake process, resulting in faster data transmission.

UDP is suitable for sending data to multiple recipients simultaneously.

UDP for resolving domain names to IP addresses because of its speed and efficiency.

A screenshot of a computer

AI-generated content may be incorrect.