Name: Cassious Kabwe

Course: Networking

Answers on "Wrapping up the IP header

1. Ipv4 uses 32bit which approximately has four billion unique IP addresses, with the rapid growth of the internet connected devices, the space became insufficient. IPV6 employs a 128 bit addressing scheme, providing an astronomic number of addresses of 340 decillion, ensuring that organizations won't run out of IP addresses anytime soon.
2. - IPv4 uses a 32-bit addressing system, resulting in approximately 4.3 billion unique addresses. However, with the proliferation of internet-connected devices, this address space became insufficient while IPv6 employs a 128-bit addressing scheme, offering an astounding number of addresses—over 1,000 times more than IPv4.
   - IPv4 headers are more complex due to various fields, including checksums and options while IPv6 simplifies the header format, making it more efficient.
3. It ensures data authentication, data integrity and encryption.
   IpV6 offers a lager address space compared to IPV4.
4. Header checksum: In IPv6, the checksum was eliminated, error detection is done on the link layer.
   Options and padding**:** IPv6 moved these options to separate extension headers, reducing the common case header size.

5. A flow refers to a sequence of packets sent from a specific source to a particular unicast or multicast destination.
6. Identification and Tracking: IP addresses serve as identifiers. Attackers can use them to Identify Vulnerabilities and Locate weaknesses in a network.
7. Aggressive Scanning: Attackers can use TTL values to perform firewalking. By sending packets with carefully crafted TTLs to a destination behind a firewall, they can map out what the firewall permits.
8. Quality of Service (QoS)**:** The ToS field allows for prioritization based on delay, throughput, and reliability. However, Misconfiguration can lead to unintended consequences.
9. Hackers exploit fragmentation by sending oversized packets purposefully and also the victimized network fragments and reassembles these packets, consuming resources and potentially causing server crashes.
10. Many IP-based systems come with default usernames and passwords and If administrators fail to change these defaults, attackers can easily gain unauthorized access.

Answers on "Reliability Concepts

1. Without reliability, corrupted or incomplete data could lead to incorrect decisions, financial losses, or even safety hazards.
2. Network layer: This is where fragmentation and reassembly is done to breaks down large packets into smaller fragments and reassembles them at the destination.

   Transport layer: Ensures data delivery from one process to another process on different hosts.

   Application layer: resents data to users through applications.

3. RTT directly impacts user experience. Lower RTT means faster response times, smoother interactions, and better QoS and network administrators use RTT to diagnose and resolve problems.
4. Ensuring that data arrives at the destination unchanged and in the correct order and also preventing data overflow at the receiver.
5. - Unreliable networks can lead to packet loss due to congestion, link failures, or other issues.

- Packets may arrive at the destination out of order due to varying network paths or parallel routes.

6. Acknowledgments (ACKs)**:** To confirm successful receipt of data
Timeouts and Retransmissions**:** To handle lost or delayed packets.
Flow Control**:** To prevent data overflow at the receiver.
Error Detection and Correction**:** To identify and correct errors in transmitted data.
Selective Repeat or Go-Back-N Mechanisms**:** To handle out-of-order packets or duplicate ACKs.
Congestion Control: To prevent network congestion.

7. Individual ACKs: Allows the sender to retransmit only lost packets and provides precise feedback about individual packets.
   Full-Information ACKs: Reduces ACK overhead compared to individual ACKs.
   Cumulative ACKs: Allows retransmission of only missing packets.

8. - When the receiver successfully receives a packet, it sends an ACK(Acknowledgments) back to the sender.

- Detection: The receiver uses these sequence numbers to track the order of received packets.

- Timeouts and Retransmissions**:** If an ACK doesn't arrive within the expected time (timeout), the sender assumes packet loss.

9. Flow Control**:** A larger window allows for more efficient use of available bandwidth, as the sender can keep the network busy with multiple packets in flight.
   Throughput and Efficiency**:** Efficient use of available bandwidth minimizes idle time and maximizes data transmission.
   Latency Reduction**:** A larger window size reduces the impact of round-trip time (RTT) on data transfer.
10. Network Bandwidth**:** Consider the link bandwidth (in bits per second) between sender and receiver.
    Round-Trip Time (RTT)**:** RTT measures the time it takes for a packet to travel from sender to receiver and back.
    Buffer Size**:** The receiver maintains a buffer to store unacknowledged data.
    Network Reliability**:** In reliable networks, a larger window size can fully utilize available bandwidth.
    Congestion Control: Adaptive congestion control algorithms dynamically adjust the window size based on network conditions.