Common Questions

Describe what is indicated by a TCP acknowledgement, what are TCP selective acknowledgements, and how do they change what is acknowledged by TCP. Explain why selective acknowledgements are useful?

- A TCP acknowledgement (ACK) is sent when a packet arrives that contains new data; the acknowledgement number indicates the next contiguous sequence number expected.
- TCP selective acknowledgements (SACK blocks) are a TCP extension that allows a receiver to signal receipt of non-contiguous packets in addition to the standard ACK.
- SACK blocks are useful because they give the sender information that it needs to avoid unnecessary retransmissions when a triple duplicate ACK is received.
- SACK blocks don't affect the congestion control algorithm; they just change what packets are retransmitted.

Do some background reading and explain what is the TCP receive window and what is the impact of window scaling on the receive window. State also the size of the receive window, in bytes, that will be used by the client in this connection.

- The receive window denotes the amount of buffer space the receiver has available to hold data received on a TCP connection.
- The range available in the TCP header proved to be too small for receivers on high-speed networks so a window scale of n increases the signalled window by a factor or 2n to allow for larger windows.

Explain the difference between the receive window and the congestion window in a TCP connection. Which is the limiting factor in TCP throughput?

- The receive window is the available buffer space at the receiver, the congestion window is an estimate of the available network capacity. Performance is limited by whichever is smaller; the receiver needs enough buffering to match the network if the full performance is to be reached.

Consider a modified version of TCP that overlaps these twophases, where the client provides some data as an additional parameter to the connect() function which is sent in the TCP segment that has the SYN bit set, with the response being returned in the SYN+ACK segment. State what would be the benefit of this idea and discuss why it is not feasible in practise.

- This is TCP Fast Open, Some benefits are: Reduce latency as data can be exchanged immediately, reduce the number of round trips, and reduce the number of packets sent.
- The main issue is that it is not secure, SYN packets can be easily spoofed. Attackers could resend previously captured SYN packets, causing servers to process old requests (Replay Attack).
- Many networks block SYN packets, so this would not work on many networks.

Briefly discuss the potential benefits and risks of remembering the congestion window.

- Benefits: Faster connection establishment, less congestion on the network.
- Risks: If the network conditions change, the congestion window may not be appropriate, leading to increased latency or packet loss.
- Risks: If some flows start with a high congestion window, they may starve other flows.

Discuss why and how server push can improve performance, giving an example to illustrate your argument, and stating by what metric are improvements measured. Explain in what circumstances server push might not help, and might even hurt, performance. Finally, state whether you think HTTP server push is likely to be a net benefit overall, justifying your answer.

- Benefits: Server push can improve performance by allowing the server to send data to the client before the client requests it.
- Example: A web page may request an HTML file, but the server can push the file and its associated resources to the client before the client requests it.
- Metrics: Throughput, latency, and resource usage.
- Risks: Server push may not help if the client already has the data, or if the network conditions are such that the client is already receiving data at a high rate.
- Risks: Server push may hurt performance if it causes the client to use more resources than it would otherwise.
- Risks: Cache redundancy, as the server may push the same data that has already been cached by the client.
- Overall, HTTP server push is likely to be a net benefit overall, as it can reduce latency and improve performance.

Discuss the trade-offs that would have been considered when selecting the size of the IPv6 address.

- Benefits: 128-bit address space, perhaps too large for the foreseeable future, but it is unlikely that we will run out of addresses.

People use domain names (e.g., google.com) to identify sites, with software applications performing a DNS lookup to convert these into IP addresses prior to use. The time it takes to perform such a DNS lookup can vary significantly. Explain what causes this variation.

- The time it takes to perform a DNS lookup can vary significantly due to the distance between the client and the DNS server, the load on the DNS server, and the time it takes for the DNS server to respond.
- DNS caching, different website can cache for different times, and the time it takes for the DNS server to respond can vary.

The changing Internet

Definition 1. *A Networked System is a cooperating set of autonomous computing devices that exchange data to perform some application goal*
Note 1. *Channel constraints bound communications speed and reliability*
Definition 2. *The OSI Reference Model: Application Layer, Presentation Layer, Session Layer, Transport Layer, Network Layer, Data Link Layer, Physical Layer*
Note 2. *Real networks don't follow the OSI Reference Model*
Physical Layer: Transmits raw bits over a physical medium.
Baseband Data Encoding: NRZ: 0 is represented by no change in voltage, 1 is represented by a change in voltage. Easy to miscount bits if long run of same value.
Manchester: Encoding: 0 is represented by a transition from high to low, 1 is represented by a transition from low to high.
Modulation: Allows multiple signals on a channel, modulated onto carriers of different frequency. Amplitude Modulation, Frequency Modulation, Phase Modulation.
Data Link Layer: provides framing, addressing, media access control, error detection, and flow control.
Framing: Separate the bitstream into meaningful frames of data.
Media Access Control: How devices share the channel. If another transmission is active, the device must wait until the channel is free.
Network Layer: provides routing, addressing, and packet switching. Internet Protocol (IP).
IPv4: 32-bit address space. Fragmentation difficult at high data rates.
IPv6: 128-bit address space. No in-network fragmentation. Simple header format.
Routing: Each network administered separately - an autonomous system (AS), different technologies and policies.
Inter-domain Rounting: Route advertisements are sent to the routing table of the destination. Border Gateway Protocol (BGP). Advertisements have AS-path.
Transport Layer: provides end-to-end error recovery, flow control, and multiplexing.
TCP: Connection-oriented, reliable, in-order delivery, flow control, congestion control.
UDP: Connectionless, unreliable, out-of-order delivery, no flow control, no congestion control.
Session Layer: provides session establishment, maintenance, and termination.
Managing Connections: How to find participants in a connection, how to setup and manage the connection.
Presentation Layer: provides data representation and encryption.
Application Layer: provides the interface to the application. Deliver email, stream video, etc.
Happy Eyeballs: The process of trying multiple connections to a server to find one that is available.