Georgiy Shevoroshkin 01.01.1980

Computer Networks 1 | CN1

Summary

CONTENTS

1. APPLICATION LAYER (7,6,5)

Combines Layers 7 (Application), 6 (Presentation) and 5 (Session).

1.1. COMMON PORTS

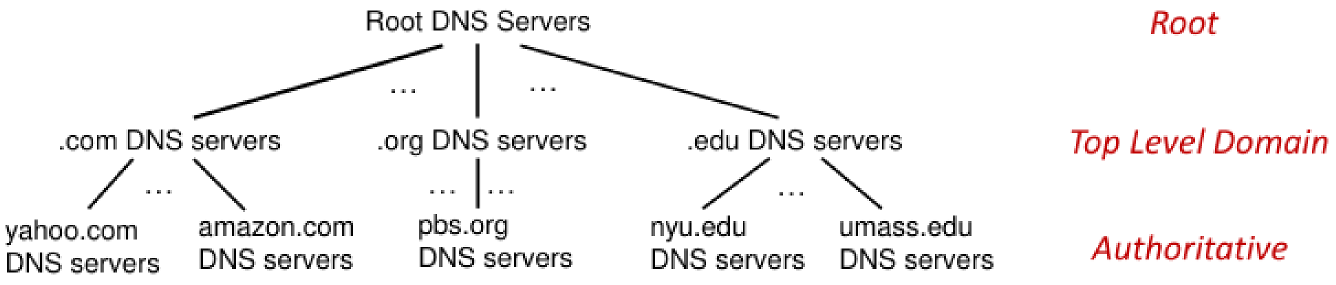
Protocol	*Port*	*Layer 4*
DNS	53	UDP, TCP
HTTP	80	TCP
HTTPS	443	TCP
FTP	20, 21	TCP
SMTP	25 (server) 587 (client)	TCP
POP3	110	TCP
DHCP	67 (server) 68 (client)	UDP

1.2. HTTP

Feature	*HTTP/1.0*	*HTTP/1.1*	*HTTP/2*	*HTTP/3*
Connection Management	One request per connection	Persistent connections by default	Multiplexing allows multiple streams	Uses QUIC for multiplexing
Request Methods	Limited (GET, POST, HEAD)	Enhanced (PUT, DELETE, OPTIONS, etc.)	Same as 1.1	Same as 1.1
Caching	Basic caching support	Improved caching with validation	Advanced caching capabilities	Same as 2 but with improved mechanisms
Header Compression	None	None	HPACK (header compression)	QPACK (header compression)
Server Push	Not supported	Not supported	Supported (automatic resource pushing)	Enhanced support for server push
Performance Improvements	None	Minor improvements over 1.0	Significant improvements in performance and latency	Further improvements in speed and efficiency
SSL/TLS Support	Not inherent	Not inherent, but commonly supported	Built-in support with ALPN (Application-Layer Protocol Negotiation)	Uses QUIC, which incorporates TLS 1.3
Transport Protocol	TCP	TCP	TCP	QUIC

1.3. DNS

Nameservers resolve domains to IP’s through a distributed, hierarchical data-base.



Term	*Definition*
Iterated query	Local DNS server iteratively asks one server after the other, descending the domain name hierarchy step after step.
Recursive query	Local DNS server asks root server for domain, which in turn asks the TLD server, which in turn asks the authoritative server etc. until the “call stack” unwinds and returns the fully resolved domain to the query sender.
Caching	

1.3.1. Record types

Term	*Definition*
A	*name*: hostname *value*: IPv4 address
AAAA	*name*: hostname *value*: IPv6 address
CNAME	*name*: alias *value*: canonical name
NS	*name*: domain *value*: hostname of authoritateive NS for this domain
MX	*name*: domain *value*: name of mailserver

1.4. E-MAIL

Term	*Definition*
ding	
dong	
your	
opinion	
is	
wrong	

2. TRANSPORT LAYER (4)

Segment size: 1440-1480b when using IPv4, ⩽1460b when using IPv6

2.1. PRIMARY RESPONSIBILITIES

- Process-to-process delivery (distinguish between multiple applications via ports)
- Ensure reliable transfer (acknowledgments, retransmissions & reordering)
- Flow control (sender does not overwhelm receiver)
- Congestion control (network is not overloaded)

Term	*Definition*
Port	***16 bit long*** numbers (0d**0**-0d**65535**) for identifying applications to send packets to. ***Well-Known***: 0d**0**-0d**1023** for universal TCP/IP applications, managed by the IANA. ***Registered***: 0d**1024**-0d**49151** for known applications, also managed by the IANA. ***Private***: 0d**49152**-0d**65535** for custom applications, not managed by the IANA.
Socket	Combination of ***IP:Port***.
Multiplexing	Sending data from multiple sockets at sender.
Demultiplexing	Delivering segments to correct socket at receiver.
Checksum	Detect errors (i.e., flipped bits) in transmitted segment.

2.2. TCP

Connection-oriented, bidirectional, reliable, managed data flow.

Term	*Definition*
Handshake	Agreement on **starting sequence numbers**, **maximum segment size** and **window scaling**. 1) SEQ 2) SEQ+ACK 3) ACK
FIN	Termination of a connection. 1) FIN 2) FIN+ACK 3) ACK
Round Trip Time	***RTT*** is the time it takes for a packet to be sent to the receiver and acknowledged back to the sender.
Buffer size	Maximum amount of data (measured in bytes) that can be stored in memory while waiting to be processed or transmitted.

Term	*Definition*
Maximum Segment Size	*MSS* is the maximum payload size of a TCP packet. In IPv4 networks, typically, the size of the MSS is **1460 bytes** because it is encapsulated in the data link layer Ethernet frame size of **1500 bytes**.

2.2.1. Reliability

Term	*Definition*
Sequence numbers	*SEQ* ensures that the packets arrive or can be reassembled in order.
Acknowledgement	*ACK* ensures that the receiver gets all of the packets.
Retransmission timeout	If an acknowledgment is not received before the timer for a segment expires, a retransmission timeout occurs, and the segment is **automatically retransmitted**.
Packet loss rate	Measures how many packets of the ones being sent actually arrive.

2.2.2. Throughput

Term	*Definition*
Throughput	Denoted by *T*, is the amount of data that can be transmitted during a specified time. $\boldsymbol{T = \frac{W}{R} \leq C_{L3}}$
Continuous sending	Sender transmits a stream of data packets in the given window size **without waiting for acknowledgments**.
Delayed ACK	Receiver waits for a short period to acknowledge **multiple segments** with a **single ACK**.
Selective ACK	Instead of asking for a retransmission of all missing segments, *SACK* (specified by the receiver) allows the sender to send only the lost segments, significantly improving efficiency.

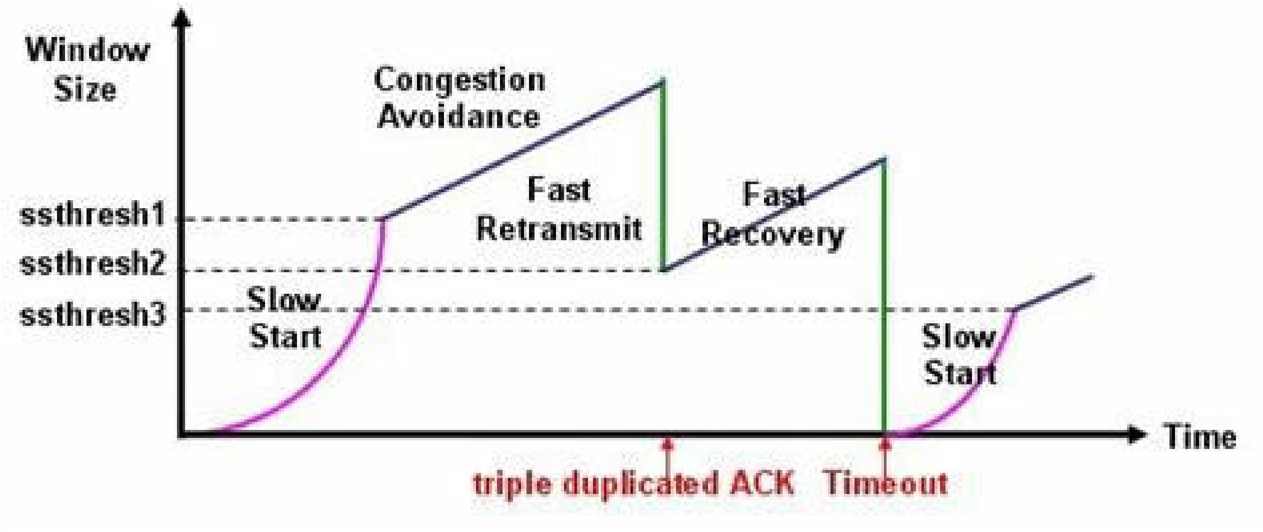
2.2.3. Flow control

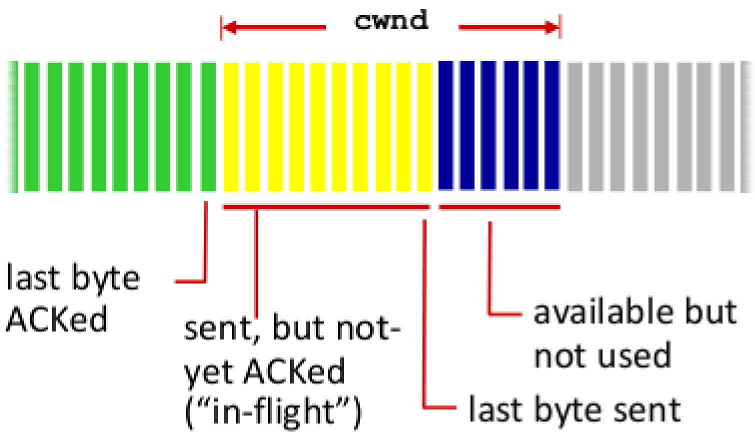
So that the sender does not overwhelm the receiver.

Term	*Definition*
Window Size	Denoted by *W*, is a *16 bit* number sent with each packet by the receiver inside of the **rwnd** header field, indicating the amount of data he still has space for.
Window scale	Used when the TCP window size needs to be increased beyond the traditional maximum of 65,535 bytes due to the demands of high-speed networks. If the handshake header includes the **window scale option** and the packet header includes the **scaling factor** then the effective window size is calculated as such: $\textbf{window size} * \textbf{scaling factor}$

2.2.4. Congestion control

To prevent network congestion.



Term	*Definition*
Congestion window	
Sliding Window	Describes the process of the congestion window sliding to the right after receiving ACKs.
Slow start	Gradual growth (doubling **cwnd** every **RTT**) within the congestion window size at the start of a connection or after a period of state of no activity. *Purpose*: Allows the sender to probe the available bandwidth in a controlled way.
Congestion avoidance	Transition from sluggish start to congestion avoidance segment after accomplishing a threshold. *Purpose*: Maintains a truthful share of the community bandwidth even as heading off excessive congestion.
Fast Retransmit	Detects packet loss through duplicate acknowledgments and triggers speedy retransmission without waiting for the **retransmission timeout**. *Purpose*: Speeds up the recuperation method with the aid of retransmitting lost packets without looking ahead to a timeout.

Term	*Definition*
Fast Recovery	Enters a quick healing state after detecting packet loss, lowering congestion window and transitioning to congestion avoidance. *Purpose*: Accelerates healing from congestion by way of avoiding a complete go back to slow begin after packet loss.
AIMD	Adjusts the congestion window size based on network situations following the **Additive Increase, Multiplicative Decrease** principle. *Purpose*: Provides a balanced approach by way of linearly growing the window all through congestion avoidance and halving it on packet loss.

2.3. UDP

2.4. QUIC

Actually a layer 7 Protocol, running on top of UDP

3. NETWORK LAYER (3)

Packet size: 1500b

4. BINARY, DECIMAL, HEX

0x**A46A** = 0b**1010010001101010** = 0d**42090**