Navyashree. A.M
2022ebcs039
TCP/IP and Internet

SCIA - 01

Network Engineering

03-10-2025

① HTTP Statelessness, Cookies, Caching, & HTTP/1.1 VS HTTP/2

Ans → Statelessness in HTTP

HTTP is a Stateless protocol, meaning each request from a client to server is treated independently with no memory of previous interactions. The server doesn't retain any client state b/w request, this simplifies server design but requires additional mechanisms for maintaining state in applications that need it.

Role of cookies

Cookies are small Data pieces sent by server to clients, which store & return them with subsequent requests They help maintain stat in HTTP by

- managing user sessions (logins, shopping cart etc)
- storing user preferences & settings
- tracking user behaviour for analytics

Role of caching

Caching stores responses for reuse in subsequent requests helping to

→ Reduce latency by serving content faster
→ Decrease network traffic & server load
→ Improve overall user Experience

caching occurs at various points; browser cache
proxy cache
CDN cache

HTTP/1.1 vs HTTP/2

HTTP/1.1

- -> Text-based protocol
- -> Each TCP connection handles one request at a time
- -> Request multiple parallel connections for dynamic pages
- -> Head of line blocking: slow requests block others
- -> NO header compression

HTTP/2

- -> Binary protocol
- -> multiplexing multiple requests/responses over single TCP connection
- -> No-head of line blocking
- -> Header compression (HPACK)
- -> Server push capability
- -> Stream prioritization

for dynamic webpages, HTTP/2 significantly improve performance by eliminating the need for multiple connections reducing latency through multiplexing -> decreasing protocol overhead

TCP/IP

② Multiplayer online Game System Design

In a multiplayer online game DNS, HTTP, TCP & UDP work together as follows

Domine Name System (DNS)

- Resolve game server domine name to IP address
- Directs players to geographically closet servers using GeoDNS
- Ex: A player in India connects to a Mumbai server rather than a Tokyo one

HTTP (Hypertext Transfer protocol)

- Handels non-real time communication
  - Authentication and login
  - game updates & patches
  - Leaderboards & statistics
  - Account managment & in-game purchases

Ex:- player credentials sent via HTTPS for authentication

Transmission control protocol (TCP)

- used for reliable, ordered delivery of
  - intial game start synchronization
  - critical game events
  - Chat message
  - Turn-based game moves

Ex:- A strategy game move is reliably delivered to all players

UDP (User Datagram protocol)

Used for real-time data where speed is critical

- player position updates
- moments & action commands
- Game state changes that can tolerate some loss

Ex:- A first person shooter constantly sends position update via UDP

Integration Ex:-

- player launches game client
- DNS resolves game.example.com to nearist server IP
- Tcp connection established for login and initial setup
- HTTP Handels Authentication & configuration
- UDP message real-time gameplay data
- Tcp ensures periodic game state consistency
- HTTP processes non criticalcations like purchess
- This combination leverages each protocol strengthens
- DNS for roughter Tcp for relability where needed
- UDP for speed & HTTP for web based surves

③ TCP Reliability, Flow control, and Congestion Control

Sequence Numbers

- Each bite of a Data has a unique sequence number
- Indicates the first byte of Data in the current Segment
- Enable detection of missing duplicate or out-of order Segments.

Ex:- If Segment with sequence numbers 1000-1499 & 1500-1999 are sent but only the second arrives the reciver knows its missing bytes 1000-1499

Acknowledgment Numbers

- Reciver uses these to confirm receipt of data
- Specifies the next sequence number the reciver Expects
- Implicitly acknowledges all previus bytes

Ex:- Recising bytes 1000-1999 result in an Ack with number 2000

Window Size

- Indicates how much Data the Sender can transmit before recising an Ack
- Part of TCP's flow control mechanism
- prevents Sender from overwhelming reciver

Ex:- with a window size of 10,000 bytes & last Ack 8000, the Sender can transmit up to sequence number 15000

Reliable, in-order Delivery:

These mechanism works together to ensure

1. Sequence numbers detect missing segments
2. Acks inform Sender of delivered data
3. Unacknowledged data is retransmitted after timeout
4. reciver uses Sequence numbers to reorder segments
5. window size regulates data flow

Flow Control vs Congestion Control

Fc:- purpouse :- prevent sender from overwhelming receiver
mechanism : Receiver advertised window size
focus :- End to end b/w sender & reciver
Trigger :- Receiver's buffer capacity
Response :- Direct adjustment based on recvers window

Cc :-
purpous :- prevent sender from overwhelming network
mechanism : Internally calculated congestion window (cwnd)
focus :- network path b/w sender & recvr
trigger :- packet loss or increased delay
Response :- gradul increase rapid decrease when congestion detected

Effective window: min (Receivers Advertised window, Congestion window)

(4) Subnetting Scheme Design

Given :
Starting IP : 10.0.0.0/24
need : 5 subnets with at least 30 usable IPs

Analysis :
- 10.0.0.0/24 provides 256 addresses (10.0.0.0 to 10.0.0.255)
- 254 usable IPs (excluding network & broadcast address)
- for 30 usable IPs need 32 total addresses
- 32 addresses required 5 bits for host portion ($2^5=32$)
- Leves 3 bits for subnet portion ($8-5=3$)
- with 3 bits can create 8 subnets ($2^3=8$)
more than required 5

The 5 Subnets

① Subnet 1

- Network Adress: 10.0.0.0/27
- usable IP range: 10.0.0.1 to 10:00:30
- Broadcast Adress: 10:0:0.31
- Total usable IPs: 30

② Subnet 2

- Network Adress: 10.0.0.32/27
- usable IP Range: 10.0.0.33 to 10:0:0
- Broad cast Address: 10.0.0.63
- Total usable IPs: 30

③ Subnet 3

- Network adress: 10.0.0.64/27
- usable IP Range: 10.0.0.65 to 10.0.0.94
- Broad cast Adress: 10.0.0.95

total usable IPs: 30

④ Subnet 4

- Network adns: 10.0.0.96/27
- usable IP Range: 10.0.0.97 to 10.0.0.126
- Broad cast adnss 10.0.0.127

total usable IP's 30

⑤ Subnet 5

network address: 10.0.0.128/27

usable IP range: 10.0.0.129 to 10.0.0.158

Broad cast address: 10.0.0.159

total usable IPs 30

⑤ Network Designing with OSPF & BGP

OSPF (Interior Gateway protocol)

- used with a single autonomous system (AS)
- Link state protocol: fast convergence hierarchical
- Requires all router in area to hall Same topology DB

BGP (Exterior Gateway protocol)

- Connects ASes (eg company AS to ISP)
- Path vector protocol policy-based routing
- Slower convergence but scalable for internet

Key Considerations:

- Redistribution: Routes from OSPF must be injected into a BGP (and vice versa) border routers (ASBRs) Risk of routing loops if not filtered
- Scalibility: OSPF areas reduce LSDB size BGP uses route summarization
- policy Control: BGP allows selective advertisment (eg. only advertise summery route 10.0.0.0/22 to ISP)
- Convergence: OSPF reacts quickly to internal failures BGP relies on keepalives (default 60s hold timer)

Ex:- A Globle Company uses OSPF in each regional office (Area 0 backbone). Border router in NY London run BGP to connect to ISP. NY router redistribute OSPF-learned routes (10.1.0.1/24 (10.2.0.0/24 via BGP. ISP advertises default route via BGP to Company Route maps prevent internal loopbacks from being advertised Extra