بسمه تعالی

تمرین 1
شبکه‌های کامپیوتری

محسن کربلائی امینی، 98242128

اردیبهشت 1403

فصل 1:

سوال 1:

شبکه‌های سوئیچ مدار (Circuit-Switch) نسبت به شبکه‌های سوئیچ بسته (Packet-Switch) دارای مزایای زیر هستند:
۱ .تضمین پهنای باند: مسیر اختصاصی برای ارتباط بین دستگاه‌ها ایجاد می‌شود و پهنای باند مشخصی به طور انحصاری در اختیار آن‌ها قرار می‌گیرد.
۲ .تعیین دقیق کیفیت سرویس: شبکه‌های سوئیچ مدار با تخصیص مسیر اختصاصی، قادر به کنترل دقیق پارامترهایی مانند تأخیر، jitter و از گم شدن بسته‌ها هستند.
۳ .اتصالات پایدار: با استفاده از مسیر اختصاصی، ارتباط بین دستگاه‌ها در شبکه‌های سوئیچ مدار به صورت پایدار حفظ می‌شود. این ویژگی برای سرویس‌هایی که نیاز به اتصال پایدار و طولانی‌مدت دارند مثل تماس‌های تلفنی، بسیار مهم است.

استفاده از TDM (تقسیم زمانی چندگانه) در شبکه‌های سوئیچ مدار نسبت به FDM (تقسیم فرکانسی چندگانه) مزیت‌هایی دارد. TDM زمان را بین کانال‌ها تقسیم کرده و هر کانال در زمان مشخص خود اطلاعات را ارسال می‌کند. این روش به شبکه‌های سوئیچ مدار امکان می‌دهد تا بیش از یک ارتباط را همزمان بر روی یک خط ارسال کنند. اما در FDM، برای انتقال سیگنال‌های مختلف، فرکانس‌های مختلفی از طیف فرکانسی استفاده می‌شود. هر سیگنال به صورت جداگانه به یک فرکانس منحصر به فرد تخصیص می‌یابد. سپس سیگنال‌ها بر روی خط ارتباطی ترکیب می‌شوند تا بتوانند همزمان انتقال داده شوند

سوال 2:

دسترسی خانگی:

1. خطوط دیجیتالی مشترک (DSL)
2. اینترنت کابلی

دسترسی سازمانی:

1. MPLS
2. وای‌فای (شبکه بی‌سیم)

دسترسی بی‌سیم منطقه گسترده:

1. 5G

سوال 3:

پروتکل Ethernet قادر است بر روی انواع رسانه‌های سخت افزاری مختلف اجرا شود، از جمله:

- کابل‌های اترنت یا LAN
- فیبر نوری

نرخ انتقال اطلاعات Ethernet بسته به استاندارد مورد استفاده متفاوت است. به عنوان مثال:

- Fast Ethernet: نرخ انتقال اطلاعات تا 100 مگابیت بر ثانیه (Mbps).
- Gigabit Ethernet: نرخ انتقال اطلاعات تا 1 گیگابیت بر ثانیه (Gbps).
- 10 Gigabit Ethernet: نرخ انتقال اطلاعات تا 10 گیگابیت بر ثانیه (Gbps).
- 40 Gigabit Ethernet: نرخ انتقال اطلاعات تا 40 گیگابیت بر ثانیه (Gbps).
- 100 Gigabit Ethernet: نرخ انتقال اطلاعات تا 100 گیگابیت بر ثانیه (Gbps).

سوال 4:

دسترسی بی‌سیم به اینترنت از طریق انواع رسانه‌های بیسیم صورت می‌گیرد. در زیر، برخی از رسانه‌های بیسیم معمول که برای دسترسی به اینترنت استفاده می‌شوند را بررسی می‌کنم و آنها را مقایسه می‌کنم:

- Wi-Fi: از طریق یک نقطه دسترسی، دستگاه‌ها می‌توانند به شبکه بی‌سیم متصل شوند و به اینترنت متصل شوند . Wi-Fiپهنای باند بیشتری را در اختیار کاربران قرار می‌دهد و می‌تواند در محدوده‌های محدودی خدمت رسانی کند. سرعت اتصال و پهنای باند ممکن است به تعداد دستگاه‌ها و محدودیت‌های فیزیکی مرتبط با محیط تحت پوشش تأثیر بگذارد.
- موبایل (شبکه همراه): ارتباط اینترنت بی‌سیم را می‌توان از طریق شبکه همراه موبایل برقرار کرد. این روش از طریق شبکه‌های تلفن همراه مانند 4G/LTE و 5G امکان‌پذیر است. این شبکه‌ها پوشش گسترده‌تری از طریق سلول‌های تلفن همراه فراهم می‌کنند و قابلیت دسترسی به اینترنت را در مسیر حرکت فراهم می‌سازند. مجددا، سرعت اتصال و پهنای باند ممکن است به ترافیک شبکه و شرایط سیگنال در منطقه تحت پوشش وابسته باشد.

سوال 5:

1. Application Layer: داده برنامه‌ها یا message در این لایه تعریف می شود.

- وظایف اصلی: ارائه خدمات شبکه برای برنامه‌های کاربردی، مانند ارسال و دریافت داده‌ها، مدیریت هویت و رمزنگاری.
- امکان اجرا در بین دو یا چند لایه: برخی از وظایف مانند رمزنگاری و فشرده‌سازی می‌توانند در الیه Transport Layer نیز انجام شوند، اما این وظایف اصلی در Application Layer قرار دارند.

2. Transport Layer: با اضافه کردن header های مورد نیاز، و یا trailer ها نظیر checksum ها و تکه تکه شدن پیام‌های اصلی، در این لایه segment ها تعریف می‌شوند.

- وظایف اصلی: تعیین نوع برقراری ارتباط موثر و قابل اطمینان بین دستگاه‌ها، کنترل جریان داده، تقسیم بندی و بازسازی داده‌ها، و تشخیص و اصلاح خطاها.
- امکان اجرا در بین دو یا چند لایه: برخی از وظایف مانند تقسیم بندی و بازسازی داده‌ها می‌توانند در الیه Network Layer نیز انجام شوند، اما وظایف اصلی Transport Layer شامل کنترل جریان داده و تشخیص و اصلاح خطاها به طور انحصاری بر عهده این لایه است.

3. Network Layer: در این لایه header های مورد نیاز برای مسیریابی نظیر اطلاعات مربوط به مبدا و مقصد اضافه می‌شوند و datagram را تشکیل می‌دهد.

- وظایف اصلی: مسیریابی بسته‌ها، تقسیم بندی داده‌ها به بسته‌ها، و مدیریت ترافیک شبکه.
- امکان اجرا در بین دو یا چند لایه: برخی از وظایف مانند تقسیم بندی داده‌ها و مدیریت ترافیک ممکن است در لایه Transport Layer نیز انجام شوند .همچنین، برخی از وظایف مسیریابی می‌توانند در لایه Link Layer نیز اجرا شوند مانند NAT.

4. Link Layer: در این لایه header های مربوط به آدرس‌دهی فیزیکی مانند پروتکل Ethernet به بسته اضافه و frame را تشکیل می‌دهد.

- وظایف اصلی: ارائه خدمات به سخت‌افزار شبکه، مدیریت ارسال و دریافت فریم‌ها، تشخیص و اصلاح خطاها، و کنترل دسترسی به رسانه انتقال.
- امکان اجرا در بین دو یا چند لایه: برخی از وظایف مانند تشخیص و اصلاح خطاها ممکن است در لایه Network Layerانجام شوند. همچنین، کنترل دسترسی به رسانه انتقال ممکن است در الیه Network Layer نیز مدیریت شود.

سوال 6:

- مسیریاب: لایه شبکه (3)
- سوییچ: لایه 2 و بعضا لایه 3
- میزبان: لایه 4 و 5

سوال 7:

مزایای Peer شدن سرویس دهندگان اینترنتی:

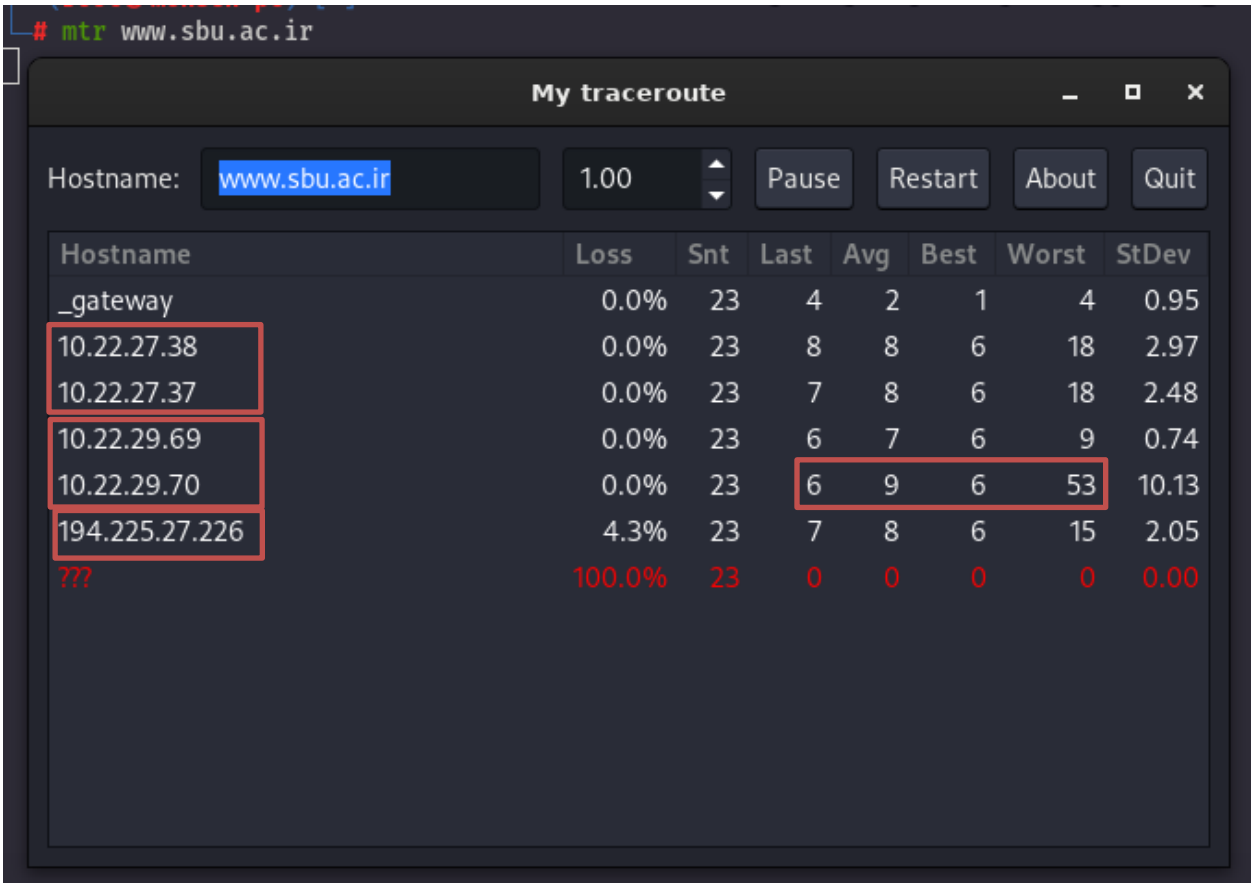
1. کاهش هزینه‌ها: با برقراری اتصال مستقیم بین سرویس دهندگان اینترنتی، نیازی به استفاده از سرویس دهندگان جایگزین (Transit Providers) برای رساندن ترافیک شبکه نیست. این موضوع منجر به کاهش هزینه‌های اتصال به اینترنت و ترافیک داده می‌شود.

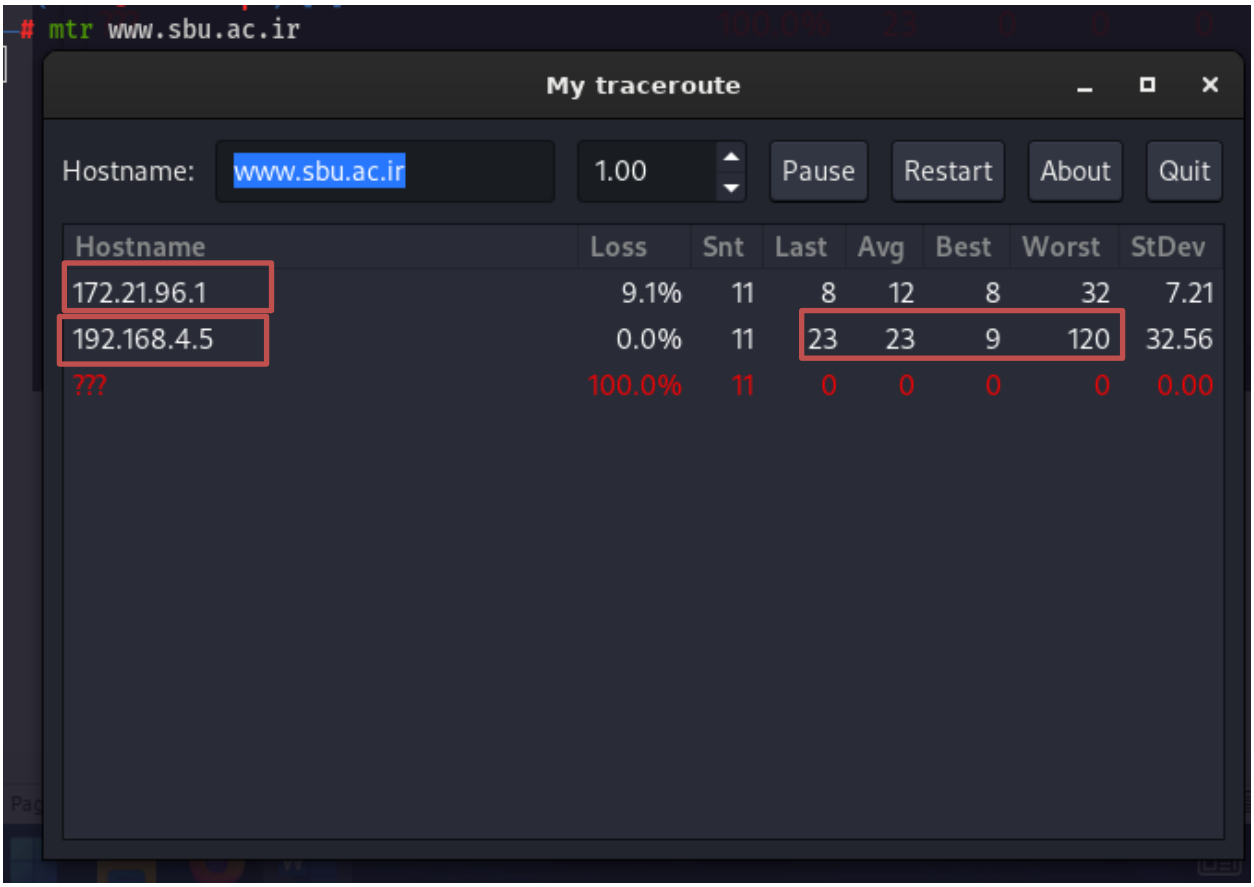
2. بهبود کیفیت: با Peer شدن با سرویس دهندگان دیگر، ترافیک شبکه می‌تواند به صورت مستقیم و بدون واسطه انتقال پیدا کند. این امر باعث کاهش تأخیر و افزایش سرعت انتقال داده می‌شود، که در نتیجه کیفیت خدمات به مشتریان بهبود می‌یابد.
3. افزایش قابلیت دسترسی: با Peer شدن در سطح محلی و منطقه‌ای، سرویس دهندگان اینترنتی به یکدیگر نزدیک‌تر می‌شوند و از طریق ارتباطات مستقیم، قابلیت دسترسی به مناطق دیگر را بهبود می‌بخشند. این امر می‌تواند به توسعه و گسترش شبکه‌های ارتباطی کمک کند.

IXP یا Internet Exchange Point نقطه تقاطعی است که در آن سرویس دهندگان اینترنتی و سرویس‌دهنده‌های محتوا ترافیک شبکه را با یکدیگر مبادله می‌کنند. نقشIXP ها در درامدزایی به شرح زیر است:

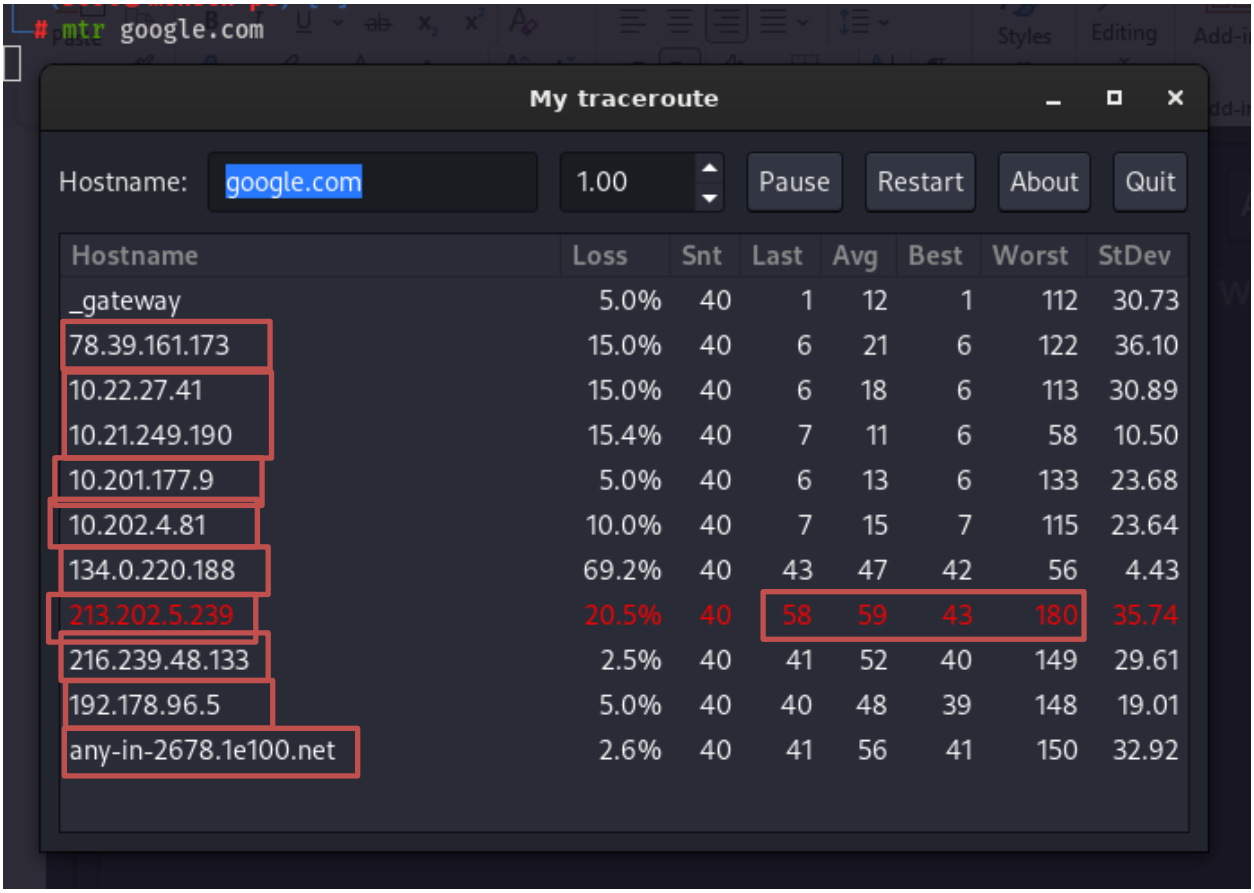
1. هزینه کاهش می‌یابد: با مبادله مستقیم ترافیک درIXP ، نیاز به استفاده از سرویس دهندگان جایگزین و پرداخت هزینه‌های بیشتر برای اتصال به شبکه‌های دیگر کاهش می‌یابد. این امر باعث کاهش هزینه‌های عملیاتی برای سرویس دهندگان اینترنتی می‌شود.
2. درآمدزاییIXP : معمولاً هزینه‌های عضویت را از سرویس دهندگان دریافت می‌کنند. همچنین، برخیIXP ها می‌توانند هزینه‌های دیگری مانند هزینهٔ بستر و پهنای باند را نیز از اعضا دریافت کنند. این درآمدها می‌توانند برای تامین هزینه‌های عملیاتی IXP و سرمایه‌گذاری در بهبود زیرساخت‌ها استفاده شوند .همچنین، IXPها می‌توانند فرصت‌های درآمدزایی دیگری از طریق ارائهٔ خدمات اضافی به اعضا فراهم کنند، مانند ارائهٔ سرویس‌های امنیتی، مانیتورینگ ترافیک و مدیریت ترافیک.

سوال 8:


mtr www.sbu.ac.ir
My traceroute
Hostname: www.sbu.ac.ir
1.00
Pause
Restart
About
Quit
Hostname Loss Snt Last Avg Best Worst StDev
_gateway 0.0% 23 4 2 1 4 0.95
10.22.27.38 0.0% 23 8 8 6 18 2.97
10.22.27.37 0.0% 23 7 8 6 18 2.48
10.22.29.69 0.0% 23 6 7 6 9 0.74
10.22.29.70 0.0% 23 6 9 6 53 10.13
194.225.27.226 4.3% 23 7 8 6 15 2.05
??? 100.0% 23 0 0 0 0 0.00



ظاهرا پروتکل ICMP بر روی این آدرس توسط فایروال فیلتر شده و امکان ping این مقصد وجود ندارد. اما همچنان از دو مسیر متفاوت رسیدن به این مقصد قابل مشاهده است. آدرس‌های نزدیک به هم وبیشترین تاخیر در تصاویر مشخص شده‌اند. البته که در این تصاویر IP های رنج‌های private لزوما نمی توانند مربوط به یک سرویس دهنده اینترنت باشند، اما با چنین فرضی تعداد ISP ها تا مقصد 3 و 2 می‌باشد. در تصویر بعدی گزارش مربوط به google.com به همین شکل آمده است:



فصل 2:

سوال 1:

خیر. در هر نشست می توان نقش‌های سروری و کلاینتی را تعریف کرد. به طور کلی میزبانی که درخواست را ارسال میکند کلاینت و میزبانی که درخواست را پاسخ دهد سرور است. تفاوت پروتکل‌های P2P در این است که یک میزبان هر دو نقش را می‌تواند بر عهده بگیرد اما در یک ارتباط کلاینت سروری، این نقش‌ها همیشه ثابت هستند.

سوال 2:

- IP Address
- Port
- Protocol

سوال 3:

UDP
این پروتکل به دلیل عدم وجود چک‌های متعدد برای صحت و تمامیت و ترتیب درست بسته‌های ارسالی، سرعت بهتری نسبت به TCP دارد و تاخیر به حداقل میرسد، اما ممکن است در این ارتباط برخی از اطلاعات گم شود و به مقصد نرسد.

سوال 4:

این پروتکل برای ایجاد رمزنگاری جهت محافظت از تمامیت، محرمانگی، تایید هویت وانتقال امن داده‌ها توسعه داده شده است و این پروتکل میان لایه کاربرد و انتقال قرار دارد. به عبارت دیگر، TLS بر روی ارتباط TCP در لایه‌ی انتقال قرار می‌گیرد و ویژگی‌های امنیتی را برای برنامه‌های کاربردی که از ارتباط TCP استفاده می‌کنند، فراهم می‌کند.
برای ایجاد ارتباط TLS نیاز به یک الگوریتم رمزنگاری نامتقارن وجود دارد که Certificate توسط یک Certificate Authority امضا شده و به عنوان نهاد سوم مورد اعتماد کلاینت و سرور قرار می‌گیرد. در سمت سرور(توسعه دهنده) باید یک Certificate و یک کلید خصوصی قرار گیرد تا این رمزنگاری به شکل صحیح انجام شود. سپس برنامه نویس باید مراحل مذاکره و تبادل پارامترهای امنیتی (Handshake) را با استفاده از توابع مربوطه در کتابخانه TLS انجام دهد. این مراحل شامل تأیید هویت سرور، توافق بر روی الگوریتم‌های رمزنگاری و شناسایی کلیدها است. و در نهایت انتقال داده‌ها از کانال امن ایجاد شده.

سوال 5:

- IMAP و SMTP
به این دلیل که تمامیت محتوای یک ایمیل بسیار دارای اهمیت است و نمیتوان بخشی از یک محتوی را از دست داد. UDP یک پروتکل ساده و بدون وضعیت است اما ساختار پیچیده و چند وضعیتی TCP امکاناتی بیشتری را در اختیار این پروتکل‌ها قرار می‌دهد.
- HTTP
به این دلیل که دریافت نشدن بخشی از یک Hypertext مثلا یک فایل باینری عملا می‌تواند آن را بی استفاده کند. این پروتکل بر پایه ارتباطات درخواست-پاسخ می‌باشد که ارتباط پایداری که TCP برقرار می کنند بسیار برای این مورد مناسب است.

سوال 6:

- توزیع بار: سرورهای CDN باید قادر باشند به صورت پویا ترافیک را توزیع کنند و بهترین مسیر را برای انتقال محتوا انتخاب کنند.
- موقعیت جغرافیایی: موقعیت جغرافیایی سرورهای CDN بسیار اهمیت دارد. سرورهایی که در نزدیکی کاربران قرار دارند، به طور عمومی زمان پاسخ کمتری داشته و می‌توانند تاخیر بارگیری را کاهش دهند.
- قابلیت مقیاس‌پذیری: سرورهای CDN باید قابلیت مقیاس‌پذیری داشته باشند، به این معنی که بتوانند به صورت افزونه و به میزان نیاز، تعداد سرورها را افزایش داده و بار ترافیکی را به طور موثر توزیع کنند.

سوال 7:

اختلال HOL (Head-of-Line) Blocking یک مشکل در پروتکل HTTP/1.1 است که در انتقال و تحویل محتوا ممکن است رخ دهد. وقتی که یک درخواست HTTP شامل چندین منبع مثلاً تصاویر، فایل‌های CSS و جاوااسکریپت ارسال می‌شود، اگر یکی از منابع به هر دلیلی طولانی‌تر از سایر منابع زمان ببرد، سایر منابع نیز باید منتظر اتمام بارگیری آن منبع باشند. به عبارتی دیگر، تمام درخواست‌های بعدی باید به ترتیب انتقال یابند و هیچ درخواستی نمی‌تواند جلوتر از دیگری قرار بگیرد. این باعث ایجاد تاخیر در بارگیری وب‌سایت می‌شود و عملکرد کلی شبکه را کاهش می‌دهد.

اما در پروتکل HTTP/2، این مشکل به طور قابل توجهی کاهش یافته است. HTTP/2 از مکانیزمی به نام "مولد جریان (Stream Multiplexing) "استفاده می‌کند که به سرور امکان ارسال همزمان چندین درخواست و پاسخ را می‌دهد. در این حالت، هر درخواست و پاسخ در یک جریان (Stream) جداگانه قرار می‌گیرد و ترتیب ارسال و دریافت آنها مستقل از یکدیگر است. این به ارسال همزمان منابع مختلف اجازه می‌دهد و اختلال HOL Blocking را کاهش می‌دهد. در نتیجه، منابعی که زمان بیشتری برای بارگیری نیاز دارند، قادر به انتقال و دریافت می‌شوند و جریان عملکرد سریع‌تر و بهبود یافته‌ای را فراهم می‌کند.

سوال 8:

در پروتکل SMTP (Simple Mail Transfer Protocol)، انتهای بدنه پیام با استفاده از یک نقطه مشخص می‌شود.

در مقابل، در پروتکلHTTP ، انتهای بدنه پیام با استفاده از مقدار هدر "Content-Length" یا "Transfer-Encoding"مشخص می‌شود. در صورت استفاده از"Content-Length" ، طول بایتی بدنه پیام در هدر اعلام می‌شود و سرور می‌تواند با استفاده از این طول بدنه را برش‌های مناسب تشخیص داده و به خواندن آن بپردازد. در صورت استفاده از"Transfer-Encoding" ، پیام به شکل فشرده یا تکه‌تکه ارسال می‌شود و انتهای بدنه با استفاده از برخی نشانگرهای خاص مشخص می‌شود.

اگرچه اصولاً HTTP از روش مشابه SMTP برای مشخص کردن انتهای بدنه پیام استفاده نمی‌کند، اما می‌توان با استفاده از ترکیبی از هدرها و قوانین مشخص کردن ساختار پیام، مانند Content-Type و Content-Length، انتهای بدنه را تشخیص داد. با این حال، به دلیل اینکه HTTP در اصل برای انتقال محتواهای مختلف مانند HTML، تصاویر و فایل‌ها طراحی شده است، بدنه پیام‌ها در HTTP معمولاً به شکل فایل‌های جداگانه انتقال می‌یابند و نیازی به تعیین انتهای دقیق بدنه پیام در بدنه اصلی HTTP نیست.

سوال 9:

- /cs453/index.html
- 1.1
- پایدار به دلیل وجود keep alive
- Windows;U; Windows NT 5.1; en-US;) User-Agent: Mozilla/5.0 (rv:1.7.2
  - چه فونت‌هایی دستگاه ما استفاده می‌کند؟ آیا نیاز به ارسال فونت‌های مناسب وجود دارد؟
  - ابعاد صفحه به چه شکل است؟ (موبایل یا مانیتور یا ...)

سوال 10:

- بله. GMT12:39:45 Date: Tue, 07 Mar 2008
- Last-Modified: Sat, 10 Dec2005 18:27:46 GMT
- Content-Length: 3874
- بله. Connection: Keep-Alive