



دانشکده مهندسی کامپیوتر

بسته‌های
دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)
دانشکده مهندسی کامپیوتر

درس شبکه‌های کامپیوتری، نیم سال دوم سال تحصیلی ۱۴۰۱-۱۴۰۰

پایخ تمرین سری سوم

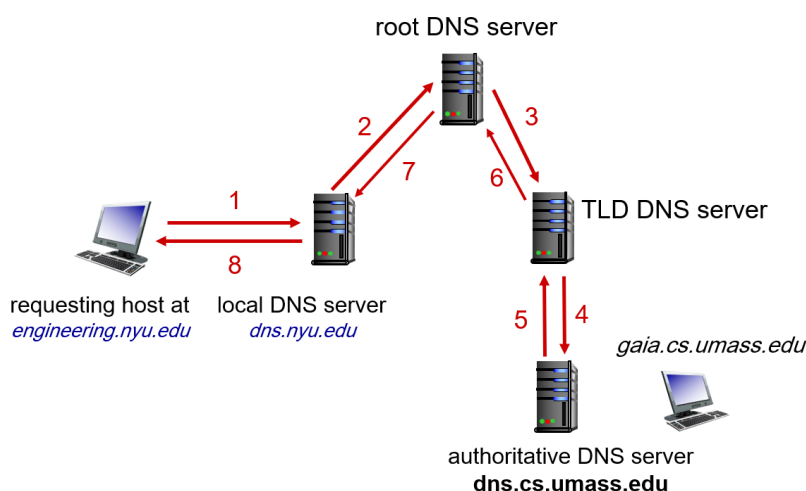


دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

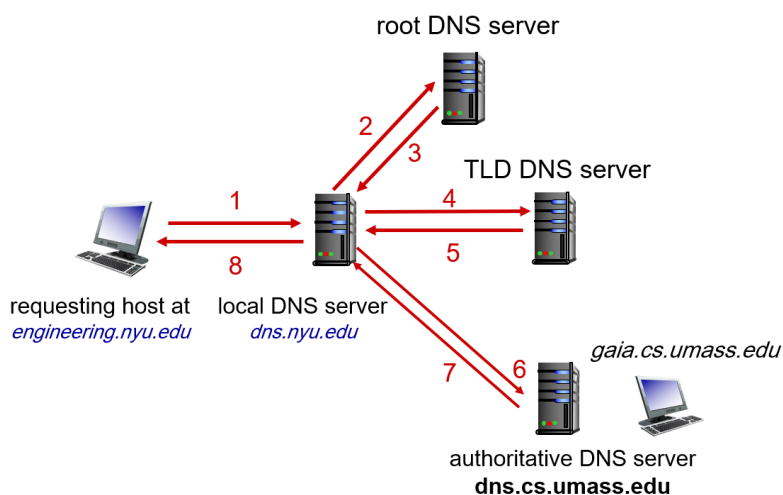
پاسخ سوال ۱:

الف:

در یک پرسمان بازگشتی، مطابق با شکل زیر، سرور DNS محلی، درخواست کلاینت را به سرور DNS ریشه می‌دهد و سرور DNS ریشه این درخواست را به سرور DNS، TLD داده و به همین ترتیب ادامه پیدا می‌کند تا نهایتاً آن درخواست به سرور DNS ذیصلاح می‌رسد. سرور DNS ذیصلاح در پاسخ آدرس IP را به صورت بازگشتی بر می‌گرداند، تا نهایتاً پاسخ به سرور DNS محلی رسیده و سرور DNS محلی پاسخ را به کلاینت می‌دهد. اما در روش پرسمان تکرارشونده مطابق با شکل، سرور DNS محلی، درخواست کلاینت را به سرور DNS ریشه داده و سرور DNS ریشه در پاسخ به این درخواست آدرس DNS، TLD را بر می‌گرداند و سپس سرور DNS محلی آن درخواست را به سرور DNS، TLD داده و آدرس سرور DNS بعدی را در پاسخ می‌گیرد. این روند به صورت تکرارشونده ادامه پیدا می‌کند تا نهایتاً سرور DNS محلی آن درخواست را به سرور DNS ذیصلاح داده و در پاسخ آدرس IP مورد نظر را دریافت کرده و آن را به کلاینت ارسال می‌کند.



(پرسمان بازگشتی)



(پرسمان تکرارشونده)



ب:

فرض کنید سلسله مراتب نام دامنه‌ای که قرار است آدرس IP آن بدست آید، n باشد. آنگاه درخواست پس از دریافت توسط سرور DNS محلی به صورت بازگشتی یا به صورت تکرار شونده باید به n سرور DNS دیگر داده شود. زمان پاسخ برابر است با:

برای روش تکرارشونده:

$$ResponseTime_{Iterative} = RTT_1 + nRTT_r$$

برای روش بازگشتی:

$$ResponseTime_{Recursive} = RTT_1 + RTT_r + \sum_{k=1}^{n-1} RTT_{k,k+1}$$

که در این رابطه $RTT_{k,k+1}$ ، تأخیر رفت و برگشت بین سرورهای DNS، k و $k+1$ است.

پ:

با توجه به این که رکورد DNS مورد نظر در سرور DNS محلی وجود دارد در نتیجه:

$$ResponseTime_{Iterative} = ResponseTime_{Recursive} = RTT_1$$

پاسخ سوال ۲:

رکوردهای DNS با نوع MX برای نگاشت نام دامنه سرور ایمیل به آدرس IP آن استفاده می‌شوند. در حالی که، رکوردهای نوع CNAME برای نگاشت نام دامنه مستعار (Alias) به نام دامنه اصلی مورد استفاده قرار می‌گیرند. اگر در یک سازمان، نام دامنه سرور ایمیل و سرور وب (یا سرور دیگر) یکسان ولی آدرس IP سرور ایمیل و سرور وب با هم متفاوت باشند (یعنی این دو سرور در دو میزبان متفاوت اجرا می‌شوند)، لازم است سرور DNS، رکورد تبدیل نام دامنه به آدرس IP سرور ایمیل را از رکورد تبدیل نام دامنه به آدرس IP سرور وب تفکیک نماید و بر اساس درخواست رسیده، آدرس IP سرور ایمیل یا سرور وب را برگرداند. برای این تفکیک از نوع MX برای رکورد سرور ایمیل استفاده می‌شود. اگر سرور ایمیل و سرور وب هر دو بر روی یک میزبان اجرا می‌شوند، یعنی آدرس IP یکسانی دارند، نیازی به این تفکیک وجود ندارد.

پاسخ سوال ۳:

با نگهداری موقت (cache) آدرس‌های IP در سرورهای DNS محلی، پاسخ درخواست‌ها از طریق سرورهای DNS محلی داده می‌شوند، بنابراین بار زیاد درخواست‌ها در حمله DDOS به سرور DNS ریشه منتقل نمی‌شود و این بار بین سرورهای DNS محلی پخش شده و امکان ممانعت از سرویس سرور DNS ریشه از طریق حمله DDOS وجود ندارد.

پاسخ سوال ۴:

$$F = 2 \text{ GB} = 2 \times 2^{30} \times 8 = 2^{34} \text{ bit}$$

$$u_s = 20 \text{ Mbps}$$

$$d_i = 5 \text{ Mbps} \quad \text{for } i = 1, 2, \dots, N$$

$$u_i = 500 \text{ Kbps} \quad \text{for } i = 1, 2, \dots, N$$

$$D_{CS} = \max \{NF/u_s, F/d_{\min}\}$$

$$D_{P2P} = \max \{F/u_s, F/d_{\min}, NF/(u_s + \sum_{i=1}^N u_i)\} = \max \{F/u_s, F/d_{\min}, NF/(u_s + Nu_i)\}$$

		NF/u_s	F/d_{\min}	F/u_s	$NF/(u_s + Nu_i)$	D_{CS}	D_{P2P}	D_{CS}/D_{P2P}
N	10	8590	3436	859	6872	8590	6872	1.25
	100	85899	3436	859	24543	85899	24543	3.50
	1000	858993	3436	859	33038	858993	33038	26.00

همانطور که انتظار می‌رفت حداقل زمان توزیع فایل در معماری P2P از معماری Client-Server کمتر است و هر چه تعداد نظیرها بیشتر شود تفاوت بیشتر می‌شود.



پاسخ سوال ۵:

شبکه‌های هم‌پوشانی (Overlay) شبکه‌هایی هستند که بر روی یک شبکه دیگر پیاده‌سازی می‌شوند و معمولاً توپولوژی شبکه زیرین (Underlay) تأثیری در تحلیل این شبکه‌ها ندارند و فقط میزبان‌ها (گره‌های انتهایی) و اتصالات مستقیم بین آن‌ها دارای اهمیت هستند. طبق صورت سوال، با توجه به اینکه هر نظیر به نظیر دیگر یک اتصال TCP دارد، در نتیجه توپولوژی این شبکه هم‌پوشانی یک گراف کامل با N رأس است. در یک گراف کامل هر رأس به $N - 1$ رأس دیگر متصل است، بنابراین با توجه به دوطرفه بودن اتصال‌ها، این شبکه دارای N گره و $N(N - 1)/2$ یال است.

پاسخ سوال ۶:

(الف)

ردیف	گره‌ها	پروتکل مورد استفاده
۱	بین کلاینت فرستنده ایمیل و سرور ایمیل فرستنده	SMTP
۲	بین سرور ایمیل فرستنده و سرور ایمیل گیرنده	SMTP
۳	بین سرور ایمیل گیرنده و کلاینت گیرنده ایمیل	Mail Access

(ب)

برای ارسال ایمیل حاوی محتوایی مانند عکس و موارد مختلف دیگر، روشی به نام Multipurpose Internet Mail Extensions (MIME) ارائه شده است. با استفاده از این روش می‌توان انواع محتوای زیر را از طریق ایمیل ارسال و دریافت کرد:

- پیامی شامل کاراکترهایی غیر از کاراکترهای ASCII ۷ بیتی (مانند کاراکترهای زبان فارسی)
- پیام غیرمتنی، مانند عکس و ویدیو
- پیامی شامل چندین بخش (Multipart Message)
- اضافه کردن سرآیند با کاراکترهایی غیر از ASCII

خیر، امکان کدگذاری مستقیم رشته‌ی باینری به ASCII وجود ندارد، بدلیل اینکه در بعضی موارد دنباله‌ای از صفر و یک‌ها، ممکن است کاراکترهای کنترلی ناخواسته ایجاد کنند و پیام را دچار خطا کنند. منظور از کاراکترهای کنترلی، کاراکترهایی با معنای خاص هستند، به عنوان نمونه، کاراکتری برای اعلام پایان یک پیام. کدگذاری رشته‌های باینری به کمک ASCII مشکلات دیگری هم دارد، مانند مشکل ۷ بیتی بودن ASCII. به همین دلیل از روش‌های کدگذاری مانند روش کدگذاری Base64 استفاده می‌شود.

(پ)

پروتکل SMTP از روش Push برای ارسال ایمیل استفاده می‌کند. یعنی فرستنده‌ی ایمیل، با ایجاد اتصال TCP با گیرنده، ایمیل خود را ارسال می‌کند. در این روش گیرنده، سرور است و فرستنده به عنوان کلاینت با دانستن آدرس IP گیرنده، اتصال TCP را برقرار کرده و ایمیل را ارسال می‌کند. از آنجایی که کلاینت گیرنده نهایی ایمیل، همیشه به اینترنت دسترسی ندارد و همچنین آدرس IP آن نیز ممکن است ثابت نباشد، بنابر این ارسال ایمیل از طریق پروتکل SMTP به کلاینت گیرنده نهایی وجود ندارد و کلاینت گیرنده ایمیل باید با استفاده از یک برنامه به عنوان عامل کاربر ایمیل (Mail User Agent) و با استفاده از یک پروتکل دسترسی ایمیل (Mail Access Protocol) با روش سرکشی (Pull)، ایمیل‌های دریافتی خود را از سرور ایمیل خود دریافت نماید.

پروتکل‌های Mail Access مورد استفاده عبارتند از:

- POP3 با پورت ۱۱۰
- IMAP با پورت ۱۴۳
- HTTP با پورت ۸۰



پاسخ سوال ۷:

(الف)

در حالت download-and-delete پس از آنکه کاربر از طریق پروتکل POP ایمیل‌های خود را از سرور ایمیل دریافت می‌کند (یعنی ایمیل‌ها از سرور ایمیل به برنامه عامل کاربر ایمیل (Mail User Agent) منتقل می‌شوند)، ایمیل‌ها از سرور ایمیل حذف و فقط در کامپیوتر محلی کاربر نگهداری می‌شوند. این روش مزایا و معایبی دارد. مزیت عمده این روش این است که ایمیل‌های منتقل شده از سرور ایمیل حذف شده و باعث جلوگیری از پر شدن فضای محدود (Quota) اختصاص داده شده به کاربر در سرور ایمیل می‌گردد. اما عیب عمده آن، بدلیل حذف ایمیل‌ها از سرور، عدم امکان دریافت ایمیل‌های رسیده از طریق دستگاه‌های دیگر نظیر گوشی همراه، تبلت و یا کامپیوتر شخصی دیگر است.

در حالت download-and-keep، پس از آنکه کاربر از طریق پروتکل POP ایمیل‌های خود را از سرور ایمیل دریافت می‌کند، ایمیل‌ها از سرور ایمیل حذف نمی‌شوند و همچنان یک کپی از آن‌ها در سرور باقی می‌ماند. این روش نیز مزایا و معایبی دارد. از جمله مزایا آن این است که پس از دریافت ایمیل از سرور ایمیل، بدلیل باقی ماندن ایمیل‌ها در سرور، امکان دسترسی به ایمیل‌ها از طریق دستگاه‌های دیگر وجود دارد. از جمله معایب این روش، پر شدن فضای محدود اختصاص داده شده به کاربر در سرور ایمیل و همچنین رفتار غیر کاربر پسندی است که هر بار کاربر از طریق یک دستگاه جدید دیگر می‌خواهد به ایمیل‌هایش دسترسی پیدا کند، کلیه ایمیل‌های موجود در سرور ایمیل، شامل ایمیل‌های بسیار قدیمی را مجدداً دریافت می‌کند.

(ب)

```
C: dele 1
C: retr 2
S: (blah blah ...
S: .....blah)
S: .
C: dele 2
C: quit
S: +OK POP3 server signing off
```

(پ)

```
C: retr 2
S: blah blah ...
S: .....blah
S: .
C: quit
S: +OK POP3 server signing off
```

پاسخ سوال ۸:

پس از برقراری ارتباط بین کلاینت (کاربر) و سرور ایمیل، برای ارسال یک ایمیل، کلاینت فرمان‌های HELO، MAIL FROM، RCPT TO و DATA را به ترتیب به سرور داده و پاسخ آن را دریافت می‌کند. ارسال هر فرمان و دریافت پاسخ آن یک زمان رفت و برگشت (RTT) طول می‌کشد. پس از دریافت پاسخ فرمان DATA، کلاینت متن ایمیل را برای سرور ارسال می‌کند و سرور پاسخ تاییده دریافت پیام (ایمیل) را به کلاینت می‌دهد. اگر اندازه متن ایمیل کوچک باشد، ارسال متن و دریافت تاییده آن نیز یک زمان رفت برگشت طول می‌کشد. بنابر این ارسال یک ایمیل حداقل ۵ زمان رفت و برگشت طول می‌کشد.

لازم به توضیح است، کلاینت پس از دریافت تاییده دریافت پیام توسط سرور می‌تواند با ارسال فرمان QUIT به این ارتباط خاتمه دهد یا اینکه ایمیل(های) بعدی را ارسال کند. بنابر این زمان ارسال فرمان QUIT و دریافت پاسخ آن در زمان ارسال ایمیل محاسبه نمی‌شود.



پاسخ سوال ۹:

طبق بخش ۴.۱ سند **RFC 959**، دستورات سرویس گیرنده که توسط این RFC پشتیبانی می‌شوند به سه گروه زیر تقسیم شده‌اند:

۱- دستورات کنترل دسترسی (Access Control Commands):

دستورات کنترل دسترسی، دستوراتی هستند که بخشی از فرایند ورود و احراز هویت کاربر، برای دسترسی به منابع و یا بخشی از فرایند کنترل جلسه را انجام می‌دهند. دستورات این گروه عبارتند از:

USER, PASS, ACT, CWD, CDUP, SMNT, REIN, QUIT

۲- دستورات پارامتر انتقال (Transfer Parameter Commands):

دستورات پارامتر انتقال، دستوراتی هستند که پارامترهای چگونگی انتقال داده‌ها را مشخص می‌کنند. برای مثال، مشخص نمودن نوع داده فایلی که قرار است ارسال شود، یا مشخص نمودن استفاده از اتصالات داده غیرفعال یا فعال، و یا موارد مشابه دیگر از جمله دستورات این گروه هستند. دستورات این گروه عبارتند از:

PORT, PASV, TYPE STRU, MODE

۳- دستورات سرویس FTP (FTP Service Commands):

دستورات سرویس FTP، دستوراتی هستند که عملیات اصلی FTP بر روی فایل (ها) نظیر دریافت لیست فایل‌ها، ارسال، دریافت، حذف، یا تغییر نام فایل و موارد مشابه دیگر را انجام می‌دهند. دستورات این گروه عبارتند از:

RETR, STOR, STOU, APPE, ALLO, REST, RNFR, RNTD, ABOR, DELE, RMD, MRD, PWD, LIST, NLST, SITE, SYST, STAT, HELP, NOOP

پاسخ سوال ۱۰:

زمانی که بار ترافیکی درخواست‌ها به اندازه‌ای زیاد است که یک سرور به تنهایی نمی‌تواند به همه آن‌ها سرویس دهد، همزمان از چند سرور موازی برای سرویس‌دهی استفاده می‌شود و بار ترافیکی بین آن‌ها توزیع می‌گردد. به توزیع بار بین سرورها موازی توزان بار (Load Balancing) می‌گویند. از جمله مزایای دیگر استفاده از چند سرور موازی و توازن بار بین آن‌ها بالا بردن قابلیت اطمینان (Reliability) و قابلیت در دسترس بودن (Availability) سرویس است. زیرا اگر یکی از سرورها، به هر دلیلی از سرویس خارج شود، سرورهای دیگر به وظیفه ارائه سرویس خود ادامه می‌دهند و احتمال در دسترس بودن سرویس بسیار بالا است.

در روش توازن بار مبتنی بر DNS (DNS Load Balancing)، سرور DNS لیست آدرس‌های IP سرورهای موازی مربوط به یک نام دامنه را نگهداری می‌کند و با هر بار درخواست DNS (DNS Query) ترتیب آدرس‌های IP درون لیست را تغییر می‌دهد. از آنجایی که معمولاً کلاینت‌ها اولین آدرس لیست را استفاده می‌کند و درخواست خود را برای آن سرور ارسال می‌کنند، بار ترافیکی درخواست‌ها بین سرورها توزیع می‌شود. روش متداول در تغییر ترتیب لیست آدرس‌های IP در سرورهای DNS، روش چرخشی (Round Robin) است. روش توازن بار مبتنی بر DNS مزایا و معایب زیر را دارد:

مزایا:

- عدم وابستگی به یک پروتکل خاص (برای توازن هر نوع سرویس با هر پروتکل لایه کاربرد قابل استفاده است).
- تأخیر کمتر (به دلیل اینکه بین کلاینت و سرور هیچ سرور واسطی وجود ندارد).
- امکان قرارگیری سرورها در مراکز داده مختلف که از نظر جغرافیایی در نقاط مختلف جهان قرار دارند.

معایب:

- عدم توزیع بهینه بار به دلیل ذخیره‌سازی موقت (Cache) لیست آدرس‌های IP در سرورهای DNS میانی و کلاینت
- عدم قابلیت اطمینان و قابلیت در دسترس بودن بالا به دلیل عدم بررسی و عدم تشخیص وضعیت شبکه و سرورها توسط سرور DNS.
- عدم انعطاف‌پذیری در افزایش یا کاهش تعداد سرورها بر اساس میزان بار ورودی



در روش توازن بار مبتنی بر HTTP (HTTP Load Balancing)، همه درخواست‌ها به یک سرور واسط (پراکسی) متوازن‌ساز بار (Load Balancer) داده می‌شود و سرور متوازن‌ساز بار درخواست‌ها را بین سرورها توزیع می‌کند. معمولاً سرور متوازن‌ساز بار از روش چرخشی برای توزیع بار استفاده می‌کند. روش توازن بار مبتنی بر HTTP مزایا و معایب زیر را دارد:

مزایا:

- توزیع بهینه بار بین سرورها به دلیل وجود استفاده از سرور متوازن‌ساز بار متمرکز.
- قابلیت اطمینان و قابلیت در دسترس بودن بالا بدلیل اطلاع از وضعیت سرورها توسط سرور متوازن‌ساز بار.
- انعطاف‌پذیری بالا در افزایش یا کاهش تعداد سرورها بر اساس میزان بار ورودی

معایب:

- قابل استفاده فقط برای برنامه‌های کاربردی مبتنی بر وب که برای ارسال و دریافت پیام‌های خود از پروتکل HTTP استفاده می‌کنند.
- وجود سرور واسط متوازن‌ساز بار به عنوان گلوگاه (Bottleneck) و تنها نقطه شکست (Single Point of Failure) سرویس.
- محدودیت قرارگیری همه سرورها در یک مراکز داده.