

شبکه‌های کامپیوتری

نیم‌سال دوم ۱۴۰۳-۰۴
استاد: امیرمهدی صادق‌زاده



دانشکده‌ی مهندسی کامپیوتر

پاسخ‌دهنده: معین آعلی - ۴۰۱۱۰۵۵۶۱

تمرین سوم

فهرست مسائل

۲	مسئله ۱
۲	آ
۲	ب
۲	ج
۳	مسئله ۲
۴	مسئله ۳
۴	آ
۴	ب
۶	ج
۸	مسئله ۴
۸	آ
۸	ب
۸	ج
۹	مسئله ۵
۹	آ
۹	ب
۱۰	مسئله ۶
۱۲	مسئله ۷

پاسخ مسئله‌ی ۱.

آ

پرتازه‌های A و B به عنوان کلاینت عمل می‌کنند و از پورت‌های موقت استفاده می‌کنند. (Ephemeral-Port) اما پرتازه C که در این سناریو به عنوان سرور HTTP است، که باید با یک پورت ثابت کار کند. چون صورت سوال اشاره کرده است که در پروتوکل ارتباطی ما HTTP است، پس پورت پرتازه C برابر با ۸۰ است.

ب

در حالت عادی، این امکان وجود ندارد. چون که پورت و آیدی با هم Socket-Address را تشکیل می‌دهند و باید یک کلید یکتا باشد. پس اگر یک پرتازه بخواهد روی یک پورت خاص bind کند، سیستم عامل آن پورت را برای این پرتازه رزرو می‌کند و دیگر اجازه نمی‌دهد که پرتازه دیگری روی آن پورت bind کند. اما حالات استثنا و خاص هم وجود دارد، مانند:

- فرض کنیم یک هاست دارای چند آیدی است. می‌توان یک پرتازه روی یک آیدی و پورت و پرتازه دیگر روی همان پورت و آیدی دیگر گوش کند.
- با استفاده از قابلیت SO_REUSEPORT می‌توان کاری کرد که دو پرتازه روی یک پورت گوش دهند و سیستم عامل بین آن‌ها load-balancing انجام دهد.
- و موارد دیگر...

ج

با اینکه در لایه‌ی لینک روش‌هایی برای تشخیص خطا وجود دارد، اما این روش‌ها فقط خطاهای local را در هر لینک مجزا بین دو گره تشخیص می‌دهند. در مسیر یک بسته از مبدا تا مقصد، بسته از چندین لینک و روتر عبور می‌کند و خطاهایی ممکن است در بافر روترها یا حافظه‌ی آن‌ها رخ دهد. پس برای اطمینان از اینکه بسته به برنامه‌ی مقصد به درستی رسیده است، نیاز است در لایه‌ی انتقال یک checksum داشته باشیم.

پاسخ مسئله‌ی ۲.

- UDP ساده‌تر از TCP است (بدون کنترل اتصال، شماره‌گذاری بسته‌ها یا کنترل ازدحام)، پس سرعت انتقال داده بیشتر می‌شود.
 - نیاز به حداقل تأخیر در برنامه‌هایی که نیاز دارند داده خیلی سریع برسد. مثل تماس صوتی یا لایو استریم. تأخیر کم مهم‌تر از تحویل تضمینی همه داده‌ها است. TCP به خاطر مکانیسم‌های تصحیح خطا، تأخیر بیشتری دارد که برای این نوع اپلیکیشن‌ها مناسب نیست.
 - این اپلیکیشن‌ها طوری طراحی شده‌اند که حتی اگر برخی بسته‌ها از دست برود، همچنان به کار ادامه می‌دهند (مثلاً در تماس صوتی، یک کلمه گم شود ولی مکالمه قطع نشود).
- برای مثال می‌توان به برنامه تماس تصویری و تماس صوتی و بازی‌های آنلاین اشاره کرد.

پاسخ مسئله‌ی ۳.

آ

در پروتکل **Go-Back-N**، اندازه پنجره نقش بسیار مهمی در کارایی و کارکرد صحیح شبکه دارد. در صورتی که اندازه پنجره به درستی انتخاب نشود، دو حالت مشکل‌زا ممکن است رخ دهد:

پنجره بسیار کوچک

- کارایی پایین شبکه: ارسال‌کننده نمی‌تواند بسته‌های زیادی را قبل از دریافت تایید ارسال کند، که منجر به زمان‌های بیکار زیاد می‌شود.
- استفاده ناکارآمد از پهنای باند: ظرفیت لینک به خوبی استفاده نمی‌شود، زیرا اغلب اوقات ارسال‌کننده منتظر دریافت تأییدها است.

پنجره بسیار بزرگ

- سرریز بافر گیرنده (**Receiver-Buffer-Overflow**): اگر گیرنده نتواند با سرعت کافی بسته‌ها را دریافت و پردازش کند، بسته‌ها از بین خواهند رفت.
- افزایش احتمال ارسال مجدد بسته‌ها: در صورت از دست رفتن یک بسته، همه بسته‌های بعدی باید دوباره ارسال شوند که باعث افزایش بار شبکه می‌شود.

اندازه بهینه پنجره معمولاً بر اساس رابطه زیر تعیین می‌شود:

$$\text{Window-Size}_{\text{optimal}} = \text{Bandwidth-Delay-Product} + 1$$

که در آن **Bandwidth-Delay-Product** بیانگر مقدار داده‌ای است که می‌تواند در مسیر شبکه در جریان باشد (در حال انتقال). عدد ۱ اضافه می‌شود تا اطمینان حاصل شود که حتی در هنگام انتظار برای تأیید آخرین بسته، ارسال‌کننده بتواند ارسال را ادامه دهد.

انتخاب اندازه پنجره باید به گونه‌ای باشد که هم کارایی شبکه را افزایش دهد و هم از سرریز بافر جلوگیری کند. این اندازه معمولاً با محاسبه دقیق **BDP** و اعمال حاشیه امن به دست می‌آید.

ب

داده‌های مسئله:

- $100\text{ms} = RTT$
- اندازه هر بسته = ۱۰۰۰ بیت = ۸۰۰۰ بیت
- نرخ لینک = ۱ Gbps = 10^9 bps
- احتمال خطا در هر بسته = p

زمان ارسال هر بسته:

$$t_{\text{trans}} = \frac{1000}{10^9} = 1\text{ }\mu\text{s}$$

پروتکل Stop-and-Wait

در Stop-and-Wait، پس از ارسال هر بسته باید یک RTT صبر کنیم.
کارایی:

$$U_{SW} = \frac{t_{trans}}{t_{trans} + RTT} = \frac{8 \times 10^{-6}}{8 \times 10^{-6} + 0.1} \approx 7.999 \times 10^{-5}$$

یعنی کارایی حدوداً ۰/۰۰۸٪ است.

کارایی با احتمال خطا p :

$$U_{SW} = \frac{t_{trans}}{t_{trans} + RTT} \times (1 - p)$$

$$U_{SW} \approx 7.999 \times 10^{-5} \times (1 - p)$$

پروتکل Go-Back-N

ابتدا اندازه پنجره N را محاسبه می‌کنیم:

$$N = \frac{RTT}{t_{trans}} = \frac{0.1}{8 \times 10^{-6}} = 12500$$

بنابراین، $N = 12500$ برای پر کردن خط لوله کافی است.

در حالت بدون خطا:

$$U_{GBN} = \frac{N \times t_{trans}}{RTT + t_{trans}} \approx \frac{12500 \times 8 \times 10^{-6}}{0.1} = 1$$

یعنی کارایی ۱۰۰٪ در حالت بدون خطا.

در حضور خطا با احتمال p ، کارایی کاهش می‌یابد. کارایی تقریبی:

$$U_{GBN} \approx \frac{1}{1 + p(N - 1)}$$

Repeat Selective

در این حالت نیز پنجره N به همان مقدار است.

در حالت بدون خطا:

$$U_{SR} = 1$$

در حضور خطا:

$$U_{SR} \approx 1 - p$$

زیرا فقط بسته‌های دارای خطا دوباره ارسال می‌شوند.

با افزایش p :

- در Stop-and-Wait، کارایی به شدت پایین است و تغییر زیادی با خطا نمی‌کند زیرا در بهترین حالت هم کارایی بسیار کم است.
 - در Go-Back-N، با افزایش p ، کارایی شدیداً افت می‌کند زیرا باید همه بسته‌های بعد از یک خطا را دوباره ارسال کرد.
 - در Selective-Repeat، افت کارایی بسیار ملایم‌تر است، زیرا فقط بسته‌های معیوب بازفرست می‌شوند.
- برای لینک‌هایی که احتمال خطا در آن‌ها زیاد است، استفاده از پروتکل Selective-Repeat مناسب‌تر است زیرا کارایی آن در مقابل خطا مقاوم‌تر است.

ج

پروتکل Go-Back-N

در این پروتکل اگر یک بسته گم شود، تمام بسته‌های بعدی (تا انتهای پنجره) باید دوباره ارسال شوند. تعداد متوسط بسته‌های ارسالی:

$$\text{Expected-transmissions-per-packet} = \frac{1}{1-p}$$

اما، چون در Go-Back-N از لحظه‌ای که یک خطا رخ دهد تمام بسته‌های بعدی نیز دوباره ارسال می‌شوند، میانگین تعداد بسته‌های اضافی در اثر خطا تقریباً:

$$\text{Overhead-per-lost-packet} \approx N - 1$$

پس، تعداد متوسط بسته‌های ارسالی برای ارسال M بسته:

$$\text{Total-packets} \approx M \times \left(\frac{1}{1-p} + p \times (N - 1) \right)$$

تعداد متوسط ACK ها:

$$\text{Total-ACKs} = M$$

چون فقط بسته‌های دریافت‌شده نیازمند ACK هستند و ACK ها گم نمی‌شوند.

پروتکل Repeat Selective

$$\text{Expected-transmissions-per-packet} = \frac{1}{1-p}$$

پس، برای M بسته:

$$\text{Total-packets} = M \times \frac{1}{1-p}$$

تعداد متوسط ACK ها:

$$\text{Total-ACKs} = M$$

چون هر بسته‌ای که دریافت می‌شود، بلافاصله ACK می‌شود.

پروتکل TCP

در TCP بدون ACK Delayed برای هر بسته دریافت‌شده، بلافاصله یک ACK ارسال می‌شود.

تعداد متوسط بسته‌های ارسالی:

TCP از Repeat Selective مشابه‌تر است. در صورت از دست رفتن بسته، تنها همان بسته بازفرست می‌شود:

$$\text{Expected-transmissions-per-packet} = \frac{1}{1-p}$$

پس:

$$\text{Total-packets} = M \times \frac{1}{1-p}$$

تعداد متوسط ACK ها:

$$\text{Total-ACKs} = M$$

نتیجه‌گیری

- در Go-Back-N، به علت ارسال مجدد کل پنجره پس از هر خطا، تعداد بسته‌های ارسالی بسیار بیشتر از Selective-Repeat و TCP است.
- در Selective-Repeat و TCP، فقط بسته‌های از دست‌رفته دوباره ارسال می‌شوند و تعداد ACK ها برای هر سه پروتکل برابر با تعداد کل بسته‌ها است.
- بنابراین Selective-Repeat و TCP بهینه‌ترین عملکرد را از نظر تعداد بسته‌های ارسالی دارند.

پاسخ مسئله‌ی ۴.

آ

ب

ج

پاسخ مسئله‌ی ۵.

آ

این دستور قصد دارد آدرس آیی متناظر با دامنه sharif.edu را پیدا کند. با این تفاوت که از یک DNS سرور با آدرس 4.2.2.4 استفاده می‌کند نه از DNS سرور پیش فرض سیستم. پاسخ داده شده دارای اطلاعات زیر هست:

- آدرس آیی ورژن ۴ متناظر با این دامنه
- مقدار TTL مربوط به این آدرس آیی . این مقدار برابر ۸ است در این درخواست.
- زمان پاسخ سرور DNS برابر با ۲۲۱ msec است.
- پاسخ روی پورت ۵۳ و پروتوکل UDP ارسال شده است.
- زمان اجرای دستور. البته احتمالا در این مورد زمان ست نشده بوده و در جواب زمان Unix-Timestamp برگردانده شده است.
- اندازه‌ی پیام ارسال شده از سمت سرور که در این جواب ۵۵ بایت است.
- عبارت Truncated یعنی پاسخ DNS خیلی بزرگ بوده، داخل UDP جا نشده، و dig فقط بخشی از آن را نشان داده است.

ب

رکورد MX مشخص می‌کند که ایمیل‌هایی که به این دامنه ارسال می‌شوند، باید به کدام سرورهای ایمیل تحویل داده شوند. این درخواست از DNS سرور نوشته شده درخواست می‌کند تا رکوردهای MX دامنه‌ی sharif.edu را پیدا کند.

پاسخ داده شده دارای اطلاعات زیر هست:

- این دامنه دارای دو رکورد MX است.
- این رکوردها هر دو دارای اولویت ۱۰ هستند.
- این رکوردها دارای TTL برابر ۶۰ هستند.
- باقی اطلاعات مشابه با بخش قبل هستند.

وقتی ایمیلی ارسال می‌شود، سرور فرستنده تلاش می‌کند ایمیل را به سروری با کمترین عدد اولویت بفرستد. اگر چند سرور اولویت یکسان داشته باشند، یکی از آن‌ها انتخاب می‌شود (اغلب به طور تصادفی یا بر اساس load-balancing).

پاسخ مسئله‌ی ۶.

در ادامه هر یک از روش‌ها را جدا توضیح می‌دهیم:

TCP-Scanning

در این روش، اسکنر تلاش می‌کند اتصال کامل TCP را با پورت مقصد برقرار کند. یعنی ابتدا بسته‌ی SYN ارسال می‌شود، اگر پورت باز باشد SYN-ACK برمی‌گردد، و سپس ACK ارسال می‌شود تا اتصال کامل شود. مزایا:

- بسیار دقیق است. وقتی ارتباط کامل برقرار شد، کاملاً مطمئن هستید که پورت باز است.

معایب:

- بسیار راحت توسط سیستم مقصد شناسایی می‌شود (در لاگ‌ها ثبت می‌شود).
- نسبت به روش‌های دیگر کندتر است.
- به راحتی فایروال جلوی آن را می‌تواند بگیرد

SYN-Scanning

در این روش، فقط بسته‌ی SYN ارسال می‌شود. اگر پورت باز باشد، SYN-ACK پاسخ داده می‌شود، ولی اسکنر دیگر ACK نمی‌فرستد و اتصال را نیمه‌کاره رها می‌کند. مزایا:

- سریع‌تر از Scanning TCP است.
- در لاگ‌های سیستم هدف کمتر دیده می‌شود.

معایب:

- ممکن است توسط فایروال‌ها یا IDS/IPS ها مسدود شود.

FIN-Scanning

در این روش، بسته‌ی FIN به پورت مقصد ارسال می‌شود. اگر پورت بسته باشد، دستگاه پاسخ RST می‌دهد. اگر باز باشد، هیچ پاسخی نمی‌دهد (بر اساس استاندارد TCP). مزایا:

- می‌تواند از بعضی فایروال‌ها عبور کند

معایب:

- روی سیستم‌های ویندوز اغلب کار نمی‌کند، چون ویندوز به بسته FIN پاسخ RST می‌دهد حتی اگر پورت باز باشد.
- قابل اطمینان نیست مگر در سیستم‌های خاص (مثل Unix/Linux).

UDP-Scanning

در این روش، بسته UDP به پورت ارسال می‌شود. اگر پورت بسته باشد، معمولاً پیام ICMP-Port-Unreachable برمی‌گردد. اگر باز باشد، معمولاً پاسخی دریافت نمی‌شود.
مزایا:

- تنها روش کاربردی برای شناسایی پورت‌های باز UDP

معایب:

- سخت‌ترین روش برای تشخیص وضعیت واقعی (باز یا بسته).
- کند است چون نیاز به تایم‌اوت دارد.
- ممکن است توسط فایروال‌ها مسدود شود.

جمع‌بندی موارد:

- TCP دقیق و کند و آشکار
- SYN سریع و نیمه مخفی
- FIN مخفی‌تر ولی کمتر قابل اطمینان
- UDP تنها راه برای بررسی UDP ولی کند و غیرقابل پیش‌بینی

سوال عملی

توضیحات نحوه کار کردن nmap

پاسخ مسئله‌ی ۷.