به نام خداوند بخشنده مهربان

دانشگاه صنعتی شریف
مدرس: مهدی خرازی

تمرین برنامه نویسی اول [*]
شبکه‌های رایانه‌ای

دانشکده‌ی مهندسی کامپیوتر
بهار ۱۳۹۵

اهداف تمرین

- آشنایی با پروتکل‌های DHCP ، DNS و ARP
- آشنایی با فیلد جمع کنترلی[۱] در سرآیند UDP و TCP
- آشنایی با تأخیرهای موجود در ارسال بسته‌ها
- آشنایی با مسیریابی IP و مفهوم Proxy

۱. تمرین تئوری

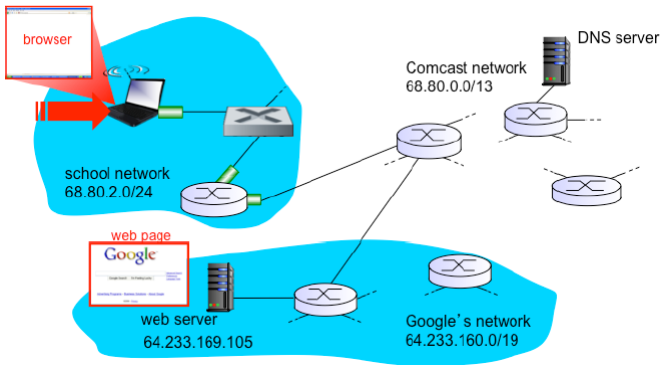
۱.۱ آشنایی با پروتکل‌های DHCP ، DNS و ARP

در این تمرین **سناریوی ارسال درخواست وب** مورد بررسی قرار می‌گیرد. با توجه به شکل ۱ به سؤالات پاسخ دهید.

۱. به عنوان اولین گام در این تمرین، فرض می‌کنیم که لپ‌تاپِ در حال اتصال، نیاز دارد تا آدرس IP خودش، آدرس مسیریاب موجود در اولین گام و آدرس سرور DNS را بدست آورد. بطور دقیق توضیح دهید که با استفاده از پروتکل DHCP این آدرس‌ها چگونه بدست می‌آید؟

۲. قبل از اینکه کارخواه بتواند درخواست HTTP خود را به سمت کارگزار www.google.com ارسال کند، باید آدرس IP آن را از طریق DNS بدست آورد. با جزئیات توضیح دهید که چگونه درخواست DNS اجرا

[*] با سپاس از سولماز سلیمی، زینب ساسان، پارسوآ خورسند، پیمان عزتی، رضا میرعسگر شاهی
[۱] Checksum



شکل ۱: سناریوی ارسال درخواست وب

می‌شود؟ در نظر داشته باشید که کارخواه هنوز آدرس MAC مربوط به واسطِ مسیریاب موجود در اولین گام را نمی‌داند!

۳. پس از اینکه کارخواه آدرس IP کارگزار را بدست آورد، می‌تواند درخواست HTTP را ارسال کند. ابتدا توضیح دهید که ارتباط TCP چگونه برقرار می‌شود و سپس نحوه‌ی اجرای درخواست HTTP را شرح دهید. (منظور از نحوه‌ی اجرای درخواست HTTP روندی است که در لایه‌های مختلف معماری شبکه برای ارسال درخواست و بازگرداندن پاسخ رخ می‌دهد.)

۲.۱. محاسبه جمع کنترلی

UDP و TCP از مکمل یگانی[۲] برای جمع کنترلی خود استفاده می‌کنند. فرض کنید سه بایت ۰۱۰۱۰۰۱۱، ۰۱۱۰۰۱۱۰ و ۰۱۱۱۰۱۰۰ را در اختیار داریم.

۱. جمع مکمل یگانی این سه بایت چیست؟ (البته TCP و UDP کلمات ۱۶ـ بیتی را با هم جمع می‌کنند نه ۸ـ بیتی را) تمام مراحل کار را نشان دهید.

۲. با این روش گیرنده چگونه وجود خطا را تشخیص می‌دهد؟

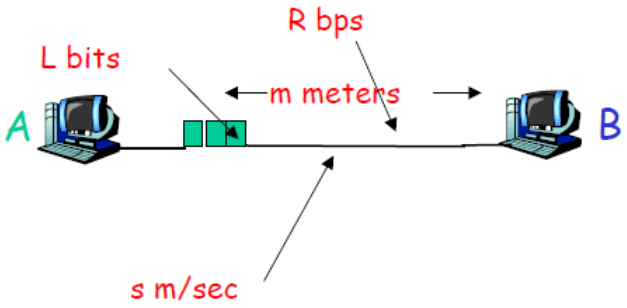
۳. آیا امکان دارد خطای ۱ـ بیتی تشخیص داده نشود؟

۴. خطای ۲ـ بیتی چطور؟

۳.۱. محاسبه‌ی تأخیر

دو میزبان A و B را در نظر بگیرید که با لینکی با نرخ R بیت بر ثانیه، بهم متصل شده‌اند. فرض کنید که دو میزبان m متر از یکدیگر فاصله دارند و سرعت انتشار در لینک برابر با S متر بر ثانیه است. میزبان A بسته‌ای به طول L را

[۲] 1's complement



شکل ۲: فرضیات ارسال بسته از A به B

به سمت میزبان B ارسال می‌کند. فرضیات در نظر گرفته شده در شکل ۲ نشان داده شده است، باتوجه به این نکات، به سؤالات زیر پاسخ دهید.

۱. تأخیر انتشار بر حسب m و S چقدر خواهد بود؟

۲. تأخیر انتقال را بر حسب L و R حساب کنید.

۳. اگر از تأخیر پردازش و صف صرفنظر شود، تأخیر انتها به انتها چقدر خواهد بود؟

۴. فرض کنید میزبان A در لحظه $t. = ۰$ شروع به انتقال بسته نماید. در لحظه $t = d_{trans}$ [۳] آخرین بیت از بسته کجا قرار دارد؟

۵. فرض کنید تأخیر انتشار از تأخیر انتقال بیشتر باشد. در لحظه $t = d_{trans}$ اولین بیت از بسته کجا قرار دارد؟

۶. فرض کنید تأخیر انتشار از تأخیر انتقال کمتر باشد. در لحظه $t = d_{trans}$ اولین بیت از بسته کجا قرار دارد؟

۷. فرض کنید $S = ۲/۵ \times ۱۰^۸$ ، $L = ۱۰۰bit$ و $R = ۲۸Kbps$ باشد. فاصله m را طوری پیدا کنید که تأخیر انتقال برابر با تأخیر انتشار باشد.

۲. تمرین عملی

۱.۲ مقدمه

در این تمرین با مفهوم پروکسی آشنا خواهید شد که در ادامه این بخش توضیحاتی درباره آن آمده است.

سرور پروکسی یک کامپیوتر یا سیستم نرم‌افزاری است که بر روی یک کامپیوتر اجرا می‌شود و به عنوان واسطی بین سیستم‌های میزبان نهایی قرار می‌گیرد. یکی از مزیت‌های مهم سرور پروکسی نگهداری صفحات پربازدید وب در حافظه نهان[۴] است که این ویژگی زمان پاسخ به کاربر را بطور چشمگیری کاهش می‌دهد. وقتی یک سرور پروکسی

[۳] تأخیر انتقال
[۴] Cache

درخواستِ یک منبع اینترنتی را دریافت می‌کند، در حافظه‌ی نهان خود فایل مورد نظر را جستجو می‌کند. اگر منبع مربوطه را در حافظه‌ی نهان خود پیدا کرد، بدون ارسال درخواست به سمت کارگزار، آن را برای کارخواه ارسال می‌کند. اگر منبع موردنظر در حافظه نهان سرور پروکسی وجود نداشت، سرور پروکسی به نمایندگی از کارخواه همچون کارخواه جدیدی عمل می‌کند و با استفاده از آدرس IP خودش، درخواست را به سمت کارگزار ارسال می‌نماید و پس از دریافت پاسخ، آن را به سمت کارخواه برمی‌گرداند.

سرورهای پروکسی می‌تواند با اهداف قانونی و غیرقانونی مورد استفاده قرار گیرند. در داخل یک سازمان، سرور پروکسی برای موارد امنیتی، کنترل سطح دسترسی و امکان استفاده از حافظه نهان در سرویس‌دهی مورد استفاده قرار می‌گیرند. در استفاده شخصی از سرورهای پروکسی نیز مزیت‌هایی همچون حفظ حریم خصوصی[۵] و گمنامی[۶] برای گشت‌وگذار در وب وجود دارد. سرورهای پروکسی همچنین می‌توانند برای اهداف منفی همچون مانیتور کردن ترافیک و تضعیف حریم خصوصی کاربر مورد استفاده قرار گیرند.

کاربران می‌توانند بطور آنلاین یا با پیکربندی تنظیمات مرورگر خود به سرور پروکسی دسترسی داشته باشند. تنظیمات مرورگر شامل گزینه‌هایی برای تشخیص خودکار سرور پروکسی و یا تنظیم دستی برای سرورهای پروکسی همچون SSL ، HTTP و SOCKS است. رایج ترین کاربرد پروکسی فراهم کردن امکان دسترسی کاربر به دامنه هایی است که در حالت عادی نمی‌توان به طور مستقیم به آنها متصل شد. (به طور مثال آدرس هایی که پروکسی DNS اجازه ترجمه آن ها را نمی دهد.) در این شرایط کاربر می‌تواندبسته‌های خود را به واسطه یک پروکسی که خود در لیست فیلتر شبکه قرار ندارد، به مقصد ارسال کند.

۲.۲. توپولوژی شبکه

توپولوژی شبکه متشکل از تعدادی مسیریاب است که هرکدام می تواند در نقش ارسال کننده یا دریافت کننده پیام و یا proxy ظاهر شوند. در این متن زمانی که یک مسیریاب در نقش ارسال کننده یا دریافت کننده پیام عمل کند به آن CR [۷] می گوییم. همچنین مسیریابی که در نقش proxy ظاهر شود را PR [۸] می نامیم. هر مسیریاب دارای یک جدول مسیریابی IP ثابت است که برای انتقال بسته‌ها در شبکه استفاده می‌شود. در صورتی که اطلاعات این جدول برای رساندن بسته‌ای به مقصد کافی نباشد، نیاز به استفاده از proxy داریم. هر مسیریاب جدولی از مسیریاب های proxy دارد که که در صورت نیاز می‌تواند از آن استفاده کند.

بنابر توضیحات فوق تمام مسیریاب‌هایی شبکه یکسان هستند و تفاوت رفتار آن‌ها تنها به واسطه جداول پیکربندی تعیین می‌شود.

---

[۵] Privacy
[۶] Anonymity
[۷] Client Router
[۸] Proxy Router

۳.۲. پروتکل UNPP

بسته Ping

درخواست Ping از طرف یک CR برای CR دیگر ارسال می‌شوند. یک CR با ارسال پاسخ Ping به درخواستهای Ping دریافتی پاسخ می دهد. بار داده[۹] در پاسخ Ping همان بار داده در درخواست Ping است. CR مقصد محتوای بار داده‌ی درخواست Ping را به قطعه‌های دوبایتی تقسیم می‌کند و اگر تعداد این قطعه‌ها فرد بود یک بایت تمام صفر به پیام اضافه کرده و در نهایت آن‌ها را با هم جمع می‌کند. اگر عملیات جمع، رقم نقلی تولید کند در فیلد وضعیت[۱۰] بسته پاسخ مقدار OK و در غیر این صورت مقدار Not OK قرار می‌گیرد. همچنین توجه داشته باشید که ترتیب قرارگیری بایت‌های بار داده بصورت Big-endian خواهد بود.

بسته Proxy

چنانچه یک CR برای ارسال Ping آدرس CR مقصد را در جدول مسیریابی خود نداشته باشد، باید از PR کمک بگیرد. بسته‌های Proxy برای ارتباط با PR ها استفاده می‌شوند. برای اتصال به یک PR و استفاده از آن به عنوان واسط، یک بسته درخواست Proxy به آن PR ارسال می‌شود که بار داده در آن همان بار داده در بسته Ping است که در نظر داریم برای مقصد ارسال کنیم. یک PR پس از دریافت درخواست Proxy ، IP مسیریاب ارسال کننده را در لیست سیاه خود چک می‌کند و در صورت مجاز بودن آدرس ، CR مقصد را Ping می‌کند و یک بسته پاسخ Proxy با وضعیت valid برای CR متقاضی ارسال می‌کند. در صورتی که آدرس CR متقاضی در لیست سیاه وجود داشته باشد، مسیریاب PR بسته درخواست Proxy دریافتی را حذف کرده و با ارسال یک بسته پاسخ Proxy با وضعیت invalid به CR متقاضی پاسخ می‌دهد.

فرمت پیام‌ها در UNPP

پروتکل UNPP بر بستر پروتکل UDP کار می‌کند و متشکل از یک سرآیند یک بایتی و بار داده‌ی حداکثر ۳۲ بایتی است. بنابراین حداکثر طول یک بسته UNPP برابر ۳۳ بایت است.

سرآیند بسته UNPP متشکل از ۴ فیلد است:

- Type : این فیلد تک بیتی نوع بسته را مشخص می‌کند.

Value	Type
0	Ping
1	Proxy

- Direction : این فیلد تک بیتی پاسخ یا درخواست بودن بسته را مشخص می‌کند.

---

[۹] Payload
[۱۰] Status

Value	Direction
1	Response
0	Request

- Status : این فیلد نیز تک بیتی است و جواب مسیریاب مقصد به بسته ارسالی را مشخص می‌کند.

Value	Status
0	OK/Valid
1	Not Ok/Invalid

- Len : این فیلد ۵ بیتی طول بار داده را به بایت مشخص می‌کند. بنابراین بار داده می‌تواند حداکثر ۳۲ بایت باشد.

پس ساختار نهایی سرآیند UNPP به شکل زیر خواهد بود :

Type	Direction	Status	Len

۴.۲ پیاده سازی

برنامه‌ای که شما می‌نویسید باید قابلیت مدیریت ارسال و دریافت انواع مختلف بسته‌ها و اجرای روند مسیریابی با قاعده انطباق طولانی‌ترین پیشوند را داشته باشد. در ادامه روند پیاده‌سازی برای ارسال و دریافت انواع پیام‌ها و نحوه‌ی مسیریابی توضیح داده شده است. برنامه شما بر روی سامانه پرتو اجرا می‌شود.

۱.۴.۲ ارسال درخواست Ping

هر مسیریاب می‌تواند سایر مسیریاب های موجود در شبکه را Ping کند. این کار با وارد کردن دستور زیر انجام می‌شود:

```
ping <Dest-IP> <Payload>
```

`Dest-ip` : آدرس مسیریاب مقصد.

`Payload` : پیامی که به عنوان بار داده در بسته درخواست UNPP ارسال می‌شود. این پیام حداکثر ۳۲ کاراکتر است و نباید Null-Terminated باشد. در صورتی که تعداد کاراکتر های بار داده بیشتر از ۳۲ باشد مسیریاب با چاپ پیام زیر اجرای دستور را لغو می‌کند:

```
Payload length exceeds legal amount
```

۲.۴.۲. دریافت درخواست Ping

یک مسیریاب با دریافت درخواست Ping خروجی زیر را چاپ می‌کند:

```
ping request from <Src-IP> with payload <Payload> status <Status>
```

`Src-IP` : آدرس IP مسیریاب مبدا.
`Payload` : مقدار بار داده بسته UNPP دریافت شده.
`Status` : برابر با مقدار وضعیت در بسته پاسخ ارسالی که می‌تواند OK و یا Not OK باشد.

۳.۴.۲. دریافت پاسخ Ping

با دریافت پاسخ Ping در یک مسیریاب پیام زیر چاپ می‌شود:

```
ping response from <Src-IP> with payload <Payload> status <Status>
```

`Src-IP` : آدرس IP مسیریاب مبدا.
`Payload` : مقدار بار داده بسته UNPP دریافت شده.
`Status` : برابر با مقدار وضعیت در بسته پاسخ دریافتی که می‌تواند OK و یا Not OK باشد.

۴.۴.۲. ارسال درخواست Proxy

در صورت نیاز به استفاده از proxy برای برقراری ارتباط با یک مسیریاب پیام زیر در خروجی چاپ می‌شود:

```
proxy request sent to <PR-IP> for accessing <CR-IP>
```

`PR-IP` : آدرس IP مربوط به مسیریاب proxy .
`CR-IP` : آدرس IP مربوط به مسیریاب مقصد که مستقیم قابل دسترسی نبوده است.

۵.۴.۲. دریافت درخواست Proxy

چنانچه یک مسیریاب PR بسته درخواست proxy دریافت کند خروجی زیر را چاپ می‌کند:

```
proxy request from <Src-IP> responded with status <Status>
```

`Src-IP` : آدرس IP مسیریاب مبدا.
`Status` : برابر با مقدار وضعیت در بسته پاسخ ارسالی که می‌تواند Valid و یا Invalid باشد.

۶.۴.۲. دریافت پاسخ Proxy

با دریافت پاسخ یک درخواست proxy خروجی زیر چاپ می‌شود:

```
proxy response from <Src-IP> with status <Status>
```

`Src-IP` آدرس IP مسیریاب مبدا.

`Status` : برابر با مقدار وضعیت در بسته پاسخ دریافتی که می‌تواند Valid و یا Invalid باشد.

۷.۴.۲. روند مسیریابی

ارسال بسته‌های Ping می‌تواند به طور مستقیم و یا به واسطه PR انجام شود. مسیریاب فرستنده باید ابتدا جدول مسیریابی IP خود را با استفاده از قاعده انطباق طولانی‌ترین پیشوند بررسی کند و در صورتی که موجودیتی متناظر با آدرس مقصد پیدا کرد بسته را به آن ارسال کند. در غیر این صورت بسته باید از طریق یکی از Proxy های مشخص شده ارسال شود. توجه کنید که ممکن است مقصد Ping در لیستِ سیاه تعدادی از این Proxy ها باشد و از ارسال آن امتناع کنند. بنابراین ممکن است نیاز به امتحان کردن چند Proxy باشد و بسته از طریق اولین Proxy که پاسخ Valid بازگرداند ارسال می‌شود. مذاکره با PR ها به همان ترتیبی که در جدول Proxy آمده انجام می‌شود.

با توجه به مکانیزم فوق، ممکن است مسیریاب PR هم برای رساندن بسته به مقصد مجبور به استفاده از proxy دیگری شود. همچنین لزوماً مسیر رفت و برگشت یکسان نخواهد بود و امکان دارد با توجه به پیکربندی جداول، پاسخ Ping به طور مستقیم و یا توسط Proxy دیگری دریافت شود.

اطلاعات مسیریابی برای مسیریاب‌هایی که به طور مستقیم به آنها متصل هستیم در جدول مسیریابی وجود نخواهد داشت.

ساختار جدول مسیریابی IP به شکل زیر است:

Dest IP	Mask	IP	Interface	MAC
192.168.110.0	255.255.255.240	192.168.113.7	1	78:31:c1:d4:57:c4
192.168.117.0	255.255.255.240	192.168.116.3	2	78:42:e1:d4:57:c4

`Dest IP` : آدرس‌هایی که از طریق این مسیریاب می‌توان به آن‌ها رسید.

`Mask` : اگر حاصل AND این فیلد و آدرس IP مقصد برابر Dest IP شود، مقصد از طریق این مسیریاب قابل دسترسی است.

`IP` : آدرس IP مسیریاب .

`Interface` : شماره واسطی که از طریق آن به مسیریاب مورد نظر متصل هستیم.

`MAC` : آدرس سخت افزاری مسیریاب.

ساختار جدول Proxy نیز به صورت زیر است:

IP	Interface	MAC
192.168.113.7	1	78:31:c1:d4:57:c4
192.168.116.3	2	78:42:e1:d4:57:c4

`IP` : آدرس IP مسیریاب PR .

`Interface` : شماره واسطی که از طریق آن به مسیریاب مورد نظر متصل هستیم.

`MAC` : آدرس سخت افزاری مسیریاب.

همچنین مسیریاب های PR علاوه بر اطلاعات مسیریابی به اطلاعات لیستِ سیاه هم نیاز دارند:

IP	Mask
192.168.110.0	255.255.255.240
192.168.117.0	255.255.255.240

`IP` : مجموعه آدرس‌های IP غیرمجاز برای این مسیریاب.

`Mask` : اگر حاصل AND شدن این فیلد و آدرس مسیریاب درخواستی برابر مقدار IP شود، مسیریاب مقصد غیرمجاز است.

اطلاعات فوق در قالب متغیر از نوع رشته CustomInformation در دسترس شما قرار دارد.

چنانچه یک بسته توسط مسیریابی IP فرستاده شود پیام زیر چاپ خواهد شد:

```
ping packet sent with IP routing to <IP> on interface <Interface>
```

`IP` : آدرس مسیریاب next hop

`Interface` : شماره واسطی که بسته از طریق آن ارسال شده است.

۸.۴.۲. توضیح Custom Information

جدول اطلاعات مسیریابی IP در این قسمت قابل دسترسی است.

برای دریافت CustomInformation از تابع getCustomInformation() استفاده کنید که به عنوان خروجی یک رشته برمی‌گرداند. نمونه خروجی این تابع به شکل زیر است :

Routing Table

Dest IP	Mask	IP	Interface	MAC
192.168.110.0	255.255.255.240	192.168.113.7	1	78:31:c1:d4:57:c4
192.168.117.0	255.255.255.240	192.168.116.3	2	78:42:e1:d4:57:c4

Proxy Table

IP	Interface	MAC
192.168.113.7	1	78:31:c1:d4:57:c4
192.168.116.3	2	78:42:e1:d4:57:c4

Blacklist Table

IP	Mask
192.168.110.0	255.255.255.240
192.164.0.0	255.255.0.0

نکات ضروری

- به علت اینکه نمره‌ی تمرین به صورت خودکار داده می‌شود، ساختار پیام‌های گفته شده باید دقیقاً به صورت گفته شده باشد.
- نحوه‌ی ارزیابی ممکن است دچار تغییراتی شود و تست‌های دیگری اضافه شوند.
- در صورتی‌که هر مشکل یا پرسشی داشتید که فکر می‌کنید پاسخ آن برای همه مفید خواهد بود، آن را به گروه اینترنتی درس ارسال کنید.
- از فرستادن جواب تمرین به گروه اینترنتی درس خودداری کنید.
- تمام برنامه‌ی شما باید توسط خود شما نوشته شده باشد. فرستادن کل یا قسمتی از برنامه‌تان برای افراد دیگر، یا استفاده از کل یا قسمتی از برنامه‌ی فرد دیگری، حتی با ذکر منبع، تقلب محسوب می‌شود.
- پس از اتمام کارتان لازم است پوشه‌ی user-router را به همراه Makefile فشرده کرده (می‌توانید این کار را با اجرای دستور `make archive` انجام دهید) و از طریق وب‌سایت پرتو ارسال نمایید .
- بخش تمرین تئوری را در قالب فایل PDF به آدرس ایمیل sasan@ce.sharif.edu ارسال کنید و همچنین ایمیل salimi@ce.sharif.edu را CC نمایید. نام فایل ارسالی و عنوان ایمیل باید بصورت YourLastName-443-PA1 باشد.