

تمرین اول شبکه

حدیث غفوری 9825413

سوال 1.

A: تفاوت های ADSL , HFC ؟

در روش HFC برای هر مصرف کننده یک Uplink یا downlink نداریم در واقع این کانال ها اشتراکی است اما ADSL اختصاصی است.

مشتری ها تجربه بسیار بهتری در Hybrid Fiber Coaxial (HFC) نسبت به ADSL دارند.

Cable سرعت بارگیری حداکثر 100 مگابیت بر ثانیه را در مقایسه با 22 مگابیت در ثانیه در ADSL (که تنها در صورتی امکان پذیر است که فاصله چند صد متر باشد) به مشتریان ارائه می دهد. از نظر تنوری کابل 5 برابر سریعتر است و مانند ADSL تحت تأثیر تداخل و مسافت قرار نمی گیرد.

برای ADSL از زیرساخت تلفن و HFC از زیرساخت تلویزیون استفاده میکند مانند ADSL به مودم نیاز داریم اما نوع مودم متفاوت است.

B: روترها به کدام یک از لایه های internet protocol دسترسی دارند؟

روتر یک وسیله ای است که اطلاعات را بین دو یا چند شبکه منتقل میکند.

یک روتر ادرس ایپی بسته ی مقصد را بررسی میکند.

Network/link/physical

C: Botnet چیست و چه اقداماتی با استفاده از آن میتوان انجام داد؟

بات نت ها شبکه هایی هستند که با در اختیار گرفتن مجموعه ای از کامپیوترها که بات (bot) نامیده می شوند، تشکیل می شوند. این شبکه ها توسط یک یا چند مهاجم که botmasters نامیده می شوند، با هدف انجام فعالیت های مخرب کنترل می گردند. به عبارت بهتر، ربات ها کدهای مخربی هستند که بر روی کامپیوترهای میزبان اجرا می شوند تا امکان کنترل نمودن آنها از راه دور را برای botmaster ها فراهم نمایند و آنها بتوانند این مجموعه را وادار به انجام فعالیت های مختلف نمایند. کامپیوترها در یک بات نت وقتی که یک نرم افزار مخرب را اجرا می کنند، می توانند مشترک تصمیم بگیرند. آنها با فریب دادن کاربران نسبت به ایجاد یک درایو با استفاده از دانلود کردن، بهره برداری از آسیب پذیری های web browser، یا از طریق فریب

کاربران برای اجرای یک اسب ترویان که ممکن است از ضمیمه یک فایل پیاید، می‌توانند این کار را انجام دهند. این بردافزار به‌طور معمول مایکروسافت را نصب خواهد کرد که باعث می‌شود کامپیوتر توسط اپراتور بات نت فرمان دهی و کنترل شود. یک ترویان بسته به پیکونگی نوشته شدن آن، ممکن است خودش را حذف کند یا برای پرورسانی و حفظ مایکروسافت باقی بماند.

مثلاً در یکی از این اقدامات در عملیات denail-of-service توزیعی، تعداد زیادی درخواست در هر ممکن از طرف چندین سیستم به یک کامپیوتر یا سرور می‌شود و سرور زیادی برایش ایجاد می‌کنند و از پاسخ دادن به درخواست‌های قانونی جلوگیری می‌کنند. یک مثال عمده به یک شماره تلفن قربانی است. قربانی با تماس‌های تلفنی بات که قصد دارد به اینترنت متصل شود، بمباران می‌شود.

بات‌نت‌ها می‌توانند فعالیت‌های مخربی از جمله spamming، انجام عملیات DDoS، توزیع بردافزارها مثل Trojan horses، ابزارهای جاسوسی و keyloggerها، به سرقت بردن نرم‌افزارها، کشف و سرقت اطلاعات، سرقت هویت، دستکاری بازی‌های آنلاین و نظر سنجی‌ها، عملیات phishing و کشف کامپیوترهای آسیب‌پذیر را انجام دهند.

D: Ethernet برپه بسترهای فیزیکی پیاده سازی میشود؟

سیستم‌های Ethernet با سیم‌های زوج به هم تابیده (مسی) توسعه یافتند. (با سرعت 1 Gbps) (و همین‌طور فیبر نوری)

E: برتری روش packet switch نسبت به cuircuit switch در چیست؟

در شبکه‌های Packet Switching، پهنای باند را می‌توان به‌طور کامل مورد استفاده قرار داد، در حالی که استفاده از پهنای باند در شبکه‌های Circuit Switching بدلیل اینکه هر ارتباطی نیاز به پهنای باند اختصاصی دارد کمتر کارآمد خواهد بود. (می‌توان از منابع به صورت کارآمدتری استفاده نمود) با توجه به اینکه در شبکه‌های Packet Switching هر بسته از آدرس‌های خود استفاده می‌کند می‌توانیم در این شبکه‌ها افزونگی داشته باشیم، در حالی که در شبکه‌های Circuit Switching از پیش تعریف شده است. (امکان توسعه بیشتر است) زمانی که تعداد کاربران افزایش می‌یابد شبکه‌های Packet Switching می‌توانند به اشتراک گذاشته شوند، در حالی که حداکثر تعداد کانال‌های موجود شبکه‌های Circuit Switching محدود است.

F: مفاهیم زیر را تعریف کنید.

Host and endsystems در حقیقت یک مفهوم هستند. از رایانه متصل به شبکه به عنوان سیستم انتهایی یاد می‌شود. اینها در حقیقت در لبه شبکه قرار دارند. کاربر نهایی همیشه با سیستم‌های نهایی ارتباط برقرار می‌کند. سیستم‌های نهایی دستگاه‌هایی هستند که اطلاعات یا فرامات را ارائه می‌دهند. از سیستم‌های پایانی که به اینترنت متصل هستند نیز به عنوان میزبان

اینترنت یاد می شود. این به این دلیل است که آنها برنامه های اینترنتی مانند یک مرورگر وب یا یک برنامه بازیابی ایمیل را میزبانی (اجرا) می کنند. با ظهور اینترنت اشیا، وسایل منزل (مانند یخچال) و همچنین کامپیوترهای دستی و دوربین های دیجیتال قابل حمل، به عنوان سیستم نهایی به اینترنت متصل می شوند. سیستم های انتعایی با استفاده از دستگاه های سوئیچینگ شناخته شده به عنوان روتر به یکدیگر متصل می شوند.

تقسیم زمان با دسترسی چندگانه (TDMA) یک روش دسترسی برای شبکه های مشترک شده است. چند کاربر جهت اشتراک کانال با فرکانس مشابه با تقسیم سیگنال به شیارهای زمانی متفاوت می توانند از این روش استفاده کنند. کاربران به سرعت تغییر می یابند، یکی بعد از دیگری، هر کدام با استفاده از شیار زمانی خودشان. این امر به ایستگاه های متعدد امکان اشتراک وسیله انتقال مشابهی را می دهند (مثل کانال فرکانس رادیویی) در حالیکه تنها بخشی از ظرفیت کانال خود استفاده می کنند.

تقسیم فرکانس با دسترسی چندگانه (FDMA) روشی برای تقسیم پهنای باند فرکانس مویور برای فرستادن امواج رادیویی است. در این قسمت به جای تقسیم در زمان فرکانس ها تقسیم میشوند. این روش معمولاً در ارتباط با ماهواره ها مورد استفاده قرار می گیرد. از مشکلات این روش تحت تاثیر قرار گرفتن فرکانس های مختلف توسط یکدیگر و ایجاد اختلال در عین انتقال داده است

تأخیر انتشار مقدار زمانی است که طول می کشد بالاترین سیگنال از فرستنده به گیرنده جابه جا شود. این را می توان به عنوان نسبت بین طول پیوند و سرعت انتشار امواج در میان آن محاسبه کرد. تأخیر پخش برابر است با d/s که در آن d فاصله است و S سرعت پخش موج است. در ارتباطات بی سیم $S=C$ یعنی سرعت نور است. در سیم مسی، سرعت ها به طور کلی از محدوده میلی ثانیه است این تأخیر مانع اصلی در توسعه رایانه های با سرعت بالا است و گلوگاه اتصال در سیستم های IC نامیده می شود.

تأخیر انتقال مدت زمان لازم برای وارد کردن همه بیت های بسته به داخل سیم است. به عبارت دیگر، این تأخیر ناشی از بیت ریت لینک است. تأخیر انتقال تابعی از طول بسته است و هیچ ارتباطی با فاصله بین دو گره ندارد. این تأخیر متناسب با طول بسته و تعداد بیت هر بسته است، (N/R) ثانیه (تعداد بیت ها است، و R سرعت انتقال است (بیت بر ثانیه) و از مرتبه میکرو تا میلی ثانیه است

سوال 2.

A: بیشترین تعداد ارتباط که این شبکه در یک لحظه میتواند برقرار کند؟

$$10+19+15+15= 59$$

B: فرض کنید هر ارتباط هتما به دو Hop متوالی نیاز دارد تا ارتباط برقرار شود و این Hop ها در جهت ساعتگرد صورت می گیرند. به عنوان مثال ارتباط می تواند از A به C با استفاده از B برود یا از B به D با استفاده از C. بیشترین تعداد ارتباطاتی که این شبکه می تواند در لحظه برقرار کند چه تعداد است؟

$$10+15=25$$

اگر از A به C و از C به A برود در اینصورت از C به A تا 15 و از A تا 10 برود و هر دو را اشغال میکند و از A به C 10 و 19 تا که چون همه منابع همزمان اشغال میشوند وقتی 10 curicuit پر شود دیگر امکان ارتباط اضافی نیست و همان 10 تا حداکثر است.

C: در حالت ساعتگرد، اگر به 15 ارتباط از A به C و 12 ارتباط از B به D احتیاج باشد، آیا این شبکه توانایی برقراری این ارتباط ها را دارد

فیر زیرا وقتی یک منبع مشغول باشد دیگر نمیتواند در اختیار راه دیگری قرار گیرد.

سوال 3.

A: فرض کنید یک پیام بدون Segmentation را از مبدا به مقصد می فوایم ارسال کنیم. مقدار طول می کشد تا این پیام به مقصد برسد؟

$$8 \times 10^6 / 2 \times 10^6 = 4s$$

4 ثانیه طول میکشد تا یک پیام از یک لینک عبور کند و چون 3 تا لینک داریم $4 \times 3 = 12$ ثانیه ارسال کل پیام طول میکشد

B: چه مدت طول میکشد که بسته اول وارد سویچ اول شود؟

بسته دوم چه زمانی به صورت کامل وارد سویچ دوم میشود؟

چه مدت طول میکشد تا بسته به طور کامل به مقصد برسد؟

$$20 \times 10^3 / 2 \times 10^6 = 0.01s$$

بعد از 0.01 ثانیه بسته اول به روتر اول میرسد پس از 0.01 دیگر این بسته به روتر دوم و بسته دوم به روتر اول میرسد

پس از 0.01 ثانیه دیگر بسته اول به مقصد و بسته دوم به روتر دوم میرسد و بسته سوم به روتر اول میرسد و به همین

ترتیب جلو میرود بنابراین به صورت کلی 0.03 ثانیه نیاز است تا بسته دوم به سویچ دوم برسد

پس از 4.02 ثانیه کل بسته ها به مقصد می‌رسند.

C: زمان های مراحل الف و ب را با هم مقایسه کنید و اعلام کنید که کدام روش بهتر است ؟

تقسیم کردن بسته ها روش بهتری از نظر تأخیر است.

D: مزایا و معایب Segmentation Message را به اختصار توضیح دهید.

یک مزیت تقسیم بندی شبکه ، بهره وری ترافیک است. هنگامی که رایانه ها با یکدیگر ارتباط برقرار می کنند ، آنها بیت هایی از اطلاعات را به نام "بسته" شامل مفتوای ارتباطات و همچنین اطلاعات مربوط به فرستنده و گیرنده ارسال می کنند. اگر دو رایانه به طور همزمان داده های دیگری را ارسال کنند - یا اگر چندین رایانه داده ها را به یکدیگر ارسال کنند - "برفورد بسته" ممکن است رخ دهد که اطلاعات ارسالی را خراب کرده و ارتباط را خراب می کند. هنگام برفورد با شبکه های بزرگ ، همه رایانه ها می توانند با همه رایانه های دیگر ارتباط برقرار کنند ، و احتمال برفورد وجود دارد. با استفاده از یک شبکه تقسیم شده ، رایانه ها تحت اکثر شرایط می توانند در داخل بخشها ارتباط برقرار کنند ، بنابراین حجم ترافیک شبکه عمومی را کاهش می دهند و احتمال برفورد بسته ها را کاهش می دهند. تقسیم بندی شبکه همچنین امکان افزایش کارایی ارتباطات را فراهم می کند. تقسیم بندی چندین مزیت امنیتی به شما می دهد. اولین مورد مربوط به داشتن بخشهایی است که ترافیک مشترک ندارند ، به این معنی که اگر رایانه ای در یک بخش به خطر بیفتد ، به طور فوکار به معایم دسترسی به رایانه های قسمت دیگر را نمی دهد. این میزان مواجهه با تهدید را محدود می کند. در مرحله دوم ، می توانید از طریق نرم افزار امنیتی و فایروال ها هر بخش را به طور متفاوتی ایمن کنید ، بنابراین یک معایم مجبور است برای دسترسی به بخشهای مختلف ، مجموعه های امنیتی مختلفی را نقض کند ، به همین دلیل به خطر انداختن کل سیستم دشوارتر می شود.

سوال 4.

A: حداکثر تعداد کاربرانی که به طور همزمان می توانند از شبکه استفاده کنند چقدر می باشد؟

$$[50/15]=3$$

B: حداکثر درصد فعال بودن کاربران بایر چقدر باشد تا با احتمال بالای 95 ، همه ی کاربران از شبکه استفاده کنند ؟

توزیع دو جمله ای : از قسمت الف میتوان فهمید که تا سه کاربر را شبکه بدون هیچ مشکلی به طور همزمان هندل میکند بنابراین حالات 0 و 1 و 2 و 3 را در نظر میگیریم باید دید در این حالات اگر کاربر در چند درصد مواقع فعال باشد با احتمال 0.95 همه کاربران احتمال دسترسی دارند. در واقع برای هر حالت به عنوان مثال 2 کاربر باید 2 تا از 10 تا را انتخاب کنیم این ها با احتمال p فعالن و مجموع همه این حالات باید 0.95 شود که همان توزیع دو جمله ای است.

[illegible]

سوال 6.

A: تأخیر دسترسی خود را به دو مقصد **دلفواه یک وبسایت داخلی و یک وبسایت خارجی** را بررسی کنید و **خروجی ترمینال خود** را در پاسخ خود قرار دهید.

```
Administrator: Command Prompt

C:\Windows\system32>ping www.google.com

Pinging www.google.com [216.58.209.132] with 32 bytes of data:
Reply from 216.58.209.132: bytes=32 time=161ms TTL=111
Reply from 216.58.209.132: bytes=32 time=160ms TTL=111
Reply from 216.58.209.132: bytes=32 time=231ms TTL=111
Reply from 216.58.209.132: bytes=32 time=158ms TTL=111

Ping statistics for 216.58.209.132:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 158ms, Maximum = 231ms, Average = 177ms

C:\Windows\system32>ping www.downloadly.ir

Pinging www.downloadly.ir [185.120.222.190] with 32 bytes of data:
Reply from 185.120.222.190: bytes=32 time=35ms TTL=57
Reply from 185.120.222.190: bytes=32 time=35ms TTL=57
Reply from 185.120.222.190: bytes=32 time=35ms TTL=57
Reply from 185.120.222.190: bytes=32 time=130ms TTL=57

Ping statistics for 185.120.222.190:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 130ms, Average = 58ms

C:\Windows\system32>
```

B: با توجه به خروجی ترمینال خود، چه اطلاعاتی توسط این دستور قابل برداشت می باشد؟

سرعت اتصال به سایت های داخلی بیشتر از خارجی است.

C: دسترسی خود به مقصد **127.0.0.1**، را بررسی کنید. چرا زمان دسترسی نسبت به قسمت قبل کمتر می باشد؟

زیرا همان سیستم خودمان است و localhost است.

:D

```
C:\Windows\system32>tracert www.google.com
```

```
Tracing route to www.google.com [172.217.18.132]  
over a maximum of 30 hops:
```

1	9 ms	1 ms	1 ms	192.168.1.1
2	*	*	*	Request timed out.
3	27 ms	33 ms	28 ms	172.16.35.85
4	*	*	*	Request timed out.
5	25 ms	25 ms	25 ms	172.16.2.173
6	30 ms	29 ms	25 ms	10.202.6.18
7	49 ms	44 ms	43 ms	10.21.0.11
8	*	45 ms	45 ms	10.21.0.11
9	558 ms	311 ms	387 ms	213.202.4.172
10	271 ms	166 ms	238 ms	213.202.5.239
11	166 ms	158 ms	159 ms	216.239.48.87
12	162 ms	167 ms	159 ms	172.253.51.135
13	211 ms	203 ms	158 ms	arn02s05-in-f132.1e100.net [172.217.18.132]

```
Trace complete.
```

```
C:\Windows\system32>tracert www.downloadly.ir
```

```
Tracing route to www.downloadly.ir [185.120.222.190]  
over a maximum of 30 hops:
```

1	5 ms	5 ms	3 ms	192.168.1.1
2	135 ms	63 ms	67 ms	10.142.33.8
3	33 ms	34 ms	33 ms	172.16.35.81
4	34 ms	32 ms	33 ms	172.16.34.45
5	37 ms	34 ms	34 ms	172.16.2.173
6	36 ms	34 ms	36 ms	172.16.3.18
7	35 ms	33 ms	35 ms	hosted-by.hostdl.com.asiatech.ir [185.120.222.190]

```
Trace complete.
```

```
C:\Windows\system32>
```



E: اولین hop ای که بسته شما از آن عبور می کند چیست؟ برای مقصد های دیگر این موضوع را بررسی کنید. دلیل یکسان بودن اولین hop در همه مقصد ها چه می باشد؟

اولین hop همان اولین دسترسی است به عنوان مثال میتواند اولین روتر در مودم باشد به همین دلیل همواره یکسان است

F: مشخص کنید که بسته تا رسیدن به مقصد خود چند hop را طی می کند ؟


گوگل ۱۳ تا و سایت داندلودی ۷ تا

G: برای مقصد خارج از کشور خود مشخص کنید که بسته از چند کشور عبور می کند.


Country	Region	City
Iran (Islamic Republic of) 	Esfahan	Isfahan
Organization	Latitude	Longitude
Not Available	32.6572	51.6776


[info.io](https://www.info.io) (Product: API, real-time)

Country	Region	City
Iran 	Isfahan	Isfahan


Country	Region	City
Oman 	Masqat	Muscat
Organization	Latitude	Longitude
Not Available	23.6133	58.5933

[info.io](#) (Product: API, real-time)

Country	Region	City
Luxembourg 	Diekirch	Mertzig
Organization	Latitude	Longitude
OmanMobile	49.8339	6.0075

Country	Region	City
United States of America 	California	Mountain View
Organization	Latitude	Longitude
Not Available	37.4060	-122.0785

[pinfo.io](#) (Product: API, real-time)

Country	Region	City
United States 	California	Mountain View
Organization	Latitude	Longitude
Google LLC (google.com)	37.4056	-122.0775

۳ کشور ایران و عمان و امریکا

H: تغییرات ناگهانی در تأخیر دسترسی به بعضی از node ها به چه دلیل می باشد؟

لینک های بین قاره ای و فاصله های طولانی در مسیر

i: دستور traceroute چگونه عمل می‌کند؟ توضیح دهید.

زمانیکه شما به یک وب سایت متصل می‌شوید، ترافیک ارسالی از مسیرها و واسطه‌های مختلفی عبور می‌کند تا به مقصد برسد. همچنین شما می‌توانید با استفاده از این دستور میزان تأخیر بوجود آمده در هر توقف را نیز مشاهده کنید. اگر گاهی اوقات مشکلی در رسیدن به وب سایت مورد نظر دارید اما می‌دانید که آن وب سایت بدرستی کار می‌کند، قطعاً در مسیر مشکلی وجود دارد، دستور Traceroute به شما نشان می‌دهد که مشکل در کدام قسمت از مسیر است.

از منظر فنی دستور Traceroute یک ترتیب متوالی از بسته‌ها را با استفاده از پروتکل ICMP ارسال می‌کند. هر کدام از این بسته‌ها مقداری را بررسی می‌کنند و دارای یک زمان مشخص می‌باشند. هرگاه زمان هر بسته‌ای به صفر برسد، روتر مورد نظر آن را برگشت داده و پیام خطا نمایش داده می‌شود. با ارسال بسته‌ها به این شیوه، Traceroute مطمئن می‌شود که هر روتر در مسیر فعال هست یا نه.

این دستور برای ردیابی مسیر حرکت و سنجش تأخیر انتقال بسته‌های شبکه‌ای در شبکه‌ای با پروتکل اینترنت (IP) مورد استفاده قرار می‌گیرد. ابزار تریس روت به وسیله افزایش مقدار تی‌تی‌ال برای هر فوشه ارسال شده از بسته‌ها کار می‌کند. سه بسته فرستاده شده نسبت تی‌تی‌ال مقدار یک دارند. بسته‌های بعدی مقدار تی‌تی‌ال دو دارند و به همین ترتیب مقدار تی‌تی‌ال بسته‌ها زیاد می‌شود. وقتی یک بسته به یک میزبان می‌رسد، به‌طور عادی یک عدد از مقدار تی‌تی‌ال آن کم می‌شود، و پس از آن بسته به مقصد بعدی ارجاع داده می‌شود. ولی هنگامی که یک بسته با مقدار تی‌تی‌ال یک به میزبانی برسد، میزبان بسته را دور می‌ریزد و پیام آی‌سی‌ام‌پی با مفتوای از حد زمانی تجاوز شده (نوع ۱۱) به فرستنده بازپس می‌فرستد. ابزار تریس روت از این نوع بازگشت بسته (رد کردن بسته) استفاده می‌کند تا تسیتی از میزبان‌هایی که بسته با مسیریابی منتقل شده تا به مقصد برسد را تولید کند. در ضمن سه مقدار زمانی (از فاصله تا میزبان) برای هر یک از میزبان‌هایی که بسته باید طی کند با واحد میلی‌ثانیه بازگردانده می‌شود. (البته می‌توان چرآگانه میزبان‌ها را پینگ کرد.)