به نام خدا

کامیار جان پروری – ۹۶۲۶۰۱۵ تمرین سری دوم شبکه های کامپیوتری موعد تحویل: ۲۶ اردیبهشت

سؤال اول- مزایا و معایب لایه بندی:

- مزایا:

۱- لایه بندی با تقسیم فرایند کلی ارتباطات به بخش ها ، طراحی ، پیاده سازی و آزمایش را ساده می کند.

۲- پروتکل در هر لایه می تواند جداگانه از لایه های دیگر طراحی شود.

۳- پروتکل "تماس"ها (calls) را برای خدمات از لایه زیرین ایجاد می کند.

۴- لایه بندی انعطاف پذیری را برای اصلاح و تغییر پروتکل ها و خدمات، بدون نیاز به تغییر لایه های زیر فراهم می کند.

۵- معماریهای بدون لایه یکپارچه پرهزینه ، انعطاف پذیر و به زودی منسوخ هستند.

۶- سیستم تست پذیرتر خواهد شد و هر لایه مورد آزمایش کمتر و نتیجه آزمایش بیشتر خواهد داشت.

- معایب:

۱- هزینه های مدیریت اگر لایه های زیادی وجود داشته باشد زیاد خواهد شد.

۲- با افزودن لایه های بیشتر ، عملکرد کندتر می شود.

۳- Leaky abstraction می تواند هدف لایه لایه شما را مختل کند.

۴- هر لایه یک overhead اضافه می کند.

۵- تعامل بد بین لایه ها به سختی قابل حل است.

سؤال دوم-

اگر لایه data likn یک سرویس connection-oriented را به لایه شبکه ارائه می دهد ، پس لایه شبکه باید جلوتر قبل از انتقال اطلاعات با یک روش connection setup متصل باشد.

اگر سرویس connection oriented شامل اطمینان از اینکه frame اطلاعات به صورت صحیح و به ترتیب توسط لایه پیوند داده منتقل می شود ، لایه شبکه می تواند فرض کند که بسته های ارسال شده به همسایه خود یک pipe بدون خطا را طی می کند.

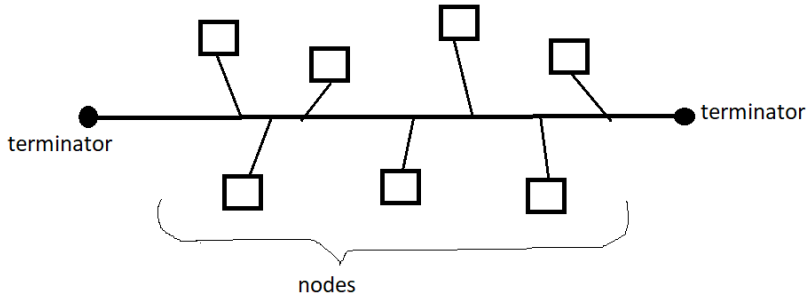
از طرف دیگر ، اگر لایه data link، connection-less باشد ، سپس هر frame به طور مستقل از طریق data link ارسال می شود ، احتمالاً به روشی تأیید نشده (بدون تأیید یا انتقال مجدد). در این حالت ، لایه شبکه نمی تواند فرضیه هایی درباره توالی یا صحت بسته هایی که با همسایگان خود مبادله می کند ، داشته باشد.

شبکه محلی ethernet نمونه ای از انتقال connection-less فریم های data link را ارائه می دهد. انتقال frame با استفاده از سرویس "Type 2" در Logical Link Control یک مثال از کنترل data link، connection-oriented را ارائه می دهد.

سؤال سوم-

خیر، نیازی نیست. زیرا لایه ی شبکه دو وظیفه دارد: ۱- routing ۲- forwarding

که در این مدل نیازی به این‌ها نیست. زیرا در این توپولوژی یک سیم مشترک وجود دارد و همه device ها به عنوان گره هایی به آن متصل اند و وقتی داده ای توسط گره ای ارسال می شود و در سیم مشترک به سمت دو انتها حرکت می کند و تمام گره‌ها را می پیماید و گره مورد نظر آن را بر می‌دارد و پیام در انتهای سیم از بین می‌رود.



سؤال چهارم-

- Multiplexing: به این صورت عمل می‌کنند که داده‌هایی که از لایه‌های بالاتر می‌رسد هرکدام با یک header مجزا encapsulate می‌شود و به لایه ی بعدی داده می‌شود. وقتی این‌ها به لایه متناظر برسد می‌تواند با این header ها آن‌ها را متمایز کند (که در demultiplexing توضیح داده شده است).
  برای مثال در لایه transport داده هایی که از سوکت های مختلف از لایه .App دریافت شده را با header های مخصوص encapsulate می کند و segment های حاصل را به لایه network می‌دهد.
  لایه شبکه نیز همین کار را می‌کند و نتایج حاصل را به data link می‌دهد. Data link علاوه بر ابتدا نیز در انتهای آن ها هم بخشی می‌گذارد و یک frame را تشکیل می‌دهد.
- Demultiplexing: دقیقا برعکس بالا عمل می‌کند. مثلا در لایه transport این داده‌ها را از header های آن‌ها تشخیص می‌دهد و متمایز می‌کند و به سوکت مربوطه تحویل می‌دهد. (با port number سوکت مقصد را تشخیص می‌دهد.

سؤال پنجم-

الف)

برای محاسبه این کافیست تأخیر رسیدن بسته از مبدأ به سوییچ را محاسبه کنیم، سپس آن را ضرب در ۲ کنیم.

Delay = $2(D_{trans} + D_{prop})$ $$D_{trans} = \frac{L}{R} = \frac{5000}{10\times10^6} = 50 \times 10^{-5}$$

$$Delay = 2\left(50 \times 10^{-5} + 10 \times 10^{-6}\right) = 1.02 \times 10^{-3}$$

ب)

$$Delay = 4(D_{trans} + D_{prop}) = 2.04 \times 10^{-3}$$

ج)

زمان انتقال ۲۰۰ بیت اول به سوییچ: $$\frac{200}{10\times10^6} + 10 \times 10^{-6} = 3 \times 10^{-5}$$

زمان انتقال کل بسته از سوییچ به مقصد: $$\frac{5000}{10\times10^{-6}} + 10 \times 10^{-6} = 51 \times 10^{-5}$$

مجموع تأخیرها : 5.4×10^{-4}

سؤال ششم-

الف) در قسمت الف چون یک بسته است بسته تأخیر ناشی از صف نداریم.

$$D_{Trans} = \frac{L}{R} \qquad D_{nodal} = D_{trans} + D_{Prop} \qquad D_{total} = d_1 + d_2 + d_3 + d_4$$

$$d_1 = (2 \times 10^{-3}) + \left(\frac{1500}{10^6}\right) = 3.5 \times 10^{-3}$$

$$d_2 = (20 \times 10^{-3}) + (\frac{1500}{5 \times 10^5}) = 23 \times 10^{-3}$$

$$d_3 = (30 \times 10^{-3}) + (\frac{1500}{10^6}) = 31.5 \times 10^{-3}$$

$$d_4 = (2 \times 10^{-3}) + (\frac{1500}{2 \times 10^6}) = 2.75 \times 10^{-3}$$

$$d_{total} = \ 60.75 \ ms$$

ب)

زمان رسیدن بسته اول به انتها = ۶۰.۷۵ میلی‌ثانیه

وقتی بسه اول به دست bob می‌رسد، بسته دوم در سوییچ سوم است و آماده ارسال و بسته سوم در حال ارسال از سوییچ دوم به سوییچ سوم است که از ۱.۵ میلی‌ثانیه لازم برای رسیدن از سوییچ دوم به سوم ۰.۲۵ میلی‌ثانیه باقی‌مانده است .

زمان رسیدن بسته سوم = ۱.۵ میلی‌ثانیه

زمان کل = ۶۲.۲۵ میلی‌ثانیه

ج)

بسته‌های 1,2,3,4,5,6 به مقصد می‌رسد و مابقی در اثر پر بودن صف سوییچ اول از بین می‌روند.

د)

چون تأخیر لینک دوم از لینک اول خیلی بیشتر است پس خیلی از بسته ها را از دست می‌دهیم.

با سرعت ذکر شده یعنی هر ۰.۷۵ میلی‌ثانیه یک بسته جدید ارسال می‌شود

75درصد از بین می‌رود زیرا گلوگاه لینک ۵۰۰ کیلوبایت است و داده ها با سرعت ۲ مگابایت ارسال می‌شوند

سؤال هفتم-

۱- Volume Based : در این نوع حمله تعداد زیادی request به سیستم target داده می‌شود. ، مهاجمان بطور معمول قربانی را با حجم زیاد بسته ها یا اتصالات ، تجهیزات شبکه ، سرورها یا منابع پهنای باند قربانی می کنند. اینها معمولی ترین حملات DDoS هستند.

- راهکار: تقویت پروتکلی برای شناسایی درخواست‌های غیر واقعی

۲- Application Based : در این نوع حمله، ورودی های نرم‌افزار دستکاری می‌شود و به داده های محرمانه یا... دست پیدا خواهد شد.

- راهکار: تقویت حفره های لایه Application

۳- Protocol Based : هدف از حمله DDoS مبتنی بر پروتکل شبکه ، استفاده از یک ضعف پروتکل است. مهاجمان می توانند با ارسال تعداد زیادی از دستورات SYN به سرور از این فرآیند سوء استفاده کنند.

- راهکار: تقویت encryption .

سؤال هشتم-

میانگین حجم بسته ها : $\frac{20*1000 + 50*1500 + 30*1200}{100} = 1310$

تاخیر:

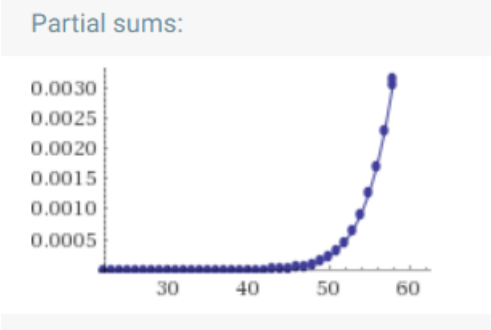
سؤال نهم-

الف) در روش circuit switching : $\frac{2.2\times10^6}{10^5} = 22$ پس ۲۲ نفر می‌توانند هم زمان استفاده کنند. و در این روش مهم نیست هر کاربر چند درصد اوقات متصل است.

$$\sum_{k=22}^{n} 0.2^{22} \times 0.8^{k-22} \binom{k}{22} =$$

در روش packet switching : p = 0.2

همان طور که در نمودار مشاهده می‌شود، احتمال اینکه در ۵۵ کاربر بیشتر از ۲۲ کاربر به طور هم زمان در حال کار باشند نزدیک ۰.۰۰۰۵ است.



ب) بدیهی است که در روش circuit برای همه‌ی کاربران تضمین وجو دارد که در هر موقع می‌توانند اتصال مطمئن داشته باشند اما از منابع به صورت بهینه استفاده نمی‌شود، در روش packet تعداد بیشتری از کاربران می‌توانند از سرویس بهره ببرند و از منابع بهینه‌تر استفاده شود، اما با اینکه احتمال اتصال همزمان تعداد بیش از حد کاربران کم است، تضمینی نیست که مشکلی پیش نیاید.

سؤال دهم-

گلوگاه لینک ۴۰ مگابایتی است. پس هر کاربر باید حداکثر در هرثانیه ۴ مگابایت استفاده کند.

یعنی هر کاربر حد اکثر هر 0.375ms یک بسته بفرستد.

$$\frac{1500}{4 \times 10^6} = 3.75 \times 10^{-4}$$

سؤال یازدهم-

Eternalblue به باج افزار اجازه داد به سایر دستگاه های موجود در شبکه دسترسی پیدا کند. مهاجمان می توانند از DoublePulsar ، که توسط گروه equation توسعه یافته و توسط Shadow Brokers نیز بیرون آمده است ، به عنوان payload برای نصب و راه اندازی یک نسخه از باج افزار بر روی هر هدف آسیب پذیر ، استفاده کنند.

EternalBlue از آسیب پذیری در اجرای پروتکل Server Message Block (SMB) مایکروسافت سوءاستفاده می کند. این آسیب پذیری با ورود CVE-2017-0144 در کاتالوگ آسیب پذیریها و قرار گرفتن در معرض (CVE) مشخص شده است. این آسیب پذیری به دلیل وجود سرور SMB نسخه ۱ (SMBv1) در نسخه های مختلف مایکروسافت ویندوز ، به ویژه بسته های ساخته شده مهاجمان از راه دور است و به آنها امکان اجرای کد دلخواه را در رایانه هدف می دهد.

EternalBlue توسط NSA توسعه داده‌شد و توسط گروهی که بالا گفته شد به بیرون درز کرد. این اتفاقات در آپریل ۲۰۱۷ افتادند.

سپس در ماه می ۲۰۱۷ باج افزار جهانی WannaCry از این exploit برای حمله به رایانه های unpatched استفاده کرد. این حمله در ۱۲ می آغاز شد و infection اولیه احتمالا از طریق یک درگاه آسیب پذیر SMB اتفاق افتاده بود (اما ابتدا فرض کرده بودند از طریق email phishing بوده) و طبق گزارش بیش از ۱۵۰ کشور و ۲۳۰ هزار رایانه ر آلوده کرد

این اتفاق دوباره در حمله سایبری notPetya در ژوئن ۲۰۱۷ رخ داد.

سؤال دوازدهم-

به طور کلی لایه حمل و نقل وظیفه تحویل فرایند به فرایند کل پیام را دارد ، در حالی که لایه شبکه نظارت بر تحویل بسته های جداگانه از میزبان به میزبان را دارد.

Transport Layerجایی است که تصمیم به استفاده از TCP / UDP گرفته می شود. در بین پروتکل های متداول در این لایه ، TCP قابل اعتماد است ، UDPنیست. بسته به نوع انتخابی ، هدرهای مربوطه به بسته شما وصل می شوند TCP .به عنوان مثال فقط از-SYN ACK، مکانیسم های three-way handshake می داند ، اما آدرس نقطه انتهایی از راه دور یا مکانیسم دریافت بسته در شبکه را نمی داند.

کنترل تراکم ، کنترل جریان با تنظیم تعداد بسته های ارسال شده ، اطمینان حاصل می کند که شبکه با بسته ها flooded نمی شود.

اکنون ، پس از افزودن هدر TCP / UDP ، آن را به سمت لایه شبکه حرکت می کند. تا این مرحله ، آدرس IP نقطه پایان از راه دور به هیچ وجه جزئی از بسته نبود. در این مرحله است که آدرس های IP Source & Destination به بسته اضافه می شوند. این لایه در واقع نقطه انتهایی از راه دور را می شناسد.