دانشگاه صنعتی امیرکبیر

(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

تمرین دوم

شبکه‌های کامپیوتری

نگارش

محمدرضا اخگری زیری

استاد درس

دکتر صبایی

فروردین ۹۹

فهرست مطالب

صفحه

سوال اول

سـرعت رشـد علم و فناوری در دنیای امروز به حدی زیاد اسـت که هر لحظه باید منتظر ورود فناوری جدیدی باشـیم. این امر در مورد شـبکه های کامپیوتری نیز صـادق بوده ، به نحوی که دنیای شـبکه باید در هر لحظه منتظر ورود نرم افزار، سـخت افزار ، پروتکل و ... جدیدی باشـد تا آنها را تحت پوشـش خود قرار دهد. این نکته به روشـنی بیان می کند که برای تحت پوشـش قرار دادن فناوری های جدید توسط شبکه ، باید سرعت توسعه شبکه نیز با سرعت رشد و توسعه سایر فناوری های دیگر هماهنگ باشد.

یکی از راه حل های مناسب برای افزایش سرعت توسعه شبکه ، استفاده از معماری های شبکه لایه بندی شده می باشد زیرا لایه بندی می تواند مشکلات پیچیده را به قطعات کوچکتر و قابل کنترل تر تبدیل کند.

مزایا:

۱. **طراحی** : **(Design)** در یک مدل لایه ای ، چون هر لایه بصـورت جداگانه طراحی می شـود واهداف، سـاختار و پروتکل های خاص خود رو دارد، در نتیجه یک طراح می تونه در یک لایه خاص تخصص داشته باشه و فقط به توسعه آن لایه بپردازد ، بدون اینکه نگرانی راجع به وضعیت لایه های دیگر داشته باشد. همانگونه که می بینید فرآیند طراحی در چنین مدلی ساده تر بوده و اضافه کردن خدمات جدید و مدیریت زیرساختهای شبکه آسان تر می باشد.

۲. یادگیری : (Learning) لایه بندی سـبب می شـود تا یک مجموعه بسـیار پیچیده از مباحث به گروه های کوچک تر و البته به هم پیوسته تبدیل شوند و در نتیجه یادگیری و درک وظایف و فعالیت های هر لایه ساده تر می شود.

۳. **انعطاف پذیری** : **(Flexibility)** معماری لایه ای باعث افزایش میزان انعطاف پذیری مدل در زمان ایجاد تغییرات و توسعه خدمات شبکه می گردد .

٤. **عیب یابی** : **(Troubleshooting)** در مدل های لایه بندی شـده، چون برای هرلایه یک سـری اهداف خاص تعیین شده و تمام پروتکل ها و داده های درون آن لایه به آن هدف مربوط می شوند، اگر در حین فعالیت مدل مشکلی پیش آید ، به سرعت لایه محل بروز مشکل را شناسایی کرده و تمام تمرکز خود را در آن لایه جهت رفع مشکل قرار می دهیم.

۵. **پیمانه ای کردن** : **(modularity)** پیمانه ای کردن یک سیستم بزرگ و پیچیده سبب شود تا پیاده سازی و تغییر سرویس های درون هر لایه ، آسان تر گردد.

معایب:

۱. احتمال تکرار برخی از عملکردها در لایه های مختلف . مانند **Error control** :و **Flow control**که هم **در لایه پیوند داده ها** بر روی **لینک** صـــورت میگیرد و هم در **لایه انتقال** بر روی **میزبان های مبدا و مقصد** انجام میشود.

۲. امکان دارد اطلاعات مورد نیاز عملکردهای یک لایه فقط در لایه دیگرموجود باشد. مانند مقدار برچسب زمانی (Time Stamp)که این موضوع باعث نقض هدف استقلال لایه ها خواهد شد.

۳. نکته مهم در معماری لایه ای شبکه آن است که تعداد لایه ها باید در حداقل ممکن که پاسخ گوی تمام نیاز های شبکه است، قرار بگیرد. چون لایه بندی بیش از حد منجر به نقض اصل سادگیو اغلب باعث **افزایش پیچیدگی** خواهد شـــد .همچنین چون هر لایه برای انجام امور خود نیاز دارد تا به دیتای دریافتی از لایه قبلی هدر یا تریلر و یا هردو را اضـافه کند، در نتیجه هر چه تعداد لایه ها بیشـتر شـود، سـربار بیشـتری به سـیسـتم تحمیل می شـود . هم **سـربار مکانی** (چون فریم نهایی بزرگ می شود) و هم **سربار زمانی** (چون افزودن هدرها و انجام تغییرات در آنها زمان بر خواهد بود) و سربار بیشتر یعنی هزینه بیشتر.

سوال دوم

لایه شبکه[1] وظیفه مسیریابی را دارد و طبق معماری لایه‌ای نوع سرویس لایه پیوند تاثیری در وظیفه‌ی این لایه ندارد ولی برای سرویس بدون اتصال لایه شبکه هر موقع خواست می‌تواند بسته‌های انتقالی را به لایه پیوند بدهد؛ برای سرویس اتصال‌گرا قبل از ارسال بسته باید درخواست ایجاد ارتباط به لایه پیوند بدهد و بعد از آن بسته را منتقل کند.

[1] Network

سوال سوم

اگر بتوان به وسیله‌ی دیگری عملکرد لایه شبکه را انجام داد، دیگر احتیاج به این لایه نیست.

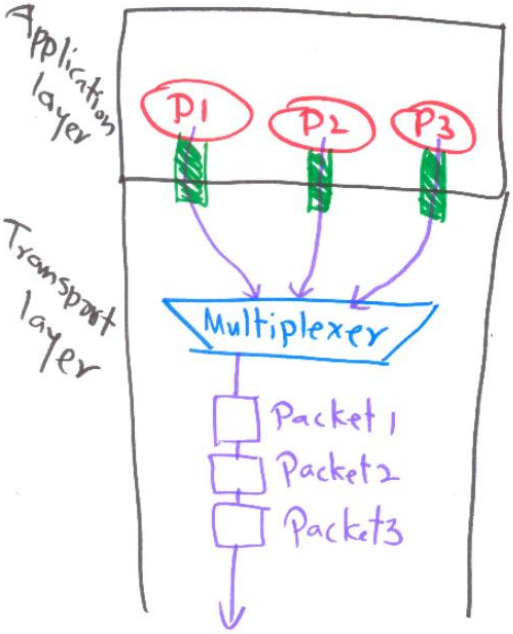
وظیفه‌ی لایه شبکه مسیریابی و جلوبری بسته‌هاست، در شبکه‌های همه‌پخشی همه گره‌ها به هم متصل‌اند، در صورت ارسال به همه گره‌ها ارسال می‌شود و به مسیریابی احتیاجی نیست، پس به لایه شبکه احتیاج نیست. (سوال چهار تمرین یک)

سوال چهارم

Multiplexing:

جمع آوری داده ها از چندین فرآیند کاربردی فرستنده ، پوشاندن آن داده ها با یک سرآیند و ارسال آنها به طور کلی برای گیرنده‌ی در نظر گرفته شده ، multiplexing **نام دارد.**

لایه انتقال:



UDP **و** TCP **کارهایی با** demultiplexing **و** multiplexing **را با دو فیلد ویژه در قسمتهای** segment **انجام می دهند: شماره پورت منبع و قسمت شماره پورت مقصد.**

و با توجه به شماره پورت بسته‌ها را به لایه شبکه ارسال می‌کنند و بعداً هم با همان شماره پورت بسته را در مقصد به برنامه مربوطه می‌دهد.

لایه شبکه:

آدرس مبدا و مقصد را به سرآیند بسته‌ها اضافه می‌کند و با استفاده از مسیریاب‌ها و استفاده از لینک‌های مشترک برای جابجایی بسته‌ها استفاده می‌کند.

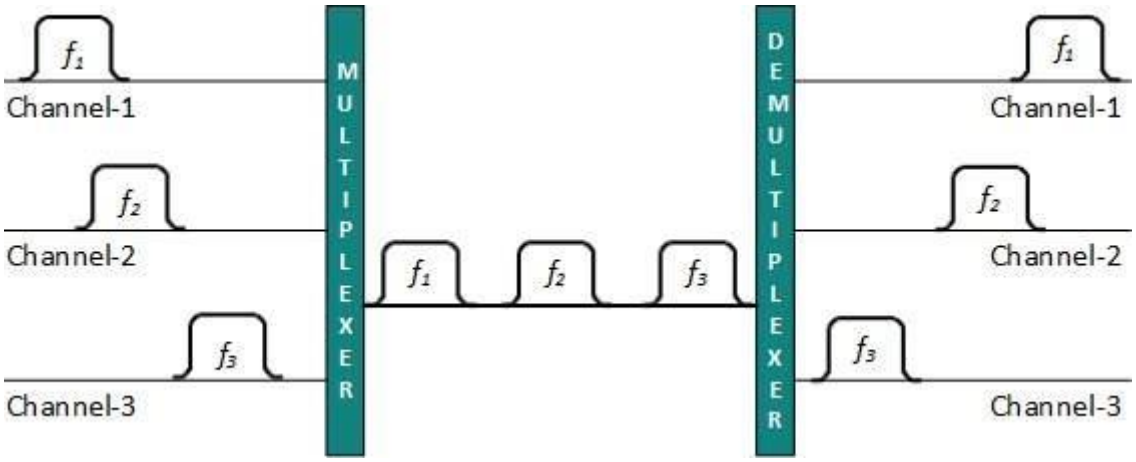
لایه داده:

زمانی که فرستنده‌ها تلاش می‌کنند چیزی را روی یک رسانه منفرد ارسال کنند، یک دستگاه به نام Multiplexer **کانال فیزیکی را تقسیم می‌کند و به هر یک، یک کانال اختصاص می‌دهد. در**

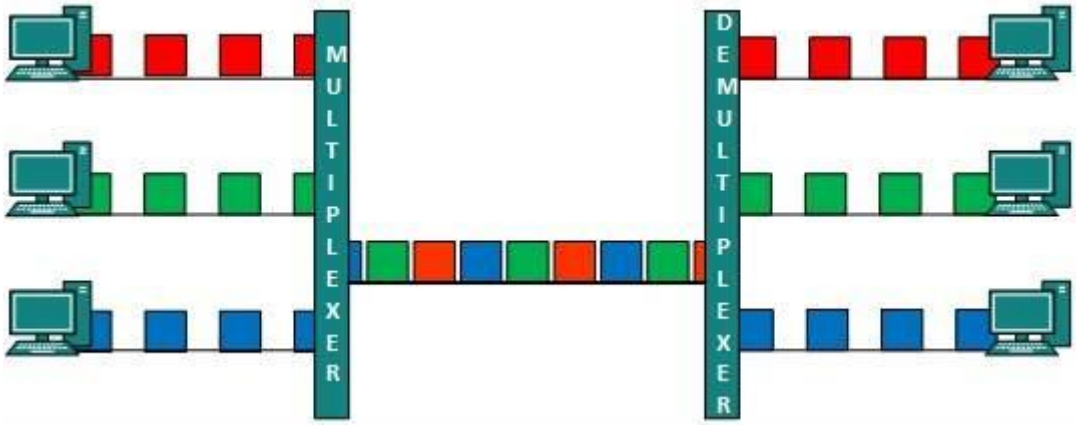
سوی دیگرِ ارتباط، یک دستگاه De-multiplexer **داده‌ها را از رسانه منفرد دریافت می‌کند و با جداسازی هر کدام آن‌ها را به گیرنده‌های مختلف ارسال می‌کند.**

انواع مالتی پلکسینگ به شرح زیر انجام می‌گیرد:

- **مالتی پلکسینگ تقسیم فرکانسی**FDM: Frequency Division Multiplexing

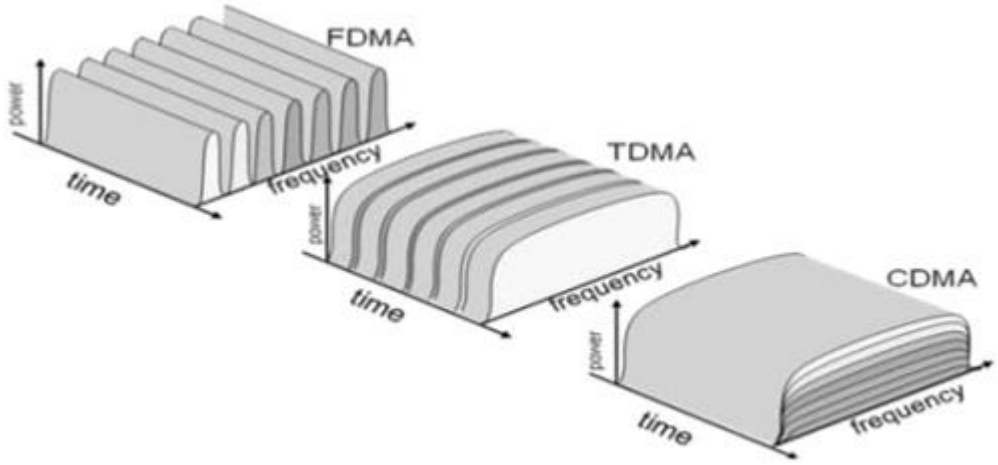


- **مالتی پلکسینگ تقسیم زمانی**TDM: Time Division Multiplexing



- **مالتی پلکسینگ تقسیم طول موج**WDM: Wave Length Division Multiplexing

- **مالتی پلکسینگ تقسیم کد**CDMA: Code Division Multiple Access



سوال پنجم

الف)

$$d_{\text{end to end}} = 2\left(\frac{L}{R} + t\right) = 1.04 \text{ msec.}$$

ب)

$$d_{\text{end to end}} = \frac{L}{R_1} + t_1 + \frac{L}{R_2} + t_2 + \frac{L}{R_3} + t_3 + \frac{L}{R_4} + t_4$$
$$= 4\left(\frac{5000}{10 \times 10^6}\right) + 4(10 \times 10^{-6}) = 2040 \times 10^{-6} = 2.04 \text{ msec.}$$

ج)

برای کل بیتها که تاخیر انتشار مانند قسمت الف است، ولی برای تاخیر انتقال، پس از ورود ۲۰۰ بیت، باقی بسته‌ها شروع به حرکت می‌کنند و چون لینک ورود و خروج دارای سرعت یکسان هستند باقی بیت ها فقط تاخیر خروج از مبدا را خواهند داشت:

$$d_{\text{end to end}} = 2\left(\frac{200}{10 \times 10^6} + 10 \times 10^{-6}\right) + \left(\frac{4800}{10 \times 10^6}\right) = 0.06 + 0.48 \text{ msec}$$
$$= 0.54 \text{ msec.}$$

سوال ششم

الف)

$$d_{\text{end to end}} = \frac{L}{R_1} + \frac{L}{R_2} + \frac{L}{R_3} + \frac{L}{R_4} + t_1 + t_2 + t_3 + t_4$$
$$= \frac{(1500 \times 8b)}{1 \times 10^6 bps} + 24 + 12 + 6 + 2 + 20 + 30 + 2 = 108 \text{ msec.}$$

ب)

$$d_{\text{end to end}} = t_{\text{perv part}} + (k-1) \times \max\left(\frac{L}{R_1}, \frac{L}{R_2}, \frac{L}{R_3}, \frac{L}{R_4}\right) = 108 + 2 \times 24$$
$$= 156 \text{ msec.}$$

ج) صف فقط در گره A تشکیل می‌شود، چون سرعت خروج اطلاعات از ورود به گره کمتر است. مدت زمان لازم برای وارد شدن یک بسته به گره برابر با ۱۲ میلی‌ثانیه است (از زمان انتشار صرف نظر کردم) و مدت زمان لازم برای خروج ۲۴ میلی‌ثانیه است، بسته دوم در زمان ۱۲ وارد می‌شود، به همین ترتیب بسته k ام در زمان $12 \times (k-1)$ وارد می‌شود، طول صف در زمان $12 \times (2k-1)$ برابر با k می‌شود یا به عبارتی در هنگام ورود بسته m طول صف برابر است با $\left\lfloor \frac{m}{2} \right\rfloor$. پس می‌توان فهمید اولین drop در ۱۲ امین بسته اتفاق می‌افتد و پس از آن یک در میان بسته‌ها drop می‌شوند (نرخ ورود به خروج ۲ است). پس ۵ بسته drop می‌شود و ۱۵ بسته به مقصد می‌رسد.

1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20

د) در این قسمت جهت برعکس است، ولی طبق قسمت قبل می‌توان فهمید که نصف داده‌ها از گره C رد می‌شود و نصف باقیمانده آن از B رد می‌شود (سرعت خروج نصف است)، پس ۷۵٪ داده‌ها از دست می‌روند.

$$\text{loss\_rate} = 1 - \frac{1Mbps}{2Mbps} \times \frac{0.5Mbps}{1Mbps} = \frac{3}{4} = 75\%.$$

سوال هفتم

DOS مخفف کلمه Denial of Service **به معنی ، جلوگیری از ارائه خدمات می‌باشد. ایجاد وقفه در دسترسی کاربران به سرور و سایت، یکی از دلایل اصلی این نوع حمله میباشد تا سرویس مد نظر از دسترس خارج گردد. حملات** DDOS **مشابه حملات** DOS **می‌باشد و هدف اصلی هکر ها در این نوع حملات نیز ایجاد وقفه در ارائه خدمات سرور مد نظر و یا ازسرویس خارج کردن آنها میباشد. در این نوع حملات هکر یا هکر ها به جای یک سرور، از چندین سرور یا کلاینت مبدا اقدام به حملات میکنند و با ایجاد ترافیک جعلی لود سرور و ترافیک آنها را بالا می‌برند تا سرویس از دسترس خارج گردد.**

انواع متدهای اتک

Smurf Attack: **این نوع حمله به پیکربندی نامناسب تجهیزات شبکه که اجازه ارسال بسته‌ها به همه کامپیوترهای میزبان روی یک شبکه خاص با آدرس‌های همه پخشی را می دهد، متکی است. در چنین حمله‌ای مهاجمان با یک آی پی جعلی یک تقاضای** ping **به یک یا چندین سرور همه پخشی ارسال کرده و آدرس آی پی ماشین هدف (قربانی) را ست می‌کنند .سرور همه پخشی این تقاضا را برای تمام شبکه ارسال می‌کند. تمام ماشین‌های شبکه پاسخ را به سرور، ارسال همه پخشی می‌کنند. سرور همه پخشی پاسخ‌های دریافتی را به ماشین هدف هدایت یا ارسال می‌کند. بدین صورت زمانی که ماشین حمله‌کننده تقاضائی را به چندین سرور روی شبکه‌های متفاوت همه پخشی می نماید، مجموعه پاسخ‌های تمامی کامپیوترهای شبکه‌های گوناگون به ماشین هدف ارسال می گردند و آن را از کار می اندازند. بنابراین پهنای باند شبکه به سرعت استفاده می‌شود و از انتقال بسته‌های مجاز به مقصدشان جلوگیری به عمل خواهد آمد.**

برای مبارزه با حمله منع سرویس در اینترنت سرویس‌هایی مانند Smurf Amplifier Registry **توانایی تشخیص پیکربندی‌های نامناسب شبکه وانجام عملیات مناسب مثل فیلترینگ را می‌دهند.**

همچنین میتوانید از سیستم هایی نظیر Cloudflareو استفاده از پروکسی های چندگانه که وب سرور و سایر سرویس ها از طریق پروکسی های تو در تو آماده سرویس دهی میباشند نیز استفاده کنید.

SYN Flood: **هر جلسه TCP نیاز به برقراری ارتباط سه جانبه بین دو سیستم دارد. با استفاده از یک سیلSYN ، مهاجم به سرعت به هدف با درخواست های اتصال بسیاری می پردازد که نمی تواند آن را حفظ کند و منجر به اشباع شبکه شود. در واقع زمانی اتفاق می افتد که میزبانی از بسته‌های سیل آسای TCP/SYN استفاده کند که آدرس فرستنده آن‌ها جعلی است. هر کدام از این بسته‌ها همانند یک درخواست اتصال بوده و باعث می‌شود سرور درگیر اتصالات متعدد نیمه باز بماند و با فرستادن یا برگرداندن بسته‌هایTCP/SYN ACK ، منتظر بسته‌های پاسخ از آدرس فرستنده بماند ولی چون آدرس فرستنده جعلی است هیچ پاسخی برگردانده نمی‌شود. این اتصالات نیمه باز تعداد اتصالات در دسترس سرور را اشباع می‌کنند و آن را از پاسخگویی به درخواست‌های مجاز تا پایان حمله بازمیدارد. بنابر این منابع سرور به اتصال‌های های نیمه باز اختصاص خواهد یافت. وامکان پاسخ گویی به درخواستها از سرور منع می‌شود.**

برای جلوگیری می‌توان در مکانیزم اختصاص منابع به کاربران(پروتکل) تغییر ایجاد کرد و یا از فیلترینگ با Firewall ها استفاده کرد.

سوال هشتم

متوسط اندازه بسته‌ها برابر است با:

$$\bar{L} = \frac{20}{100}(1000) + \frac{50}{100}(1500) + \frac{30}{100}(1200)B = 1310B = 10480b$$

نرخ ورود بسته‌ها برابر است با:

$$\lambda = 150\frac{\text{packets}}{\text{sec}}$$

نرخ سرویس‌دهی برابر است با:

$$\mu = \frac{R}{\bar{L}}$$

میانگین تاخیر به ازای هر بسته:

$$T = \frac{1}{\mu - \lambda} \rightarrow T < 1$$

$$\lambda < \mu \rightarrow \frac{R}{10480} > 150 \rightarrow R > 1.572 \text{ Mbps.}$$

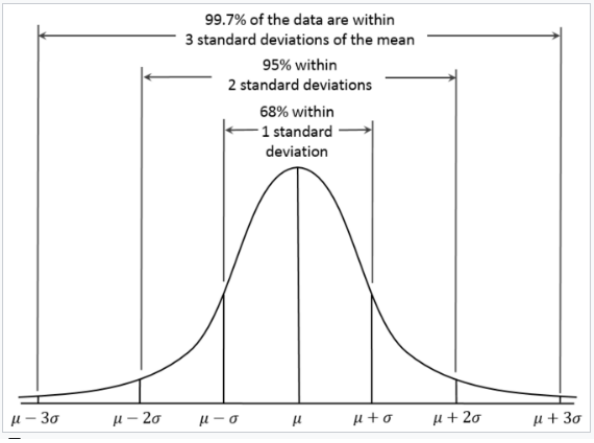
سوال نهم

الف)

$$\text{circuit switch} = \frac{2.2Mbps}{100Kbps} = 22$$

$$\text{packet switching} \rightarrow \mu = E[X] = n \times 0.2,$$

$$Var[X] = n \times 0.2 \times 0.8 = \sigma^2 \rightarrow \sigma = 0.4\sqrt{n}$$



طبق توزیع نرمال می‌دانیم که در صورت وجود n کاربر در شبکه به طور متوسط μ کاربر با انحراف‌معیار σ همزمان از این سیستم استفاده می‌کنند، طبق قانون ۶۸-۹۵-۹۹.۷ می‌دانیم برای اینکه تعداد کاربران همزمان از ۲۲ به ندرت تجاوز کند (طبق همان قانون در ۹۹.۷ هر یک سال یک بار به طور متوسط اتفاق می‌افتد) باید عبارت زیر برقرار باشد:

$$\mu + 3\sigma \leq 22 \rightarrow n \leq 62.5 \rightarrow n = 62$$

پس تعداد کاربران برابر با ۶۲ می‌شود.

ب) روش circuit برای زمان‌هایی توصیه می‌شود که کاربران به صورت طولانی مدت و به طور مکرر از پهنای باند استفاده کنند یا در مواردی مثل تلفن که به تاخیر حساس است.

روش packets در مواقعی استفاده می‌شود که شرایط قبلی برقرار نباشد (غیرمکرر، غیر حساس به تاخیر و ...)

سوال دهم

تعداد بسته‌های ارسالی هر کاربر: k

متوسط ارسالی هر کاربر: $1500 \times 8 \times k$

متوسط ارسالی هر کاربر باید از ظرفیت خطوط متصل به سوییچ کمتر باشد:

$$12000k < 10 \times 10^6 bps \rightarrow k < 0.8\overline{3} \times 10^3$$

متوسط ارسال کاربران باید از مقدار ظرفیت سوییچ باید کمتر باشد:

$$120000k < 80 \times 10^6 bps \rightarrow k < 6.\overline{66} \times 10^2$$

متوسط ارسال کاربران باید از مقدار مسیر مسیریاب تا شبکه کمتر باشد:

$$120000k < 40 \times 10^6 bps \rightarrow 3.\overline{33} \times 10^2$$

سوال یازدهم

به اشتراک‌گذاری در شبکه توجه کنید، فناوری‌ای که به کاربران اجازه می‌دهد فایل‌ها و فولدرها را از طریق شبکه به اشتراک بگذارند. پیش از این اشتراک گذاری فایل و فولدر در شبکه یک هدفِ محبوب برایWorm های کامپیوتری محسوب می‌شدند، اما در سال‌های اخیر از محبوبیت آن‌ها کاسته شده و برعکس حملات به ایمیل‌ها و وب‌سایت‌ها و نفوذ به آن‌ها افزایش یافته است. تا اینکه ۱۹ ماه پیش WannaCryمسیر چشم انداز تهدیدات را تغییر داد و مجددا توجه‌ها دوباره به سوی اشتراک‌گذاری شبکه‌ای و به خصوص پروتکل Server Message Block (این سرویس در واقع یک پروتکل است که اجازه به اشتراک گذاری فایل، پرینتر، پورتهای سریال بین نودهای یک شبکه را میدهد) یا SMB که برای بسیاری از زیرساخت‌ها حیاتی می‌باشد، کشیده شد.

در گذشته، SMB یکی از محبوب‌ترین پروتکل‌ها برای تسهیل این نوع اشتراک‌گذاری‌ها بوده است. بیشتر محبوبیت آن را می‌توان به دلیل بکارگیری، پیاده‌سازی و سرمایه‌گذاری مایکروسافت بر روی این پروتکل که از دهه‌ی ۹۰ میلادی آغاز شد، نسبت داد که در آن راه‌اندازی، پیکربندی و استفاده از SMB در ویندوز آسان بود و برای اهداف مختلفی استفاده می‌شد.

بدون شک پروتکل SMB به دایر کردن بسیاری از شبکه‌های داخلی کمک شایانی کرده است؛ با این حال، این سهولت در استفاده، عواقب بدی را نیز به همراه داشت. این پروتکل نیاز به احراز هویت و رمزگذاری بسـ یاری کمی داشت. امنیت آن در نسخه‌های بعد بهبود یافت اما به لطف سازگاری با نسخه‌های قدیمی، نسخه‌های ناامن منسوخ شده هنوز هم کار می‌کردند و استفاده می‌شدند.

ظهور EternalBlue

آسیب‌پذیری‌ها، Wormها و SMB همه در سال ۲۰۱۷ به یک نقطه فاجعه آمیز رسیدند. یک نقص بزرگ در SMB نسخه ۱ (SMB1) کشف شد و EternalBlue نام‌گذاری شد. این Exploit یک عامل مخرب را قادر می‌ساخت که نرم‌افزارهای مخرب را بر روی هر کامپیوتری که در حال اجرای SMB1 بود نصب کند.

EternalBlue به وسیله گروه هکری Shadow Brokers به عموم عرضه شد. همانطور که شدت این آسیب‌پذیری آشکار گشت، مایکروسافت یک Out-of-Band Patch برای این آسیب‌پذیری به نام MS17-010 را برای تمام نسخه‌های پشتیبانی شده‌ی ویندوز منتشر نمود.

اجرای WannaCry

WannaCry با استفاده از آسیب‌پذیری EternalBlue، به سرعت در کامپیوترهای آسیب‌پذیر پخش شد. در صورت فعال بودن SMB1، WannaCry می‌توانست بدون هرگونه عملی از سوی کاربر از این آسیب‌پذیری سوءاستفاده کرده، Payload باج‌افزار خود را نصب کرده و به دنبال کامپیوترهای بیشتری که SMB1 در آن‌ها فعال است بگردد و آن‌ها را نیز آلوده کند.

WannaCryحملات خود را با رمزگذاری تمامی فایل‌های موجود در PC آلوده صورت می‌دهد و هر سیستم دیگری که از طریق شبکه به آن متصل باشد را نیز درگیر می‌کند؛ سپس در ازای تحویل فایل‌ها درخواست مبلغی به میزان ۳۰۰ تا ۶۰۰ دلار می‌نماید که در صورت عدم پرداخت این مبلغ در یک مدت زمان مشخص، تهدید به حذف فایل‌های رمزشده می‌گردد.

WannaCry موفق به ایجاد مشکلات جدی در سازمان‌های دولتی و صنایع، سازمان‌های مراقبت‌های بهداشتی بزرگ، شرکت‌های خودروسازی، مخابرات و سازمان‌های حمل و نقل در سراسر جهان شد. در یک حرکت بی‌سابقه مایکروسافت حتی یک Patch برای نسخه‌های منسوخ شده‌ی ویندوز از جمله ویندوز XP نیز منتشر کرد.

مقابله با حملات مربوط به SMB

بهترین راه امن بودن در مقابل حملات مربوط به SMB، استفاده نکردن از این پروتکل می‌باشد. دلایلی بسیار معدودی برای استفاده از این پروتکل وجود دارند. در واقع، از آوریل ۲۰۱۸، این پروتکل دیگر در ویندوز به صورت پیش فرض نصب نشده است. به جای به اشتراک گذاری فایل‌ها با اتصال کامپیوترها از طریق SMB، از یک سرور فایل اختصاصی یا یک راهکار مبتنی بر Cloud بایداستفاده کرد. همچنین پرینترهای شبکه‌ای را باید به نحوی تنظیم کرد که از پروتکل‌های دیگر استفاده کنند. اگر نمی‌توانید SMB را در محیط خود خاموش کنید، حداقل مطمئن شوید که SMB1 غیرفعال است. برای اطمینان از اینکه ارتباطات SMB محدود به شبکه داخلی می‌باشد، پورت‌های TCP 445 و ۱۳۹ را در فایروال‌های شبکه Block کنید و نکته‌ی دیگر این است که کلاینت‌ها نباید بتوانند با یکدیگر از طریق SMB ارتباط برقرار کنند.

سوال دوازدهم

لایه انتقال ارتباط بین فرآیندهاست و لایه شبکه ارتباط بین میزبانان.

مرتب‌سازی بایتی **یا** Byte Orientation **: به جای اینکه برنامه کاربردی پیام‌های دریافت شده از سیستم ارتباطی را بر اساس فرمتی نامشخص پردازش کند، اغلب** جریان داده **را به صورت ترتیبی از** بایت‌ها **می خواند که این کار به مراتب آسان تر خواهد بود. این ساده‌سازی به برنامه کاربردی امکان می دهد که بتواند با فرمت‌های مختلفی از پیام‌ها کار کند.**

تحویل با ترتیب یکسان : لایه شبکه **معمولاً قادر به تضمین این مسئله نیست که داده‌های بسته‌های دریافت شده دقیقاً همان ترتیبی را دارند که از سیستم ارسال‌کننده فرستاده شده‌اند. وظیفه مرتب‌سازی بسته معمولاً در لایه انتقال صورت می پذیرد.**

قابلیت اطمینان : **به دلیل خطاها و تراکم‌های شبکه‌ای احتمال اینکه بسته‌های اطلاعاتی از بین بروند وجود دارد. با استفاده از تکنیک‌های** کد شناسایی خطا **از قبیل** مجموع مقابله‌ای **یا** checksum**، پروتکل انتقال بررسی می‌کند که آیا داده‌ها سالم هستند یا خیر. این پروتکل نتیجه بررسی خود را بوسیله ارسال کند** ACK **(به معنای صحت داده ها) و** NACK **(به معنای خرابی داده ها) به فرستنده اعلام می‌کند. ممکن است طرح‌های** درخواست تکرار خودکار **برای ارسال دوباره اطلاعات آسیب دیده یا از بین رفته مورد استفاده قرار گیرد.**

کنترل جریان **یا** : Flow Control **بعضی اوقات نرخ انتقال اطلاعات بین دو نود بایستی مدیریت شود تا از ارسال سریع تر فرستنده نسبت به گیرنده اطلاعات که می‌تواند منجر به سرریز** بافر **داده‌ای گیرنده شود جلوگیری به عمل آید.**

پیشگیری از تراکم **یا** : Congestion Avoidance کنترل تراکم **می‌تواند ترافیک وارد شده به شبکه مخابراتی را مدیریت کرده و با اعمال ممنوعیت ورود هر نوع امکان ارتباطی یا پردازشی از سوی نودهای شبکه تصادم یا تراکم را کاهش دهد.**

تسهیم یا مالتی پلکسینگ : (Multiplexing) پورتها **می‌تواند چندین مقصد پایانی را بر روی یک نود فراهم آورد. برای مثال، نام موجود در آدرس پستی می‌تواند نمایانگر نوعی از تسهیم و تفکیک بین چندین گیرنده در یک محل باشد. برنامه‌های کاربردی بر روی پورت‌های مخصوص به خودشان به اطلاعات گوش می دهند که این کار این امکان را فراهم می‌آورد که از چندین** سرویس شبکه **به صورت هم‌زمان استفاده کنیم. این سرویس بخشی از لایه انتقال در مدل** TCP/IP **است، اما در مدل** OSI **این سرویس بخشی از** لایه نشست **می‌باشد.**

لایه "اینترنت"، مسئول آدرس دهی ، بسته بندی و روتینگ داده ها ، است. لایه فوق ، شامل چهار پروتکل اساسی است :

- Internet Protocol(IP) **. پروتکل فوق ، مسئول آدرسی داده ها بمنظور ارسال به مقصد مورد نظر است .**
- Address Resoulation Protocol(ARP) **. پروتکل فوق ، مسئول مشخص نمودن آدرس** Media Access Control(MAC) **آداپتور شبکه بر روی کامپیوتر مقصد است.**
- Internet Control Message Protocol(ICMP) **. پروتکل فوق ، مسئول ارائه توابع عیب یابی و گزارش خطاء در صورت عدم توزیع صحیح اطلاعات است .**
- Internet Group Managemant Protocol IGMP) **. پروتکل فوق ، مسئول مدیریت** Multicasting **در** TCP/IP **را برعهده دارد.**