تمرین کامپیوتری شماره 3

محمد سعید غفاری 810197635

2.3) سوالات:

**پاسخ اول:**

قسمت اول:

پروتکل TCP (پروتکل کنترل انتقال) و UDP (پروتکل دیتاگرام کاربر) دو پروتکل پرکاربرد برای انتقال داده ها از طریق شبکه هستند. تفاوت اصلی بین این دو در **نحوه انتقال** داده است:

TCP یک پروتکل اتصال گرا است که تحویل داده ها را قابل اطمینان، سفارش داده شده و خطا را بررسی می کند. قبل از انتقال داده، یک ارتباط امن بین دو دستگاه برقرار می کند و اطمینان می دهد که تمام داده ها به درستی در انتهای دیگر دریافت می شوند.

از سوی دیگر، UDP یک پروتکل بدون اتصال است که تحویل مطمئن داده ها را تضمین نمی کند. اتصال ایمن ایجاد نمی کند و خطاها را بررسی نمی کند. در عوض، به سادگی بسته های داده را برای گیرنده ارسال می کند، که مسئول بررسی یکپارچگی آنها است. این باعث می‌شود UDP سریع‌تر و کارآمدتر از TCP باشد، اما نسبت به UDP قابل اطمینان‌ نیست.

به طور خلاصه، تفاوت های اصلی بین TCP و UDP در قابلیت اطمینان، ترتیب داده ها، بررسی خطا و سرعت است.

قسمت دوم:

TCP (پروتکل کنترل انتقال) و UDP (پروتکل دیتاگرام کاربر) بسته به نیاز برنامه برای اهداف متفاوتی استفاده می شوند. در اینجا چند مورد استفاده رایج برای هر پروتکل آورده شده است:

TCP:

Web browsing (HTTP، HTTPS)

انتقال فایل (FTP)

ایمیل (SMTP، POP، IMAP)

Remote desktop (RDP)

Secure shell (SSH)

UDP:

Streaming media (به عنوان مثال، ویدئو، صدا)

بازی های آنلاین

جستجوهای DNS (DNS lookups)

اتصالات شبکه خصوصی مجازی (VPN).

صدا از طریق IP (VoIP)

به طور کلی، TCP زمانی ترجیح داده می‌شود که داده‌های در حال انتقال مهم هستند و باید به طور قابل اعتماد و با ترتیب صحیح تحویل داده شوند، در حالی که UDP برای برنامه‌هایی که نیاز به سرعت و تأخیر کم دارند و می‌توانند مقداری از دست دادن داده را تحمل کنند، ترجیح داده می‌شود.

**پاسخ دوم:**

Go-Back-N و Selective Repeat دو روش کنترل خطا هستند که در انتقال داده های قابل اعتماد استفاده می شوند. در اینجا به مزایا و معایب هر کدام می پردازیم:

Go-Back-N:

مزایای:

پیاده سازی ساده و پیچیده تر از تکرار انتخابی.

به حافظه کمتری برای ذخیره بسته های خارج از ترتیب نیاز دارد.

گیرنده فقط باید شماره توالی مورد انتظار را پیگیری کند و پیاده سازی آن را آسان تر می کند.

معایب:

استفاده ناکارآمد از منابع شبکه، زیرا فرستنده باید به طور مداوم تمام بسته های تایید نشده را ارسال کند تا زمانی که یک تاییدیه برای قدیمی ترین بسته تایید نشده دریافت کند.

تاخیر زیاد در صورت گم شدن بسته های متعدد، زیرا همه بسته های تایید نشده باید دوباره ارسال شوند.

Selective repeat:

مزایای:

استفاده کارآمدتر از منابع شبکه، زیرا فقط بسته های از دست رفته یا آسیب دیده دوباره ارسال می شوند.

تاخیر کمتر در مقایسه با Go-Back-N، زیرا گیرنده می تواند بلافاصله درخواست ارسال مجدد بسته های گم شده یا آسیب دیده را بدهد.

معایب:

پیاده سازی پیچیده تر است، زیرا گیرنده باید تمام بسته های دریافتی و شماره ترتیب آنها را پیگیری کند.

برای ذخیره بسته های دریافتی به حافظه بیشتری نیاز دارد.

به طور خلاصه، Go-Back-N روش ساده‌تری است که به حافظه کمتری نیاز دارد و پیاده‌سازی آن آسان‌تر است، اما از نظر استفاده از شبکه کارایی کمتری دارد و می‌تواند منجر به تاخیرهای بیشتر شود. تکرار انتخابی پیچیده تر است، اما از نظر استفاده از شبکه کارآمدتر است و منجر به تاخیر کمتر می شود.

نحوه پیاده سازی:

Go-Back-N:

در Go-Back-N، فرستنده یک پنجره کشویی (sliding window) با حداکثر اندازه "N" نگه می دارد و یک متغیر برای پیگیری شماره دنباله بعدی که قرار است ارسال شود، نگه می دارد. فرستنده به طور مداوم تمام بسته های موجود در پنجره را ارسال می کند تا زمانی که یک تأییدیه از گیرنده برای قدیمی ترین بسته موجود در پنجره دریافت کند. اگر بسته ای گم شود یا آسیب ببیند، گیرنده برای آن بسته تأییدیه ای ارسال نمی کند. فرستنده به ارسال مجدد همه بسته های تایید نشده ادامه می دهد تا زمانی که تأییدیه قدیمی ترین بسته را در پنجره دریافت کند.

مثال:

فرض کنید حداکثر اندازه پنجره 4 است و فرستنده داده هایی برای ارسال با اعداد دنباله ای 0، 1، 2، 3، 4، 5، 6، 7 دارد. فرستنده ابتدا بسته های 0، 1، 2 و 3 را ارسال می کند و منتظر می ماند تا یک تصدیق اگر تأیید بسته 2 از بین برود، گیرنده برای هیچ یک از بسته ها تأییدیه ارسال نمی کند و فرستنده به ارسال مجدد همه بسته های تأیید نشده (یعنی بسته های 0، 1، 2، 3) ادامه می دهد تا زمانی که یک تأییدیه برای بسته دریافت کند. .

تکرار انتخابی:

در تکرار انتخابی، فرستنده همچنین یک پنجره کشویی با حداکثر اندازه "N" نگه می دارد، اما فقط بسته های گم شده یا آسیب دیده را مجددا ارسال می کند، به جای اینکه همه بسته های تایید نشده مانند Go-Back-N را مجددا ارسال کند. گیرنده تمام بسته های دریافتی و شماره ترتیب آنها را پیگیری می کند و بلافاصله درخواست ارسال مجدد بسته های گم شده یا آسیب دیده را ارسال می کند.

مثال:

فرض کنید حداکثر اندازه پنجره 4 است و فرستنده داده هایی برای ارسال با اعداد دنباله ای 0، 1، 2، 3، 4، 5، 6، 7 دارد. فرستنده ابتدا بسته های 0، 1، 2، 3 را ارسال می کند و منتظر می ماند تا تصدیق. اگر تأیید بسته 2 از بین برود، گیرنده درخواستی برای ارسال مجدد بسته 2 ارسال می کند. فرستنده بسته 2 را مجددا ارسال می کند و به ارسال بسته های باقی مانده ادامه می دهد. گیرنده به پیگیری همه بسته های دریافتی و شماره ترتیب آنها ادامه می دهد و بلافاصله درخواست ارسال مجدد بسته های گم شده یا آسیب دیده را خواهد داد.

به طور کلی، تکرار انتخابی منجر به استفاده کارآمدتر از منابع شبکه و تاخیر کمتر در مقایسه با Go-Back-N می شود، اما پیاده سازی آن پیچیده تر است.

**بخش دوم :**

**پرسش اول:**

چندین راه برای به روز رسانی جداول مسیریابی در شبکه وجود دارد:

مسیریابی استاتیک: مدیر شبکه به صورت دستی جدول مسیریابی را با افزودن، حذف یا تغییر مسیرها پیکربندی می کند.

مسیریابی پویا: جدول مسیریابی به طور خودکار توسط پروتکل های مسیریابی مانند OSPF، BGP یا EIGRP به روز می شود. این پروتکل ها اطلاعات مسیریابی را با دیگر روترهای شبکه مبادله می کنند و جدول مسیریابی را بر این اساس به روز می کنند.

پروتکل اطلاعات مسیریابی (RIP): این یک پروتکل مسیریابی بردار فاصله است که اطلاعات مسیریابی را بین روترها مبادله می کند. جدول مسیریابی بر اساس اطلاعات دریافتی از روترهای دیگر به روز می شود.

Open Shortest Path First (OSPF): این یک پروتکل مسیریابی حالت پیوند است که اطلاعات دقیق در مورد توپولوژی شبکه را با روترهای دیگر مبادله می کند. از این اطلاعات برای محاسبه کوتاه ترین مسیر به مقصد و به روز رسانی جدول مسیریابی بر این اساس استفاده می کند.

پروتکل دروازه مرزی (BGP): این پروتکل برای تبادل اطلاعات مسیریابی بین روترها در سیستم‌های مستقل مختلف (ASes) استفاده می‌شود و معمولاً در شبکه‌های بزرگ سازمانی یا ارائه‌دهندگان خدمات اینترنتی (ISP) استفاده می‌شود.

پروتکل مسیریابی دروازه داخلی پیشرفته (EIGRP): این یک پروتکل مسیریابی ترکیبی است که از تکنیک های فاصله-بردار و حالت پیوند برای تبادل اطلاعات مسیریابی و به روز رسانی جدول مسیریابی استفاده می کند.

بهترین پروتکل مسیریابی به الزامات و محدودیت های خاص شبکه بستگی دارد.

مسیریابی استاتیک: پیکربندی آن ساده است و برای شبکه های کوچک با تغییرات دینامیکی کم یا بدون تغییرات ایده آل است.

مسیریابی پویا: مقیاس پذیرتر است و می تواند به طور خودکار با تغییرات شبکه سازگار شود.

OSPF: برای شبکه های سازمانی بزرگ که به زمان همگرایی سریع نیاز دارند، کارآمد و مناسب است.

BGP: برای ارائه دهندگان خدمات اینترنتی بزرگ (ISP) یا محیط های سیستمی چندگانه که نیاز به تبادل اطلاعات مسیریابی بین AS های مختلف دارند، ایده آل است.

EIGRP: این یک پروتکل انعطاف پذیر است که می تواند در محیط های مختلف شبکه استفاده شود و زمان همگرایی سریع را فراهم می کند.

در نهایت، بهترین پروتکل مسیریابی به عواملی مانند اندازه شبکه، پیچیدگی، مقیاس پذیری و نوع ترافیکی که مسیریابی می شود بستگی دارد.

**پرسش دوم:**

مسیریابی برداری فاصله - Distance Vector Routing

این یک الگوریتم مسیریابی پویا است که در آن هر روتر فاصله ای را بین خود و هر مقصد ممکن یعنی همسایگان نزدیک خود محاسبه می کند.

روتر دانش خود را در مورد کل شبکه با همسایگان خود به اشتراک می گذارد و بر این اساس جدول را بر اساس همسایگان خود به روز می کند.

به اشتراک گذاری اطلاعات با همسایگان در فواصل زمانی معین صورت می گیرد.

برای ساخت جداول مسیریابی از الگوریتم بلمن-فورد استفاده می کند.

مشکلات :

- شمارش تا بی نهایت مسئله که با تقسیم افق قابل حل است.

- اخبار خوب به سرعت پخش می شود و اخبار بد به آرامی پخش می شوند.

- مشکل حلقه دائمی یعنی حلقه برای همیشه وجود خواهد داشت.

مسیریابی وضعیت پیوند – Link state routing

این یک الگوریتم مسیریابی پویا است که در آن هر روتر دانش همسایگان خود را با هر روتر دیگری در شبکه به اشتراک می گذارد.

یک روتر اطلاعات خود را در مورد همسایگان خود فقط برای همه روترها از طریق flooding ارسال می کند.

به اشتراک گذاری اطلاعات تنها زمانی انجام می شود که تغییری ایجاد شود.

از الگوریتم Dijkstra برای ساخت جداول مسیریابی استفاده می کند.

مشکلات - ترافیک سنگین به دلیل سیل بسته ها.

- سیل می تواند منجر به حلقه بی نهایت شود که با استفاده از فیلد Time to live (TTL) قابل حل است.

**بخش سوم:**

Random Early Detection (RED) و Explicit Congestion Notification (ECN) دو الگوریتمی هستند که برای مدیریت ازدحام شبکه در شبکه های کامپیوتری استفاده می شوند.

RED با رها کردن تصادفی بسته ها قبل از پر شدن صف عمل می کند تا احتمال سرریز بافر را کاهش دهد. از سوی دیگر، ECN به روترها اجازه می‌دهد تا بسته‌های دریافتی را به‌جای رها کردن بسته‌های دریافتی، با کدی علامت‌گذاری کنند که تراکم را نشان دهد. سپس گیرنده پایانی می تواند به بسته های علامت گذاری شده واکنش نشان دهد و سرعت فرستنده را کاهش دهد.

انتخاب الگوریتم مورد استفاده به نیازهای خاص شبکه و نوع ترافیک منتقل شده بستگی دارد. به طور کلی، ECN نسبت به RED کارآمدتر و کم نفوذتر دیده می شود، زیرا از افت غیر ضروری بسته جلوگیری می کند و بازخورد ازدحام سریع تری را برای فرستنده فراهم می کند. با این حال، ECN نیاز به پشتیبانی از هر دو مسیریاب و سیستم های پایانی دارد و برخی از سیستم های قدیمی ممکن است از آن پشتیبانی نکنند.