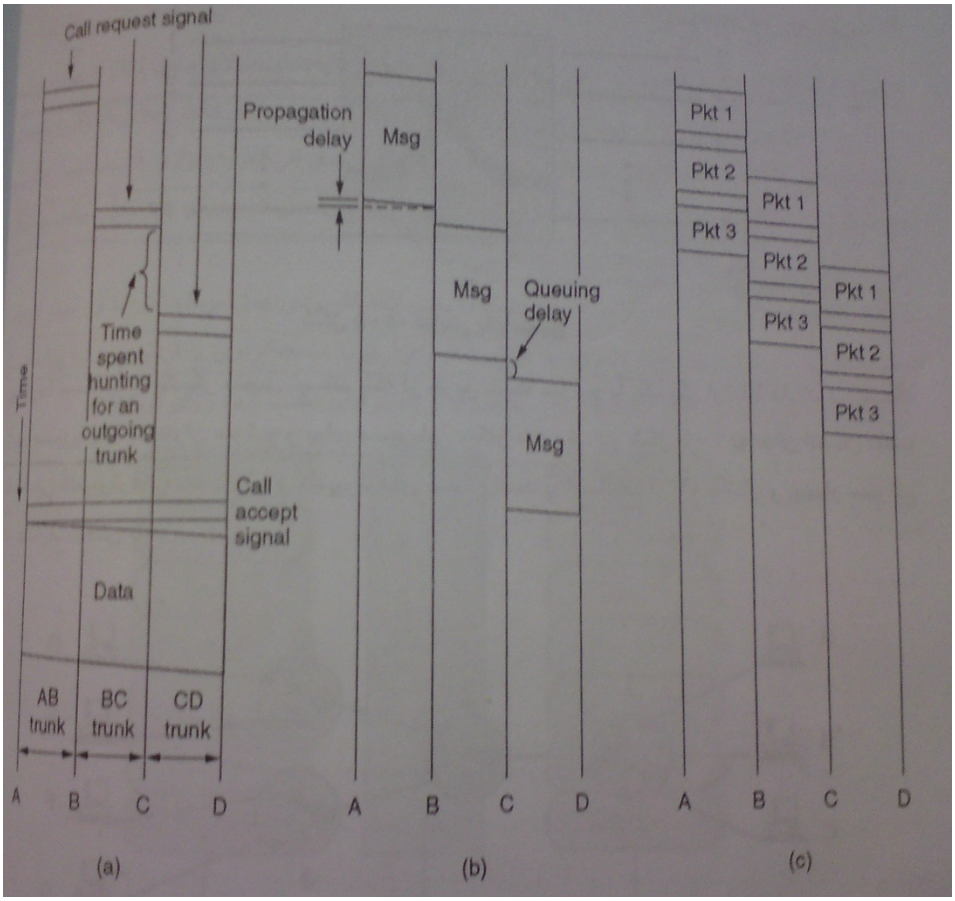
۱.

سوئیچینگ مداری: در ایجاد یک مدار اختصاصی و مسیر فیزیکی واقعی بین دستگاه های فرستنده و گیرنده از روش سوئیچینگ مداری در لایه فیزیکی استفاده می شود. این مدار فقط مختص فرستنده و گیرنده است و دیگر کامپیوتر ها نمی توانند از این مدار استفاده کنندو برای برقراری مدار و اتصال اولیه بین فرستنده و گیرنده زمانی صرف می شود. در این نوع شبکه ها داده به صورت stream منتقل می شود و نیاز به بسته بندی (packeting) و قرار دادن آدرس مبدا و مقصد برای پیام در حال ارسال و در مدار فیزیکی اختصاصی بین دو کامپیوتر نمی باشد. Circuit Switching دارای سه مرحله برقراری ارتباط بین فرستنده و گیرنده، مرحله انتقال داده و مرحله قطع ارتباط می باشد. انتقال صدا در تلفن در PSTN(Public Switch Telephone Network) بدین صورت است.

سوئیچینگ بسته ای: داده به بسته هایی تقسیم می شود و بسته ها توسط بلوک هایی با طول متفاوت اما محدود (packet) به صورت واحدهایی گسسته در کانال انتقال می یابند که حداکثر طول بسته ها توسط شبکه تعیین می شود. بسته ها در شبکه از یک سوئیچ به سوئیچ دیگر منتقل می شوند و در هر سوئیچ ابتدا ذخیره می شوند و سپس با بررسی هدر آن که آدرس مقصد در آن نوشته شده است و جداول مسیریابی به سمت مقصد هدایت می شوند. چون اول ذخیره می کنند و بعد با توجه به هدر آن را هدایت می کنند گاهی اوقات به آن Store & Forward گویند.

Packet Switching خود به دو صورت است Virtual Circuit و Datagram که در مدار مجازی ابتدا مسیر رزرو شده و بسته ها برچسب گذاری می شوند و همه ی بسته ها از یک مسیر می روند (از این جهت به این روش مدار مجازی گویند که مانند روش مداری قبل از ارسال داده مدار را ایجاد می کند و همه داده ها از یک مسیر می روند اما دیگر فرستنده ها نیز می توانند از این مسیر استفاده کنند در صورتی که در Circuit Switching مسیر رزرو شده و فقط مختص یک فرستنده است) ولی در data Gram هر بسته دارای آدرس مبدا و مقصد است و به طور جداگانه توسط لایه شبکه مسیر یابی می شوند.

شکل زیر نشان دهنده سه روش switching می باشد:



Circuit Switching (A Message Switching (B Packet Switching (C

مزایای Circuit Switching: ظرفیت اختصاصی داده شده تا آخر ارتباط تضمین می شود و کیفیت خوب و ثابتی داریم.

هیچ پردازشی در گره ها صورت نمی گیرد بنابراین تاخیر بسیار اندک است.

عیب آن هم این است که اگر کانال اشغال شود دیگران نمی توانند از آن استفاده کنند (مثلا برای ارسال پیغام ضروری و فوری ممکن است مدار خالی برای رزرو وجود نداشته باشد) و اینکه برای گرفتن مدار و رزرو آن زمان به هدر می رود.

مزایای Packet Switching: از منابع به بهترین نحو استفاده می شود. همزمان سازی ارسال و دریافت بسته ها توسط سوئیچ ها باعث کاهش تاخیر می شود اما همچنان تاخیر آن از Circuit Switching بیشتر است.

عیب آن نیز ممکن است نتوان کیفیت سرویس را تضمین نمود (به علت گر بودن بافر ها و یا ازدحام و ...) همچنین تاخیر صف بندی و تاخیر پردازش در این روش وجود دارد. در داده گرام ممکن ترتیب دریافت بسته ها توسط گیرنده حفظ نشود.

مزیت اصلی Packet Switching نسبت به Circuit Switching این است که فرستنده های مختلف به طور همزمان می توانند از یک کانال استفاده نمایند.

به طور کلی packet switching مدار اختصاصی ندارد، نیاز به برقراری ارتباط ندارد و Circuit Switching جدول مسیریابی ندارد، تاخیرش کمتر است.

۲.

حالت اول: در این روش حتی اگر داده ها در شبکه به دلایل مختلف (ازدحام، پر بودن بافر، Timeout و ...) از بین بروند منابع هنوز در این ارتباط وجود دارد و از بین نمی رود پس می تواند از منابع حداکثر استفاده را برد بدون آن که محدودیت زمانی و خطا بر روی آن تاثیری بگذارد.

یکی از معایب این روش این است که اگر داده ای برای مدت طولانی ارسال نشود منابع همچنان درگیر هستند و هدر می روند و همچنین اگر پیغام آزاد کردن منابع از بین برود باعث می شود منابع آزاد نشده و همچنان درگیر این ارتباط باشند.

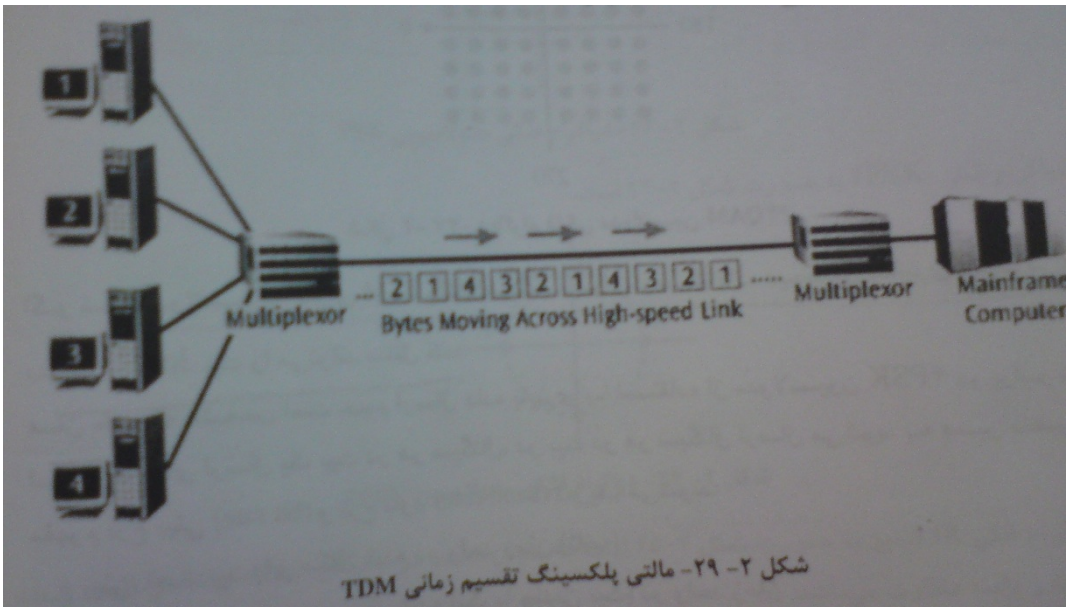
حالت دوم: اگر داده برای مدت طولانی فرستاده نشود بعد از مدت زمانی و عدم دریافت Connection Refresh و تمام شدن سهم زمانی و بروز Timeout منابع آزاد می شوند می توانند در اختیار ارتباطی دیگر قرار گیرند.

یکی از معایب ان است که اگر در حال ارسال اطلاعات باشیم و پیغام Connection Refresh نرسد و از بین برود منابع از ما گرفته می شود و همچنین اگر بسته ای از دست رفت منابع از دستمان می رود. همچنین گاهی به دلیل دیر رسیدم پیام ممکن است منابع مشغول باشند در صورتی که به آنها نیازی نیست.

مسلما در حالت دوم تاخیر بیشتری داریم چون مرتبا یک پیغام ارسال می شود همچنین بخشی ار پهنای باند در اختیار Connection Refresh است و در حالت اول پهنای باند هدر رفته کمتر است.

۳. مالتی پلکسینگ عمل انتقال سیگنال های اطلاعاتی فرستنده مختلف بر روی یک کانال مشترک است که به عبارت صحیح تر پهنای باند یک کانال مشترک بین چندین خط فرستنده به اشتراک گذاشته می شود که باعث کاهش هزینه می شود.

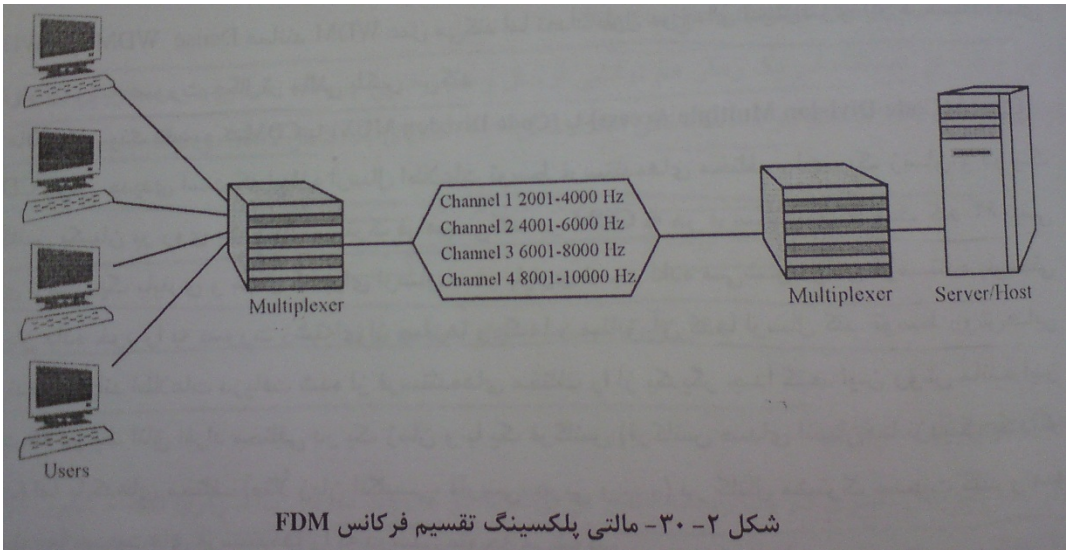
TDM یک روش MUX دیجیتالی است که زمان استفاده از کانال مشترک را بین چند خط فرستنده به صورت مساوی تقسیم می کند. پیاده سازی TDM بسیار ساده است و با یک سوئیچ ساده قابل پیاده سازی است. اما عیب آن این است که اگر فرستنده نیاز به ارسال اطلاعات نداشته باشد این زمان هدر می رود و از طرفیت کانال به درستی استفاده نمی شود. در این روش چون کل پهنای باند در اختیار یک ایستگاه قرار می گیرد اطلاعات سریعتر منتقل می شوند.



شکل ۲- ۲۹- مالتی پلکسینگ تقسیم زمانی TDM

FDM یک روش MUX آنالوگ است که قدیمی ترین روش Multiplexing می باشد. این روش پهنای باند یک کانال بر حسب هرتز به چندین پهنای باند کوچکتر تقسیم شده و هر پهنای باند (محدوده فرکانسی خاص) در اختیار یک فرستنده قرار می گیرد. بنابراین فرستنده در یک زمان و در محدوده های فرکانسی مختلف ارسال را انجام می دهند مانند ایستگاه های رادیو و تلویزیون. –این محدوده های فرکانسی دارای یک Guard Band هستند که ار برخورد فرکانسی جلوگیری می کند-

FDM نسبت به TDM، Latency (دوره بیکاری) بهتری دارد و TDM منعطف پذیر تر است.



شکل ۲- ۳۰- مالتی پلکسینگ تقسیم فرکانس FDM

۴.

$\frac{\text{نرخ ارسال در بافر یک گره}}{\text{نرخ دریافتی بافر در آن گره}}$: بهره مالتی پلکسینگ آماری در packet Switch ها

اگر بزرگتر از ۱ باشد با سرعت بیشتری نسبت به سرعت دریافت آن را ارسال می کنیم.

۵.

The four layers in the internet protocol stack are - from top to down – the application layer, the transport layer, the network layer, the network interface layer (link layer, and the physical layer).

برای مشاهده وظایف لایه‌ها به کتاب مراجعه کنید.

صفحه ۵۲ کتاب top-down

۶.

The delay components are processing delays, transmission delays, propagation delays and queuing delays. All of these delays are fixed, except for the queuing delays which are variable.

اما در روش Circuit Switching فاقد processing delays و queuing delays است.

۷.

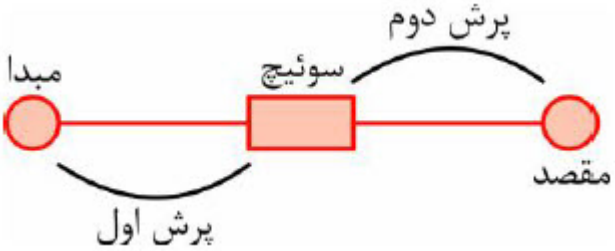
برابر زمانی است که طول می کشد تا Router همه بیت ها را ارسال کند و همه بیت ها به مقصد برسد:

$$\frac{L}{R}+\frac{d}{S}$$

۸. اندازه بسته : 64KB، MTU : 2KB ، هدر : 32Byte، $R = 50 * 10^{6}$ bps ، $V = 3 * 10^{8} {}^{m}/_{S}$،
فاصله: 10^{6}

سربار داده – کل بسته : اندازه داده

در این شبکه دو پرش یا Hop وجود دارد بنابراین تعداد switch ها برابر 1 – hop است یعنی یکی مطابق شکل زیر:



$$\frac{64kb}{2kb-32b}=\frac{64\times1024}{2\times1024-32}\approx 33$$

یعنی این پیام به 33 بسته یا Packet شکسته می شود، داریم:

$$T_{prop}=\frac{d}{v}=\frac{10^6}{3*10^8}=3.33ms$$

$$T_{trans}=\frac{l}{R}=\frac{2*1024*8}{50*10^6}=327.68\mu s$$

$$t_{delay}=2*t_{prop}+34*t_{trans}=6.6ms+11.2ms=17.8ms\approx 18ms$$

برای فهمیدن فرمول t_{delay} یا می توان فرمول زیر را حفظ کرد!!

$$t_{delay}=(n+1)T_{prop}+[n+(k-1)]T_{trans}+T_{trans}$$

که در آن n تعداد Switch هاست و k تعداد packet ها .

ولی می توان با استدلال بدون حفظ فرمول نیز مسئله را حل کرد. می دانیم که هر سوئیچ با دریافت کامل بسته می تواند آن را هدایت کند در حالی که به طور همزمان می توان بسته بعدی را دریافت کند (در Packet Switching) پس در اولین زمان ارسال اولین بسته از مبدا به سوئیچ می رسد، در دومین زمان ارسال همزمان اولین بسته از سوئیچ به سمت مقصد می رود و دومین بسته از مبدا به سوئیچ می رسد. پس در کل به ۳۴ زمان برای ارسال هر ۳۳ بسته نیاز داریم. با توجه به مفهوم تاخیر انتشار باید $2*t_{prop}$ داشته باشیم.

۹.

تاخیر ناشی از ایجادیک بسته t: $\frac{56*8}{64*10^3}=7\ ms$

$$t_{trans}=\frac{56*8}{2*10^6}=0.224ms$$

$$t_{total}=10\left(t_{prop}\right)+0.224(t_{trans})+7(t)=17.224\ ms$$

۱۰.

a. حداکثر تعداد کاربران: $\frac{1G}{100k} = 10000$ نفر

b. $\sum_{i=N+1}^{M}(M)p^i\,(1-p)^{M-i}$

.۱۱

Bandwidth-delay product of a link is the maximum number of bits that can be in the link.

این مقدار برابر است با ماکزیمم تعداد بیت هایی که می تواند روی لینک فیزیکی بین گره ها قرار بگیرد.

.۱۲

$$T_{prop} = \frac{20000}{2.5 * 10^8} = 0.08s$$

a) $bandwidth\ delay\ product = T_{prop} * R = 0.08 * 2Mbps = 160kb$

b) تعداد بیت هایی که به طور همزمان در کانال موجود است برابر مقداری ثابت و برابر ماکزیمم بیت های قابل ارسال یعنی 160K می باشد.

.۱۳

A DoS attack renders a network, host, or other piece of infrastructure unusable by legitimate users. Web servers, e-mail servers, DNS servers, and institutional networks can all be subject to DoS attacks. Internet DoS attacks are extremely common, with thousands of DoS attacks occurring every year. Most Internet DoS attacks fall into one of three categories:

- *Vulnerability attack:* this involves sending a few well-crafted messages to a vulnerable application or operating system running on a largered host. If the right sequence of packets is sent to a vulnerable application or operating system, the service can stop or, worse, the host can crash.
- *Bandwidth flooding:* The attacker sends a deluge of packets to the targeted host – so many packets that the target's access link becomes clogged, preventing legitimate packets from reaching the server.
- *Connection flooding:* the attacker establishes a large number of half-open or fully open TCP connections at the target host. The host can become so bogged down with these bogus connections that it stops accepting legitimate connections.

.۱۴

Connection Less: در این نوع سرویس در ایتدا هیچ اتصالی بین فرستنده و گیرنده برقرار نمی شود و فرستنده اطلاعات را به صورت فریم های مستقل و متوالی برای گیرنده ارسال می کند.. فرستنده هیچ گاه خاموش بودن گیرنده یا آمادگی دریافت اطلاعات توسط گیرنده را بررسی نمی کند. ممکن است قابلیت اطمینان این روش در مقابل رخداد خطا پایین باشد (از Connection Oriented پایین تر است) چون هیچ تضمینی در انتقال وجود ندارد بنابراین بهتر است در کانال های مطئن مانند فیبر نوری از آن استفاده شود در این روش نرخ انتقال اطلاعات بالاتر است و می توان از آن برای سرویس هایی که در آن تاخیر مهم است استفاده کرد.

Connection Oriented: در این سرویس ۱- علاوه بر اتصال اولیه بین فرستنده و گیرنده (Connection Setup) ۲- انتقال فریم داده همراه با دریافت پاسخ از گیرنده (Data Transfer) ۳- در انتها نیز اتصال اولیه به روش Graceful Close قطع می شود (Connection Close) و منابع آزاد می شود. بنابراین در این روش قبل ار ارسال هر فریم اطلاعاتی روشن بودن گیرنده و آمادگی آن برای دریافت اطلاعات بررسی می شود، دارای قابلیت اطمینان بالا است و تضمین در انتقال وجود دارد همچنین نرخ انتقال کمتر است و به دلیل سربارهای که استفاده می‌کند تاخیر بیشتری دارد.

.۱۵

به طور خلاصه اگر خطا برایمان مهم است (داده با اطمینان بالا) ⟵ اتصال گرا

اگر تاخیر برایمان مهم است (داده سریع ارسال شود) ⟵ بدون اتصال

زیرا اتصال گرا سربار می گذارد و سرعت را پایین می آورد ولی امنیت بالاتری دارد و بدون اتصال reliable نیست و تضمینی برای ارسال وجود ندارد و به دلیل عدم سربار گذاری و هدر کمتر سرعت بیشتری دارد.

۱۶.

$$\frac{(1.5 * 2^{20}) + 20}{1480} = 1062$$

$$1062 * 20 = 21240 \text{ Segmentation Overhead}$$

۱۷.

a. انتخاب مسیر بر عهده لایه شبکه (Network) است
b. لایه انتقال (Transport)
c. لایه پیوند داده (Data Link)

۱۸.

پروتکل: به طور خلاصه مجموعه قواعد و قوانینی که قالب و چگونگی انتقال داده را مشخص می کند برای مثال برای جواب به تلفن شخص ابتدا سلام می کند سپس سلام می شنود و سپس مکالمه و انتقال داده شروع می شود و در انتهای مکالمه هر دو خداحافظی می کنند. در پروتکل مواردی که طرفین باید بر سر آن با یکدیگر توافق داشته باشند مشخص می شود.

POP: به یک یا مجموعه ای از روتر ها در شبکه که هر مجموعه ای از روتر ها می توانند به بکدیگر وصل شوند...

ISP: (Internet Service Provider) برنامه های کاربردی به ISP متصل می شوند تا سرویس های مورد نیاز کاربران را فراهم کنند...

Wimax: در استاندارد های مربوط به IEEE در قسمت IEEE 802.16 می باشد که یک پوشش رادیویی در محدوده خاصی ایجاد می کند که گیرنده هایی که در آن محدوده گیرنده رادیویی داشته باشند می توانند داده ها را دریافت کنند و یا ارسال کنند...

3G: نسل سوم تلفن همراه که درآن امکان ارائه اینترنت و مکالمه تصویری قرار داده شده که رایت سل از آن استفاده می کند. قبل از آن ایرانسل و همراه اول از نسل 2.5 (در واقع نسل دوم که قابلیت اینترنت به آن اضافه شده!) استفاده می کردند.

Wi-Fi: استاندارد IEEE 802.11 است یک access network ایجاد می‌کند ...

Botnet: شبکه ای از رایانه های متصل به اینترنت که همگی تحت کنترل یک دستگاه واحد به نام Bot Master قرار گرفته اند...