

مفاهیم اولیه

فصل اول

Office Protocols

PPP : Point to Point Protocol

PSK : Phase Shift Keying

QAM : Quadrature Amplitude Modulation

RF : Radio Frequency

RIP : Routing Information Protocol

RTS : Request To Send

RTT : Round Trip Time

SC : Subscriber Connector

SHF : Super High Frequency

SIFS : Short Inter Frame Space

SLIP : Serial Line Internet Protocol

SMTP : Simple Mail Transfer Protocol

SONET : Synchronous Optical NETwork

SS : Slow Start

ST : Straight Tip connector

STP : Shielded Twisted Pair

STX : SStart of teXt

TCP : Transmission Control Protocol

TDM : Time Division Multiplexing

TIA/EIA : Telecommunication Industries Association/ Electronic IA

TR : Telecommunication Room

TSI : Time Slot Interchange

UDP : User Datagram Protocol

UTP : Unshielded Twisted Pair

VHF : Very High Frequency

UHF : Ultra High Frequency

VLF : Very Low Frequency

WAN : Wide Area Network

WDM : Wavelength Division Multiplexing

۱- مقدمه

تاثیر کامپیوتر بر زندگی امروزه بشر انکارناپذیر است و دنیای بدون کامپیوتر حتی برای چند لحظه غیر قابل تصور می‌باشد. اجازه بدھید سوال را مطرح کنیم و آن این است که آیا اگر کامپیوترها از هم منفک بودند و با همدیگر هیچگونه رابطه‌ای نداشتند باز هم به این اندازه بر زندگی بشر تاثیرگذار بودند؟ مسلماً جواب منفی است. استفاده از شبکه‌های کامپیوتری به شدت در حال گسترش است و سازمانها و ادارات زیادی اقدام به بریایی شبکه نموده‌اند.

در زمان طراحی یک شبکه سوالات متعددی مطرح می‌شود:

- برای طراحی یک شبکه باید از کجا شروع کرد؟
- چه پارامترهایی را باید در نظر گرفت؟
- هدف از پرپاسازی شبکه چیست؟
- انتظار کاربران از شبکه چیست؟
- آیا می‌خواهیم شبکه موجود را ارتقا دهیم و یا یک شبکه از ابتدا طراحی کنیم؟
- چه سرویس‌ها و خدماتی بر روی شبکه ارائه خواهد شد؟

قبل از طراحی فیزیکی یک شبکه کامپیوتری، ابتدا باید خواسته‌ها شناسایی و تحلیل شوند، یعنکه هدفمان از ایجاد یک شبکه چیست و این شبکه باید چه سرویس‌ها و خدماتی را ارائه نماید؛ برای تامین سرویس‌ها و خدمات مورد نظر کاربران، چه اقداماتی باید انجام داد؛ مسائلی چون بروتکل مورد نظر برای استفاده از شبکه، سرعت شبکه و از همه مهمتر مسائل امنیتی شبکه، باید به دقت مورد بررسی قرار گیرند.

شبکه کامپیوتری چیست؟

این فصل را با این سوال آغاز می‌کنیم که اساساً یک شبکه کامپیوتری چیست؟ جوابهای متعددی ممکن است به ذهن شما برسد اما ساده‌ترین تعریف این است که: یک شبکه کامپیوتری شامل دو یا بیش از دو کامپیوتر و ابزارهای جانبی مثل چاپگرها هستند که از طریق یک محیط ارتباطی به همدیگر متصل شده‌اند و از قوانین ارتباطی مشخصی به نام پروتکل پیروی می‌کنند. خود این تعریف چندان واضح نیست چرا که در آن مشخص نشده محیط ارتباطی چیست و یا

اینکه منظور از اتصال به چه صورت می‌باشد. هر کدام از این موارد در بخش‌های بعدی توضیح داده خواهد شد.

~~پردازش انتقالی از شبکه را می‌توان به صورت زیر عنوان کرد:~~

(۱) اشتراک منابع

استفاده مشترک از یک منبع اطلاعاتی یا امکانات جانبی کامپیوتر، بدون توجه به محل جغرافیایی هریک از منابع، از جمله دلایل ایجاد یک شبکه کامپیوتری است. توجه داشته باشید که منظور از اشتراک منابع هم به صورت نرم‌افزاری (اشتراک فایلها) و هم به صورت سخت افزاری (اشتراک یک چاپگر) می‌باشد.

(۲) کاهش هزینه‌ها

استفاده مشترک از منابع منجر به کاهش هزینه‌ها خواهد شد. حالتی را تصور کنید که مجبور باشیم برای هر کامپیوتر یک چاپگر هم تهیه کنیم. مسلماً با استفاده اشتراکی از کامپیوترهای داخل یک شبکه از یک چاپگر، هزینه کمتری صرف خواهد شد.

(۳) قابلیت اطمینان

این ویژگی به معنای وجود سرویس دهنده‌های پشتیبان در شبکه می‌باشد؛ بدین معنا که می‌توان از منابع گوناگون اطلاعاتی و سیستم‌ها در شبکه نسخه‌های دوم و پشتیبان تهیه کرد و در صورت عدم بسترسی به یکی از منابع اطلاعاتی در شبکه (عملت از کار افتادن سیستم)، از نسخه‌های پشتیبان استفاده کرد. به این ترتیب، کارآئی، فعالیت و آمادگی دائمی سیستم افزایش خواهد یافت.

(۴) قابلیت توسعه

یکی دیگر از مزایای یک شبکه کامپیوتری، امکان توسعه تدریجی آن است. بدین معنی که می‌توان بدون تغییر در ساختار اصلی، آن را توسعه داد و تبدیل به یک شبکه بزرگتر کرد. البته این امر به شرطی امکان‌پذیر است که در هنگام طراحی اولیه، امکانات اضافی برای گسترش شبکه در نظر گرفته شود.

۴- تقسیم‌بندی شبکه‌ها

شبکه‌های کامپیوتری را می‌توان بر اساس معیارهای مختلفی دسته بندی نمود که ذیلاً به چند مورد آن اشاره می‌کنیم:

- ۱- دسته بندی بر اساس مقیاس یا فاصله جغرافیایی
- ۲- دسته بندی بر اساس نحوه تبادل اطلاعات
- ۳- دسته بندی بر اساس نحوه سرویس

انواع شبکه از لحاظ مقیاس

از نظر مقیاس یا فاصله جغرافیایی می‌توان شبکه‌های کامپیوتری را به دسته‌های زیر تقسیم نمود:

۵- ایجاد بستر ارتباطی

شبکه کامپیوتری با استفاده از سرویسهایی مانند سرویس Email (پست الکترونیکی) و یا FTP (سرویس انتقال فایل) امکان تبادل پیغام و یا فایل را به کاربران می‌دهد.

قبل از راه اندازی شبکه مواردی که در طراحی شبکه باید مد نظر قرار گیرند عبارتند از:

- اندازه سازمان
- سطح امنیت
- نوع فعالیت و برنامه‌های کاربردی
- سطح مدیریت
- مقدار ترافیک
- بودجه

شبکه‌های کامپیوتری

۶- شبکه محلی یا (Local Area Network) LAN

ارتباط و اتصال بیش از دو یا چند کامپیوتر در فضای محدود یک ساختمان و یا یک سازمان (در حد یک دانشکده و خداکش در حد یک دانشگاه) را شبکه محلی گویند. از خصوصیات شبکه‌های محلی می‌توان به موارد زیر اشاره کرد:

- اساساً در محیط های کوچک کاری قابل اجرا و پیاده‌سازی می‌باشند.
- از سرعت نسبتاً بالایی برخوردارند.

- دارای یک ارتباط دائمی بین کامپیوترها از طریق کابل شبکه و یا بصورت بی‌سیم می‌باشند.

۷- اجزای یک شبکه مطابق عبارتند از:

الف- کامپیوترها

ب- کارت واسط شبکه

ج- بروتکل ارتباطی

د- سوئیچ یا هاب

ه- محیط ارتباطی (باسیم یا بی‌سیم)

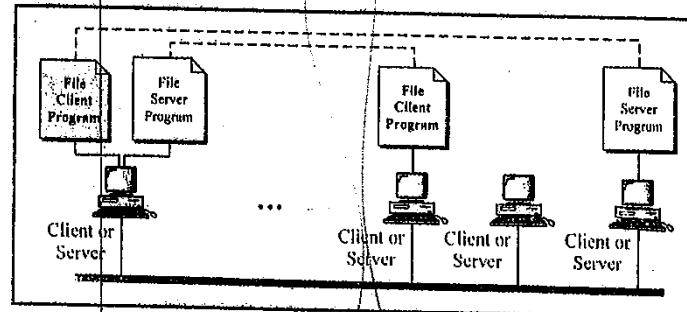
از جمله پروتکلهای موجود برای ایجاد شبکه‌های محلی می‌توان به اترنت (Ethernet)، حلقه نشانه (Token Ring)، گذرگاه نشانه (Token Bus) و شبکه محلی بی‌سیم (WLAN) اشاره نمود.

۷/ اصول شبکه‌های کامپیوتری

جزئی شبکه

ک مدل شبکه نظیر به نظر

در این نوع شبکه‌ها، کامپیوتر ویژه‌ای جهت نگهداری فایل‌های اشتراکی و سیستم عامل شبکه وجود ندارد. هر استگاه می‌تواند به منابع سایر استگاه‌ها در شبکه دسترسی پیدا کند. هر کامپیوتر خاص می‌تواند هم عنوان Server و هم عنوان Client عمل کند، یعنی هم به کامپیوتر دیگری سرویس پرداز و هم از کامپیوتر دیگری سرویس پذیرد و کامپیوتراها نسبت به هم برتری و ارجحیت نداشته باشند. شبکه‌های مبتنی بر Windows NT، از این نوع هستند. شکل (۱-۱) چنین شبکه‌ای را نشان می‌دهد.



شکل (۱-۱)- مدل نظیر به نظر

نخواه مزایای یک شبکه نظیر به نظر می‌توان به موارد زیر اشاره نمود:

- ۱- ممکن است یک کامپیوتر سرویس دهنده نیست؛ بنابراین، اگر یک کامپیوتر برای مدتها از شبکه خارج شود، احتمال ایجاد اختلال زیاد نیست.
- ۲- اگر اعضای شبکه اختیار و حق دستیابی به اطلاعات را داشته باشند، آنگاه می‌توانند بطور موقت داده‌ها را با همکاران خود به اشتراک بگذارند.
- ۳- نیازی به مدیر شبکه ندارد.
- ۴- هزینه این نوع شبکه برای سازمانهای کوچک که توانایی پرداخت هزینه مدیریت شبکه را ندارند، پایین است.

اما این نوع شبکه معایبی نیز دارد که عبارتند از:

- ۱- هنگامی که دیگر کاربران بخواهند از اطلاعات به اشتراک گذاشته شده توسط شما استفاده کنند، سرعت کامپیوترتان کاهش می‌یابد.

شبکه شهری MAN (Metropolitan Area Network)

ارتباط کامپیوترها در محدوده جغرافیایی یک شهر را شبکه شهری یا MAN گویند. بیشتر پروتکلهای مورد استفاده برای یک شبکه شهری، همان پروتکلهای شبکه‌های گسترده هستند.

شبکه گسترده WAN (Wide Area Network)

اتصال شبکه‌های محلی از طریق خطوط تلفنی، کابل‌های ارتباطی، ماهواره و یا دیگر سیستم‌هایی مخابراتی چون خطوط استیجاری در یک منطقه بزرگتر در مقابس یک کشور و یا حتی یک قاره را شبکه گسترده با WAN گویند. در این شبکه، کاربران یا کامپیوتراها از مسافت‌های دور و از طریق خطوط مخابراتی به یکدیگر متصل می‌شوند. در شبکه گسترده، سرعت انتقال داده نسبت به شبکه‌های محلی کمتر است.

از جمله پروتکلهای موجود برای ایجاد شبکه‌های گسترده می‌توان به SONET، ATM، ISDN، Frame Relay و DSL اشاره نمود.

شبکه جهانی Internet

بزرگترین شبکه کامپیوتری است که از ترکیب تمام شبکه‌های LAN و MAN و WAN ایجاد شده است.

دقیق کنید که اصطلاح internet (با) به معنی شبکه‌ای مشکل از چند شبکه دیگر است ولی اصطلاح Internet (با) به معنی شبکه جهانی اینترنت می‌باشد.

انواع شبکه از لحاظ نوع سرویس

(در یک شبکه، یک کامپیوتر می‌تواند سرویس دهنده یا سرویس گیرنده و یا هردو باشد) یک سرویس دهنده (Server)، کامپیوترا برای اشتراک فایل‌های اشتراکی و همچنین سیستم عامل شبکه که مدیریت عملیات شبکه را بهره‌دار دارد را نگهداری می‌کند.

برای آنکه سرویس گیرنده (Client) می‌تواند به سرویس دهنده دسترسی پیدا کند، ابتدا سرویس گیرنده باید اطلاعات مورد نیازش را از سرویس دهنده تقاضا کند. سپس سرویس دهنده اطلاعات درخواست شده را به سرویس گیرنده ارسال خواهد کرد.

تقسیم بندي شبکه‌ها از اين لحاظ به صورت زير است:

۱- شبکه نظیر به نظر (Peer-to-Peer)

۲- شبکه سرویس دهنده / سرویس گیرنده (Client Server)

- امنیت شبکه بسیار پایین است.

- اگر امکان دستیابی کامل به فایل‌های روی کامپیوتر خود را به دیگر اعضا بدهید، ممکن است

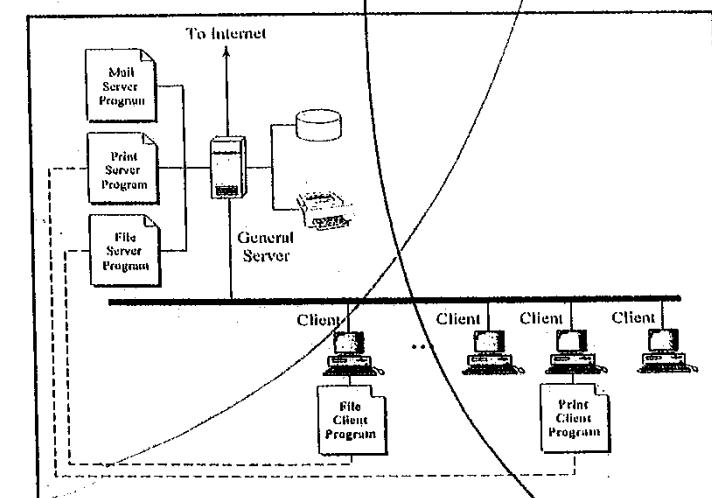
این فایلها توسط آنها خراب شده و یا حتی حذف شوند.

- در شبکه‌هایی با تعداد حداقل ۱۰ تا ۱۵ کامپیوتر می‌تواند بکار رود و در شبکه‌های بزرگتر

جوابگو نیست.

۴) مدل سرویس دهنده / سرویس گیرنده

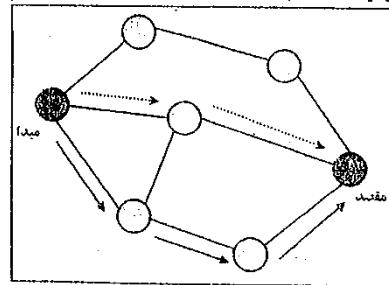
در این مدل، یک یا چند کامپیوتر به عنوان سرویس دهنده در نظر گرفته می‌شوند که معمولاً از نظر قدرت محاسبه و اطمینان حافظه، در حد بالایی قرار دارند. ممکن است برای هر سرویس خاص یک کامپیوتر منفرد در نظر گرفته شود مثلاً یک کامپیوتر به عنوان سرویس دهنده پست الکترونیکی (Mail Server)، یک کامپیوتر به عنوان سرویس دهنده وب (Web Server) و ...؛ و یا اینکه یک کامپیوتر تمام سرویسهای مورد نیاز را ارائه دهد. سرویس گیرنده در خواست انجام کارش را به سرویس دهنده ارائه می‌دهد و سرویس دهنده پس از اجرای وظیفه محوله، نتایج حاصل را به ایستگاه درخواست کننده ارائه می‌دهد. (شکل (۲-۱))



شکل (۲-۱)- مدل سرویس دهنده / سرویس گیرنده

۵) شبکه‌های نقطه به نقطه

در این نوع شبکه‌ها اگر کامپیوتری بخواهد اطلاعاتی را برای کامپیوتر دیگری ارسال نماید، این اطلاعات باید از طریق کامپیوترهای میانی و مسیر به مسیر به جلو رانده شود. (Store and Forward) همان طور که در شکل (۲-۱) نیز نشان داده شده است، بر اساس ترافیک و وضعیت فعلی شبکه، این مسیرها می‌توانند متفاوت باشند.



شکل (۲-۱)- شبکه‌های نقطه به نقطه

۴- اجزاء شبکه (Network Components)

هر شبکه اساساً از چهار بخش اصلی زیر تشکیل می‌شود:

- ابزارهایی که به پیکربندی اصلی شبکه متصل می‌شوند. بعنوان مثال: کامپیوترها، چاپگرهای و هابها (Hubs) • رسانه انتقال: (Transmission Medium)، که کامپیوترها را به یکدیگر متصل کرده و موجب برقراری ارتباط بین کامپیوترهای یک شبکه می‌شود. برخی از متداولترین رسانه‌های انتقال عبارتند از:

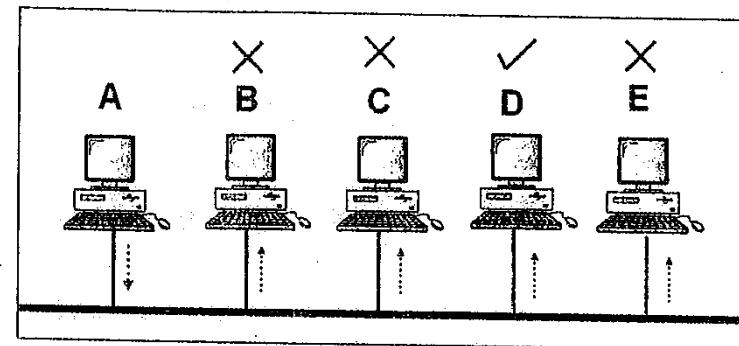
الف: محیط‌های پاسیم شامل: زوج سیم بهم تابیده (Twisted-Pair)، کابل هم محور (Coaxial) و فیبر نوری (Fiber-Optic).

ب: محیط‌های بی‌سیم شامل: امواج مادون قرمز (Infrared)، فرکانس‌های رادیویی (Radio Frequency) و امواج مایکروویو (Microwave). این بخش در فصل دوم مفصل بحث خواهد شد.

• سازگارکننده‌ها (Adapters)، که بعنوان اتصال دهنده کابل‌ها به کامپیوتر هستند. سازگارکننده به دریافت و ترجمه سیگنالهای ورودی از شبکه، و ترجمه و ارسال خروجی به شبکه می‌پردازد.

• سیستم عامل شبکه یا NOS، که بر روی سرویس‌دهنده اجرا می‌شود و سرویس‌های مختلفی مانند اجازه ورود به سیستم (Login)، رمز عبور (Password)، چاپ فایل‌ها و مدیریت شبکه را در اختیار کاربران می‌گذارد.

شبکه‌های پخشی (Broadcast Networks)
در این نوع شبکه‌ها اطلاعات بر روی محیط مشترکی در شبکه پخش شده و تمام استگاهها آن را می‌بینند ولی تنها ایستگاهی اطلاعات را برمی‌دارد که آدرس خود را بر روی آن مشاهده نماید. مثلاً در شکل (۴-۱) کامپیوتر A می‌خواهد بسته‌ای را برای کامپیوتر D ارسال کند. ابتدا آدرس مقصود را به بسته چسبانده و سپس آن را به گذرگاه مشترک می‌فرستند. تمام کامپیوترهای دیگر این بسته را می‌بینند ولی فقط کامپیوتر D که آدرس خود را روی آن مشاهده می‌کند، بسته را برمی‌دارد و بقیه آن را نادیده می‌گیرند.



شکل (۴-۱)- شبکه‌های پخشی

کسبه پخشی بروکر (Broadcast)

انتقال اطلاعات از طریق کامپیوترها (غیربرگ) می‌تواند از سطح تماارسکهای

کامپیوترهای پخشی (Broadcast) کامپیوترهای پخشی (Broadcast)

امنیت کم

کارایی پایین

توپولوژی حلقوی (Ring)

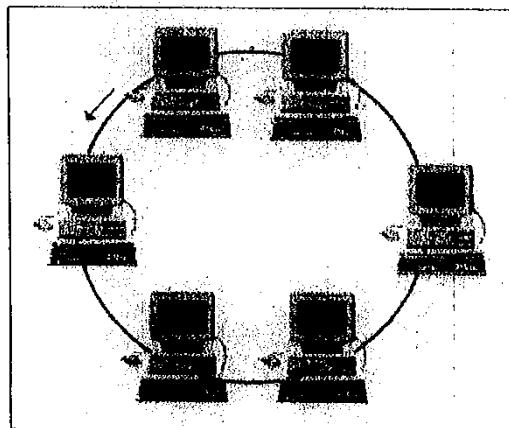
در این توپولوژی کلیه کامپیوترها به گونه‌ای به یکدیگر متصل هستند که مجموعه آنها یک حلقه را می‌سازند (شکل ۱-۶). کامپیوتر مبدا اطلاعات را به کامپیوتر بعدی در حلقه (درجهت یا خلاف جهت عقربه‌های ساعت) ارسال نموده و آن کامپیوتر به آدرس اطلاعات نگاه کرده آدرس مربوط به او بود، آن را برای خود کمی می‌کند در غیر این صورت اطلاعات را به کامپیو بعدی در حلقه منتقل خواهد کرد و به همین ترتیب این روند ادامه پیدا می‌کند تا اطلاعات کامپیوتر مقصد برسد. مثال بارز برای این نوع توپولوژی، شبکه Token Ring است. در بعضی پروتکلها مانند FDDI برای تحمل پذیری بیشتر در برابر خرابی، از دو حلقه مجزا استفاده می‌شود.

نقاط ضعف توپولوژی فوق عبارتند از:

- اگر یک کامپیوتر از کار بیفتند، کل شبکه متوقف می‌شود.
- به سخت افزار پیچیده نیاز دارد (کارت شبکه آن گران قیمت است).
- برای اضافه کردن یک ایستگاه به شبکه باید کل شبکه را متوقف کرد.

نقاط قوت توپولوژی فوق عبارتند از:

- نصب شبکه با این توپولوژی ساده است.
- در این توپولوژی از فیبر نوری می‌توان استفاده کرد.



شکل (۱-۶)- توپولوژی حلقوی

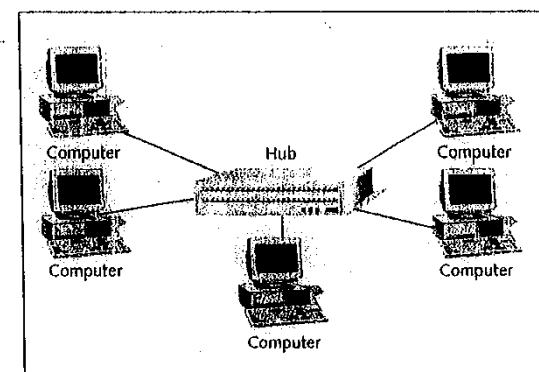
۱۴- همبندیهای شبکه (Network Topologies)

در تعریف یک شبکه کامپیوتری از اتصال کامپیوترها به همدیگر صحبت کردیم ولی در مورد چگونگی اتصال سخنی به میان نیامد. همبندی یا توپولوژی شبکه، تشریح کننده نحوه اتصال کامپیوترها در یک شبکه به یکدیگر است. پارامترهای اصلی در انتخاب توپولوژی، قابل اعتماد بودن و مقررین به صرفه بودن هستند. انواع متدائل توپولوژی‌ها در شبکه‌های کامپیوتری عبارتند از:

توپولوژی ستاره‌ای (Star)

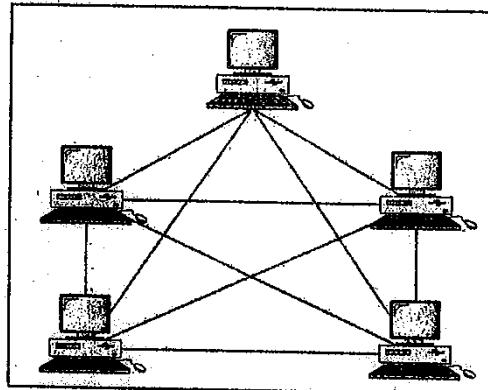
در این توپولوژی، کلیه کامپیوترها به یک کنترل کننده مرکزی یا هاب متصل هستند. هرگاه کامپیوتری بخواهد با کامپیوتر دیگر تبادل اطلاعات نماید، کامپیوتر منبع ابتدا باید اطلاعات را به هاب ارسال نماید. سپس از طریق هاب آن اطلاعات به کامپیوتر مقصد منتقل شود (شکل ۱-۵)). نقطه ضعف این توپولوژی آن است که هاب وابسته است. این بدان معناست که اگر هاب از کار بیفتند، کل شبکه به هاب وابسته است. این بدان از:

- نصب شبکه با این توپولوژی ساده است.
- توسعه شبکه با این توپولوژی به راحتی انجام می‌شود.
- اگر یکی از خطوط متصل به هاب قطع شود، فقط یک کامپیوتر از شبکه خارج می‌شود.



شکل (۱-۵)- توپولوژی ستاره‌ای

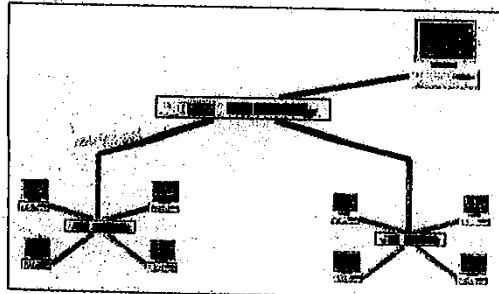
به نود و نه پورت و نود و نه خط ارتباطی با سایر ایستگاهها می‌باشد. تعداد کابل‌های مورد نیاز در این توپولوژی با رابطه $\frac{N(N-1)}{2}$ محاسبه می‌شود که در آن N تعداد ایستگاه‌های شبکه می‌باشد. (شکل (۸-۱))



شکل (۸-۱)- توپولوژی توری

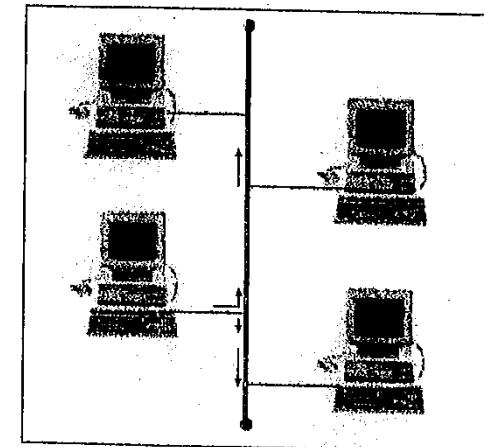
Tree

آن توپولوژی از یک یا چند هاب و یا سوئیچ که به صورت سلسله مراتبی متصل شده‌اند تشکیل می‌گردد. به طوری که در پایینترین لایه که کاربران قرار گرفته‌اند، از هاب و یا سوئیچهای ضعیفتر، و در لایه‌های بالاتر، از سوئیچهای پرقدرت‌تر استفاده می‌کنیم. خطوط ارتباطی لایه‌های بالاتر نیز باید از پهنه‌ای باند بیشتری برخوردار باشند. در شکل (۹-۱) مثالی از این نوع توپولوژی نشان داده شده است.



شکل (۹-۱)- توپولوژی درختی

توپولوژی گذرگاهی (BUS)
در یک شبکه گذرگاهی چندین کامپیوتر به یک کابل بنام BUS متصل می‌شوند. در این توپولوژی، رسانه انتقال بین کلیه کامپیوترا مشترک است. برای جلوگیری از انکاس سیگنال، در دو سر کابل مقاومت‌های مخصوصی به نام Terminator قرار می‌دهند. سادگی، کم هزینه بودن و توسعه آسان این شبکه، از نقاط قوت این توپولوژی می‌باشد. نقطه ضعف عمدی این شبکه آن است که اگر کابل اصلی که بعنوان پل ارتباطی بین کامپیوتراهای شبکه می‌باشد قطع شود، کل شبکه از کار خواهد افتاد. (شکل (۷-۱))



شکل (۷-۱)- توپولوژی گذرگاهی

Mesh

در این توپولوژی، هر کامپیوتر مستقیماً به کلیه کامپیوتراهای شبکه متصل می‌شود. مزیت این توپولوژی آن است که هر کامپیوتر با سایر کامپیوترا ارتباطی مجزا دارد. بنابراین، این توپولوژی دارای بالاترین درجه امنیت و اطمینان می‌باشد. اگر یک کابل ارتباطی در این توپولوژی قطع شود، شبکه همچنان فعال باقی می‌ماند.

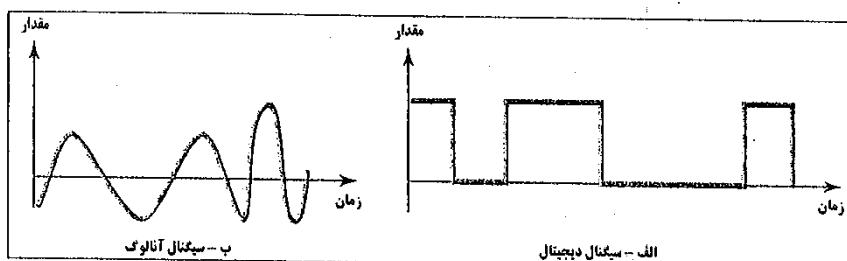
از نقاط ضعف اساسی این توپولوژی آن است که از تعداد زیادی خطوط ارتباطی استفاده می‌کند، مخصوصاً زمانی که تعداد ایستگاه‌ها افزایش یابند. به همین جهت این توپولوژی از نظر اقتصادی مفروض به صرفه نیست. برای مثال، در یک شبکه با صد ایستگاه کاری، هر ایستگاه نیازمند

۵- مشخصه‌های انتقال

نوع سیگنال انتقالی (آنالوگ یا دیجیتال)

یک سیگنال می‌تواند آنالوگ یا دیجیتال باشد. مقدار یک سیگنال آنالوگ با گذشت زمان به صورت پیوسته تغییر می‌کند و مقدار عددی که اتخاذ می‌کند سطح مشخصی ندارد. (مانند سیگنال صحبت انسان در یک میکروفون).

اما یک سیگنال دیجیتال، یک سیگنال چند سطحی (مثلاً دو سطحی) است که با گذشت زمان بصورت گیسته تغییر می‌کند. به عبارت دیگر دارای پرشهای ناگهانی است. سیگنالهای آنالوگ نسبت به تویز حساس هستند اما در مورد سیگنالهای دیجیتال با تقویت کردن، حساسیت به تویز از بین می‌رود.



شکل (۱-۱۰)- سیگنالهای دیجیتال و آنالوگ

توبولوژی ترکیبی (Hybrid)

این توبولوژی ترکیبی است از چند شبکه با توبولوژی متفاوت که توسط یک کابل اصلی بنام استخوانبندی (Backbone) به یکدیگر مرتبط شده‌اند. هر شبکه توسط یک پل ارتباطی به کابل استخوانبندی متصل می‌شود.

لوبولوژی Mesh

۱) دلای دا لاسین دربه» اهیت و لطینان

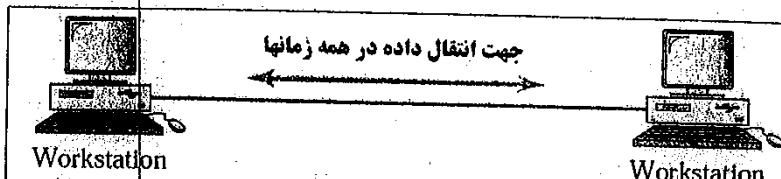
(۲

سرعت انتقال سیگنال در یک کانال

این مشخصه برای سیگنالهای دیجیتال اندازه‌گیری می‌شود و منظور از آن تعداد بیت‌هایی است که در واحد زمان (ثانیه) از کانال عبور می‌کند. همانطور که مشخص است واحد آن بیت بر ثانیه (bps) می‌باشد.

اصطلاح دیگری به نام **Baud rate** وجود دارد که به معنای تعداد تغییرات سیگنال در ثانیه می‌باشد که بسته به اینکه هر بیت با چند سطح ولتاژ و یا هرچند بیت با یک سطح ولتاژ نشان داده شوند، ممکن است بیشتر، کمتر و یا برابر bps باشد.

نوع سوم ارتباط، به صورت دوطرفه کامل است که در آن طرفین در آن واحد هم می‌توانند فرستنده باشند و هم گیرنده؛ مانند مکالمه تلفنی عادی و یا اتصال به اینترنت از طریق مودم.



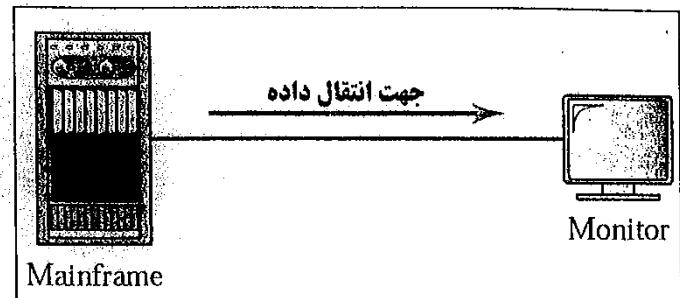
شکل(۱۳)- ارتباط دوطرفه کامل

تک کاناله یا چند کاناله بودن

در ارتباط تک کاناله که به آن باندپایه یا Baseband نیز گفته می‌شود، در کانال فقط یک سیگنال حاوی اطلاعات به صورت دیجیتال وجود دارد؛ مثلاً بازی این نوع ارسال شبکه است. اما در ارتباط چند کاناله، سیگنالهای مختلفی با فرکانس‌های متفاوت بصورت تلفیق شده می‌توانند همزمان در کانال وجود داشته باشند؛ مانند تلویزیونهای کابلی. در مناطقی که امکان پوشش تلویزیونی از طریق امواج وجود ندارد، سیگنالهای تلویزیونی شبکه‌های مختلف از طریق کابل وارد منازل می‌شود. به طوری که در داخل کابل سیگنال مربوط به همه کانالها همزمان وجود دارد. در شکل(۱۴) ارسال به روش Baseband و Broadband نشان داده شده است.

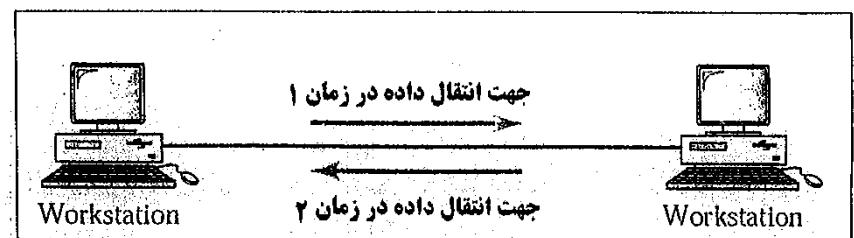
جهت حرکت دیتا (یکطرفه - نیمه‌دوطرفه - دوطرفه کامل)

در ارتباط یک طرفه، یک طرف همیشه گیرنده و طرف دیگر همیشه فرستنده است و داده تنها در یک جهت انتقال می‌باید. ارتباط کنترل از راه دور تلویزیون با دستگاه تلویزیون از این نوع است.



شکل(۱۱)- انتقال یکطرفه

در ارتباط نیمه‌دوطرفه، طرفین هم می‌توانند گیرنده باشند هم فرستنده. ولی در هر لحظه یک طرف می‌تواند گیرنده باشد و طرف دیگر فرستنده. دستگاه‌های تلفن نظامی از این قبیل ارتباط استفاده می‌کنند. به طوری که اگر شخص بخواهد صحبت کند باید شاسی مخصوصی را فشار بدهد و غیر اینصورت فقط قادر به گوش کردن خواهد بود.



شکل(۱۲)- ارتباط نیمه دوطرفه

۶- مدل‌های لایه‌ای:

قوانين کامپیوترا بصورت نرمافزاری و سخت افزاری برای انتقال و دریافت داده مشخص شده‌اند که به پروتکل موسومند. پروتکل در واقع زبان مشترک کامپیوتراهای یک شبکه است. پروتکل، تعیین کننده مشخصه‌های شبکه، روش دسترسی و انواع فیزیکی ترابولوژی‌ها، سرعت انتقال داده‌ها و نوع کابل کشی است.

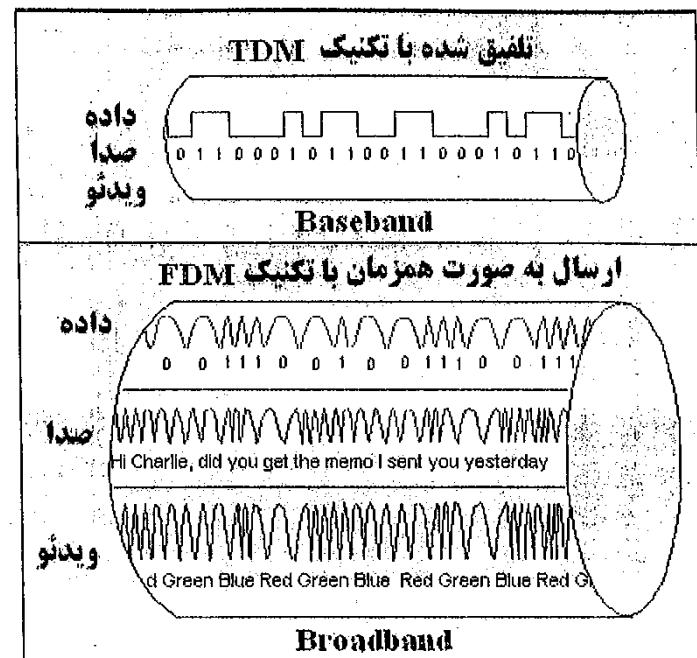
برقراری ارتباط بین کامپیوتراهایی که ممکن است از هر لحظه متفاوت باشند، امر بسیار پیچیده‌ای است. شبکه اینترنت مشکل از تعداد بسیار زیادی کامپیوترا با معماری‌های کاملاً متفاوت و سیستم‌عامل‌های مختلف می‌باشد. واضح است که ارتباط این کامپیوتراها نیاز به مدلی دارد که قادر باشد پاسخگوی تمامی این اختلافات باشد. ما در اینجا تنها دو تا از مهمترین مدل‌های شبکه را معرفی می‌کنیم:

مدل OSI

این مدل مبتنی بر قراردادی است که سازمان استانداردهای جهانی ISO عنوان مرحله‌ای از استانداردار سازی قراردادهای لایه‌های مختلف شبکه، توسعه داده است. این مدل هفت لایه دارد. در مدل OSI هر لایه با لایه همسطح خود در طرف مقابل در ارتباط است. به عنوان مثال لایه چهارم در طرف فرستنده با لایه چهارم در طرف گیرنده، از طریق پروتکلهای لایه چهارم با هم ارتباط دارند. این ارتباط به صورت مجازی بوده و ارتباط حقیقی از طریق پایینترین لایه که همان کانال فیزیکی است انجام می‌گردد. در هر طرف، هر لایه مستقیماً تنها با یک لایه بالاتر و یک لایه پایینتر از خود ارتباط دارد. در طرف فرستنده، هر لایه داده را از لایه بالاتر تحویل گرفته و پس از چسباندن یک سری اطلاعات اضافی به نام سرآیند (Header)، آن را به لایه پایینتر تحویل می‌دهد. وقت کنید که داده و اطلاعات چسبانده شده به آن، به عنوان داده در لایه پایینتر محسوب می‌شود (شکل ۱۵-۱). این کار را کپسوله کردن اطلاعات یا Encapsulation می‌نامند. در طرف گیرنده، هر لایه Header مربوط به خود را برداشت و داده را تحویل لایه بالاتر می‌دهد.

مزایای استفاده از مدل لایه‌ای عبارتند از:

- سازندگان محصولات شبکه، محصولاتشان را مطابق استانداردهای تعریف شده در لایه‌های این مدل می‌سازند و بدین ترتیب مشکل عدم سازگاری برطرف خواهد شد.
- هر لایه می‌تواند مستقل از سایر لایه‌ها تغییر کند.



شکل (۱۴-۱)- ارسال تک کاناله و چند کاناله

- نحوه شروع و خاتمه ارتباط چگونه باشد؟
- ...
- در فصل دوم در مورد این لایه مفصلابحث خواهد شد.

لایه پیوند داده (Data link Layer)

در این لایه با frame (روش‌های از بیتها) سروکار داریم، هر فریم دارای قسمتهای مختلفی جهت نشان دادن شروع فریم، پایان فریم، اندازه فریم، کنترل خط و اطلاعات کنترلی می‌باشد. در شکل(۱۶)، ساختار یک فریم نوعی نشان داده شده است.

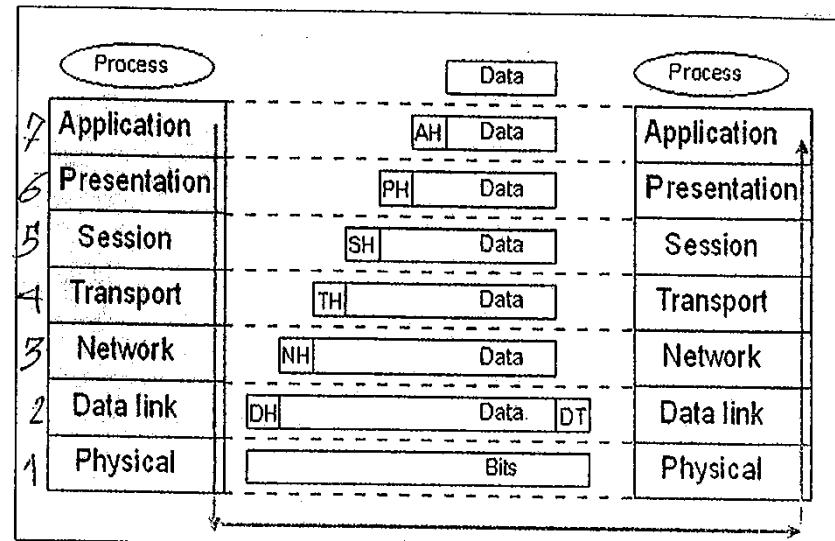


شکل(۱۶)- ساختار یک فریم نوعی

وظایف این لایه شامل موارد زیر است:

- ایجاد و مدیریت frame‌ها.
- کنترل خط (شامل تشخیص و در صورت امکان تصحیح خط).
- کنترل جریان. منظور این است که تدبیری اتخاذ کنیم که فرستنده بیش از ظرفیت بافر گیرنده اطلاعات ارسال نکند.
- کنترل دسترسی به رسانه مشترک همانطور که در شکل(۱۷-۱) مشخص است، هدف این لایه، ارسال صحیح اطلاعات در یک تکه (Hop) از مسیر است. هر کدام از وظایف فوق را در فصل سوم بحث خواهیم کرد.

- طراحی مازلار خواهد بود.
- یادگیری و یاددهی اصول شبکه راحتتر خواهد شد.



شکل(۱۵)- مدل مرجع OSI

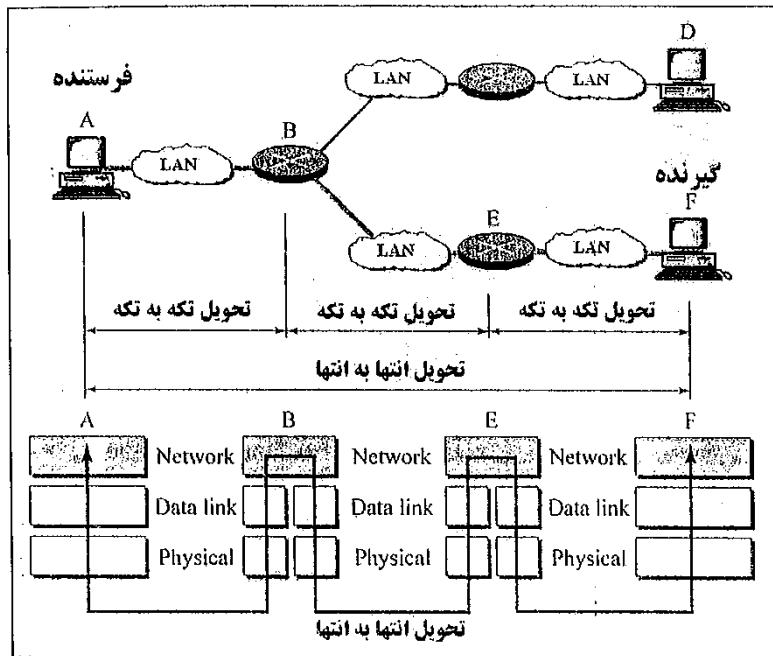
اکنون هفت لایه را به نوبت از لایه پایین مورد بحث قرار می‌دهیم: در صورتی که با کلمات و عبارات ناآشنایی (مانند نام پروتکلهای) برخورد نمودید، بدون نگرانی به خواندن ادامه دهید و مطمئن باشید که در فصلهای بعدی در مورد آنها صحبت خواهد شد.

لایه فیزیکی (Physical Layer)

واحد انتقالی در این لایه، بیت می‌باشد. به عبارت دیگر انتقال بیتها خام بروی کانال ارتباطی از وظایف این لایه است. در این لایه با خصوصیات فیزیکی کانال سروکار داریم. موارد زیر از جمله مشغولیتهای این لایه به شمار می‌روند:

- چه ولتاژهایی برای '۱' و '۰' در نظر گرفته شود؟
- از چه نوع مدولاسیونی (AM, FM, PM, ...) استفاده گردد؟
- چه نرخی برای انتقال داده استفاده شود؟

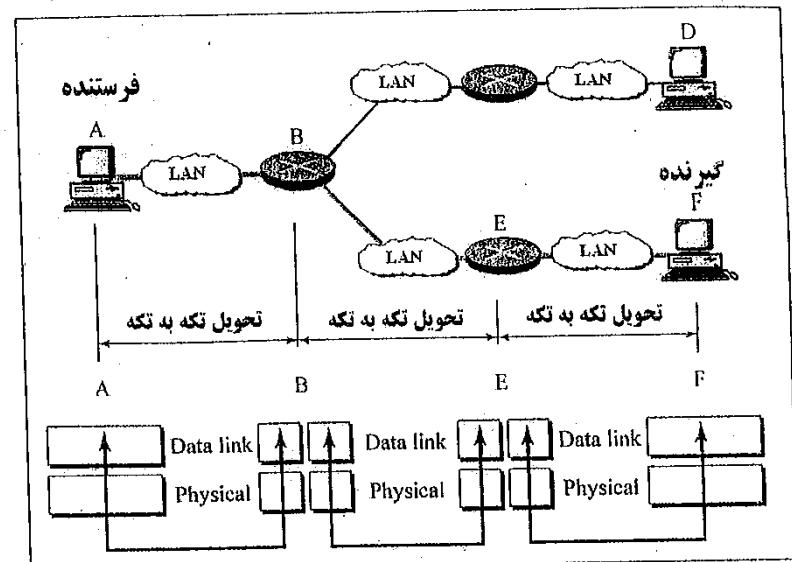
از جمله پروتکلهای مشهور این لایه می‌توان IP و IPX را نام برد. پروتکلهای مختلف این لایه و همچنین مفهوم مسیریابی را در فصل چهارم توضیح خواهیم داد.



شکل(۱۸-۱)- ارسال انتهای به انتهای در لایه شبکه

لایه انتقال (Transport Layer)

این لایه برای سرویسی که لایه پایینتر (لایه شبکه) برایش فراهم می‌کند، می‌تواند ارتباط بین دو برنامه مختلف که در کامپیوترهای مبدأ و مقصد اجرا می‌شوند را فراهم سازد. این لایه بر اساس اینکه لایه بالاتر چه وظیفه‌ای به آن سخون کرده است می‌تواند سرویسهای قابل اطمینان و غیر قابل اطمینان و همچنین اتصالگرا و غیر اتصالگرا را فراهم نماید. در مورد این سرویسها در فصل پنجم مفصلًا بحث خواهد شد. از جمله پروتکلهایی که در این لایه کار می‌کنند می‌توان به TCP و UDP در TCP/IP و SPX در NOVELL اشاره کرد.



شکل(۱۷-۱)- ارسال hop به hop در لایه ارتباط داده

لایه شبکه (Network Layer)

در این لایه از سطح بالاتری به شبکه نگاه می‌شود و هدف، ارسال اطلاعات به مقصد نهایی از مناسبترین مسیر است. مهمترین وظیفه این لایه، مسیریابی (Routing) می‌باشد. مسیریابی عبارتست از تعیین مسیر مناسب با توجه به پارامترها و معیارهایی که تعیین می‌کنیم. دستگاهی که این کار را انجام می‌دهد، مسیریاب یا Router گفته می‌شود.

واحد اطلاعات در این لایه، بسته (packet) است. Packet ها بسته‌های اطلاعاتی مستقلی هستند که با استفاده از یک سری اطلاعات اضافی به نام header می‌توانند مسیر خود را پیدا کنند. Packet های مربوط به یک برنامه خاص می‌توانند از مسیرهای مستقلی به مقصد برسند و در نتیجه احتمال اینکه خارج از ترتیب دریافت شوند، وجود دارد. برای جلوگیری از این مشکل هر بسته در قسمت header خود دارای شماره ترتیب (Sequence Number) می‌باشد که مقصد می-

تواند از روی آن بسته‌ها را به ترتیب به هم بچسباند. در این لایه برای شناسایی هر کامپیوتر در شبکه از آدرس منطقی (مثلاً آدرس IP) استفاده می‌شود. لایه شبکه، آدرس منطقی هر بسته را بررسی می‌کند و آن بسته را بر اساس جدولی موسوم به جدول مسیریابی (Routing table) به مسیریاب بعدی می‌فرستد تا به مقصد نهایی برسد.

لایه کاربرد (Application Layer)

این لایه مستقیماً با کاربر سروکار دارد و از آنجاکه کاربران اهداف و انتظارات مختلفی از شبکه دارند، این امکان دسترسی کاربران به سرویسهای گوناگون شبکه مانند Email و Web را فراهم می‌کند. از جمله پروتکلهای این لایه می‌توان به SMTP و POP3 (برای ارسال و دریافت ایمیل)، HTTP (برای انتقال صفحات وب)، FTP (برای انتقال فایل)، DNS (نام‌گذاری حوزه‌ها) و ... اشاره کرد. این پروتکلهای انتقالی را در فصل ششم توضیح خواهیم داد.

برای سهولت به خاطر سپاری ترتیب لایه‌ها عبارت زیر را در ذهن داشته باشید:

All People Seem To Need Data Processing

بروتکل TCP/IP

این پروتکل در حقیقت بصورت پشتهای از پروتکلهای است که در چهار لایه روی هم قرار گرفته‌اند.

این لایه‌ها عبارتند از:

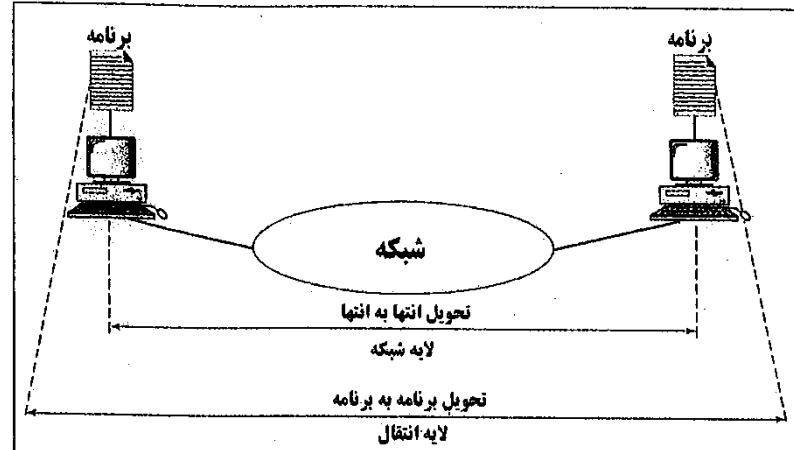
الف: لایه کاربرد (Application)

ب: لایه انتقال (Transport)

ج: لایه اینترنت (Internet)

د: لایه دسترسی شبکه (Network Access)

در شکل (۲۰-۱) مدل TCP/IP در مقایسه با مدل مرجع OSI نشان داده شده است. همانطور که در شکل دیده می‌شود، لایه کاربرد مدل TCP/IP معادل سه لایه بالایی مدل OSI می‌باشد. لایه انتقال مدل TCP/IP معادل لایه انتقال مدل OSI، لایه اینترنت در مدل TCP/IP معادل لایه شبکه در مدل OSI و بالاخره لایه دسترسی شبکه در مدل TCP/IP معادل دو لایه پایینی مدل OSI می‌باشد.



شکل(۱۹-۱)- طرز کار لایه انتقال

لایه اجلاس (Session Layer)

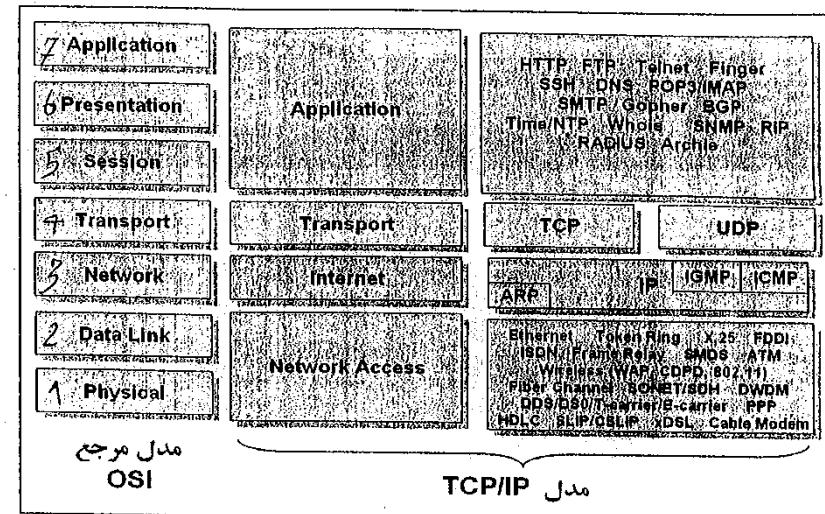
این لایه را می‌توان مشابه اپراتورهای سیستمهای تلفن قدیمی تصور نمود. در اوایل پیدایش سیستم تلفن، اگر می‌خواستید با شخصی صحبت کنید باید با اپراتوری در یک مرکز تلفن تماس برقرار نموده سپس او تماس شما را با فرد مورد نظر برقرار می‌نمود. پس از خاتمه مکالمه نیز، اپراتور وظیفه داشت که اتصال فیزیکی بین دو طرف را قطع نماید. وظیفه این لایه کنترل مکالمه و یا به عبارت دیگر برقراری، مدیریت و خاتمه اجلاس‌هاست. این لایه در بسیاری از پروتکلهای وجود ندارد و وظایف آن به لایه‌های بالاتر محول شده است.

لایه نمایش (Presentation Layer)

در بعضی از کامپیوترها مانند کامپیوترهای IBM، از روش کدگذاری EBCDIC استفاده می‌شود در حالیکه در برخی دیگر، مانند کامپیوترهای Intel، از کدگذاری ASCII استفاده می‌گردد. برای اتصال این کامپیوترها به همدیگر از طریق شبکه، باید به نحوی این کدها برای یکدیگر قابل فهم باشند. این کار وظیفه لایه نمایش است. از جمله وظایف دیگر این لایه می‌توان به اعمال فشرده‌سازی اطلاعات (جهت کاهش حجم و سرعت بخشیدن به ارسال داده) و همچنین رمزگذاری اطلاعات (جهت غیرقابل فهم کردن اطلاعات به هنگام دسترسی غیرمجاز) اشاره کرد.

از مهمترین پروتکل های ارتباطی شبکه در جهان تلقی می شود و نه تنها بروزی اینترنت و شبکه های گستردگی گوناگون کاربرد دارد، بلکه در شبکه های محلی مختلف نیز مورد استفاده قرار می گیرد. این پروتکل به دلیل سادگی مفاهیمی که در خود دارد اصطلاحاً به سیستم باز مشهور است، بر روی هر کامپیوتر و ابر کامپیوتر قابل طراحی و پیاده سازی است و بر روی هر بستر فیزیکی اعم از باسیم، یا بیسیم کار می کند.

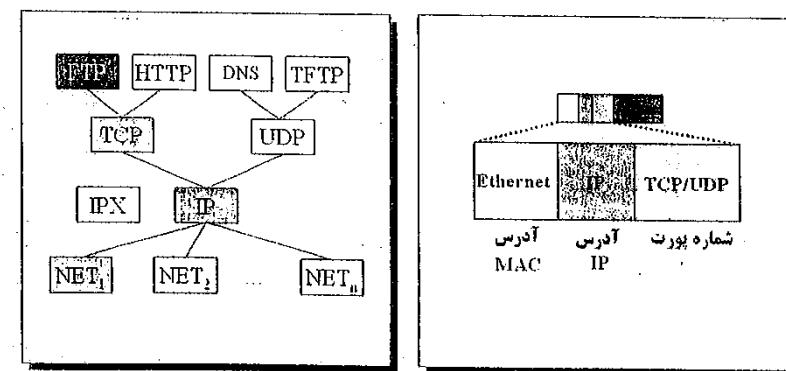
در این کتاب مدل دیگری را بررسی می کنیم که ترکیبی از دو مدل OSI و مدل TCP/IP است. در مدل ما، پنج لایه فیزیکی، پیوند داده، شبکه، انتقال و کاربرد وجود دارد که در فصلهای بعد در مورد هر کدام مفصلانه توضیح داده خواهد شد.



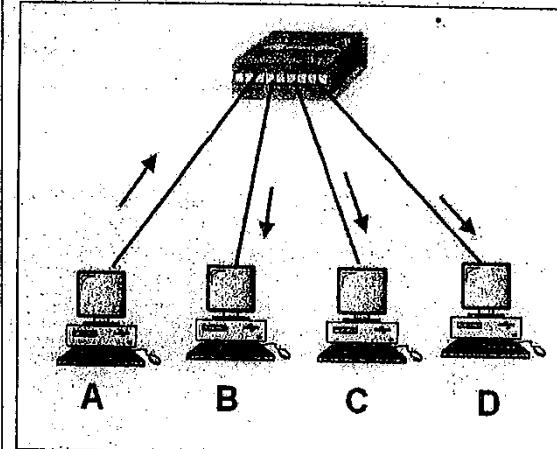
شکل(۲۰-۱)- مقایسه مدل TCP/IP با مدل OSI

پروتکلهای لایه کاربرد بر اساس نوع سرویسی که می خواهند، از یکی از دو پروتکل اتصالگرا و قابل اعتماد TCP و یا غیر اتصالگرا و غیرقابل اعتماد UDP استفاده می کنند. هر دو پروتکل TCP و UDP، از سرویسی که پروتکل IP در لایه پایینتر برایشان فراهم می کند استفاده می نمایند.

پروتکل IP با انواع پروتکلهای مختلف لایه پایینتر، سازگار است و اصولاً شبکه های مختلف تنها در دو لایه پایین با هم اختلاف دارند.



شکل(۲۱-۱)- مدل TCP/IP

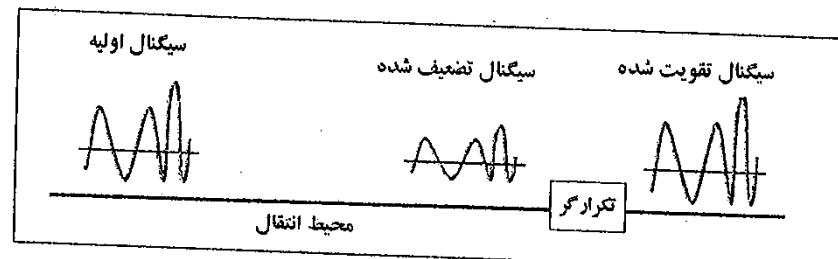


شکل(۱-۲۳)- هاب

۷- ابزارهای شبکه

در ادامه ابزارهای متدالوی که برای ایجاد شبکه‌ها استفاده می‌شوند را توضیح خواهیم داد:

تکرار کننده (Repeater) محیطهای ارتباطی به علت خواص فیزیکی خود، سیگنال را پس از طی مسافتی تضعیف می‌کنند به طوری که سیگنال اولیه دیگر قابل تشخیص نخواهد بود. بنابراین در فواصل مشخصی باید سیگنال را تقویت نماییم. تکرار کننده وسیله‌ای است که برای انتقال چندین سگمنت یک شبکه محلی به منظور افزایش وسعت مجاز آن شبکه مورد استفاده قرار می‌گیرد. هر تکرار کننده از درگاه ورودی خود داده‌ها را پذیرفته و با تقویت آنها، داده‌ها را به درگاه خروجی خود ارسال می‌کند (شکل(۱-۲۲)). یک تکرار کننده در لایه فیزیکی مدل OSI عمل می‌کند.



شکل(۱-۲۲)- تکرار کننده

هاب (Hub)

هاب ابزاری است که برای اتصال دو یا بیش از دو ایستگاه کاری به شبکه مورده استفاده قرار می‌گیرد و یک ابزار معمول برای اتصال کامپیوترهای شبکه است. هابها برای ایجاد شبکه محلی استفاده می‌شوند. یک هاب دارای چندین پورت است. وقتی اطلاعاتی در یک پورت وارد می‌شود به سایر پورتها کپی می‌شود تا اینکه تمامی سگمنت‌های شبکه محلی آن اطلاعات را بیینند. Hub را اصطلاحاً تکرار کننده چندپورته (Multiport Repeater) هم می‌گویند. بنابراین هاب نیز مانند تکرار کننده در لایه فیزیکی مدل OSI کار می‌کند. در شکل(۱-۲۳) طرز کار هاب نشان داده شده است.

00-0D-61-34-65-93

- کنترل دستیابی به رسانه یا MAC وظیفه کارت شبکه پیاده‌سازی مکانیزم MAC می‌باشد که لایه پیوند داده از آن برای منظم کردن دستیابی به رسانه شبکه استفاده می‌کند. مکانیزم‌های MAC در فصل سوم توضیح داده شده‌اند.

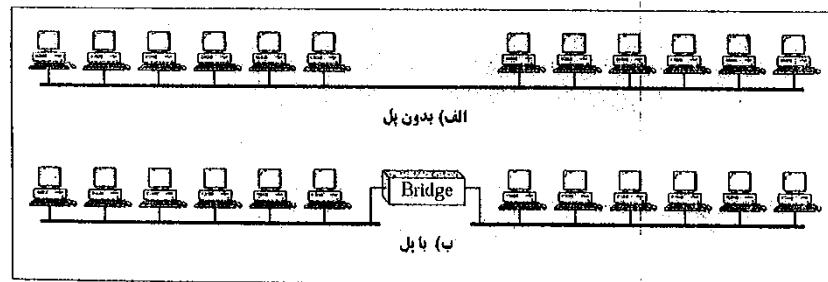
کارت شبکه را می‌توان از ابزارهای لایه Data link مدل OSI به شمار آورد.

(Bridge)

یک پل برای اتصال سگمنت‌های یک شبکه به یکدیگر مورد استفاده قرار می‌گیرد. پلها در لایه پیوند داده (Data link) عمل می‌کنند. پل‌ها فریم‌ها را بر اساس آدرس MAC مقصداًشان ارسال می‌کنند.

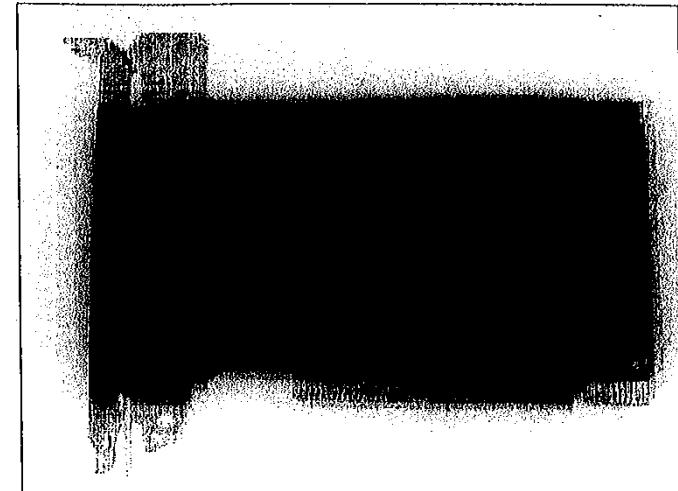
عملکرد پل عبارتست از تجزیه و تحلیل آدرس مقصد یک فریم ورودی و اتخاذ تصمیم مناسب برای ارسال آن به ایستگاه مربوطه. پل‌ها قادر به فیلتر کردن فریم‌ها می‌باشند. فیلتر کردن فریم برای حذف فریم‌های عمومی یا همگانی که غیر ضروری هستند مفید می‌باشد، بعضی از پل‌ها قابل برنامه‌ریزی هستند و می‌توان آنها را به گونه‌ای برنامه‌ریزی کرد که فریم‌های ارسال شده از طرف منابع خاصی را حذف کنند.

با تقسیم یک شبکه بزرگ به چندین سگمنت و استفاده از یک پل برای اتصال آنها به یکدیگر، توان عملیاتی شبکه افزایش خواهد یافت. پل‌ها موجب افزایش وسعت شبکه محلی می‌شوند. همچنین می‌توانند شبکه‌های با پروتکلهای مختلف را به هم‌دیگر متصل نمایند. مثلاً از آنها می‌توان برای اتصال یک شبکه Ethernet به یک شبکه Token Ring استفاده کرد.



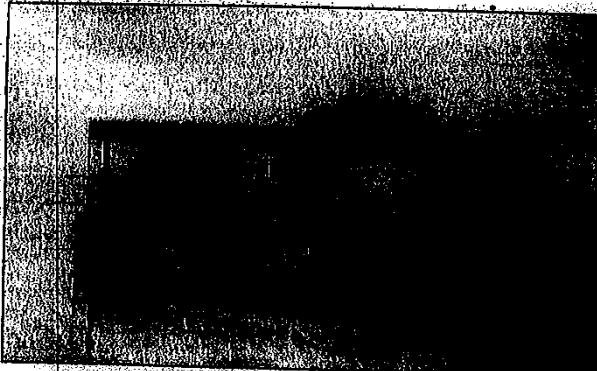
شکل (۱-۲۵)- کاربرد پل

در شکل (۱-۲۵) قسمت الف، همانطور که مشاهده می‌کنید، تعداد دوازده کامپیوتر در یک قطعه فیزیکی از شبکه قرار دارند و از یک کانال مشترک استفاده می‌کنند؛ همانطور که در فصلهای



شکل (۱-۲۴)- کارت شبکه

- به طور کلی می‌توان وظایف کارت شبکه را به صورت زیر خلاصه کرد:
- کپسوله کردن داده‌ها: کارت شبکه وظیفه دارد بسته‌های دریافت شده را به صورت فریم کپسوله کند. همچنین وظیفه خواندن فریمهای دریافت شده و انتقال آنها را به لایه شبکه دارد.
- کدگذاری و کدگشایی سیگنال‌ها: این ابزار وظیفه دارد فریمهای را جهت انتقال روی رسانه به سیگنال‌های مناسب (الکتریکی، نوری و ...) تبدیل کند و همچنین سیگنال‌های دریافتی را به اطلاعات باینری تبدیل نماید.
- بافر کردن داده‌ها: کارتهای شبکه در هر زمان فقط یک فریم داده را روی شبکه می‌فرستند یا از آن دریافت می‌کنند؛ بنابراین، بافری دارند که تا هنگام آماده شدن یک فریم برای پردازش، داده‌هایی که از طرف کامپیوتر یا شبکه دریافت می‌کنند را ذخیره می‌نمایند.
- تبدیل سریال به موازی و بر عکس؛ ارتباط بین کامپیوتر و کارت شبکه بصورت موازی است؛ (همزمان ۱۶ یا ۳۲ بیت)، اما ارتباطات شبکه بصورت سریال (بیت به بیت) است. لذا کارت شبکه مسئول تبدیل این دو روش انتقال است.



شکل (۱-۲۷). سوئیچهای سری ۲۹۵۰ شرکت CISCO

دو نوع سوئیچ وجود دارد که عبارتند از:

الف - سوئیچ Cut - through: این نوع سوئیچ، بلا فاصله پس از خواندن آدرس MAC مقصد ز روی بسته، آن را به سگمنت حاوی آدرس مقصد مذکور ارسال می‌کند؛ این در حالی است که فسمت باقی مانده بسته را از نظر خطایابی مورد بررسی قرار نمی‌دهد. مزیت آن سرعت بالای عمل سوئیچ می‌باشد.

ب - سوئیچ Store-and-forward: این نوع سوئیچ، ابتدا کل بسته را ذخیره کرده سپس آن را خطایابی می‌کند، اگر بسته‌ای دارای خطأ بود آن را حذف می‌کند، در غیر اینصورت آن بسته را به مقصد مربوطه ارسال خواهد کرد. این نوع سوئیچ برای شبکه محلی بسیار مناسبتر از نوع اول است زیرا بسته‌های اطلاعاتی خراب شده را پاکسازی می‌کند و به همین دلیل باعث کاهش بروز تصادم خواهد شد.

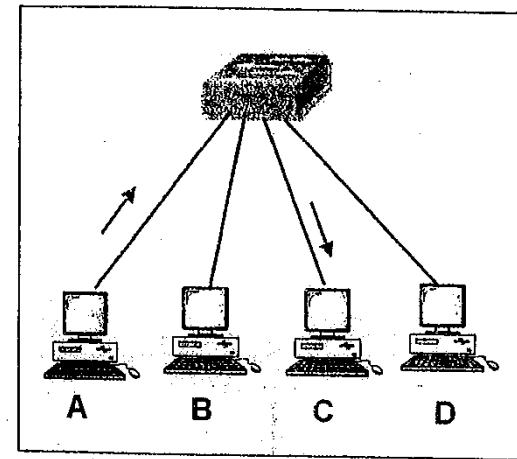
مسیریاب (Router)

در شبکه فرایند انتقال بسته‌های اطلاعاتی از یک منبع به مقصد، عمل مسیریابی است که توسط ابزاری تحت عنوان مسیریاب انجام می‌شود. مسیریابی یک عمل کلیدی در اینترنت و شامل تجزیه و تحلیل مسیر برای یافتن بهترین مسیر است. مسیریاب ابزاری است که شبکه‌های محلی را بهم متصل می‌کند و شبکه‌های بزرگتری را می‌سازد. این دستگاه، آدرس‌های منطقی (مانند آدرس

بعد خوهیم دید، در هر لحظه فقط یک کامپیوتر می‌تواند از کانال استفاده کند، به عبارت دیگر تعداد دوازده کامپیوتر بر سر تصاحب کانال به رقبات می‌پردازند. مطابق شکل، با تقسیم این شبکه به دو قطعه کوچکتر با استفاده از پل، در هر قطعه رقبات بین شش کامپیوتر وجود خواهد داشت.

سوئیچ (Switch)

سوئیچ نوع دیگری از ابزارهایی است که برای اتصال چند کامپیوتر و یا چند شبکه محلی به یکدیگر مورد استفاده قرار می‌گیرد که باعث افزایش توان عملیاتی شبکه می‌شود. سوئیچ وسیله‌ای است که دارایی درگاه‌های متعدد است که بسته‌ها را از یک درگاه می‌پذیرد، آدرس مقصد را بررسی می‌کند و سپس بسته‌ها را به درگاه مورد نظر که متعلق به ایستگاه میزبان با همان آدرس مقصد می‌پاشد، ارسال می‌کند. اغلب سوئیچ‌ها در لایه پیوند داده مدل OSI عمل می‌کنند.



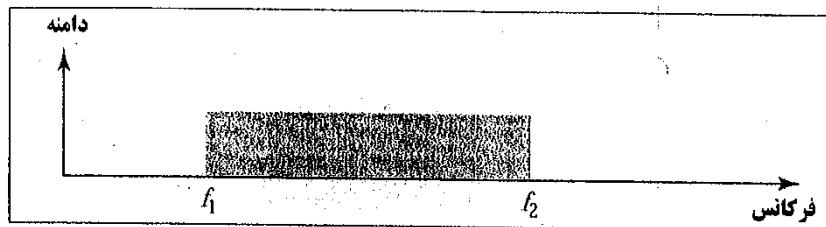
شکل (۱-۲۶). سوئیچ

سوئیچ‌ها بر اساس کاربردشان به دو دسته متقارن (Symmetric) و نامتقارن (Asymmetric) تقسیم می‌شوند.

در نوع متقارن، عمل سوئیچینگ بین سگمنت‌هایی که دارای پهنای باند یکسان هستند انجام می‌گردد یعنی 10 mbps به 10 mbps ... سوئیچ خواهد شد. اما در نوع نامتقارن این عملکرد بین سگمنت‌هایی با پهنای باند متفاوت انجام می‌شود.

۸- مفهوم پهنای باند

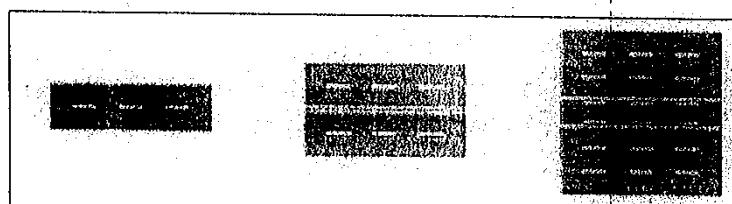
در تعریف آنالوگ، پهنای باند (Bandwidth) به تفاوت بین بالاترین و پایین‌ترین فرکانس‌هایی که از یک کانال می‌تواند عبور کند گفته می‌شود و واحد آن هرتز است. در تعریف دیجیتال، منظور از پهنای باند مقدار اطلاعاتی است که می‌تواند در یک مدت زمان معین ارسال شود و واحد آن بر حسب بیت بر ثانیه بیان می‌شود.



شکل (۱۰-۱)- پهنای باند آنالوگ

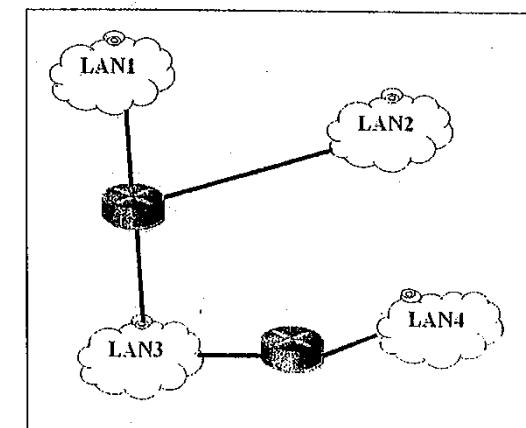
$$\text{Bandwidth} = f_2 - f_1$$

در حقیقت پهنای باند را می‌توان به تعداد باندهای یک اتوبان و یا قطر یک لوله آب تشبيه نمود. (شکل (۱۱-۱))



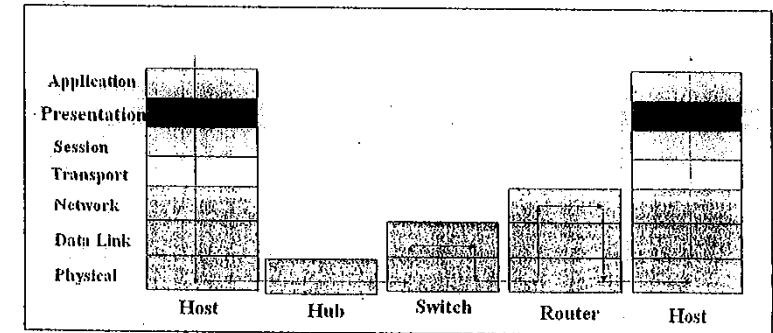
شکل (۱۱-۱)- مفهوم پهنای باند

(IP) را تشخیص داده و از روی آن با استفاده از جدولی موسوم به جدول مسیریابی می‌تواند بسته اطلاعاتی را به پورت خروجی مناسب هدایت نماید. مسیریاب در لایه شبکه مدل OSI کار می‌کند. در مورد مسیریابی در فصل چهارم بیشتر توضیح داده خواهد شد.



شکل (۱۱-۲)- نحوه اتصال چند LAN توسط مسیریاب

شکل (۱۲-۱) نحوه کار چند ابزار شبکه با توجه به مدل مرجع OSI در هر یک از لایه‌های این مدل را نشان می‌دهد:



شکل (۱۲-۱)- ابزارهای شبکه در لایه‌های مختلف مدل OSI

تاخیر کل در یک ند، جمیع چهار عامل فوق است:

$$d_{\text{nodal}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{trans}} + d_{\text{prop}}$$

اگر پهنای باند یک کانال R بیت بر ثانیه و سرعت انتشار آن S متر بر ثانیه باشد، طول یک بیت بر حسب متر برابر با S/R و طول یک بسته L بیتی، $L = S/R$ خواهد بود.

برای درک بهتر مفاهیم مذکور، به مثالهای عددی زیر توجه کنید:
مثال (۱) فرض کنید یک بسته ۲۰۰۰ بیتی از یک کانال با پهنای باند ۰.۰۵ مگابیت بر ثانیه و با

سرعت انتشار ۲۰۰ هزار کیلومتر بر ثانیه عبور کند. طول کل بسته چند متر خواهد بود؟

$$\begin{aligned} R &= 10 \text{ Mbps} \\ S &= 2 \times 10^8 \text{ m/s} \\ \text{Bit Length} &= S/R = 20 \text{ meters} \quad \rightarrow \text{Packet Length} = 2000 * 20 = 40 \text{ Km} \end{aligned}$$

بنابراین یک بسته ۲۰۰۰ بایتی در کانال مذکور، چهل کیلومتر طول خواهد داشت که عدد پسیار پزرگی است.

مثال (۲) یک فرستنده زمینی می‌خواهد مشابه شکل (۴۳-۲) از طریق یک ماهواره که در مدار GEO قرار گرفته است پیغامی را به ایستگاه گیرنده زمینی ارسال نماید. با فرض اینکه سرعت انتشار ۲۰۰ هزار کیلومتر بر ثانیه باشد، چه زمانی طول می‌کشد تا پیغام به آتن گیرنده برسد؟ (با فرض اینکه ماهواره پردازشی روی اطلاعات انجام نمی‌دهد).
فاصله ماهواره GEO از سطح زمین حدود ۳۶۰۰ کیلومتر است. بنابراین زمان تاخیر انتشار از ایستگاه فرستنده زمینی تا ماهواره برابر خواهد بود با:

$$\begin{aligned} d &= 36000 \text{ Km} \\ S &= 200000 \text{ Km/s} \\ d_{\text{prop}} &= d/S = 0.18 \text{ second} \end{aligned}$$

$$\frac{d}{S} = \frac{36 \times 10^3}{200 \times 10^3} = 1.8 \times 10^{-2} = 0.18 \text{ second}$$

زمان کل تاخیر، دو برابر این زمان یعنی برابر با ۳۶ صدم ثانیه یا ۳۶۰ میلی ثانیه خواهد بود.

۹- تحلیل تاخیر در شبکه

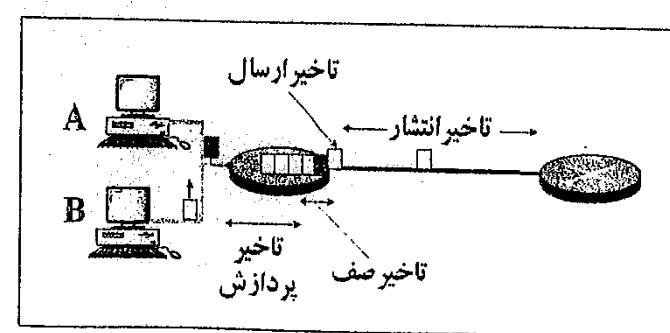
یکی از بحثهای بسیار اساسی در تحلیل کارایی شبکه و پروتکلهای تاخیر می‌باشد. همانطور که می‌دانیم، یک بسته اطلاعاتی از هنگامی که از مبدأ سفر خود را آغاز می‌نماید تا زمانی که به مقصد می‌رسد، از سویچها و روترهای بسیاری ممکن است عبور نماید. به طور کلی یک بسته اطلاعاتی ممکن است از طرف چهار عامل دچار تاخیر گردد (شکل (۴۶-۲)). این تاخیرها عبارتند از:

- تاخیر پردازش (Processing Delay). زمانی که لازم است تا سرآیند یک بسته بازرسی شود و لینک خروجی مشخص گردد و همچنین بیتها کنترل خطای چک شوند.

- تاخیر صف بندی (Queueing Delay). از آنجا که ممکن است بسته‌های زیادی در داخل یک صف مریوط به یک کانال واحد منتظر ارسال باشند، زمانی لازم است تا بسته مورد نظر به ابتدای صف برسد. این زمان را زمان تاخیر صف بندی می‌گویند.

- تاخیر ارسال (Transmission Delay). زمانی که لازم است تا کل بیتها یک بسته L بیتی از طریق یک کانال با پهنای باند R بیت بر ثانیه ارسال شوند. این زمان برابر با L/R خواهد بود.

- تاخیر انتشار (Propagation Delay). زمانی که لازم است تا یک بیت از ابتدای کانال به انتهای آن برسد. این زمان بستگی به طول کانال و سرعت انتشار سیگنال در کانال دارد. سرعت انتشار به محیط فیزیکی کانال (فیبرنوری، کابل مسی، ماهواره، ...) وابسته است و عددی بین ۲۰۰ هزار کیلومتر بر ثانیه تا ۳۰۰ هزار کیلومتر بر ثانیه می‌باشد. اگر d طول کانال و S سرعت انتشار آن باشد، زمان تاخیر انتشار برابر با d/S خواهد بود.



شکل (۴۶-۲)- انواع تاخیر در شبکه

۷- کدامیک از واحدهای داده زیر در لایه شبکه استفاده می گردد؟

- | | |
|-------------|------------|
| Frame (ب) | Bit (الف) |
| Segment (د) | Packet (ج) |

۸- واحد انتقال اطلاعات در لایه پیوند داده چیست؟

- | | |
|-------------|------------|
| Frame (ب) ✓ | Bit (الف) |
| Segment (د) | Packet (ج) |

۹- واحد اطلاعاتی در لایه فیزیکی چیست؟

- | | |
|-------------|------------|
| Frame (ب) | Bit (الف) |
| Segment (د) | Packet (ج) |

۱۰- کدام لایه در مدل OSI مسئولیت تشخیص خط را برعهده دارد؟

- | | |
|-----------------|----------------|
| Data link (ب) ✓ | Physical (الف) |
| Transport (د) | Network (ج) |

۱۱- کدامیک از عبارات زیر یک شبکه محلی (LAN) را بهتر توصیف من نماید؟

- (الف) یک شبکه که محدوده بیشتری نسبت به یک شبکه WAN را تحت پوشش قرار می دهد.
- (ب) یک شبکه که ایستگاه ها، ترمینال ها و سایر دستگاه های موجود در یک محدوده جغرافیائی وسیع را به یکدیگر متصل می نماید.
- (ج) یک شبکه که ایستگاه ها، ترمینال ها و سایر دستگاه های موجود در یک محدوده جغرافیائی محدود را به یکدیگر متصل می نماید.
- (د) یک شبکه که کاربران آن در یک محدوده جغرافیائی وسیع توزیع و به کمک امکانات متفاوت انتقال داده، اطلاعات خود را بین یکدیگر مبدل می نمایند.

۱۲- کدامیک از واژه های زیر بیانگر میزان کرفیت انتقال داده در یک شبکه است؟

- | | |
|-----------------|-----------------|
| Delay (ب) | Baud rate (الف) |
| Bandwidth (د) ✓ | Base band (ج) |

خود آزمایی:

۱- پروتکل IP یا Internet Protocol به کدام لایه مدل مرجع OSI مرتبه است؟

- | | |
|-------------------------|---------------------------|
| الف) Network (لایه سوم) | ب) Transport (لایه چهارم) |
| ج) Session (لایه پنجم) | د) Data link (لایه دوم) |

۲- طبقه بندی شبکه ها از نظر تکنولوژی انتقال در کانال، کدام است؟

- | | |
|-----------------------|-----------------------|
| الف) پخشی- محلی | ب) پخشی- گسترده |
| ج) نقطه به نقطه- محلی | د) نقطه به نقطه- پخشی |

۳- کدام لایه مدل مرجع OSI، مسئولیت رمزگاری و فشرده سازی اطلاعات را در ارتباطات شبکه ای بر عهده دارد؟

- | | |
|---------------------------|-----------------------|
| الف) Application (کاربرد) | ب) Transport (انتقال) |
| ج) Presentation (نمایش) | د) Session (اجلاس) |

۴- کدامیک از دستگاه های شبکه ای زیر متعلق به لایه فیزیکی (لایه اول) است؟

- | | |
|-------------------|------------|
| الف) Repeater (ب) | Router (ج) |
| ج) Bridge (د) | Switch (ه) |

۵- کدامیک از دستگاه های شبکه ای زیر متعلق به لایه پیوند داده (لایه دوم) است؟

- | | |
|-------------------|------------|
| الف) Repeater (ب) | Hub (د) |
| ج) Switch (ه) | Router (ه) |

۶- کدامیک از دستگاه های شبکه ای زیر متعلق به لایه شبکه (لایه سوم) است؟

- | | |
|-----------------|-------------|
| الف) Bridge (ب) | Router (ج) |
| ج) Switch (ه) | هیچکدام (د) |

۱۸- مسئولیت تحویل تکه به تکه (Hop to Hop) به عده کدام لایه است؟

- | | |
|---------------|---------------|
| Data Link (۷) | Network (۶) |
| Physical (۵) | Transport (۴) |
- الف) (۷)
ب) (۶)
ج) (۴)

۱۹- لایه بینها را به سیگنال تبدیل میکند.

- | | |
|--------------|---------------|
| Physical (۷) | Data Link (۶) |
| Session (۵) | Network (۴) |
- الف) (۷)
ب) (۶)
ج) (۴)

۲۰- فردن گنید یک بسته ۱۰۰۰ بیتی از یک کانال با پهنای باند امکانیت بر ثالثیه و با سرعته انتشار

هزار کیلومتر بر ثالثیه عبور کند. یکت بایت از این بسته چند متر طول خواهد داشت؟

- الف) ۲۰ متر ب) ۲ متر ۷) ۱۶۰ متر ۵) ۶ متر

۲۱- کدامیک از عبارات زیر در ارتباط با شبکه های LAN درست است؟

- الف) امکان ارتباط فیزیکی دستگاه های متفاوتی را فراهم می نمایند.
ب) یک حوزه جغرافیائی محدود را پوشش می دهند.
ج) کاربران متعددی به محیط انتقالی با پهنای باند بالا دستیابی خواهند داشت.

- ۷) تمام موارد

۲۲- کدامیک از عبارات زیر در ارتباط با شبکه های WAN درست است؟

- الف) امکان دستیابی از طریق اینترفیس های سریال و با سرعت پایین را فراهم می کنند.
ب) یک محدوده جغرافیائی وسیع را پوشش می دهند.
ج) امکان ارتباط تمام وقت و یا پاره وقت را فراهم می نمایند.

- ۷) تمام موارد

۲۳- کدامیک از عبارات زیر درست است؟

- الف) در توپولوژی Star تمام کامپیوترها به یک نقطه متصل می گردند.
ب) در توپولوژی Bus، از یک کابل به عنوان ستون فقرات شبکه استفاده می شود.
ج) در توپولوژی Ring، هر کامپیوتر و یا Host به کامپیوتر بعدی و آخرین کامپیوتر به اولین کامپیوتر متصل می گردد.

- ۷) تمام موارد

۲۴- کدام توپولوژی به یک کنترل کننده مرکزی یا Hub نیازمند است؟

- | | |
|----------|----------|
| Star (۷) | Ring (۶) |
| Mesh (۵) | Bus (۴) |

۲۵- ارتباط بین صفحه کلید و کامپیوتر از کدام نوع است؟

- | | |
|-----------------|-----------------|
| Half-Duplex (۷) | Simplex (۶) |
| Automatic (۵) | Full-duplex (۴) |
- الف) (۷)
ب) (۶)
ج) (۴)

فصل دوم

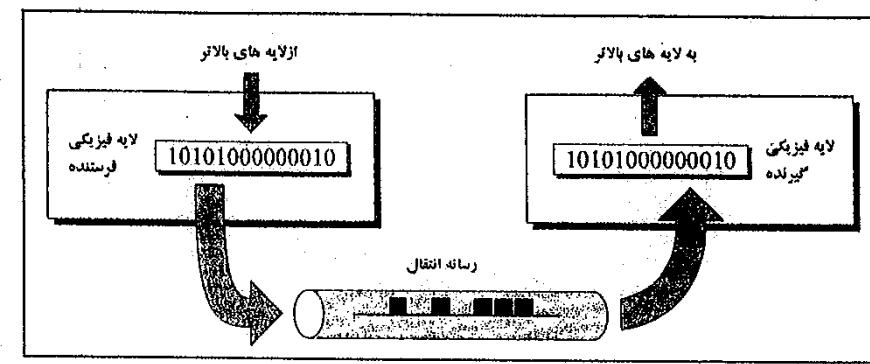
لایه فیزیکی

μ

D

۱- مقدمه

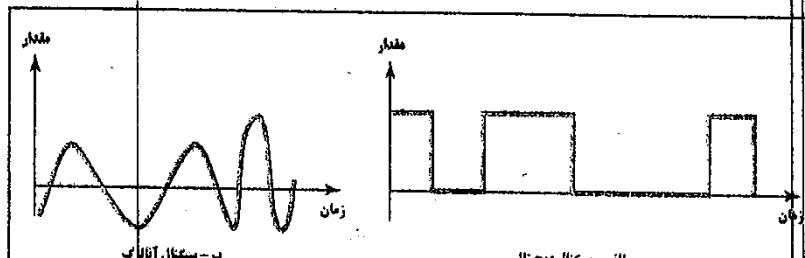
لایه فیزیکی اغماالی را که برای انتقال رشته‌ای از بیتها بر روی یک رسانه انتقال (با سیم یا بی‌سیم) لازم است، هماهنگ می‌نماید. این لایه با خصوصیات مکانیکی و الکتریکی واسطه و محیط انتقال سروکار دارد. همچنین در این لایه رویدهایی که لازم است دستگاههای فیزیکی انجام دهند تا انتقال صورت گیرد تعریف می‌شوند. شکل (۲-۱) وضعیت لایه فیزیکی را در رابطه با محیط انتقال نشان می‌دهد.



شکل (۲-۱)- لایه فیزیکی

۲- سیگنالهای آنالوگ و دیجیتال

داده می‌تواند آنالوگ یا دیجیتال باشد. به عنوان مثال، صدای انسان یک داده آنالوگ است. هنگام صحبت کردن، یک موج آنالوگ در هوا ایجاد می‌گردد. این موج را می‌توان توسط یک میکروفون به یک سیگنال الکتریکی تبدیل نموده، توسط یک سیم انتقال داد. دوباره می‌توان سیگنال آنالوگ الکتریکی حاصل را به یک بلندگو اعمال نموده و امواج صوتی تولید کرد. مثالي از داده دیجیتال می‌تواند داده‌های ذخیره شده در حافظه کامپیوتر به فرم صفر و یک باشد. این داده‌ها را می‌توانیم به فرمت دیجیتال از یک کابل عبور دهیم و یا اینکه با مدولاسیون به آنالوگ تبدیل کرده از طریق یک محیط انتقال به کامپیوتر دیگری ارسال نماییم. در شکل (۲-۲)



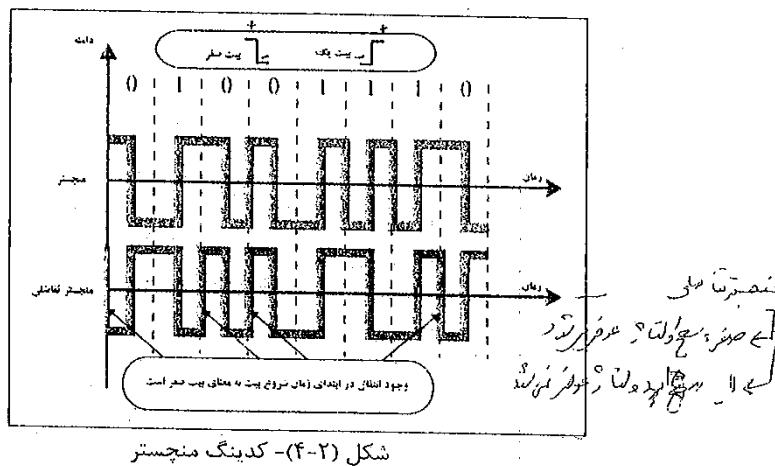
شکل (۲-۲)- سیگنالهای دیجیتال و آنالوگ

۱۴- روش‌های کدینگ و مدولاسیون

یکی از راه حل‌هایی که برای این مشکل وجود دارد، استفاده از روش‌های کدینگ است که در آنها در وسط هر بیت یک انتقال وجود دارد. روش‌های کدینگ قطبی از این خاصیت استفاده می‌کنند.

اکنون یکی از مشهورترین روش‌های کدینگ قطبی به نام کدینگ منچستر که در شبکه اترنت (Ethernet) استفاده می‌شود را توضیح می‌دهیم.

در این نوع کدینگ برای نشان دادن هر بیت از دو سطح ولتاژ مثبت و منفی استفاده می‌شود. به طوری که بیت صفر، به صورت یک لبه پایین رونده از سطح ولتاژ مثبت به سطح ولتاژ منفی و بیت یک به صورت یک لبه بالارونده از سطح ولتاژ منفی به سطح ولتاژ مثبت نشان داده می‌شود. این لبه در وسط زمان بیت قرار گرفته است و برای حصول همزمانی در ارسال و دریافت استفاده می‌شود. شکل دیگری از این نوع کدینگ وجود دارد که به کدینگ منچستر تفاصلی مشهور است. در این حالت، بیتهاي صفر و یک با وارونه شدن و یا وارونه نشدن در ابتدای زمان هر بیت مشخص می‌شوند؛ به طوری که اگر در ابتدای زمان شروع بیت، انتقال داشته باشیم، نشانگر وجود بیت صفر است. شکل (۲-۴) کدینگ منچستر و منچستر تفاصلی را نشان می‌دهد.



شکل (۲-۴)- کدینگ منچستر

ب- کدینگ بلوکی

این نوع کدینگ برای بهبود کارایی کدینگ خطی ارائه شد. در این نوع کدینگ، ابتدا رشته بیتی داده شده به صورت m بیتی دسته‌بندی شده و سپس هر بلوک m بیتی با اضافه کردن چند بیت اضافی جهت حصول همزمانی و همچنین کنترل خط، به یک بلوک n بیتی تبدیل

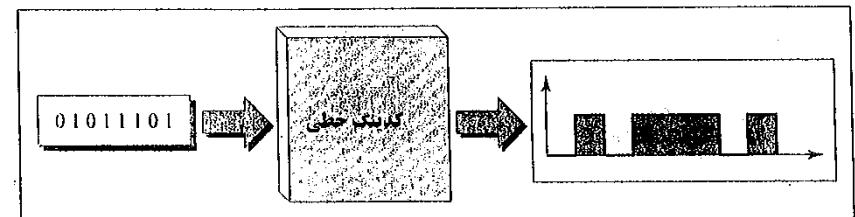
الف- کدینگ خطی

منظور از کدینگ خطی، تبدیل یک داده دودویی یا رشته‌ای از بیتها به یک سیگنال دیجیتال است. داده، متن، اعداد، تصاویر، صوت و ویدئو همه در حافظه کامپیوتر بصورت رشته‌ای از بیتها ذخیره می‌شوند. با استفاده از کدینگ خطی می‌توان این رشته بیتها را به یک سیگنال دیجیتال تبدیل نموده از جایی به جای دیگر انتقال داد. شکل (۲-۲) مفهوم کدینگ خطی را نشان می‌دهد.

انواع زیادی از این نوع کدینگ جود دارد که می‌توان آنها را به سه دسته تقسیم نمود: تک قطبی (Unipolar): در این نوع کدینگ از یک سطح ولتاژ (علاوه بر سطح صفر) استفاده می‌شود.

قطبی (Polar): در این نوع کدینگ از دو سطح ولتاژ (مثبت و منفی) استفاده می‌شود.

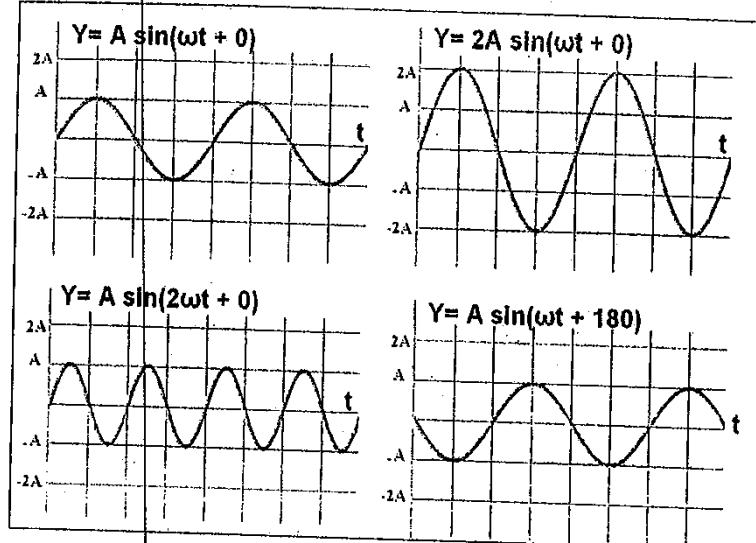
دوقطبی (Bipolar): در این نوع کدینگ از سه سطح ولتاژ استفاده می‌شود.



شکل (۲-۲)- کدینگ خطی

روش کدینگی که تاکنون با آن کار کردہ‌ایم، یعنی روشی که از سطح ولتاژ صفر برای نشان دادن بیت صفر و از سطح ولتاژ بالاتر (معمولاً پنج ولت) برای نشان دادن بیت یک استفاده می‌کنیم، یک نوع کدینگ تک قطبی است عیوبی که این روش دارد این است که اگر در هنگام ارسال، یک رشته متولّی بیت صفر و یا یک رشته متولّی بیت یک داشته باشیم، از آنجا که اسیلانتور کلار گیرنده از روی تغییرات موجود در رشته بیت خود را تنظیم می‌کند، ممکن است که همزمانی بین فرستنده و گیرنده به هم خورده و در نتیجه گیرنده نتواند تعداد بیتهاي صفر یا یک را به درستی تشخیص دهد.

که در آن A دامنه موج $\omega = 2\pi f$ ضریبی از فرکانس و ϕ فاز موج سینوسی را نشان می‌دهد. در شکل (۴-۲) یک موج سینوسی و تغییرات دامنه و فرکانس و فاز نشان داده است.



شکل (۴-۲)- تغییرات دامنه، فرکانس و فاز در موج سینوسی

در اینجا مدولاسیون سیگنالهای دیجیتال را بحث می‌کنیم که به این نوع مدولاسیون، Shift Keying گفته می‌شود. در این نوع مدولاسیون، خصوصیات یک موج سینوسی به نام سیگنال حامل بر اساس مقادیر یک رشته دیجیتال تغییر داده می‌شود. بر حسب اینکه کدام مشخصه سیگنال حامل (دامنه، فرکانس یا فاز) تغییر می‌یابد، سه نوع مدولاسیون FSK، ASK و یا PSK را خواهیم داشت.

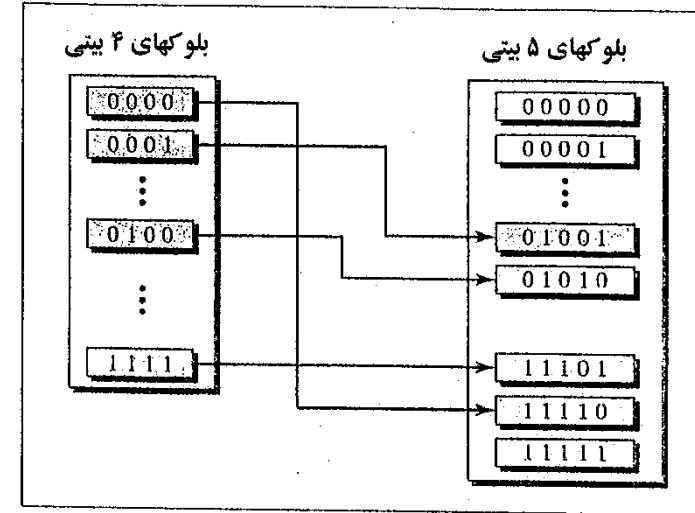
در شکل (۴-۳)، یک رشته بیت و معادل مدوله شده آن به سه روش فوق را مشاهده می‌نمایید.

۵- نمودار صورت فلکی و تلفیق مدولاسیونها

نمودار دیگری موسوم به صورت فلکی برای نمایش فازها و دامنه‌ها وجود دارد. این نمودار می‌توان مشابه مختصات قطبی تصور کرد که در آن هر نقطه توسط فاصله آن از مبدأ و زاویه آن؛ محور افق مشخص می‌گردد.

می‌گردد. در نهایت هر کدام از بلوکهای n بیتی با استفاده از کدینگ خطی به سیگنال دیجیتال تبدیل می‌شوند.

از مشهورترین روش‌های کدینگ بلوکی می‌توان $B/5B$ و $4B/10B$ را نام برد. در شکل (۴-۳) کدینگ $B/5B$ نشان داده شده است. در این نوع کدینگ مثلاً برای به جای ارسال چهار بیت ۰۰۰۰، پنج بیت ۱۱۱۱۰ ارسال می‌گردد. بدین ترتیب از ۳۲ حالت تنها ۱۶ حالت مجاز خواهد بود که این خود می‌تواند به تشخیص خطأ کمک نماید.



شکل (۴-۳)- کدینگ بلوکی

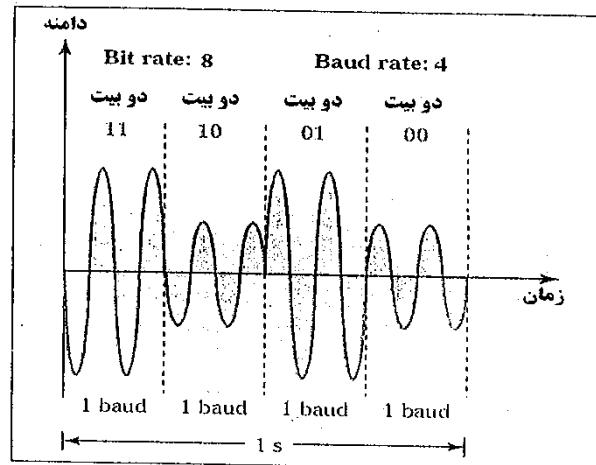
۶- مدولاسیون

مدولاسیون عملی است که در آن یک یا چند مشخصه یک سیگنال آنالوگ بر اساس اطلاعات یک سیگنال دیجیتال تغییر داده می‌شود. هنگامی که می‌خواهیم داده را از یک کامپیوتر به یک سیگنال دیجیتال انتقال دهیم، از آنجا که خطوط تلفن آنالوگ هستند و برای انتقال صوت طراحی شده‌اند، باید داده را به نحوی تغییر دهیم تا از طریق این خطوط قابل انتقال باشند. این کار در مودم انجام می‌گردد.

همانطور که می‌دانیم یک موج سینوسی با سه مشخصه توصیف می‌شود: دامنه، فرکانس و فاز. به عبارت دیگر یک موج سینوسی را می‌توان با رابطه زیر نشان داد:

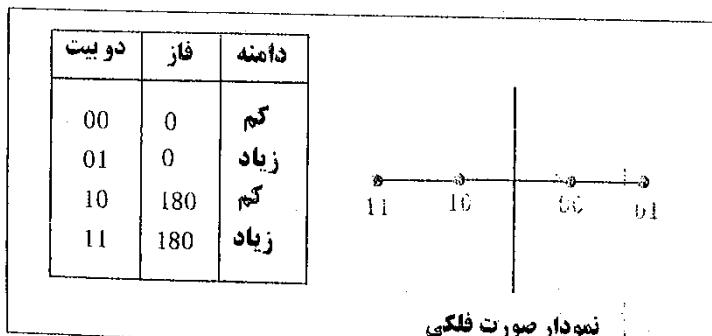
$$Y = A \sin(\omega t + \phi)$$

شکل موج ارسال شده است. همانطور که مشاهده می‌کنید برای نمایش دو بیت ۰۰، از دامنه کم و فاز صفر، برای نمایش ۰۱، دامنه زیاد و فاز صفر، برای نمایش ۱۰، دامنه کم و فاز 180° درجه و برای نمایش ۱۱، دامنه زیاد و فاز 180° درجه بکار رفته است. همانطور که مشاهده می‌گردد با این کار نرخ **Baud** کاهش یافته و به نصف رسیده است؛ زیرا تعداد بیت بر ثانیه دو برابر تعداد تغییرات سیگنال بر ثانیه است. این کار باعث می‌شود که سیگنال ارسالی پهنای باند کمتری اشغال کند.

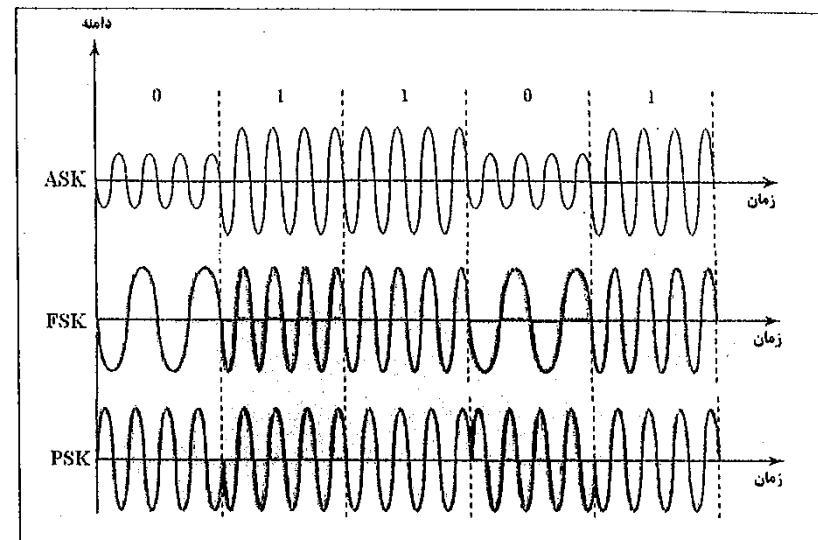


شکل (۹-۲)- تلفیق مدولاسیونها

نمودار صورت فلکی معادل شکل فوق در شکل (۱۰-۲) نشان داده شده است.

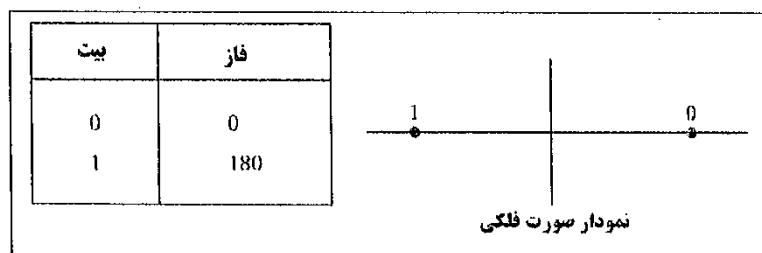


شکل (۱۰-۲)- نمودار صورت فلکی برای مدولاسیون QAM



شکل (۷-۲)- مدولاسیون

در شکل (۸-۲) نحوه نمایش دو نقطه معادل بیتهاي ۰ و ۱ توسط نمودار صورت فلکی نشان داده شده است. وقت کنید که نقطه ۰ دارای زاویه صفر با محور افق، و نقطه ۱ دارای زاویه 180° درجه با این محور است.

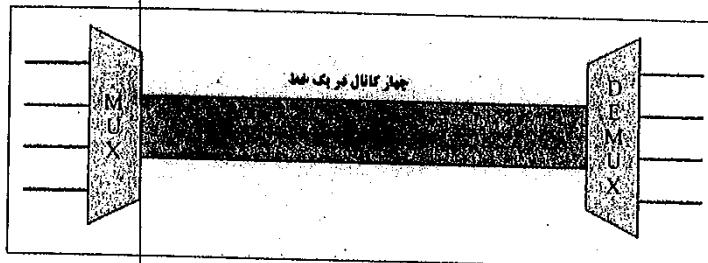


شکل (۸-۲)- نمودار صورت فلکی برای مدولاسیون فاز

با استفاده از تلفیق مدولاسیونها می‌توان سرعت انتقال را بالا برد. مثلاً می‌توان مدولاسیونهای PSK و QAM را تلفیق کرده و به جای یک شکل موج برای هر بیت، برای چند بیت یک شکل موج ارسال نمود. به این نوع مدولاسیون QAM گفته می‌شود. در شکل (۹-۲) به ازای هر دو بیت یک

۴- روش‌های تسهیم‌سازی (Multiplexing)

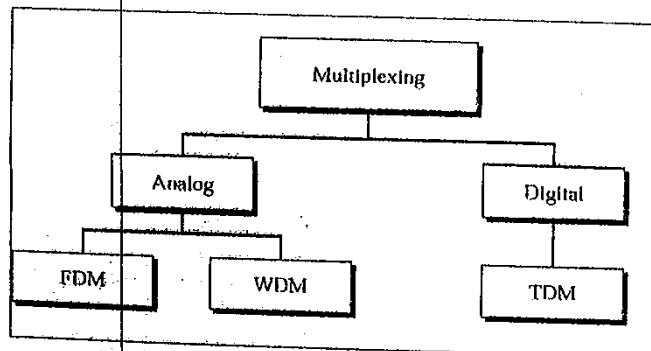
تسهیم‌سازی به مجموعه تکنیکهایی گفته می‌شود که اجازه می‌دهند چند سیگنال به طور مشترک از یک کانال منفرد استفاده کنند. (شکل ۱۲-۲))



شکل (۱۲-۲)- تسهیم سازی

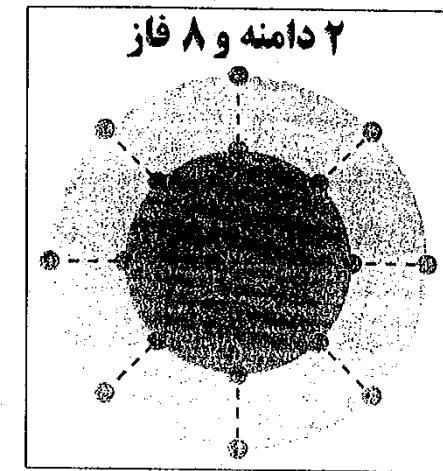
- سیگنالها را می‌توان بر اساس سه تکنیک تسهیم سازی کرد
- تسهیم سازی بر اساس تقسیم فرکانس یا **FDM**
- تسهیم سازی بر اساس تقسیم طول موج یا **WDM**
- تسهیم سازی بر اساس تقسیم طول زمان یا **TDM**

دو تکنیک اول برای سیگنالهای آنalog و تکنیک آخر برای سیگنالهای دیجیتال استفاده می‌شود. شکل (۱۳-۲) این تقسیم بندی را نشان می‌دهد.



شکل (۱۳-۲)- انواع روش‌های تسهیم سازی

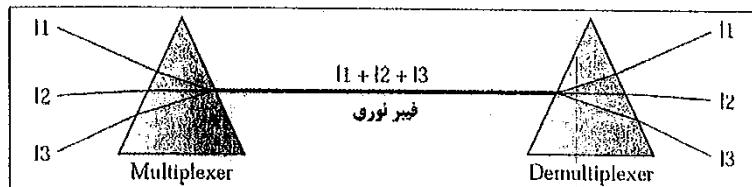
همانگونه که مشاهده می‌شود، این نمودار دارای چهار نقطه به تعداد حالت‌هایی که دو بیت می‌توانند اختیار کنند، می‌باشد. به طور کلی اگر به ازای هر n بیت یک شکل موج داشته باشیم، نمودار صورت فلکی دارای 2^n نقطه خواهد بود. در شکل (۱۱-۲) نمودار صورت فلکی با ۱۶ نقطه که تلفیقی از دو دامنه و ۸ فاز مختلف می‌باشند، نشان داده شده است. در این حالت سرعت انتقال داده چهار برابر می‌گردد.



شکل (۱۱-۲)- نمودار صورت فلکی با ۱۶ نقطه

ب- تکنیک WDM

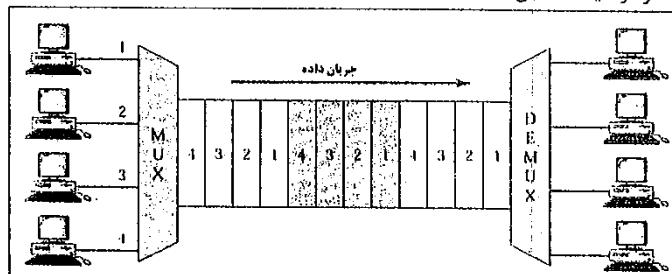
این تکنیک به منظور استفاده بهینه از پهنای باند فیبرهای نوری طراحی شده و مخصوص سیگنالهای نوری می‌باشد. در این تکنیک، نورهای با طول موجه‌های مختلف را ترکیب نموده و یک نور ترکیبی حاصل می‌گردد. در طرف گیرنده می‌توان نورهای اولیه را جداسازی نمود. همانطور که در شکل(۱۵-۲) نشان داده شده است، عمل تلفیق در فرستنده و جداسازی در گیرنده را می‌توان با منشورهایی که در زاویه مناسبی قرار گرفته‌اند انجام داد.



شکل(۱۵-۲)- تسهیم سازی WDM

ج- تکنیک TDM

همانطور که قبلاً اشاره شد، این روش تسهیم سازی برای ترکیب سیگنالهای دیجیتال استفاده می‌شود. در این روش تمام کانال برای لحظاتی از زمان در اختیار کاربر(سیگنال) خاصی قرار دارد. تلفیق سیگنالها معمولاً به صورت بایت به بایت می‌باشد به طوری که مثلاً برای تسهیم سازی سه سیگنال دیجیتال S1 و S2 و S3، ابتدا بایت اول از سیگنال S1، سپس بایت اول از سیگنال S2 و سپس بایت اول از سیگنال S3 و در ادامه بایت دوم از S1 و به همین ترتیب ارسال می‌گرددند. شکل (۱۶-۲) بیانگر توضیحات قبل است.



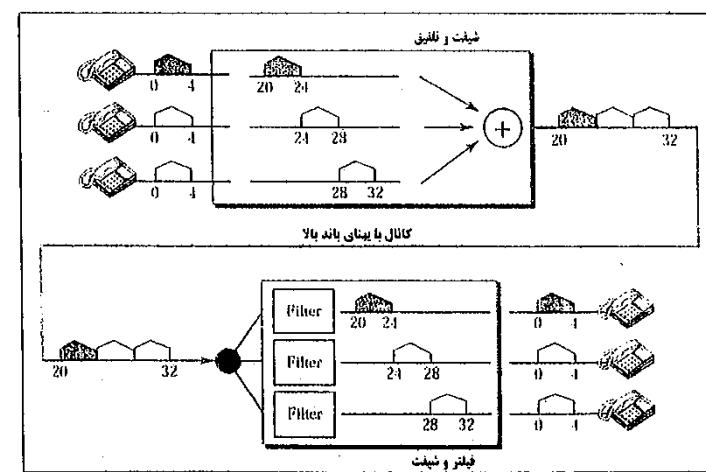
شکل(۱۶-۲)- تسهیم سازی TDM

اکنون به شرح منصادر هر کدام از روش‌های فوق خواهیم پرداخت:

الف- تکنیک FDM

یک تکنیک آنالوگ است و هنگامی استفاده می‌شود که پهنای باند یک کانال (بر حسب هرتز)، بزرگتر از مجموع پهنای باند سیگنالهایی باشد که می‌خواهیم ارسال نماییم. در تسهیم سازی FDM، محدوده‌ای از فرکانسها در تمام طول زمان به یک کاربر(سیگنال) خاص اختصاص دارد. در این روش سیگنالهایی را که می‌خواهیم باهم ترکیب کنیم، از طریق شیفت فرکانسی به باند مورد نظر برد و با در نظر گرفتن فاصله مناسب بین طیفهای دو سیگنال به عنوان باند محافظ، آنها را ارسال می‌کنیم. استفاده از باند محافظ به دلیل سهولت فیلتر کردن در طرف گیرنده می‌باشد زیرا عموماً فیلترهای میان گذر ایده‌آل نیستند و قسمتی از فرکانسها طیفهای مجاور را نیز عبور می‌دهند.

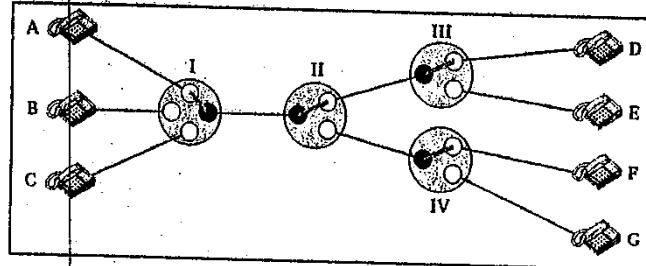
به عنوان مثال در شکل(۱۴-۲)، سه سیگنال صوتی با پهنای باند چهار کیلوهرتز پس از شیفت فرکانسی از یک کانال با پهنای باند دوازده کیلوهرتز (۲۰ تا ۳۲ کیلوهرتز) عبور داده شده‌اند. در طرف گیرنده نیز با فیلتر کردن و شیفت فرکانسی می‌توان سیگنالهای اولیه را بازیابی نمود. در این شکل چنین به نظر می‌رسد که باند محافظ در نظر گرفته نشده است اما در واقع چنین نیست؛ چراکه باند محافظ در داخل همان چهار کیلو هرتز در نظر گرفته شده است اما در واقع چون پهنای باند سیگنال صحبت انسان حدود ۳۳۰۰ هرتز می‌باشد.



شکل(۱۴-۲)- تسهیم سازی FDM

۵- روش‌های سوئیچینگ (راه‌گزینی)

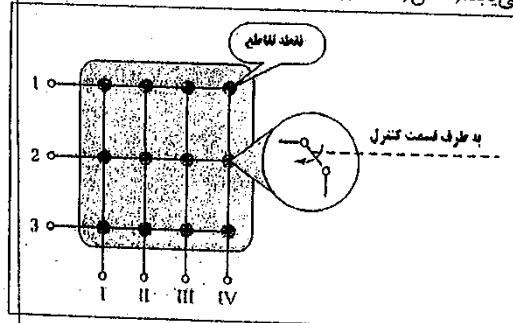
منتظر از سوئیچینگ، اتصال موقت دو نقطه (یک پورت ورودی و یک پورت خروجی) به منظور انتقال اطلاعات می‌باشد و با مفهوم مسیریابی (Routing) کاملاً متفاوت است. شاید این بحث به شبکه تلفن برمری گردد. به عنوان مثال در شکل (۱۹-۲) اگر شخص A بخواهد با شخص D مکالمه کند، باید سوئیچهای میانی I و II و III مطابق شکل بسته شوند.



شکل (۱۹-۲)- مفهوم راه‌گزینی

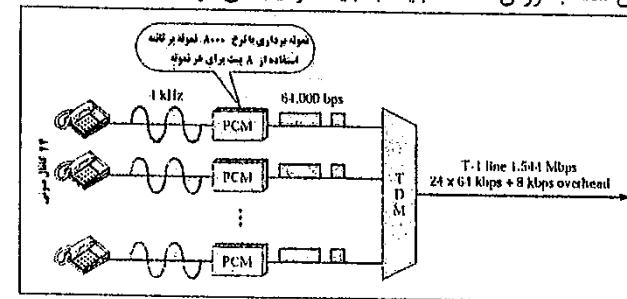
قبل از اینکه به بحث روش‌های سوئیچینگ بپردازیم، اجازه بدھید خود مفهوم سوئیچ را بیشتر توضیح دهیم.

یک سوئیچ را می‌توان به صورت یک Crossbar با n ورودی و m خروجی در نظر گرفت؛ به طوری که برای اتصال یک ورودی به یک خروجی باید نقطه‌ای (مثلاً یک ترانزیستور) بسته شود. واضح است که در این حالت با افزایش خطی تعداد ورودیها و خروجیها، تعداد ترانزیستورها به صورت نمایی افزایش می‌یابد. (شکل (۲۰-۲))



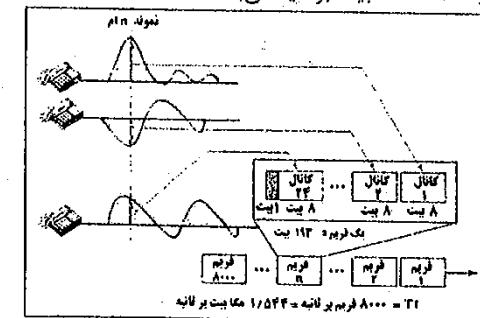
شکل (۲۰-۲)- سوئیچ

در بسیاری از موارد می‌خواهیم چند سیگنال آنalog مانند صوت انسان را به روش TDM ترکیب نماییم، به عنوان مثال در خطوط T1، ۲۴ سیگنال صوتی را با تکنیک TDM ترکیب می‌کنند. همانطور که در شکل (۱۷-۲) نشان داده شده است، روش کار بدین ترتیب است که ابتدا باید سیگنالهای آنalog مذکور را نمونه برداری کرد. بر طبق قضیه نایکوئیست سرعت نمونه برداری باید حداقل دو برابر پهنای باند سیگنال آنalog مربوطه باشد. بنابراین در مورد یک سیگنال صوتی با پهنای باند چهار کیلوهرتز، باید ۸۰۰۰ نمونه در ثانیه گرفته شود. اگر برای هر نمونه ۸ بیت در نظر گرفته شود، یک سیگنال دیجیتال با نرخ ۶۴۰۰۰ بیت بر ثانیه حاصل می‌گردد. سپس سیگنالهای دیجیتال حاصل شده به روش TDM، باید به بایت ترکیب می‌شوند.



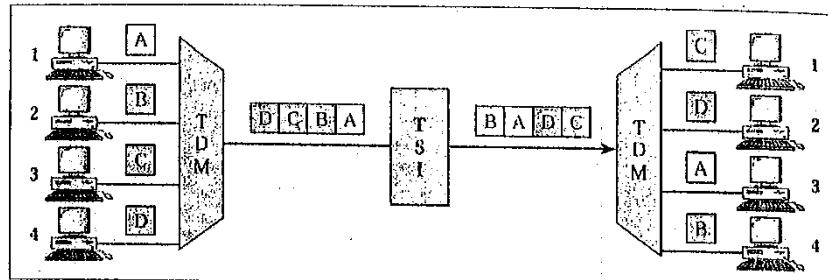
شکل (۱۷-۲)- در خطوط T1

در شکل (۱۸-۲) این مفاهیم به صورت دیگری نشان داده شده است. در این شکل نحوه ترکیب نمونه ۱۳ میلی‌سیگنالهای مذکور و ایجاد یک فریم TDM نشان داده شده است. همانطور که در شکل مشخص است، یک فریم TDM، شامل ۲۴ بایت (یک بایت برای هر کانال) و یک بیت کنترلی اضافی است که در نتیجه طول هر فریم ۱۹۳ بیت خواهد بود. سرعت یک کانال T1، برابر با ۸۰۰۰ فریم در ثانیه یا ۱/۵۴۴ مگابیت بر ثانیه می‌باشد.



شکل (۱۸-۲)- ترکیب نمونه‌ها در خطوط T1

کامپیوتر شماره ۱، توسط کامپیوتر شماره ۳ دریافت می‌شود. واضح است که در این روش زمان بیشتری نسبت به روش قبل برای سوئیچینگ لازم است.



شکل(۲۲-۲)- سوئیچ تقسیم زمانی

اکنون به بحث اصلی این قسمت یا روش‌های سوئیچینگ می‌پردازیم، به طور کلی می‌توان روش‌های راه‌گزینی را به سه دسته تقسیم نمود:

- راه‌گزینی مداری
- راه‌گزینی پیغامی
- راه‌گزینی پسته‌ای

الف- راه‌گزینی مداری

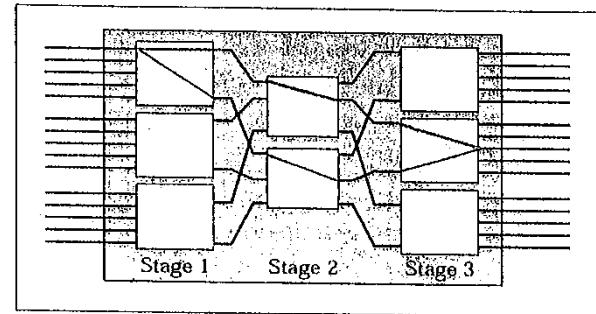
در این روش، ابتدا باید یک مسیر ثابت و پایدار بین فرستنده و گیرنده برقرار گردد، سپس ارسال اطلاعات شروع شود؛ به عبارت دیگر، فرستنده تا از وجود ارتباط اطمینان حاصل نکند، شروع به ارسال نمی‌نماید. مسیر برقرار شده تا زمان قطع اتصال، در اختیار طرفین می‌باشد حتی اگر داده‌ای برای مبادله نداشته باشند. سیستم تلفن را می‌توان مثالی از این نوع راه‌گزینی در نظر گرفت.

شکل (۲۳-۲) مفهوم راه‌گزینی مداری را نشان می‌دهد. فرض کنید ارتباط بین دو نقطه A و C از طریق سوئیچ B برقرار شود. درخواست اتصال از نقطه A پس از مدتی (زمان تاخیر انتشار)، به سوئیچ B می‌رسد. در سوئیچ B پس از طی زمانی، مسیر مربوطه برقرار می‌گردد. دوباره پس از تاخیری ناشی از انتشار سیگنال در مسیر ارتباطی BC، پیغام درخواست برقراری اتصال به نقطه C می‌رسد. در این هنگام بسته به اینکه این درخواست چه زمانی پاسخ داده شود، تاخیر دیگری

برای ساخت سوئیچهای بزرگتر با تعداد ترانزیستورهای کمتر، از قرار دادن سوئیچهای Crossbar کوچکتر به صورت چند مرحله‌ای استفاده می‌کنیم. در شکل (۲۱-۲) یک سوئیچ سه مرحله‌ای ۱۵ در ۱۵ با استفاده از سوئیچهای کوچکتر ۵ در ۲، ۳ در ۲ و ۵ در ۵ پیاده‌سازی شده است. به این نوع اتصال که در آن خروجی‌های اول سوئیچهای سطح پک به سوئیچ اول سطح دو متصل می‌شوند، شبکه Clos گفته می‌شود.

دقت کنید که اگر می‌خواستیم فقط با استفاده از یک سوئیچ اتصالات را برقرار کنیم به ۲۲۵ ترانزیستور احتیاج بود که با استفاده از این روش تعداد ترانزیستورها به ۷۸ عدد کاهش یافته است. (چرا؟)

در این شکل دو مسیر متفاوت از ورودی اول به خروجی هشتم نشان داده است.



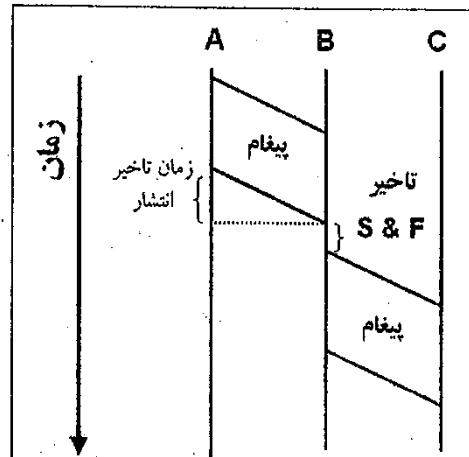
شکل (۲۱-۲)- شبکه سه مرحله‌ای Clos

روش‌های فوق به سوئیچهای تقسیم فضایی (Space Division Switch) موسوم هستند دلیل این نامگذاری این است که در این نوع سوئیچها، مسیرهای مختلف به صورت فضایی از هم دیگر تفکیک شده‌اند.

نقشه مقابله این نوع سوئیچها، سوئیچهای تقسیم زمانی هستند که در آنها مسیرهای مختلف با تقسیم زمانی از هم منفک می‌شوند. شکل (۲۱-۲) یک نمونه از این نوع سوئیچها را نشان می‌دهد. این نوع سوئیچ از دو تلقیق کننده و جدا کننده TDM و یک واحد تعویض برش زمانی (Time Slot Interchange) تشکیل شده است. کار اصلی در این نوع سوئیچ در داخل TSI انجام می‌گردد. این واحد بر اساس جدولی که در اختیار دارد برای اتصال ورودیها به خروجیها مورد نظر، جای برش زمانی داده‌های مربوطه را عوض می‌کند. مثلاً در شکل (۲۲-۲) اطلاعات ارسالی از

جلو هدایت نمایند، تاخیر ارسال زیاد خواهد بود و فقط از قسمتی از کانال که از آن پیغام عبور می‌کند، استفاده خواهد شد؛ مثلاً در شکل (۲۴-۲)، تا زمانی که کل پیغام به سوئیچ میانی B بررسی کانال بین B و C بلااستفاده خواهد ماند.

فرض کنید کانالهای ارتباطی بین نقاط A و B و C، دارای پهنای باند R بیت بر ثانیه و طول یک بلوك اطلاعاتی L بیت باشد، زمان ارسال پیغام L/R ثانیه و تاخیر ارسال $2L/R$ خواهد بود.



شکل (۲۴-۲) - راه گزینی پیغامی

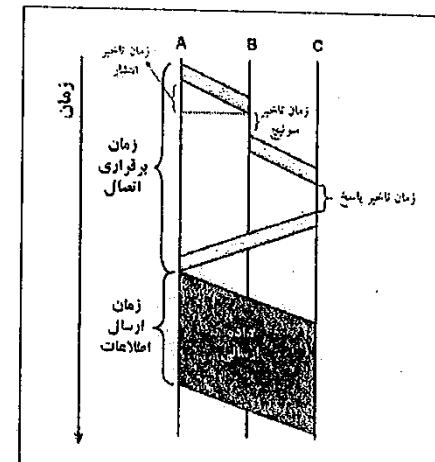
ج) راه گزینی بسته‌ای

در راه گزینی پیغامی، محدودیتی برای طول یک بلوك اطلاعاتی وجود نداشت. در روش راه گزینی بسته‌ای، یک پیغام به واحدهای کوچکتری به نام بسته (packet) شکسته می‌شود (شکل (۲۵-۲)). حداکثر طول یک بسته توسط پروتکل شبکه مشخص می‌گردد. هر بسته علاوه بر داده، شامل یک سری اطلاعات اضافی است که به صورت سرآیند به آن چسبیده شده است. بسته‌ها می‌توانند با استفاده از اطلاعات اضافی که دارند، مسیر خود را پیدا کنند. بسته‌های ارسالی از یک فرستنده می‌توانند هر کدام از مسیر جداگانه‌ای به گیرنده برسند؛ به همین دلیل گیرنده ممکن است آنها را خارج از ترتیب دریافت نماید. مرتب کردن بسته‌ها به ترتیبی که توسط فرستنده ارسال شده‌اند، از روی شماره بسته که در داخل سرآیند وجود دارد، امکان پذیر است. (شکل (۲۶-۲))

خواهیم داشت. دقت کنید که در هنگام ارسال پاسخ گیرنده از طریق سوئیچ، دیگر زمان تاخیر سوئیچ وجود ندارد زیرا سوئیچ قبله بسته شده است. مکانیزم ارتباط شامل سه فاز زیر است:

- فاز برقراری اتصال
- فاز ارسال اطلاعات
- فاز قطع اتصال

در شکل، فازهای برقراری اتصال و ارسال اطلاعات نشان داده شده است.



شکل (۲۵-۲) - راه گزینی مداری

ب- راه گزینی پیغامی

در این نوع راه گزینی هیچ مسیر فیزیکی از قبل بین گیرنده و فرستنده برقرار نمی‌گردد. در عوض، هر گاه فرستنده بلوکی از اطلاعات برای ارسال داشته باشد، آن را برای سوئیچ میانی ارسال می‌کند. سوئیچ این بلوک را به جلو می‌راند. این کار تا رسیدن اطلاعات مورد نظر به گیرنده، تکرار می‌کند. سوئیچ این بلوک را به جلو می‌راند و به جلو راندن (Store-and-forward) هم گفته می‌شود. سیستم تلگراف را می‌توان نمونه‌ای از این نوع راه گزینی به شمار آورد. بدینهای است که سوئیچهای میانی باید حافظه کافی برای ذخیره یک بلوک اطلاعات (که می‌تواند بسیار بزرگ باشد) را داشته باشند. همچنین به دلیل اینکه سوئیچهای میانی ابتدا باید کل بلوک را دریافت کنند و سپس به

۶- محیط‌های انتقال داده

به طور کلی محیط‌های انتقال داده را می‌توان به دو دسته تقسیم نمود: محیط‌های باسیم و محیط‌های بی‌سیم. محیط‌های باسیم به محیط‌های هدایت شونده و محیط‌های بی‌سیم، به محیط‌های غیرهدایت شونده نیز مشهور هستند.

(الف) محیط‌های انتقال باسیم (کابل‌ها)

پیش از اینکه در مورد انواع کابل‌ها و پهنهای باند مربوط به آنها، به بحث پردازیم، ذکر این نکته ضروری است که نوع کابل انتخابی بطور مستقیم به توبولوزی شبکه وابسته است. کابل شبکه، رسانه‌ای است که از طریق آن، اطلاعات از یک دستگاه موجود در شبکه به دستگاه دیگر انتقال می‌یابد. انواع مختلفی از کابلها بطور معمول در شبکه‌های LAN استفاده می‌شوند. در برخی موارد شبکه تنها از یک نوع کابل استفاده می‌کند، اما گاه تلفیقی از انواع مختلف کابل به کار گرفته می‌شود. غیر از عامل توبولوزی، پروتکل و اندازه شبکه نیز در انتخاب کابل شبکه مؤثرند. آگاهی از ویژگیهای انواع مختلف کابلها و ارتباط آنها با دیگر جنبه‌های شبکه برای توسعه یک شبکه موفق ضروری است.

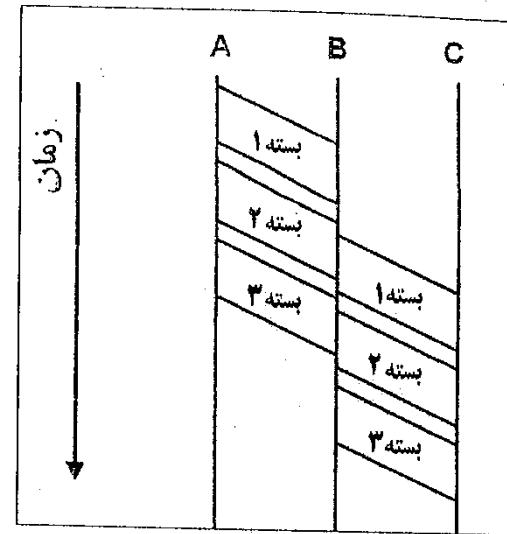
کابل‌های شبکه در سه نوع زیر موجود هستند:

- کابل هم محور (Coaxial)
- زوج به هم تابیده (Twisted Pair)
- فیبر نوری (Fiber Optic)

کابل هم محور

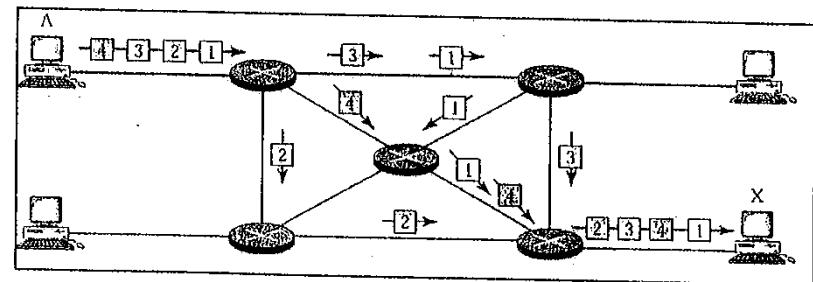
کابل‌های هم محور زمانی بیشترین مصرف را در میان کابل‌های موجود در شبکه داشت. چند دلیل اصلی برای استفاده زیاد از این نوع کابل وجود دارد:

- ۱- قیمت ارزان آن.
- ۲- سبکی و انعطاف‌پذیری.
- ۳- این نوع کابل به نسبت زیادی در برابر سیگنالهای مداخله‌گر مقاومت می‌نماید.
- ۴- مسافت بیشتری را بین دستگاه‌های موجود در شبکه، نسبت به زوج به هم تابیده پشتیبانی می‌نماید.



شکل (۲-۲)- مفهوم راه‌گزینی بسته‌ای

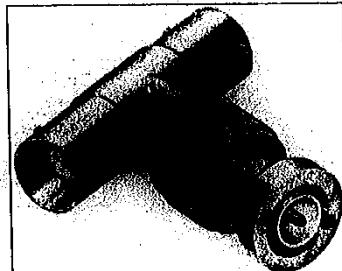
در این روش، به دلیل اینکه اندازه بسته‌ها کوچک بوده و در نتیجه ندهای میانی سریعتر می‌توانند آن را دریافت کرده و به جلو هدایت نمایند، کانالهای ارتباطی می‌توانند به صورت همزمان مشغول بوده و در نهایت زمان کمتری نیاز خواهد بود.



شکل (۲-۲)- دریافت خارج از ترتیب

اتصال دهنده (connector) مورد استفاده در کابل coaxial، گانکتور BNC می‌باشد. انواع مختلفی از سازگار کننده‌ها برای BNC ها وجود دارند که عبارتند از: Barrel، T-connector، Terminator connector.

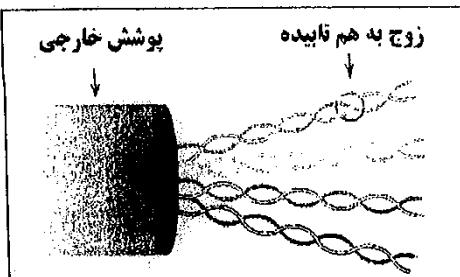
تصویر(۲۸-۲) یک T-connector را نشان می‌دهد:



شکل(۲۸-۲)- T-connector

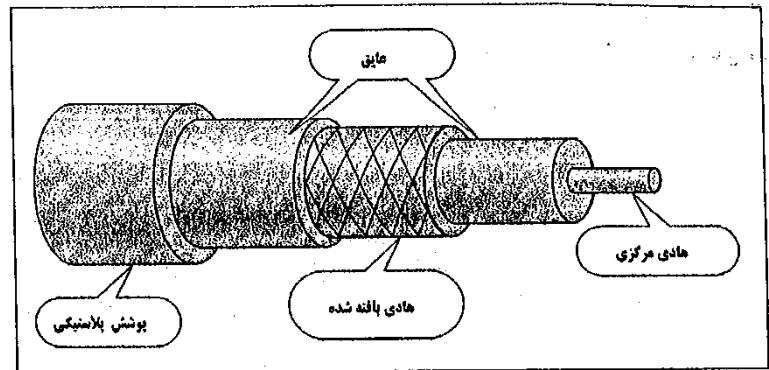
زوج به هم تابیده
امروزه متداولترین رسانه انتقال سیمی، زوج به هم تابیده (Twisted Pair) می‌باشد. قیمت آن ارزان بوده و از نمونه‌های آن می‌توان به کابل تلفن اشاره کرد. این نوع کابل که از چهار جفت سیم بهم تابیده تشکیل می‌گردد، خود به دو دسته تقسیم می‌شود:

۱- زوج به هم تابیده بدون حفاظ (UTP): کابل ارزان قیمتی است که نصب آسانی دارد و برای شبکه‌های LAN بسیار مناسب است، همچنین نسبت به نوع دوم کم وزن‌تر و انعطاف‌پذیرتر است. مقدار سرعت دینای عبوری از آن ۴ مگابیت بر ثانیه تا ۱ گیگابیت بر ثانیه می‌باشد. این کابل می‌تواند سیگنال را تا مسافت حدوداً ۱۰۰ متر بدون افت انتقال دهد.



شکل(۲۹-۲)- کابل UTP

در شکل (۲۷-۲)، ساختار کابل Coaxial مشاهده می‌شود:



شکل(۲۷-۲)- کابل هم محور

این کابل از چهار قسمت اصلی تشکیل شده است:

(۱) هادی مرکزی یا Inner Conductor که معمولاً از یک رشته سیم جامد می‌تشکیل می‌گردد.

(۲) عایق یا Insulator که معمولاً از جنس PVC یا تفلون است.

(۳) هادی خارجی یا Outer Conductor که از سیم‌های بافته شده تشکیل می‌شود و کار آن جلوگیری از نویزهای ناخواسته است و همچنین به عنوان زمین استفاده می‌شود.

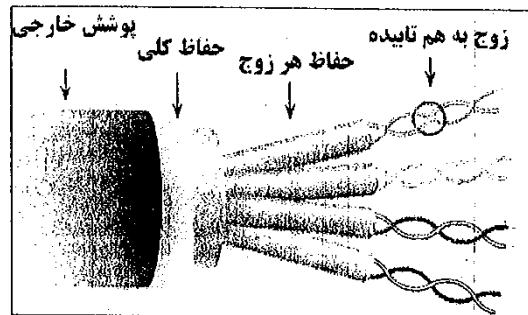
(۴) پوشش یا Jacket که جنس آن اغلب از پلاستیک بوده و نگهدارنده خارجی سیم در برابر خطرات فیزیکی است.

کابلهای هم محور بر اساس قطر هسته به دو نوع تقسیم می‌شوند:

- کابل هم محور نازک (Thin-net): کابلی است بسیار سبک، انعطاف‌پذیر و ارزان قیمت، قطر سیم در آن 0.5 میلیمتر معادل 25 آینچ است. مقدار فاصله‌ای که توسط آن پشتیبانی می‌شود در پروتکل اترنت 185 متر است.

- کابل هم محور ضخیم (Thick-net): این کابل قطری تقریباً دو برابر Thin-net دارد. کابل مذکور، پوشش محافظتی را (علاوه بر محافظت خود) دارد که از جنس پلاستیک می‌باشد. حداقل فاصله‌ای که توسط این کابل پشتیبانی می‌شود، در پروتکل اترنت 500 متر است.

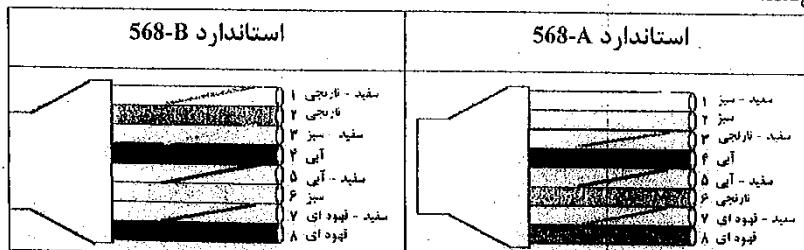
۲- زوج به هم تابیده حفاظدار (STP): در این کابل سیم‌های انتقال دیتا مانند UTP هشت سیم و یا چهار جفت دوتایی هستند. باید دانست که تفاوت آن با UTP در این است که پونتمنی از دور آن پیچیده شده که از اثرگذاری امواج بر روی دیتا جلوگیری می‌کند. این کابل از UTP گرانتر و انعطاف‌پذیری آن کمتر است. در مقایسه با UTP، موارد کاربرد STP بسیار کمتر است.



شکل(۲)-۳۱-۲

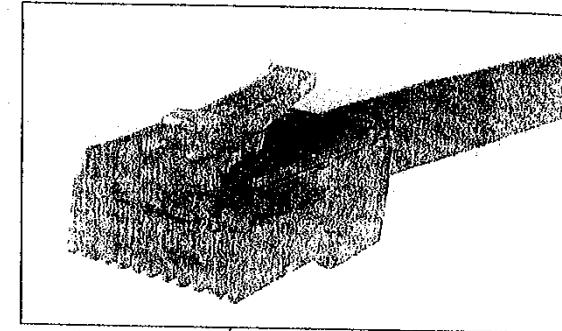
لازم به ذکر است که در پروتکل Ethernet، از این چهار جفت سیم تنها از دو جفت آن استفاده می‌شود. یک جفت برای فرستادن اطلاعات (سیمهای شماره ۳ و ۶) و دیگری برای دریافت اطلاعات (سیمهای شماره ۱ و ۴).

دو استاندارد مختلف توسط TIA/EIA برای بستن کانکتور RJ-45 به انتهای کابل تعریف شده است که به استانداردهای 568-A و 568-B مشهور هستند. تبعیت کردن از استانداردهای مذکور الزامی نیست ولی برای سازگاری کابل بندی ما با سایر شبکه‌ها بهتر است هنگام اتصال کانکتورها، از این استانداردها پیروی شود. شکل(۲-۲) ترتیب رنگها را در استانداردهای نوع A و B نشان می‌دهد.



شکل(۲)-۳۲-۲) ترتیب رنگها در استانداردهای نوع A و B

در سیم تلفن که خود نوعی از این کابل است از اتصال دهنده RJ11 استفاده می‌شود، اما در کابل شبکه، اتصال دهنده RJ45 بکار می‌رود که دارای هشت مکان برای هشت رشته سیم است. در شکل (۲-۳) یک اتصال دهنده RJ45 دیده می‌شود.



شکل(۲)-۳۰-۲) اتصال دهنده RJ45

کابل UTP دارای چند دسته مختلف است که با کلمه **CAT = CATEgory** شناخته می‌شوند. قبل از آن برای ارتباطات تلفنی استفاده می‌شد. این کابل دیگر توسط TIA/EIA به رسمیت شناخته نمی‌شود.

CAT1 قبلاً از آن برای شبکه Token-Ring با سرعت ۴ مگابیت بر ثانیه استفاده می‌شد. این کابل دیگر توسط TIA/EIA به رسمیت شناخته نمی‌شود.

CAT2 دارای پهنای باند ۱۶ مگاهرتز بوده و از آن برای پیاده‌سازی شبکه اترنت با سرعت ۱۰ مگابیت بر ثانیه استفاده می‌شود.

CAT3 دارای پهنای باند ۱۰۰ مگاهرتز بوده و از آن برای پیاده‌سازی شبکه اترنت با سرعت ۱۰۰ مگابیت بر ثانیه استفاده می‌شود.

CAT4 دارای پهنای باند ۲۰۰ مگاهرتز بوده و از آن برای پیاده‌سازی شبکه Token-Ring با سرعت ۱۶۰ مگابیت بر ثانیه استفاده می‌شود.

CAT5 دارای پهنای باند ۱۰۰۰ مگاهرتز بوده و از آن برای پیاده‌سازی شبکه اترنت با سرعت ۱۰۰ مگابیت بر ثانیه (Fast Ethernet) استفاده می‌شود.

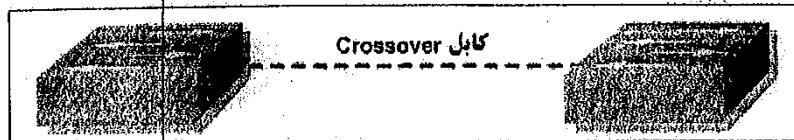
CAT5e دارای پهنای باند ۱۰۰۰ مگاهرتز بوده و از آن برای پیاده‌سازی شبکه اترنت با سرعت ۱۰۰ مگابیت بر ثانیه (Fast Ethernet) استفاده می‌شود.

CAT6 دارای پهنای باند ۲۵۰ مگاهرتز بوده و از آن برای پیاده‌سازی شبکه گیگابیت اترنت با سرعت ۱۰۰۰ مگابیت بر ثانیه استفاده می‌شود.

CAT7 دارای پهنای باند ۲۵۰ مگاهرتز بوده و از آن برای پیاده‌سازی شبکه گیگابیت اترنت با سرعت ۱۰۰۰ مگابیت بر ثانیه استفاده می‌شود.

۱۶/ اتصال شبکه‌های کامپیوتو

در کابل با اتصال Crossover، در یک طرف کابل، کانکتور را به صورت استاندارد A و در طرف دیگر به صورت استاندارد B می‌بندیم، این نوع کابل برای اتصال سوئیچ به سوئیچ یا اتصال مستقیم دو کامپیوتر استفاده می‌شود. (شکل ۳۵-۲).



شکل (۳۵-۲)- مورد استفاده کابل Crossover

در کابل با اتصال Rollover، کانکتورهای طرفین کاملاً بصورت بر عکس بسته می‌شوند، این نوع کابل برای اتصال کامپیوتر به روتراز طریق پورت کنسول روترا استفاده می‌شود. (شکل ۳۶-۲).



شکل (۳۶-۲)- مورد استفاده کابل Rollover

فیبر نوری

در فیبر نوری برخلاف کابل‌های مسی به جای اینکه سیگنال الکتریکی در داخل سیم انتقال یابد، پالسهایی از نور در میان پلاستیک یا شیشه منتقل می‌شوند. همانطور که می‌دانیم، هنگامی که نور از محیطی به محیط دیگری وارد می‌شود، زاویه شکست آن به زاویه تابش متفاوت خواهد بود و نسبت سینوس این دو زاویه با نسبت ضریب شکست دو محیط مناسب است. زاویه‌ای موسوم به زاویه حد وجود دارد که اگر نور با زاویه‌ای بیشتر از آن تابانده شود، به جای خارج شدن از محیط، دوباره بر می‌گردد. در شکل (۳۷-۲) سه پرتو نور را مشاهده می‌کنید که به ترتیب با زاویه‌های کمتر، مساوی و بیشتر از زاویه حد از محیط شیشه وارد محیط هوا شده‌اند. همانطور که مشاهده می‌گردد، پرتو سوم مجدداً به داخل شیشه برگشته است.

برای اتصال دستگاه‌های مختلف شبکه به هم دیگر لازم است که کانکتورهای دو سر کابل به روشهای متفاوتی بسته شوند، به طور کلی با توجه به نحوه بستن کانکتورها، سه نوع کابل مختلف در شبکه استفاده می‌شود که عبارتند از:

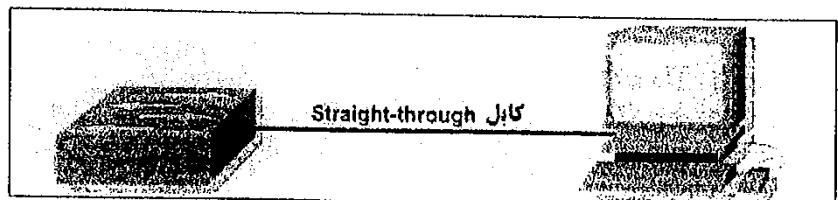
- کابل با اتصال Straight through
- کابل با اتصال Crossover
- کابل با اتصال Rollover

در شکل (۳۳-۲) نحوه اتصال دو انتهای کابل در هر نوع نشان داده شده است.

اتصال	اتصال	اتصال
Rollover	Crossover	Straight Through
Pin 1 ----- Pin 8	Pin 1 ----- Pin 3	Pin 1 ----- Pin 1
Pin 2 ----- Pin 7	Pin 2 ----- Pin 6	Pin 2 ----- Pin 2
Pin 3 ----- Pin 6	Pin 3 ----- Pin 1	Pin 3 ----- Pin 3
Pin 4 ----- Pin 5	Pin 4 ----- Pin 4	Pin 4 ----- Pin 4
Pin 5 ----- Pin 4	Pin 5 ----- Pin 5	Pin 5 ----- Pin 5
Pin 6 ----- Pin 3	Pin 6 ----- Pin 2	Pin 6 ----- Pin 6
Pin 7 ----- Pin 2	Pin 7 ----- Pin 7	Pin 7 ----- Pin 7
Pin 8 ----- Pin 1	Pin 8 ----- Pin 1	Pin 8 ----- Pin 8

شکل (۳۳-۲)- انواع اتصالات کابل UTP

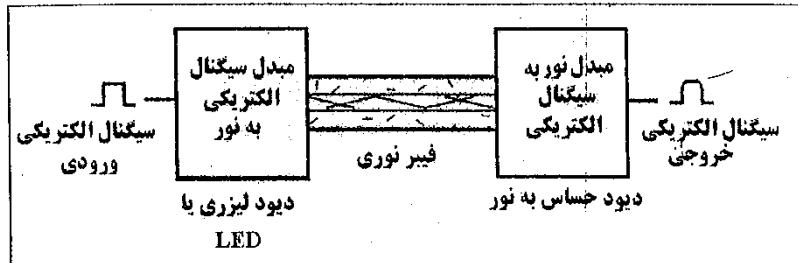
در کابل با اتصال straight، هر دو طرف کابل به یک صورت بسته می‌شوند. به عبارت دیگر، کانکتورهای هر دو سر را به صورت استاندارد A یا B می‌بندیم، این نوع کابل برای اتصال کامپیوتر به سوئیچ یا هاب استفاده می‌شود. (شکل ۳۴-۲).



شکل (۳۴-۲)- مورد استفاده کابل Straight

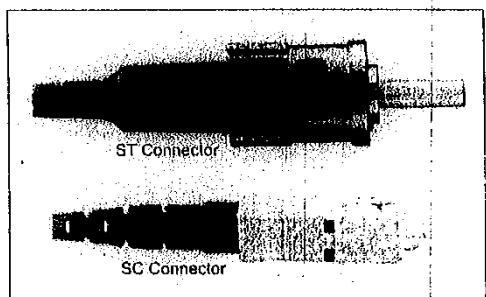
برای تبدیل سیگنال الکتریکی ورودی به نور از مبدل مخصوصی که در داخل کانکتور وجود دارد استفاده می‌شود که می‌تواند دیود لیزری یا دیود نور گسیل (LED) باشد. در طرف دیگر نیز باید نور به سیگنال الکتریکی تبدیل شود. این کار توسط دیودهای حساس به نور یا فتودیود انجام می‌گردد. شکل (۲-۳۹) مراحل مذکور را نشان می‌دهد.

هر کابل فیبر نوری شامل دو رشتہ مجزا است. دلیل این امر آن است که هر رشتہ شیشه یا فیبر سیگنالها را فقط در یک سمت می‌تواند حمل کند. به همین دلیل یک کابل برای ارسال داده و یک کابل نیز برای دریافت داده در نظر گرفته شده است.

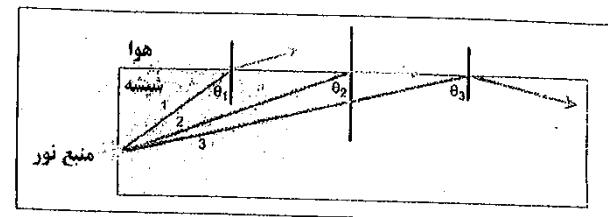


شکل (۲-۳۹)- سیستم انتقال در فیبر نوری

در دو انتهای فیبر نوری از اتصال دهنده‌های مخصوص استفاده می‌شود. البته بعضی از اتصال دهنده‌ها هم در فیبر تک حالت و هم در فیبر چند حالت استفاده می‌شوند. در شکل (۲-۴۰) دو نوع اتصال دهنده ST و SC را نشان می‌دهد.



شکل (۲-۴۰)- کانکتورهای فیبر نوری



شکل (۲-۳۷)- مفهوم زاویه حد

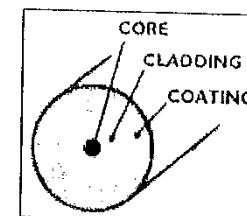
در فیبر نوری از این خاصیت برای انتقال یک پرتو نور از یک طرف دیگر کابل استفاده می‌شود. به طوری که پرتو نور مرتبا در داخل شیشه انعکاس پیدا کرده تا به انتهای کابل برسد. واضح است که پرتوهای با زاویه بیشتر از زاویه حد همه در داخل شیشه به دام می‌افتد. به عبارت دیگر می‌توان چندین پرتو با زاویه‌های مختلف را همزمان از داخل کابل عبور داد.

اجزای تشکیل دهنده سیستم فیبر نوری

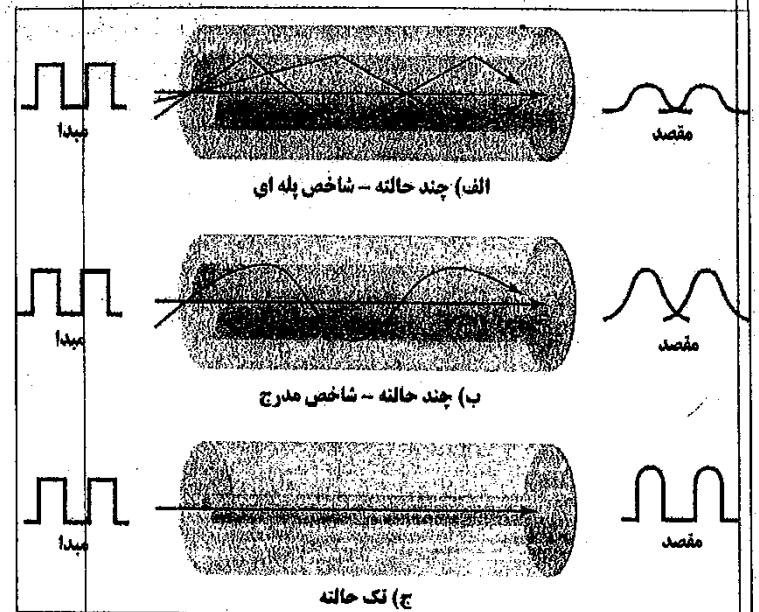
خود فیبر نوری شامل سه قسمت است:

- **core** یا هسته: یک رشتہ نازک شیشه که در مرکز فیبر است و سیگنال در داخل آن حرکت می‌کند.
- **Cladding** یا روکش: لایه شیشه‌ای دیگری است که ضربب شکست آن متفاوت بوده و باعث شکست نور می‌شود.
- **Coating** یا رویه: از جنس پلاستیک بوده و از فیبر در مقابل آسیب‌های احتمالی مانند رطوبت و تا حد کمی ضربه و احیاناً شکستن هسته حفاظت می‌کند.

شکل (۲-۳۸)- سطح مقطع یک فیبر نوری و اجزاء تشکیل دهنده آن را نشان می‌دهد.



شکل (۲-۳۸)- اجزاء تشکیل دهنده فیبر نوری



شکل (۴-۲)- انواع فیبر نوری

مزایا و معایب فیبر نوری نسبت به کابل مسی

مزایای فیبر نوری عبارتند از:

- در مسافت‌های بالا هزینه آن نسبت به سیم‌های مسی کمتر است.
- پهنای باند آن بسیار بیشتر از کابل مسی است.
- ضعیف سیگнал در فیبرهای نوری نسبت به سیم‌های مسی بسیار ناچیز بوده و سرعت آن بالاتر است.
- سیگنالهای موجود در یک فیبر بر فیبر دیگر تاثیر نخواهد گذاشت، همچنین میدانهای الکترومغناطیسی هیچ تاثیری بر روند انتقال داده‌ها در یک فیبر نوری ندارد.
- منیت در استفاده از آن به دلیل مشکل بودن انشعاب گیری، بالاست.
- بسیار سبک و نازک است.

انواع فیبر نوری

فیبرهای نوری بر اساس قطر هسته و همچنین تعداد پرتوهای نوری که از آن عبور می‌کنند به دو دسته تقسیم می‌شوند.

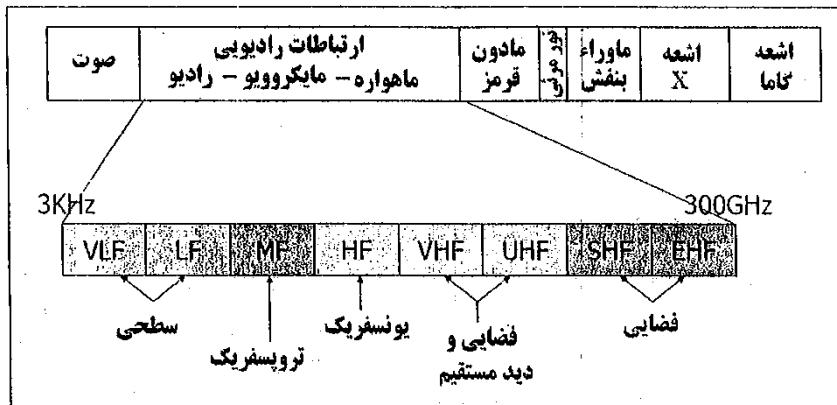
۱- فیبر تک حالت (Single Mode)، در این نوع فیبر، قطر هسته بسیار نازک (در حدود ۹/۱۲۵ میکروم) بوده و فقط یک پرتو نور می‌تواند از آن عبور کند. روی آن عددی مثلاً به صورت ۹/۱۲۵ نوشته می‌شود که در آن قطر هسته فیبر نوری و ۱۲۵ مجموع قطر هسته و Cladding به میکروم می‌باشد. مولد نور در این نوع فیبر یک دیود لیزری است. این نوع فیبر که خاصیت انعطاف‌پذیری کم و قیمت بالایی دارد، می‌تواند مسافت بیشتری (نسبت به نوع چندحالته) نور را انتقال دهد و برای شبکه‌های تلویزیونی و مخابراتی استفاده می‌گردد.

۲- فیبر چندحالته (Multi Mode)، در این نوع فیبر قطر هسته قطورتر از نوع قبل (در حدود ۶۲/۵ میکروم) بوده و چند پرتو نور همزمان می‌توانند از آن عبور کند. روی آن عددی مثلاً به صورت ۶۲.۵/۱۲۵ نوشته می‌شود که در آن قطر هسته فیبر نوری و ۱۲۵ مجموع قطر هسته و Cladding به میکروم می‌باشد. مولد نور در این نوع فیبر LED است. در این نوع فیبر، نور مسافت کوتاه‌تری را نسبت به نوع تک حالت طی می‌کند ولی قابلیت انعطاف‌پذیری بیشتری دارد. قیمت آن نیز ارزان‌تر بوده و در شبکه‌های کامپیوتری استفاده می‌شود.

فیبر چند حالته خود به دو دسته شاخص پلهای (Step-index) و شاخص مدرج (Graded-index) تقسیم می‌شود. در نوع مدرج، ضریب شکست هسته به تدریج کم می‌شود به طوری که در مرکز هسته ضریب شکست بیشترین مقدار است. در نوع پلهای ضریب شکسته هسته ثابت است.

در شکل (۴-۲) انواع حالت‌های فوق نشان داده شده است.

بتوانند از نقطه‌ای به نقطه دیگر منتقل شوند. فرکانس‌های بسیار بالا برای ارتباطات فضایی استفاده می‌شوند زیرا این امواج می‌توانند از لایه‌های جو عبور کنند. از باندهای MF و LF برای ارتباطات رادیویی AM، از باند VHF برای ارتباط رادیویی FM و از باندهای VHF و UHF برای ارتباطات تلویزیونی استفاده می‌شود.



شکل(۴۲-۲)- طیف امواج الکترومغناطیس

در شبکه‌های بی‌سیم از امواج رادیویی، مایکروویو و مادون قرمز استفاده می‌شود. بنابراین این دسته امواج را بیشتر توضیح خواهیم داد.

فرکانس‌های رادیویی (RF)

اگرچه نقطه تمایز مشخصی بین فرکانس‌های رادیویی و مایکروویو وجود ندارد، اما به طور کلی فرکانس‌های ۳ کیلوهرتز تا یک گیگاهرتز را امواج رادیویی می‌نامند. تولید امواج رادیویی ساده است، مسافت زیادی را طی می‌کند و به راحتی در ساختمان‌ها نفوذ می‌کند. لذا هم برای ارتباط درونی (داخل ساختمان) و هم برای ارتباط بیرونی (خارج ساختمان) بطور گسترده مورد استفاده قرار می‌گیرد. امواج رادیویی چند سویه است، یعنی از منبع به تمام جهات منتشر می‌شود، به طوری که نیازی نیست فرستنده و گیرنده از لحظه فیزیکی خود را تنظیم کنند و به عبارت دیگر احتیاجی به دید مستقیم نیست. در فرکانس‌های پایین، امواج رادیویی از موانع عبور می‌کند، اما قادرند آن با فاصله گرفتن از منبع و حرکت در هوا به شدت کاهش می‌یابد. در فرکانس‌های بالا، امواج رادیویی

و ممایب آن عبارتند از:

- این نوع رسانه برای شبکه‌های معمولی و کوچک بسیار پر هزینه است.

- نصب فیبرهای نوری کاری دشوار است و به افراد متخصص نیاز دارد. حتی برای قطع کردن

- آن دقت بسیار زیادی مورد نیاز است زیرا در غیر این صورت رازوه شکست نور تغییر می‌کند و

روند انتقال داده‌ها دچار اختلال می‌شود.

- تجهیزات مورد نیاز برای فیبرهای نوری نسبت به سیمهای مسی بسیار گران‌تر است.

- یکی از اصلی‌ترین اشکالات فیبرهای نوری شکننده بودن فیبر داخل کابل است. در صورت

خم کردن بیش از اندازه سیم، فیبر مورد نظر شکسته شده و دیگر آن کابل به درد نمی‌خورد.

ب- محیط‌های انتقال بی‌سیم

کابل‌ها علی‌رغم ساده و ارزان بودن دارای محدودیت‌های نیز هستند. مثلاً نمی‌توان دو دفتر یک شرکت را که در دو نقطه از یک شهر واقع هستند، توسط کابل به هم ارتباط داد. به علاوه استفاده از کابل در بسیاری از مواقع دست‌وپاگیر است. به طور کلی در مواردی که کابل کشی مشکل یاشد یا مقولون به صرفه نباشد و یا اینکه کاربران متحرک باشند، از محیط‌های انتقال بی‌سیم استفاده می‌شود. در بعضی از شبکه‌ها، از سیستم بی‌سیم برای پشتیبانی از شبکه در هنگام آسیب‌دیدگی کابل‌ها استفاده می‌شود.

طیف امواج الکترومغناطیس

امواج الکترومغناطیس به امواجی گفته می‌شود که در آنها میدان الکتریکی بر میدان مغناطیسی عمود بوده و می‌توانند در فضای آزاد (حتی در خلاء) انتشار یابند. این امواج محدوده بسیار وسیعی از فرکانس‌ها را شامل بوده و پسته به فرکانس آنها رفتارهای بسیار متفاوتی از خود نشان می‌دهند. در شکل(۴۲-۲) طیف امواج الکترومغناطیس نشان داده شده است. همانطور که مشاهده می‌کنید این امواج از فرکانس‌های بسیار پایین قابل شنیدن تا فرکانس‌های بسیار بالا که برای کاربردهای هسته‌ای استفاده می‌شود را شامل می‌گردد. بخشی از طیف، یعنی فرکانس‌های ۳۰۰ گیگاهرتز تا ۳۰۰۰ گیگاهرتز برای کاربردهای ارتباطی استفاده می‌گردد. این بخش خود به ۸ باند تقسیم پندی شده است. رفتار این باندها از نظر نحوه انتشار متفاوت است به طوری که در باندهای با فرکانس کمتر امواج می‌توانند از انحنای کره زمین پیروی کرده و در سطح آن انتشار یابند. در فرکانس‌های بالاتر، امواج بایستی به لایدهای جو (یونسفر و تروپوسفر) برخورد کرده و بازگردند تا

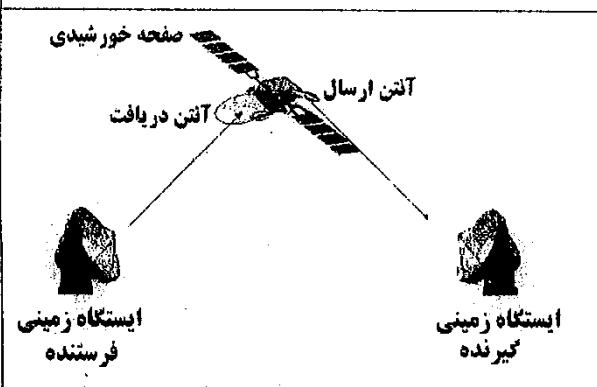
برگشت پیدا می‌کنند. همچنین فرمته و گیرنده مادون قرمز احتیاج به دیستانسیتیم دارند. سیستم‌های کنترل از راه دور که در وسایلی چون تلویزیون و استریووها به کار می‌روند با انتقال مادون قرمز کار می‌کنند.

ارتباطات ماهواره‌ای

سیستمهای ارتباطی ماهواره‌ای، از ماهواره برای انتقال سیگنال بین ایستگاههای زمینی استفاده می‌کنند؛ و به این ترتیب می‌توان ارتباط فواصل دورتر را فراهم نمود. ماهواره‌های مخابراتی به دو دسته فعال و غیرفعال تقسیم بندی می‌شوند. یک ماهواره غیرفعال تنها سیگنالهای رادیویی دریافتی را به طرف زمین برمی‌گرداند و در واقع مثل یک آینه عمل می‌کند. اما یک ماهواره فعال مانند یک تکرارگر عمل می‌کند و سیگنالهای دریافتی را تقویت کرده سپس به طرف زمین ارسال می‌کند.

چون قرار دادن یک ماهواره مخابراتی در مدار زمین گران تمام می‌شود، یک ماهواره عموماً شامل چندین فرستنده-گیرنده مستقل است. هر فرستنده-گیرنده در یک فرکانس رادیویی(کانال) کار می‌کند؛ بنابراین برقراری چندین ارتباط بطور همزمان امکان پذیر می‌گردد. به علاوه، به دلیل اینکه یک کانال ماهواره می‌تواند به طور مشترک استفاده شود مشترکین متعددی از آن بهره می‌برند.

شکل (۴۳-۲) یک ارتباط ماهواره‌ای را بین دو ایستگاه زمینی فرستنده و گیرنده نشان می‌دهد. این دو ایستگاه می‌توانند از هم بسیار دور بوده حتی در دو طرف یک اقیانوس باشند.



شکل (۴۳-۲)- ارتباط ماهواره‌ای

تمایل دارند در خط مستقیم حرکت کنند و با برخورد به موانع منعکس می‌شوند. چون امواج رادیویی می‌توانند مسافت‌های زیادی را طی کنند، تداخل بین کاربران به عنوان یک منساله مطرح است. به همین دلیل برای استفاده از این امواج نیاز به اخذ مجوز است.

مایکروویو (Microwave)

برخی دیگر از شبکه‌های بی‌سیم، از باند فرکانسی مایکروویو به عنوان محیط انتقال استفاده می‌کنند. امواج مایکروویو برخلاف امواج RF، فقط در یک جهت منتشر می‌شوند؛ بنابراین آنتنهای فرستنده و گیرنده باید دقیقاً تنظیم شوند؛ این خود می‌تواند یک مزیت برای این نوع امواج باشد. چراکه یک زوج آنتن تنظیم شده مقابل هم، می‌تواند بدون تداخل با یک زوج آنتن دیگر کار کنند. معمولاً آنتنهای فرستنده و گیرنده را بر روی ارتفاعات قرار می‌دهند تا موانع طبیعی و مصنوعی و همچنین انجنای کره زمین نتوانند مانع ارتباط آنها شود. در فواصل طولانی باید از تکرارگر استفاده

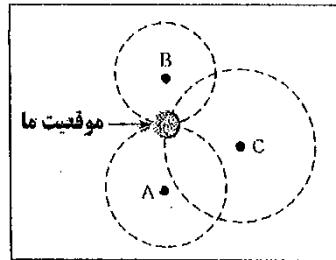
نمود. برای ارسال این امواج از آنتنهای سه‌موی یا شیپوری استفاده می‌گردد. این امواج در برابر تداخل حاصل از فعالیتهای الکترونیکی اتمسفری نظریه رعد و برق بسیار حساس هستند. در سیستم‌های مایکروویو نیز همانند امواج RF، سرعت انتقال داده به فرکانس سیگنال بستگی داشته و در ناحیه ای بین یک تا ده Mbps قرار می‌گیرد. فرکانس سیگنال در سیستم‌های مایکروویو بین ۱ تا ۳۰۰ گیگاهرتز می‌باشد.

مایکروویو تقریباً ارزان است. زیرا نصب دو برج ساده و نصب آنتن‌هایی بر آن‌ها نسبت به خرید ۵۰ کیلومتر فیبر و عبور آن از مناطق شهری شلوغ و آن هم از زیر خاک، یا عبور آنها از بین کوهها، ارزان‌تر تمام می‌شود.

مادون قرمز (IR)

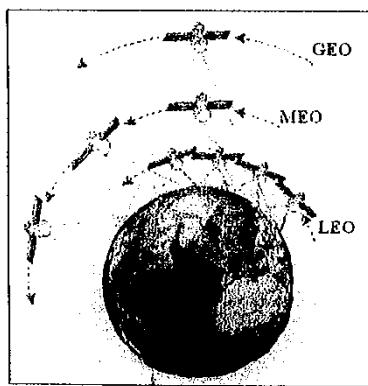
می‌توان از امواج نور در ناحیه مادون قرمز به عنوان محیط انتقال در شبکه‌های بی‌سیم استفاده کرد. استفاده از امواج نوری مادون قرمز برای محیط‌های سرسه همچنان مناسب است، مثلاً یک اتاق بزرگ می‌تواند به یک ارتباط مادون قرمز مجهز شود و دسترسی به شبکه برای تمام کامپیوترهای اتاق امکان پذیر شود. کامپیوترها می‌توانند هستگام جابجا شدن در اتاق ارتباط خود را با شبکه حفظ نمایند. شبکه‌های مادون قرمز خصوصاً برای کامپیوترهای قابل حمل مناسب‌اند؛ زیرا مادون قرمز امکان ارتباط بی‌سیم را بدون نیاز به آنتن فراهم می‌کند. از آن جایی که فرکانس امواج رادیویی در ناحیه مادون قرمز بالا است، سرعت انتقال داده در سیستم‌های مادون قرمز نیز بالا بوده و بین ۱۶ Mbps و ۱ Mbps می‌باشد. این امواج از اجسام شفاف عبور می‌کنند و در برخورد با موانع

سیستم GPS از تعداد ۲۴ هاهواره در شش مدار MEO تشکیل شده است. این مدارات به گونه‌ای در نظر گرفته شده‌اند که در هر لحظه، چهار هاهواره از هر نقطه زمین قابل مشاهده باشد. از روی فاصله نقطه زمینی از این هاهواره‌ها، موقعیت دقیق آن در زمین قابل محاسبه است.



شکل (۴۴-۲)- قانون مثلثسازی

■ هاهواره‌های همزمان با زمین یا GEO که در فاصله ۳۶۰۰۰ کیلومتری سطح زمین قرار دارند. هاهواره‌های همزمان با زمین در مداری قرار دارند که دقیقاً با گردش زمین همزمان هستند و از این رو به این نام خوانده می‌شوند. این مدار به عنوان مدار ایستان با زمین (GEO) خوانده می‌شود، زیرا هاهواره از زمین همواره در نقطه ثابتی دیده می‌شود. برای مثال، یک هاهواره همزمان در مدار دور بالای خط استوا بر روی اقیانوس اطلس می‌تواند برای رله کردن اطلاعات بین اروپا و آمریکای شمالی در تمام زمین‌ها استفاده شود چراکه همواره در نقطه بالای اقیانوس قرار دارد. با استفاده از قوانین فیزیکی می‌توان فاصله‌ای را که یک هاهواره باید از سطح زمین داشته باشد تا با گردش زمین همزمان شود، بدست آورد؛ این فاصله حدوداً ۳۶۰۰۰ (دقیقاً ۳۵۷۸۶) کیلومتر است. برای پوشش کامل سطح زمین، سه هاهواره GEO کافیست. در شکل (۴۵-۲) هاهواره‌های قرار گرفته در سه مدار مذکور نشان داده شده‌اند.



شکل (۴۵-۲)- مدارات مختلف هاهواره‌ها

هاهواره‌ها بر اساس فاصله از سطح زمین به سه دسته تقسیم می‌شوند:

■ هاهواره‌های مدار پایین یا LEO که در فاصله ۵۰۰ تا ۱۵۰۰ کیلومتری سطح زمین قرار دارند.

مشکل اصلی مدارهای پایین سرعت هاهواره در آن مدار است. با توجه به اینکه گردش هاهواره از گردش زمین سریع‌تر است، هاهواره‌های سطح پایین در بالای یک نقطه از زمین ثابت نمی‌مانند و ناظری که از زمین با تلسکوپ این هاهواره را مشاهده می‌کند، حرکت این هاهواره را شاهد است. در حقیقت یک هاهواره مدار پایین در مدت یک و نیم تا دو ساعت یک دور کامل به دور زمین می‌زند. برای اینکه پوشش مداوم و ۲۴ ساعته از یک ناحیه توسط این هاهواره‌ها فراهم شود، مجموعه‌ای از این هاهواره‌ها توسط شرکتهای مخابراتی در مدار قرار می‌گیرند. این مجموعه طوری انتخاب می‌شوند که هر نقطه از روی زمین در هر زمان، حداقل یک هاهواره را در بالای سر خود داشته باشد. مثلاً در سیستم Iridium، تعداد ۶۶ هاهواره در شش مدار LEO در ارتفاع ۷۵۰ کیلومتری زمین قرار گرفته‌اند. این هاهواره‌ها علاوه بر فرستنده-گیرنده‌هایی که برای ارتباط با ایستگاه زمینی دارند، تجهیزات رادیویی برای برقراری ارتباط با هاهواره‌های دیگر آرایه نیز دارند و در عین حال که در مدار خود حرکت می‌کنند، با هاهواره‌های دیگر نیز ارتباط برقرار می‌کنند. مثلاً فرض کنید در زمان خاصی هاهواره‌ای که بالای اروپاست اطلاعاتی را از یک ایستگاه زمینی در آلمان به مقصد آمریکا دریافت می‌نماید. هاهواره دریافت کننده ممکن است اطلاعات انتقالی را به هاهواره دیگری بفرستد، که آن هاهواره نیز به نوبه خود آن را به هاهواره‌ای تحويل دهد که به ایستگاه زمینی در آمریکا در نزدیکی مقصد دسترسی دارد.

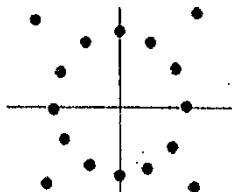
■ هاهواره‌های مدار متوسط یا MEO که در فاصله ۲۰۰۰ تا ۳۶۰۰۰ کیلومتری سطح زمین قرار دارند.

هاهواره‌های مدار متوسط حدوداً در مدت شش ساعت یک دور کامل زمین را می‌پیمایند. یکی از کاربردهای مهم این نوع هاهواره‌ها، در سیستم موقعیت‌یابی سراسری یا GPS است. مطابق قوانین ریاضی اگر در یک صفحه قرار گرفته باشیم و فاصله ما تا سه نقطه دیگر در صفحه مشخص باشد، موقعیت دقیق ما در آن صفحه مشخص خواهد شد؛ چراکه اگر به مرکز هر کدام از سه نقطه مذکور و به شعاعی برابر با فاصله ما تا آن نقاط دایره‌ای رسم کنیم، این سه دایره همدیگر را در یک نقطه قطع خواهند کرد؛ که آن نقطه، موقعیت ما در صفحه خواهد بود(شکل (۴۴-۲)). این قانون در فضای برای چهار نقطه صادق است.

خود آزمایش:

۱۳۰) اصول هسته‌های کامپیوتروی

۵- شکل زیر مربوط به نمودار حصورت فلکی استفاده شده در استاندارد ITU-V.32 مودم است. با استفاده از این استاندارد سرعت انتقال اطلاعات چند برابر می‌گردد؟



- الف) ۱۶ برابر ب) ۸ برابر ج) ۲ برابر د) ۴ برابر

۶- در یک سوئیچ 20 X 20 که به صورت یک شبکه چند مرحله‌ای Clos پیاده‌سازی شده است و سوئیچهای مرحله اول 2 X 5 هستند، تعداد کل ترانزیستورهای مورد نیاز چقدر است؟

- الف) ۱۱۲ ب) ۹۶ ج) ۱۲۰ د) ۷۸

۷- یک خط E1 با پهنای باند حدود 2 Mbps، چند مکالمه همزمان را می‌تواند عبور دهد؟ راهنمایی: برای عبور سیگنال صحبت انسان پهنای باند 4Khz کافی است.

- الف) ۲۵۰ ب) ۲۴ ج) ۳۰ د) ۶۰

۸- کدامیک از موارد زیر برای ارتباطات بی‌سیم استفاده نمی‌شود؟

- الف) مادون قرمز ب) مایکروویو
ج) ماوراء بنفش د) فرکانس‌های رادیویی

۹- تریشهای زیر را بر اساس افزایش فرکانس در طیف امواج الکترومغناطیسی از چپ به راست مرتب کنید.

Microwave - Infra red - Visible Light - X Ray - Gamma Ray - Ultra Violet

Microwave - Infra red - Visible Light - Ultra Violet - X Ray - Gamma Ray

Visible Light - Infra red - Microwave - Ultra Violet - X Ray - Gamma Ray

Infra red - Microwave - Visible Light - X Ray - Gamma Ray - Ultra Violet

۱- چرا در کابل‌های UTP، زوج سیم‌ها بهم تابیده می‌شوند؟

- الف) جهت ایجاد فضای کافی
ب) جهت ارزان تر شدن کابل‌ها
ج) به خاطر نازکتر شدن کابل‌ها
د) مسائل مرتبط با آن

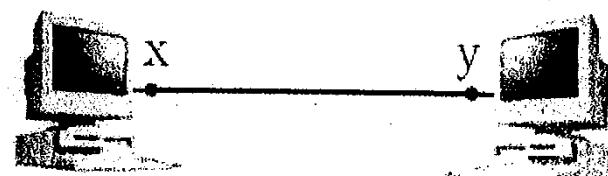
۲- کدامیک از کابل‌های زیر به منظور اتصال یک روتور به پورت سریال کامپیوتر استفاده می‌شود؟

- الف) کابل Straight
ب) کابل CrossOver
ج) کابل RollOver
د) کابل Patch

۳- کدامیک از عبارات زیر بیانگر تفاوت بین فیبر Single Mode و Multi Mode من باشد؟

- الف) Multi Mode به منظور استفاده بین ساختمان‌های متعدد توصیه شده است.
ب) Single Mode مسافت بیشتری نسبت به Multi Mode را پوشش می‌دهد.
ج) Multi Mode دارای پهنای باند بیشتری نسبت به Single Mode می‌باشد.
د) LED از عنوان مولد نور استفاده می‌نماید و در Multi Mode از لیزر بدین منظور استفاده می‌گردد.

۴- در شکل زیر اتصال کانکتورها در نقاط x و y باید به چه صورت باشد؟



الف) باید در هر دو سر به صورت نوع A بسته شوند.

ب) باید در هر دو سر به صورت نوع B بسته شوند.

ج) باید در یک طرف به صورت نوع A و در طرف دیگر به صورت نوع B بسته شوند.

د) باید سیمهای دو طرف کاملاً برعکس بسته شوند.

۱۶- کدامیک از جملات زیر در مورد راه‌گزینی مداری و راه‌گزینی بسته‌ای اشتباه است؟

- (الف) در راه گزینی مباری ابتدا اتصال برقرار می‌گردد سپس اطلاعات منتقل می‌گردد ولی در راه‌گزینی بسته‌ای از همان اول اطلاعات ارسال می‌شود.
- (ب) راه گزینی مداری نسبت به راه گزینی بسته‌ای از پهنای باند به صورت بهینه‌تر استفاده می‌کند.

- (ج) در راه گزینی مداری چه از کanal استفاده شود و چه نشود پهنای باند اشغال می‌گردد.
- (د) در راه گزینی بسته‌ای بسته‌ها می‌توانند به صورت خارج از ترتیب دریافت شوند.

۱۷- از یک کanal با پهنای باند ۲/۲ مگاهرتز، چند کanal با پهنای باند ۱۰۰ کیلوهرتز را می‌توان با

تکنیک FDM تسمیم سازی نمود؟ (باند محافظه کار ۵ کیلوهرتز در نظر بگیرید)

- (الف) ۲۰ کanal
- (ب) ۲۱ کanal
- (ج) ۲۲ کanal
- (د) ۱۹ کanal

۱۸- کدینگ منجستر جزء کدامیک از انواع زیر است؟

- | | | | |
|-------|---------|-------|------|
| ۴B/5B | Bipolar | Polar | الف) |
|-------|---------|-------|------|

- | | | |
|----|----|----|
| د) | ب) | ج) |
|----|----|----|

۱۹- ارتفاع ماهواره‌های همزمان با زمین یا GEO چقدر است؟

- (الف) حدود ۱۵۰۰ کیلومتر
- (ب) حدود ۶۰۰۰ کیلومتر
- (ج) حدود ۳۶۰۰ کیلومتر
- (د) حدود ۱۵۰۰ کیلومتر

۲۰- کدامیک از جملات زیر در مورد فیبرهای نوری صحیح است؟

- (الف) مولد نور در فیبر تک حالته دیود لیزری است و قطر هسته این نوع فیبر در حدود ۶۲/۵ میکروم می‌باشد.

- (ب) مولد نور در فیبر چند حالته دیود نورگسیل (LED) است و قطر هسته این نوع فیبر در حدود ۶۲/۵ میکروم می‌باشد.

- (ج) مولد نور در فیبر تک حالته دیود نورگسیل (LED) است و قطر هسته این نوع فیبر در حدود ۶۲/۵ میکروم می‌باشد.

- (د) مولد نور در فیبر چند حالته دیود لیزری است و قطر هسته این نوع فیبر در حدود ۶۲/۵ میکروم می‌باشد.

۲۱- از کابل straight برای اتصال کدامیک از دستگاههای زیر می‌توان استفاده کرد؟

- (الف) سوئیچ به سوئیچ
- (ب) کامپیوترا به کامپیوترا
- (ج) کامپیوترا به پورت کنسول روتر
- (د) کامپیوترا به سوئیچ

۲۲- برای پیاده سازی شبکه Fast Ethernet (با سرعت ۱۰۰Mbps) از کدام نوع کابل UTP می-

توان استفاده کرد؟

- | | | | |
|------|------|------|------|
| CAT5 | CAT4 | CAT3 | CAT2 |
|------|------|------|------|

- | | | | |
|-----|-----|-----|-------|
| (د) | (ج) | (ب) | (الف) |
|-----|-----|-----|-------|

۲۳- مسافتی که کابل UTP بدون افت می‌تواند سیگنال را انتقال دهد چند متر است؟

- (الف) ۱۰۰ متر
- (ب) ۱۲۵ متر
- (ج) ۱۵۰ متر
- (د) ۲۰۰ متر

۲۴- کاتکتور اتصال دهنده کابل هم محور به کارت شبکه کدام است؟

- (الف) RJ45
- (ب) T-Connector
- (ج) ST
- (د) SC

فصل سوم

لایه پیوند داده

۲- فریم بندی

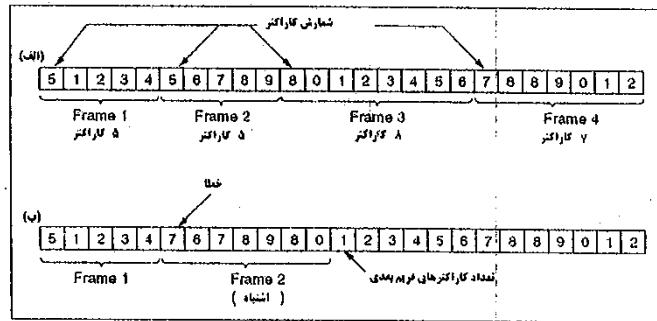
همانطور که در فصل اول گفته شد، واحد اطلاعات در لایه پیوند داده فریم است. فریم رشته‌ای از بیتهاست که دارای قسمتهای مختلفی مانند الگوی شروع فریم، پایان فریم، اندازه فریم، آدرسهای گیرنده و فرستنده، کنترل خطأ و اطلاعات کنترلی می‌باشد. اندازه و ساختار فریم به پروتکل مربوطه بستگی دارد.

روشهای مختلفی برای ساختن یک فریم وجود دارد که ذیلاً به آن می‌پردازیم:

- فریم بندی بر اساس شمارش کاراکتر (Character count)
- فریم بندی پایت‌گرا (Byte Oriented)
- فریم بندی بیت‌گرا (Bit Oriented)

الف- روش شمارش کاراکتر

در این روش یک کاراکتر در ابتدای هر فریم، طول فریم را مشخص می‌کند. این روش در شکل (۲-۳) نشان داده شده است. در این شکل، چهار فریم را که به روش شمارش کاراکتر درست شده‌اند مشاهده می‌کنید. همانطور که مشخص است، فریمهای اول و دوم پنج کاراکتر، فریم سوم هشت کاراکتر و فریم چهارم هفت کاراکتر است.

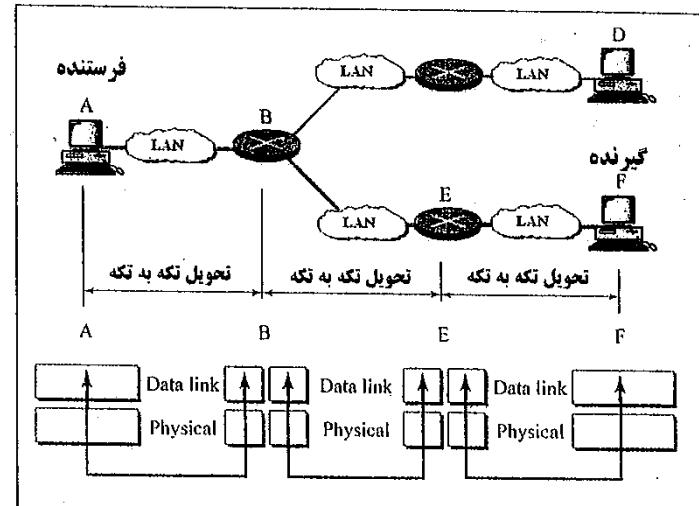


شکل (۲-۳)- روش شمارش کاراکتر

واضح است که این روش نسبت به خطأ بسیار حساس است. حالتی را در نظر بگیرید که کاراکتر حاوی طول فریم به ادلایلی خراب شود. همانطور که در شکل دیده می‌شود، تمامی فریمهای بعد از آن اشتباه خواهند بود.

۱- مقدمه

لایه پیوند داده بین لایه‌های شبکه و فیزیکی قرار گرفته است. این لایه سرویسهایی را برای لایه شبکه فراهم کرده و سرویسهایی را از لایه فیزیکی دریافت می‌نماید. هدف این لایه ارسال اطلاعات در یک تکه از مسیر یا یک جهش (Hop) است (شکل (۱-۳)). منظور از یک جهش، فاصله بین کامپیوتر ارسال گشته با اولین مسیریاب یا فاصله بین دو مسیریاب در طول مسیر است.



شکل (۱-۳)- تحويل تکه به تکه در لایه پیوند داده

به طور کلی می‌توان وظایف این لایه را به صورت زیر خلاصه کرد:

- فریم بندی
- کنترل خطأ (شامل تشخیص و تصحیح خطأ)
- کنترل جریان
- کنترل دسترسی به رسانه

اگرچه به توضیح مفصل هر کدام از وظایف فوق می‌پردازیم

درج بیت های صفر در جاهای مورد نیاز، نشان داده شده است، در طرف گیرنده، الگوی ویژه ابتدا و انتهای فریم و همچنین بیت های صفر قرار گرفته بعد از پنج بیت یک متواالی، حذف می شوند.

داده اولیه	011011111111111111110010
فریم ساخته شده	011111100110111101111101001001111110

شکل (۳-۴)- روش درج بیتی

ب- روش بایت گرا

در این روش با استفاده از بایتهای مخصوصی، ابتدا و انتهای فریم را مشخص می کنیم، مثلاً در پروتکل IMP-IMP از کاراکترهای DLE با کد اسکی 10H، STX با کد اسکی 02 و ETX با کد اسکی 03 برای مشخص کردن شروع و انتهای فریم استفاده می شود.

الگوی مشخص کننده ابتدای فریم: DLE - STX

الگوی مشخص کننده انتهای فریم: DLE - ETX

فریم زیر به این روش ساخته شده است:

DLE	STX	P	L	U	F	L	I	V	E	S	DLE	ETX
-----	-----	---	---	---	---	---	---	---	---	---	-----	-----

اگر در اطلاعات داخل فریم، کاراکتر DLE وجود داشته باشد، برای جلوگیری از بروز خطأ، کاراکتر DLE دیگری نیز در کنار آن درج می شود. به همین دلیل به این روش، روش درج بایتی (Byte Stuffing) هم گفته می شود. این مفهوم در شکل (۳-۳) نشان داده شده است.

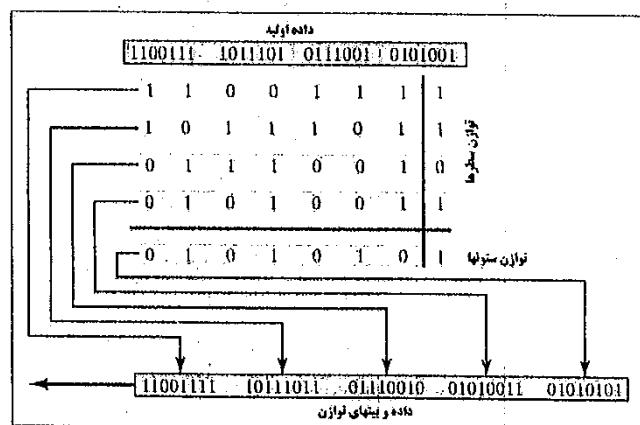
داده اولیه	A	DLE	B				
بایت اضافی درج شده							
DLE	STX	A	DLE	DLE	B	DLE	ETX

شکل (۳-۳)- درج DLE در داخل اطلاعات

ج- روش بیت گرا

در این روش از رشته بیت خاصی برای نشان دادن ابتدا و انتهای فریم استفاده می کنیم، این روش بیشتر از روش های دیگر استفاده می شود. پروتکلهای مشهور HDLC، PPP و SLIP از این روش استفاده می کنند. به عنوان مثال پروتکل HDLC از رشته بیت 01111110 به عنوان الگویی برای مشخص کردن ابتدا و انتهای فریم استفاده می کند. برای جلوگیری از ظهور الگوی ویژه در داخل اطلاعات، بعد از هر پنج بیت ۱ متواالی، یک بیت ۰ درج می شود. به همین دلیل این روش به روش درج بیتی (Bit Stuffing) هم مشهور است. در شکل (۳-۴) یک رشته بیت به عنوان داده اولیه و فریم ساخته شده به روش بیت گرا پس از قرار دادن الگوی ویژه در ابتدا و انتهای فریم و

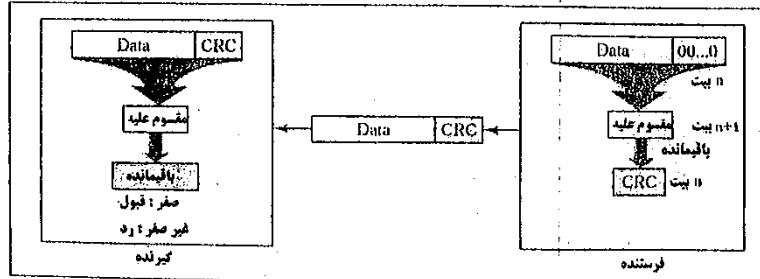
به عنوان مثال، اگر فرستنده^۰ و گیرنده روى توازن فرد توافق کرده باشند، و فرستنده بخواهد رشتہ بیت ۰۱۱۰۱۰۱۰ را برای گیرنده ارسال کند، از آنجا که تعداد بیت‌های ۱ موجود در این رشتہ بیت، زوج است باید بیت توازن نیز ۱ باشد و داده ارسالی به صورت: ۰۱۱۰۱۰۱۰ خواهد بود. از روش توازن می‌توان به صورت دو بعدی نیز استفاده کرد. این روش در شکل (۳-۵) نشان داده شده است. در این روش علاوه بر هر سطر، برای هر ستون نیز بیت توازن را بدست می‌آوریم، در این مثال توازن زوج برای سطراها و ستونها در نظر گرفته شده است.



شکل (۳-۵)- روش توازن دو بعدی برای تشخیص خطا

ب- روش CRC

این روش یکی از قدرتمندترین و پرکاربردترین روش‌های تشخیص خطا می‌باشد که هم در انتقال داده و هم در رسانه‌های ذخیره‌سازی مانند دیسکهای مغناطیسی استفاده می‌شود.



شکل (۳-۶)- روش CRC برای تشخیص خطا

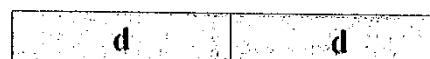
۳- روش‌های تشخیص و تصحیح خطأ

خطأ جزء لاپنهت سیستمهای مخابراتی و ارتباطی است. عوامل زیادی ممکن است باعث بروز خطأ در اطلاعات شوند. ایده‌آل نبودن محیط‌های انتقال داده، نویز، تداخل، تضعیف و بسیاری پدیده‌های دیگر ممکن است باعث شوند که اطلاعات ارسال شده با اطلاعات دریافت شده متفاوت باشند. خطأ ممکن است به صورت نگ‌بیتی و یا چند بیتی (توده‌ای) اتفاق بیفتد. خطاهای توده‌ای عموماً در سیستمهای مخابراتی به دلیل سایه انداختن یک جسم مرتفع مانند ساختمان یا تپه بر روی سیگنال حاوی اطلاعات اتفاق می‌افتد.

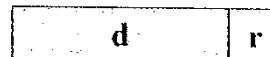
سوال این است که گیرنده از چه طریقی مطمئن شود اطلاعاتی که دریافت کرده است همان اطلاعاتی است که توسط فرستنده ارسال شده است؟

هدف از این بخش بررسی روش‌های تشخیص خطا را به دو دسته تقسیم نمود: کمک می‌کنند. به طور کلی می‌توان روش‌های تشخیص خطا را به دو دسته تقسیم نمود:

- به همراه اطلاعات، یک کپی از آن نیز ارسال شود تا گیرنده از طریق مقایسه این دو، بروز خطا را تشخیص دهد:



- اطلاعات اضافی به همراه داده اصلی ارسال شود:



از آنجا که کارایی روش اول بسیار پایین بوده و عمل نصف پهنای باند را هدر می‌دهد، بحث را روی روش‌های نوع دوم متمرکز می‌کنیم.

الف- روش توازن

در این روش با استفاده از اضافه کردن یک بیت به اطلاعات می‌توان خطا را تشخیص داد. این بیت را بیت توازن می‌نامند. روش کار بین ترتیب است که بسته به اینکه توازن زوج یا فرد را در نظر بگیریم، یک بیت را به اطلاعات چنان اضافه می‌کنیم که تعداد بیت‌های ۱ موجود در داده به احتساب بیت توازن، عددی زوج یا فرد باشد.

$$\begin{array}{r}
 x^8 + x^6 + x^5 + x^3 \\
 \underline{x^8 + x^7 + x^5} \\
 \hline
 x^7 + x^6 + x^3 \\
 \underline{x^7 + x^6 + x^4} \\
 \hline
 x^4 + x^3 \\
 \underline{x^4 + x^3 + x} \\
 \hline
 x
 \end{array}
 \quad
 \begin{array}{r}
 x^3 + x^2 + 1 \\
 \hline
 x^5 + x^4 + x
 \end{array}$$

دقت کنید که تفریقها در مازول دو انجام شده‌اند؛ بدین معنی که ضرایب x منفی نمی‌شوند.
در حقیقت در هر مرحله ضرایب جملات هم توان، با هم XOR می‌شوند.
درجه چندجمله‌ای باقیمانده یک واحد از درجه چندجمله‌ای مولد کوچکتر می‌باشد؛ بنابراین باقیمانده به صورت چندجمله‌ای $(0x^0 + 1x^1 + 0x^2 + 0x^3)$ خواهد بود که اگر رشتہ بیت معادل آنرا بدست آوریم خواهیم داشت:

$$R(x) = 0x^2 + 1x + 0 \rightarrow R = 010$$

در نهایت رشتہ بیت باقیمانده به سمت راست رشتہ بیت پیغام افزوده شده، برای گیرنده ارسال می‌شود. رشتہ بیت حاصل را Codeword هم می‌گویند:

رشته ارسال شده: **101101 010**

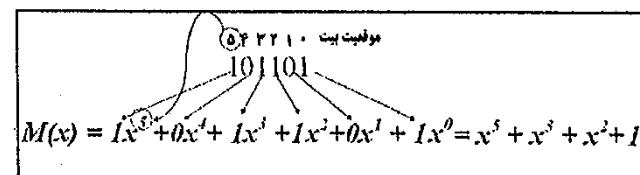
نحوه تشخیص خطأ در طرف گیرنده بدین ترتیب است:
چندجمله‌ای معادل codeword را به دست آورده بر چندجمله‌ای مولد تقسیم می‌نماییم.
اگر باقیمانده تقسیم، صفر باشد، داده دریافت شده فاقد خطأ و اگر غیر صفر باشد، خطأ دار بوده و از آن صرف نظر می‌شود. دقت کنید که خطأ هم در قسمت پیغام و هم در قسمت CRC ممکن است رخداد که این روش هر دو را می‌تواند تشخیص دهد.
در شکل (۸-۳) دو حالت خطأ دار و بدون خطأ بودن Codeword دریافتی نشان داده شده است.

در این روش، محاسباتی ریاضی بر روی بلوکی از داده‌ها انجام گرفته و اطلاعات اضافی از آن استخراج می‌شود. این اطلاعات به انتهای داده اصلی چسبانده شده، گیرنده را در ردیابی خطأ کمک می‌کند. اساسن کار این الگوریتم، یک چندجمله‌ای به نام چندجمله‌ای مولد می‌باشد. چندجمله‌ای مولد برای گیرنده و فرستنده مشخص بوده و در پروتکلهای مختلف متفاوت است. در زیر تعدادی از چندجمله‌ایهای مولد در پروتکلهای مختلف نشان داده شده است:

- CRC-16 = $x^{16} + x^{15} + x^2 + 1$ (HDL)
- CRC-CCITT = $x^{16} + x^{12} + x^5 + 1$
- CRC-32 = $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$ (Ethernet)

قبل از اینکه روش CRC را بیشتر توضیح دهیم، لازم است نکاتی را در مورد نحوه نمایش یک رشتہ بیت به صورت یک چندجمله‌ای، مذکور شویم.

یک رشتہ بیت را می‌توان به صورت یک چندجمله‌ای در آورد اگر برای هر بیت: مقدار آن بیت به عنوان ضریب چند جمله‌ای و موقعیت آن را به صورت توان چندجمله‌ای در نظر بگیریم. به عنوان مثال، چندجمله‌ای معادل رشتہ بیت 101101 به صورت $1x^5 + x^2 + x^3 + x^4 + x^5$ خواهد بود. نحوه انجام کار در شکل (۷-۳) نشان داده شده است.



شکل (۷-۳)- تبدیل یک رشتہ بیت به چندجمله‌ای

روش محاسبه CRC بدین ترتیب است که ابتدا رشتہ بیت پیغام را به صورت چندجمله‌ای در می‌آوریم:

$$M = 101101 \rightarrow M(x) = x^5 + x^2 + 1$$

سپس چندجمله‌ای حاصل را در x^n ضرب می‌نماییم که n بالاترین توان چندجمله‌ای مولد است. دقت کنید که این کار مانند افزودن n بیت صفر به سمت راست رشتہ پیغام است (شکل (۳-۶)).

مثلاً اگر چندجمله‌ای مولد $G(x) = x^3 + x^2 + 1$ باشد، داریم:

$$P(x) = M(x) \cdot G(x) = M(x) \cdot x^3 = x^8 + x^6 + x^5 + x^3$$

سپس چندجمله‌ای حاصل را بر چندجمله‌ای مولد تقسیم کرده باقیمانده تقسیم را بدست می‌آوریم:

به نظر شما اعداد فوق بر چه اساسی در هر گروه قرار رفته‌اند؟ روش محاسبه بیتهاي ۱ به اين صورت است که مثلا اگر طرفين روی توازن زوج توافق کرده باشند، برای محاسبه A_1 باید توازن بیتهاي يازدهم، نهم، هفتم، پنجم و سوم به همراه بیت ۲۱ زوج باشد. برای بیتهاي دیگر نیز به همین ترتیب عمل می‌کنیم. در شکل (۳-۱۰) نحوه به دست آوردن codeword از روی داده ثابت نشان داده شده است.

شکل (۳-۱۰)- روش بدست آوردن بیتهای افزونگی

فرض کنید که **codeword** فوق توسط فرستنده ارسال شود ولی در هنگام ارسال، بیت هفتم از سمت راست دچار خطأ گردد. در نتیجه، رشته بیت 1010010101 توسط گیرنده دریافت می‌گردد. سوال این است که گیرنده از چه طریقی متوجه خطأ شده و حتی آن را تصحیح می‌کند؟
 نحوه انجام کار در شکل (۳-۱) نشان داده شده است. همانطور که مشاهده می‌گردد، دوباره توازن هر کدام از گروههای ذکر شده، محاسبه می‌شود و برای هر گروه یک بیت به دست می‌آید. در هماییت یک رشته چهار بیتی حاصل شده و با محاسبه عدد مبنای ده معادل آن، موقعیت بیت خطأدار به دست می‌آید. تا این مرحله خطأ را تشخیص داده‌ایم و محل آن را هم مشخص نموده‌ایم، برای تصحیح خطأ کافی است بیتی که در این محل قرار گرفته است، عکس شود.

$\begin{array}{c c} x^8 + x^6 + x^5 + x^3 + x & x^3 + x^2 + 1 \\ \hline x^8 + x^7 + x^5 & x^5 + x^4 + x \end{array}$ $\begin{array}{c} x^7 + x^6 + x^3 + x \\ x^7 + x^6 + x^4 \end{array}$ $\begin{array}{c} x^4 + x^3 + x \\ x^4 + x^3 + x \end{array}$	$\begin{array}{c c} x^8 + x^6 + x^5 + x & x^3 + x^2 + 1 \\ \hline x^8 + x^7 + x^5 & x^5 + x^4 + x \end{array}$ $\begin{array}{c} x^7 + x^6 + x \\ x^7 + x^6 + x^4 \end{array}$ $\begin{array}{c} x^4 + x \\ x^4 + x^3 + x \end{array}$
$\xrightarrow{\text{با قیمتاند د صفر}} 0$	$\xrightarrow{\text{با قیمتاند د شیر صفر}} x^3$

شکل (۳-۸)- نحوه تشخیص خطا در روش CRC

ج - روش همینگ

کدگذاری همینگ روشنی برای تشخیص و تصحیح یک بیت خطای داده هفت بیتی می‌باشد. در این روش چهار بیت افزونگی به هفت بیت داده چسبانده شده و در نهایت یک بلوك یا زاده بیتی تشکیل می‌گردد. بیتهای افزونگی در موقعیتهای ۱ و ۲ و ۴ و ۸، مطابق شکل (۳-۹) قرار می‌گیرند.

برای سهولت در مراجعات بعدی، این بیستها را به ترتیب r1, r2, r4 و r8 نامگذاری می‌کنیم.

11	10	9	8	7	6	5	4	3	2	1
d	d	d	r_3	d	d	d	r_4	d	r_2	r_1

شکل (۹-۳)- موقعيت بيتهای داده و افزونگی

هر بیت^{۱۰} از طریق محاسبه بیت توازن پرای مجموعه‌ای از بیتها داده بودست می‌آید:

r1 : 1, 3, 5, 7, 9, 11
r2 : 2, 3, 6, 7, 10, 11
r4 : 4, 5, 6, 7
r8 : 8, 9, 10, 11

۴- کنترل جریان

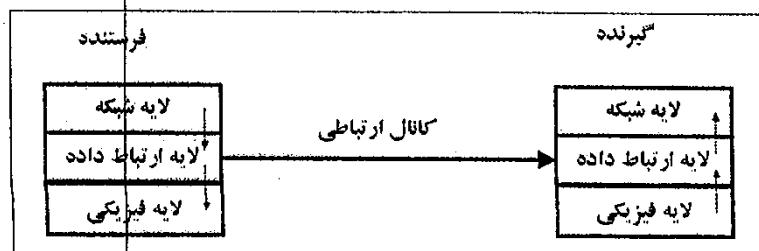
به طور مختصر منظور از کنترل جریان، مدیریت تارخ ارسال داده بین طرفین است؛ بدین معنی که تدبیری اتخاذ کنیم که فرستنده بیشتر از ظرفیت بافر گیرنده، داده ارسال نکند. این کار هم در این لایه و هم در سطح بالاتری در لایه انتقال انجام می‌گردد. اگر کنترل جریان انجام نگردد، فرستنده بدون توجه به وضعیت گیرنده داده‌ها را ارسال نموده و این کار باعث می‌شود که کانال ارتباطی اشغال گردد اگرچه در حقیقت کار مفیدی انجام نمی‌شود؛ به عبارت دیگر، از منابعی که در اختیار داریم به صورت بهینه استفاده نمی‌کنیم.

حجم بافر گیرنده و کیفیت کانال ارتباطی، مواردی هستند که باید مد نظر قرار گیرند. بررسی مساله را با ساده‌ترین حالت شروع می‌کنیم:

- حجم بافر گیرنده نامحدود باشد.
- کانال ارتباطی بدون خطا باشد.

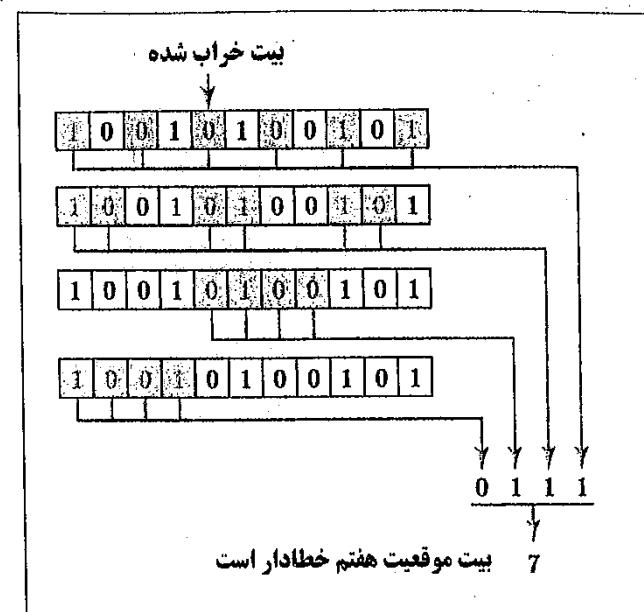
واضح است که چنین حالتی که اصطلاحاً به آن **utopia** یا همان مدینه فاضلله گفته می‌شود، در عمل امکان پذیر نیست.

لایه پیوند داده در طرف فرستنده باید اطلاعاتی را از لایه شبکه دریافت نموده و تحويل لایه فیزیکی دهد. در طرف گیرنده نیز باید اطلاعاتی را از لایه فیزیکی تحويل گرفته، به لایه شبکه تحويل نماید. (شکل (۱۲-۳))



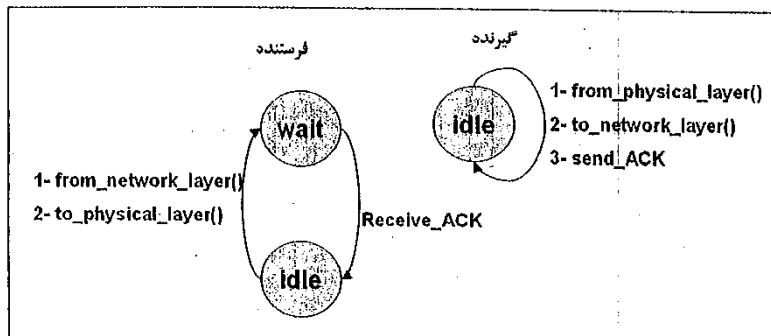
شکل (۱۲-۳)- موقعیت لایه پیوند داده

اگر فرستنده و گیرنده را به صورت ماشین حالت (State Machine) نشان دهیم، هر دو دارای فقط یک حالت **idle** یا بیکار هستند مگر اینکه اطلاعاتی برای ارسال و یا دریافت داشته باشند؛ که



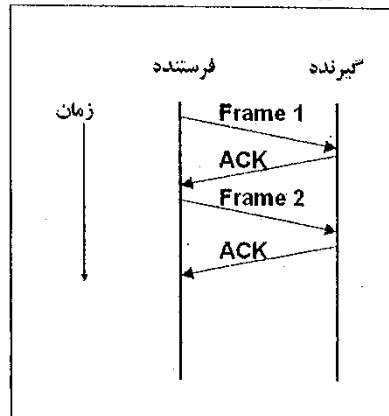
شکل (۱۱-۳)- نحوه تصحیح خطأ در روش Hamming

در این حالت گیرنده باید آمادگی خود را جهت دریافت اطلاعات به فرستنده اعلام نماید. این کار با ارسال سیگنالی به نام Acknowledge، یا به اختصار ACK توسط گیرنده انجام می‌گردد. ماشین حالت فرستنده این بار کمی متفاوت و دارای دو حالت idle و wait خواهد بود. فرستنده پس از ارسال اطلاعات، به حالت wait می‌رود و تا زمان دریافت سیگнал ACK در این وضعیت باقی می‌ماند. همچنین گیرنده، پس از تحويل اطلاعات به لایه شبکه سیگنال ACK را نیز ارسال می‌نماید.



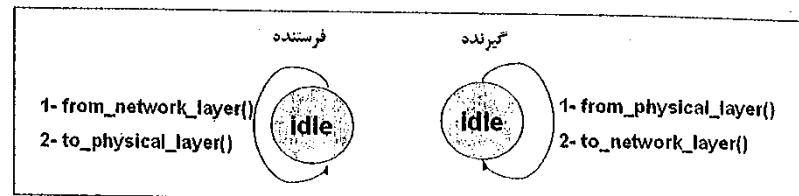
شکل(۱۵-۳)- کنترل جریان با سیگنال ACK

نمودار زمانی این حالت، به صورت شکل(۱۶-۳) خواهد بود.



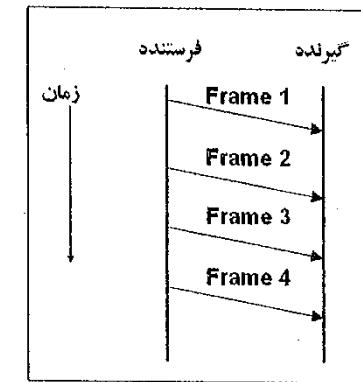
شکل(۱۶-۳)- کنترل جریان به صورت Stop & Wait

در آن صورت پس از انجام دو عمل دوباره به حالت بیکار برمی‌گردند. به عنوان مثال اگر طرف فرستنده اطلاعاتی برای ارسال داشته باشد، در لایه پیوند داده آن را از لایه شبکه گرفته، تحويل لایه فیزیکی می‌دهد. این عمل را مثلاً می‌توان به صورت دو زیربرنامه که در این لایه کار می‌کنند، در نظر گرفت. (شکل(۱۳-۳))



شکل(۱۳-۳)- ماشینهای حالت فرستنده و گیرنده در حالت ایده‌آل

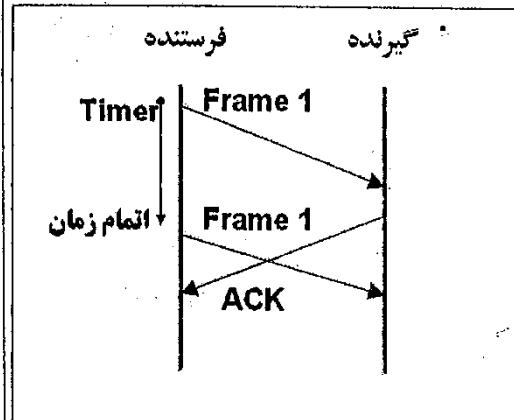
حالت فوق را اگر به صورت نمودار زمانی نشان دهیم، شکل(۱۴-۳) حاصل می‌گردد که در آن فرستنده بدون نگرانی از صحبت دریافت و یا آمادگی گیرنده، اطلاعات خود را پشت سرهم ارسال می‌نماید.



شکل(۱۴-۳)- ارسال اطلاعات به صورت متواالی

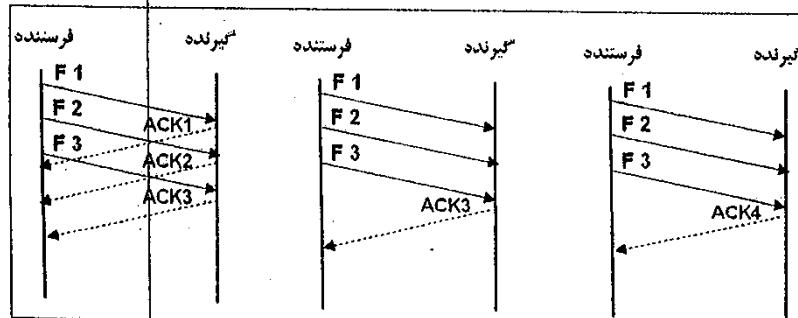
اکنون مساله را کمی واقعی‌تر کرده و فرض می‌کنیم:

- حجم بافر گیرنده محدود باشد.
- کanal ارتباطی بدون خطأ باشد.



شکل(۳-۱۸)- ارسال مجدد به دلیل به سر رسیدن زمان

کارایی روش Stop & wait به دلیل تاخیر زیاد پایین است به همین خاطر در پروتکلهای واقعی، فرستنده مناسب با ظرفیت کanal و زمان تاخیر انتشار، چندین بسته اطلاعاتی پشت سرهم ارسال می‌کند و منتظر دریافت ACK نمی‌ماند؛ به این امید که سیگنالهای ACK بعداً دریافت می‌گردند. در این مورد سیگنالهای ACK نیز باید شماره سریال داشته باشند تا معلوم شود که هر کدام مربوط به کدام بسته می‌باشند. گیرنده می‌تواند برای هر بسته داده یک سیگنال ACK ارسال نماید و یا اینکه آخرین بسته دریافت شده را ACK کند و یا اینکه بسته‌ای را که انتظار دارد دریافت کند، ACK نماید (شکل(۳-۱۹)).



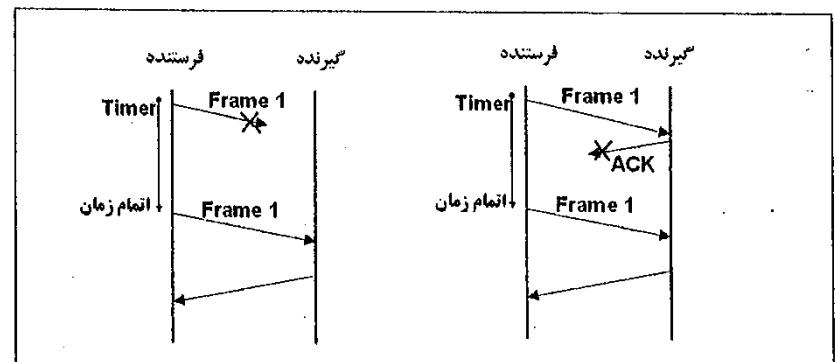
شکل(۳-۱۹)- انواع مختلف مکانیزم ACK

این وضعیت را stop and wait نیز می‌نامند. واضح است که استفاده از این روش برای مبینهای با تاخیر انتشار زیاد، مقرن به صرفه نیست؛ زیرا زمان زیادی صرف انتظار برای دریافت سیگنال ACK می‌گردد.

- اکنون حالت واقعی را بررسی می‌نماییم و فرض می‌کنیم که:
 - حجم بافر گیرنده محدود باشد.
 - کanal ارتباطی دارای خطأ باشد.

در این وضعیت امکان خراب شدن داده و یا سیگنال ACK وجود دارد. برای تشخیص این حالت فرستنده از یک Timer استفاده می‌کند. بدین ترتیب که به هنگام فرستن داده، Timer را به کار می‌اندازد و اگر قبیل از رسیدن سیگنال ACK زمان به اتمام برسد، مجدداً داده قبلی را ارسال می‌نماید.

در شکل (۳-۱۷) نحوه ارسال مجدد با به سر رسیدن زمان، نشان داده شده است.

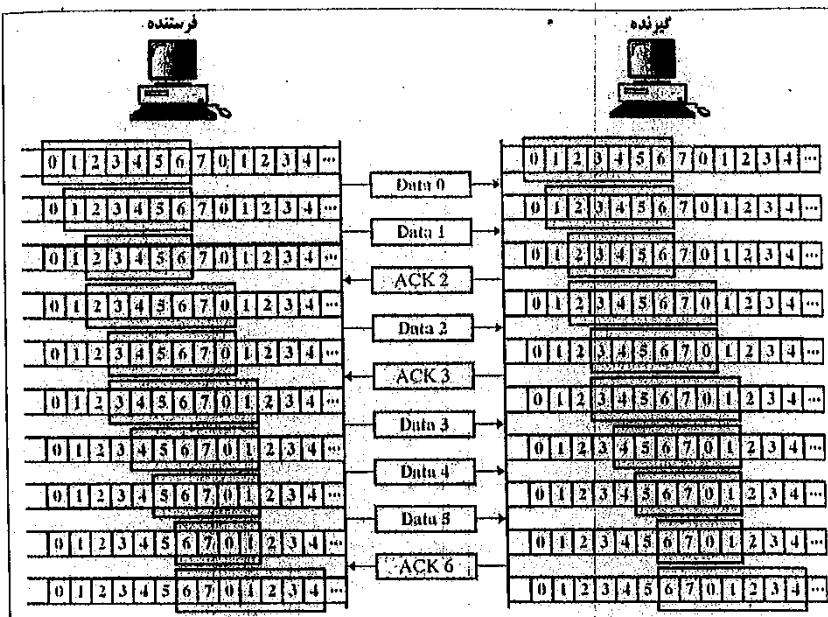


شکل(۳-۱۷)- استفاده از Timer برای ارسال مجدد

بته باید مقدار Timer طوری انتخاب شود که فرصت کافی به گیرنده برای ارسال ACK بدهد. به طوری که اگر مقدار Timer کوچک انتخاب شود مطابق شکل (۳-۱۸)، فرستنده با تصور اینکه داده قبلی به گیرنده نرسیده است، آن را مجدد ارسال می‌نماید که در این حالت گیرنده دو کپی از اطلاعات را دریافت نموده که باید از یکی صرفنظر نماید.

پروتکل پنجره لغزان

بسته‌هایی که ارسال می‌شوند دارای شماره سریال می‌باشند. از آنجا که از تعداد بیت‌های محدودی برای شماره‌گذاری بسته‌ها استفاده می‌شود، شماره‌ها بعد از مدتی تکرار خواهند شد. مثلاً اگر سه بیت را برای شماره‌گذاری اختصاص دهیم، شماره بسته‌ها از صفر تا ۷ خواهند بود و مجدداً بعد از بسته شماره ۷، بسته‌ای با شماره صفر خواهیم داشت. دقت کنید که این بسته، با بسته شماره صفر قبلی متفاوت است اگرچه دارای شماره یکسانی می‌باشد. بنابراین اگر تعداد بسته‌هایی که در روش قبل ارسال می‌شوند زیاد باشد، دو بسته با شماره یکسان به گیرنده رسیده و گیرنده به تصور اینکه این بسته‌ها تکراری بوده، فقط یکی از آنها را می‌پذیرد. برای جلوگیری از این وضعیت، فرستنده و گیرنده را موظف می‌کنیم که فقط محدوده مشخصی از بسته‌ها را ارسال و یا دریافت نمایند. این محدوده را اصطلاحاً پنجره می‌گوییم. در شکل (۲۰-۳) یک پنجره با اندازه هفت، نشان داده شده است.



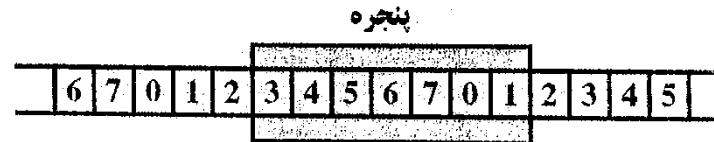
شکل (۲۰-۳)- نحوه کار روش پنجره لغزان برای کنترل جریان

در صورت خراب شدن یک بسته، برای ارسال مجدد دو استراتژی می‌توان اتخاذ نمود:

- از بسته خراب شده به بعد مجدد ارسال شوند.
- فقط بسته خراب شده مجدد ارسال شود.

حالات اول هنگامی استفاده می‌شود که ظرفیت پنجره گیرنده فقط به اندازه یک بسته باشد، و در نتیجه در صورت خرابی یک بسته، حتی اگر بسته‌های بعدی صحیح دریافت شوند، چون جایی برای نگهداری آنها و سپس مرتب کردنشان ندارد، آنها را نادیده گرفته و فرستنده باید مجدداً همه آنها را ارسال نماید.

اگر ظرفیت پنجره گیرنده بیشتر باشد، می‌تواند در صورت خرابی یک بسته، بسته‌های بعدی را نگهداری نموده پس از دریافت مجدد بسته خراب شده آنها را مرتب کرده تحويل لایه بالاتر نماید. روش اول را اصطلاحاً Go-back-N یا برگشت N تابی به عقب، و روش دوم را Selective repeat یا تکرار انتخابی می‌گویند. شکلهای (۲۲-۳) و (۲۳-۳) این دو روش را نشان می‌دهند.



شکل (۲۰-۳)- مفهوم پنجره لغزان

اندازه پنجره‌های فرستنده و گیرنده می‌تواند ثابت و یا متغیر باشد. در شکل (۲۱-۳) نحوه کار این پروتکل نشان داده شده است. در طرف فرستنده با فرستادن هر بسته داده، حد بالای پنجره یک واحد به سمت راست حرکت می‌کند و با دریافت هر سیگنال ACK، حد بالای پنجره به تعداد بسته‌های ارسال شده، به طرف راست حرکت می‌نماید. در طرف گیرنده، حد پایین پنجره با دریافت یک بسته داده، یک واحد و حد بالای آن با ارسال هر سیگنال ACK، به تعداد بسته‌های دریافت شده به سمت راست حرکت می‌کند. احتمالاً تاکتون دلیل نامگذاری این پروتکل به "پنجره لغزان" را متوجه شده باشید.

۵- کنترل دسترسی به کانال (MAC)

همانطور که قبلاً گفته شد، اجزای یک شبکه می‌توانند به صورت نقطه به نقطه و یا پخشی از یک لینک استفاده کنند. در حالت نقطه به نقطه، مشکلی به نام نحوه تخصیص کانال نداریم؛ چراکه کانال ارتباطی فقط در اختیار دو طرف گیرنده و فرستنده است. اما در حالتی که تعدادی کامپیوتر از یک کانال مشترک استفاده می‌کنند، کنترل دسترسی به آن و اینکه چه وقت و کدامک از کانال مشترک استفاده کنند، یک مساله اساسی است. یکی از مهمترین وظایف لایه پیوند داده کنترل نحوه دسترسی به یک رسانه یا کانال مشترک می‌باشد. هنگامی که چند کامپیوتر از یک کانال مشترک استفاده می‌نمایند (مثلًا در توپولوژی خطی)، باید نحوه استفاده این کامپیوترها از کانال مدیریت شود. این دقیقاً همان چیزی است که در جلسات اتفاق می‌افتد. اگر روشی برای مدیریت جلسه وجود نداشته باشد و هر کس هر وقت که دلش بخواهد شروع به صحبت نماید، مسلم است که هیچ کس حرف دیگری را متوجه نخواهد شد و جلسه کاملاً بی‌فاایده و بی‌نتیجه خواهد ماند. یک راه حل ساده این است که اگر کسی حرفی برای گفتن داشته باشد ابتدا دست خود را بالا برد و پس از کسب اجازه از مدیر جلسه، شروع به صحبت نماید.

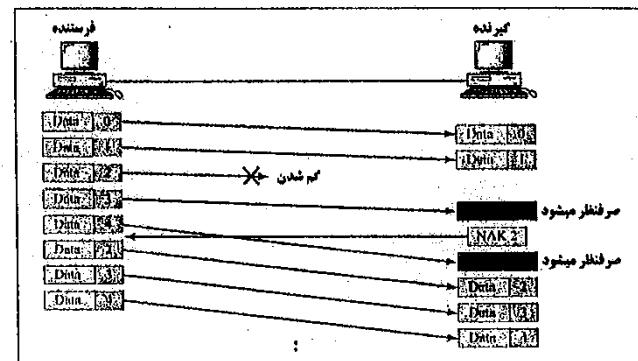
به طور کلی دو نوع روش برای تخصیص کانال وجود دارد:

- روشهای استاتیک مانند FDM و TDM؛ که در آنها محدودهای از کانال از لحاظ فرکانسی یا زمانی در اختیار کاربر خاصی قرار می‌گیرد چه اطلاعاتی برای ارسال داشته باشد چه خیر.
- روشهای دینامیک یا پویا که در آنها با توجه به وضعیت و ترافیک شبکه، در هر لحظه ممکن است تخصیص کانال متفاوت باشد.

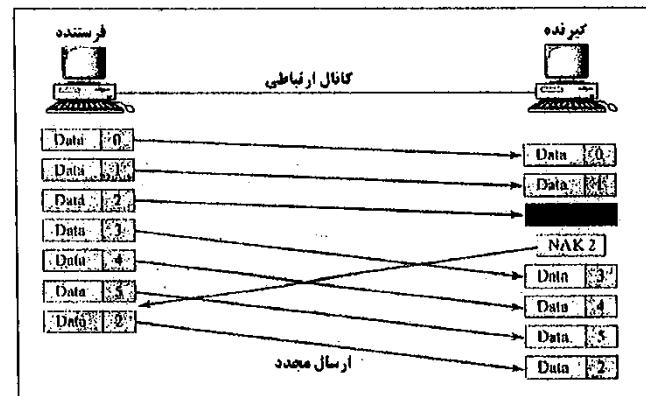
در این قسمت بحث را روی نوع دوم یا روشهای دینامیکی متمرکز می‌کنیم. قبل از اینکه وارد بحث اصلی شویم، اجازه بدھید که در مورد مفهوم collision یا تصادم در شبکه مقدماری صحبت کنیم. اگر دو یا چند کامپیوتر، در یک محیط ارتباطی مشترک، به صورت همزمان اقدام به ارسال اطلاعات نمایند، تصادم یا برخورد اتفاق می‌افتد. به عبارت دیگر سیگнал غیر معتبری در داخل کانال ایجاد می‌شود که در نتیجه اطلاعات موجود در کانال برای هیچ کدام از کامپیوترها قابل استفاده نبوده و باید مجدداً ارسال شوند. وقوع تصادم توسط کارت شبکه قابل تشخیص است.

دقت کنید که در این حالت به جای استفاده از سیگنال ACK، از سیگنال NAK به معنای عدم دریافت صحیح، استفاده می‌شود.

اگر ارتباط به صورت دوطرفه باشد، می‌توان سیگنال ACK بسته دریافتی را همراه بسته‌ای که می‌خواهیم ارسال نماییم، تلفیق نموده به صورت یک بسته واحد ارسال نمود. این روش را اصطلاحاً کول سواری یا Piggy-Backing می‌نامند که در پروتکل TCP استفاده می‌شود.



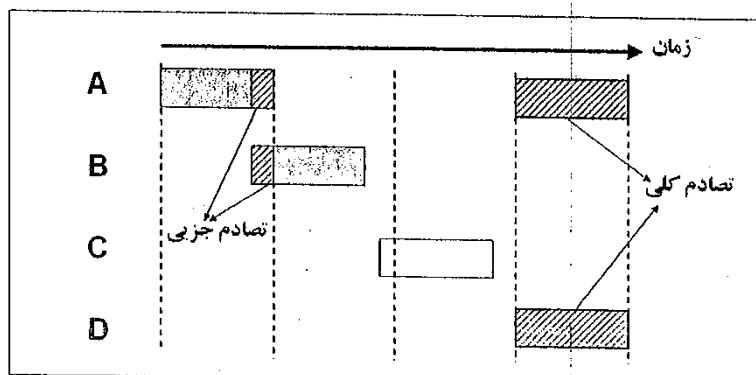
شکل (۳-۲۲)- روش Go-Back-N برای ارسال مجدد



شکل (۳-۲۳)- روش Selective-repeat برای ارسال مجدد

موحّب می‌شود که هیچ کدام از فریم‌ها قابل استفاده نباشد. وقت کنید که اگر حتی یک بیت از انتهای یک فریم با بیتی از ابتدای فریم دیگر برخورد نماید، تصادم اتفاق افتاده و فریمهای مذکور به درد نخور خواهند بود.

به حالتی که قسمتی از انتهای یک فریم با قسمتی از ابتدای فریم دیگر برخورد می‌کند، تصادم جزئی گفته می‌شود. حالت دیگر این است که دو ایستگاه دقیقاً در یک لحظه شروع به ارسال نمایند که در نتیجه دو فریم کاملاً هم پوشانی خواهند داشت و اصطلاحاً تصادم کلی اتفاق می‌افتد. همانطور که احتمالاً حدس زده باشید و در شکل نیز مشاهده می‌گردد، کارایی این روش بسیار پایین بوده و حدود ۱۸٪ می‌باشد. یعنی در هر ۱۰۰ فریم ارسالی، به طور متوسط ۸۲ فریم به علت تصادم از بین می‌روند.



شکل(۳)-۲۵-۳)-تصادم در پروتکل الوها

ب- روش الوهای برهمهای (Slotted Aloha)

اشکال عمده روش قبل این بود که هر کامپیوتر هر وقت که تمایل داشت می‌توانست اقدام به ارسال نماید. در این روش زبان به بازمهای مساوی تقسیم می‌شود و ایستگاهها فقط در ابتدای بازمهای زمانی، مجاز به ارسال هستند. واضح است که در این حالت، یا اصلاً تصادم اتفاق نمی‌افتد و یا اینکه به صورت کلی خواهد بود. کارایی این روش دو برابر حالت قبل و حدود ۳۶٪ می‌باشد.

روشهای دینامیک را می‌توان به سه دسته تقسیم نمود:

۱- روش‌هایی که احتمال تصادم در آنها وجود دارد. مانند: الوها (ALOHA)، الوهای برهمهای

CSMA/CD، CSMA و Slotted ALOHA)

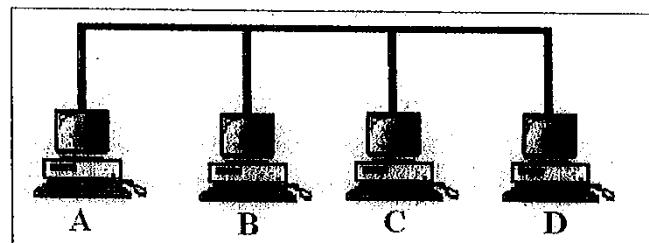
۲- روش‌هایی که احتمال تصادم در آنها وجود ندارد مانند: Bitmap یا روش رزروسازی، روش انتقال نشانه (Token passing) و روش شمارش معکوس دودوبی (Binary countdown).

۳- روش‌های بینابین که در بار کم مشابه روشهای نوع دوم و در بار زیاد مشابه روشهای نوع اول عمل می‌کنند. مانند: Adaptive Tree walk

الف- روش الوها (ALOHA)

در سال ۱۹۷۰، پروتکلی در دانشگاه هاوایی به منظور ارتباط رادیویی جزایر هاوایی برای مساله تخصیص کانال ارائه شد.

ایده اصلی Aloha بسیار ساده است: به کاربران اجازه دهید هر زمان داده‌ای برای ارسال داشته‌ند، آن را بفرستند. مسلم است که در این روش احتمال وقوع برخورد زیاد است. در صورت بروز تصادم، کاربران مجدداً برای ارسال سعی می‌کنند. در شکل(۲۴-۳) چهار ایستگاه کاری که در یک کانال مشترک هستند نشان داده شده است.



شکل(۳)-۲۴-۳)-استفاده از کانال مشترک

فرض کنید که این ایستگاهها از روش ALOHA برای ارسال اطلاعات استفاده می‌کنند. اندازه فریمهای بیکسان در نظر گرفته می‌شود. همانطور که در شکل(۲۵-۳) مشاهده می‌گردد، ایستگاهها در زمانهای دلخواه اقدام به ارسال نموده‌اند. این کار موجب شده است که در زمانهای مشخصی فریمهای ارسالی با یکدیگر برخورد نماید. مثلاً در شکل مشاهده می‌گردد که انتهای فریم ارسالی توسعه ایستگاه A، با ابتدای فریم ارسال شده توسط ایستگاه B، تصادم نموده است. این امر

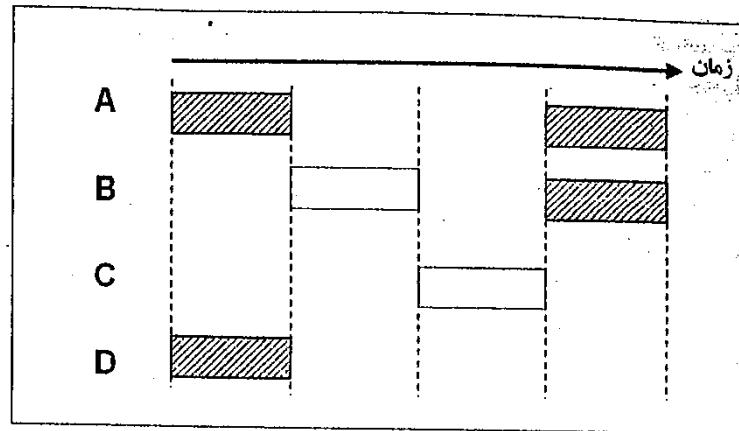
در این روش کانال کنترل می‌شود و در صورت مشغول بودن، پس از گذشت زمان تصادفی، دوباره چک می‌شود و در صورت خالی بودن، اطلاعات ارسال می‌گردد.

برای فرک بهتر دو روش فوق، حالتی را در نظر بگیرید که مثلاً برای کاری به یک اداره مراجعه نموده و با رئیس آن اداره کار داشته باشید. اگر در آن لحظه رئیس جلسه داشته باشد و نتواند شما را پیدا کرد، شما یا می‌توانید همانجا منتظر بمانید تا جلسه به انمام برسد (Persistent) و یا اینکه به سراغ کار خود رفته، پس از مدتی دوباره باز گردید (Non-Persistent).

۵- روش CSMA با تشخیص برخورد یا CSMA/CD

در این روش به محض تشخیص برخورد، از ارسال بقیه فریم ممانعت می‌شود و کارت شبکه سیگنالی موسوم به Jam جهت آگاهسازی سایرین و جلوگیری از ارسال اطلاعات توسط آنها، تولید می‌نماید. کامپیوترهایی که دچار تصادم شده‌اند، پس از گذشت مدت زمان تصادفی که با استفاده از الگوریتم Back-off محاسبه می‌شود، مجدداً اطلاعات را ارسال می‌کنند. این روش در پروتکل Ethernet مورد استفاده قرار می‌گیرد.

کار الگوریتم Back-off تولید زمان تصادفی برای انتظار و تلاش مجدد جهت ارسال می‌باشد. در این الگوریتم پس از هر برخورد، ۱۶ بار سعی در ارسال مجدد صورت می‌گیرد. روش کار بدین ترتیب است که زمان به بازه‌های مساوی ($5/12$ میکروثانیه) تقسیم می‌گردد. پس از برخورد اول، کامپیوترهای صفر یا یک بازه زمانی منتظر می‌مانند و سپس مجدداً اقدام به ارسال می‌کنند. اگر هر دو کامپیوتر مثلاً یک بازه زمانی صبر کنند، مجدداً برخورد اتفاق افتاده و این بار باید به طور تصادفی، ۱، ۲، ۳ یا ۴ بازه زمانی صبر کنند. به طور کلی در برخورد n ام باید یکی از (-2^n) بازه زمانی را انتخاب نمایند. در برخورد دهم باید یکی از ۱۰۲۳ بازه زمانی انتخاب شود. این تعداد دیگر افزایش نمی‌یابد و تا سعی مجدد شانزدهم، همان ۱۰۲۳ بازه باقی می‌ماند. روش کار الگوریتم Back-off در شکل (۲۷-۳) نشان داده شده است.



شکل (۲۶-۳)- تصادم در الوهای برهه‌ای

ج- روش دسترسی چندگانه با حس کردن حامل یا CSMA در این روش ایستگاه‌ها قبل از ارسال، کنترل می‌کنند که آیا کانال خالی است یا خیر؟ در صورت مشغول بودن کانال منتظر می‌مانند و در صورت خالی بودن، اقدام به ارسال اطلاعات می‌کنند.

ظاهراً چنین به نظر می‌رسد که دیگر احتمال برخورد وجود ندارد. اما اگر دو کامپیوتر با هم کانال را کنترل کنند و هر دو آن را خالی تشخیص نهند، همزمان شروع به ارسال کرده که منجر به بروز تصادم می‌گردد. حتی اگر با هم شروع به ارسال ننمایند نیز، به علت تاخیر انتشار سیگнал در کانال، احتمال وقوع برخورد وجود دارد.

پیاده‌سازی این روش به دو صورت امکان پذیر است:
• Persistent CSMA: در این روش کانال کنترل می‌شود و در صورت خالی بودن، اطلاعات ارسال می‌شود. در غیر اینصورت به طور مداوم کانال چک می‌شود تا به محض خالی شدن، ارسال انجام گردد.

این روش خود دارای دو نوع پیاده‌سازی است: ۱-persistent و p-persistent. در حالت اول بعد از خالی شدن خط، با احتمال یک (100%)، و در حالت دوم با احتمال p ، ارسال انجام می‌گردد که در نتیجه حالت اول سریعتر ولی با احتمال بروز برخورد بیشتر و حالت دوم کندرتر ولی با احتمال برخورد کمتر می‌باشد.

بیشترین کارایی این روش هنگامی است که تمام ایستگاهها بخواهند اطلاعات ارسال کنند و در نتیجه از زمان رزروسازی استفاده بهینه می‌شود.
اگر یک ایستگاه بلا فاصله پس از عبور بیت مربوط به خود در زمان رزروسازی، تصمیم به ارسال نماید، باید تا زمان رزروسازی بعدی منتظر بماند.

و- روش شمارش معکوس دودویی (Binary countdown)

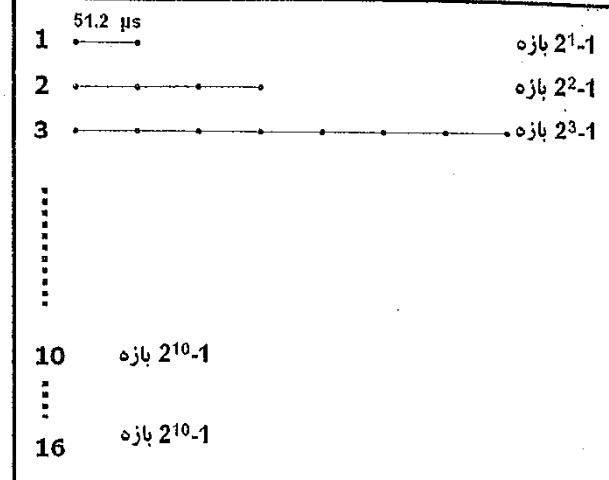
در این روش به هر ایستگاه یک عدد باینری به عنوان آدرس آن، نسبت داده می‌شود. ایستگاههایی که قصد ارسال داده را داشته باشند، ابتدا اولین بیت از سمت چپ را اعلام نموده و سپس این بیتها با هم دیگر OR می‌شوند. ایستگاههایی که نتیجه OR با بیت مذکورشان یکی نباشد از چرخه رقابت کنار می‌روند. به عبارت دیگر ایستگاههای با آدرس بیشتر باقی می‌مانند. سپس دومین بیت سمت چپ ایستگاههای باقیمانده اعلام می‌شود. این کار ادامه می‌یابد تا زمانی که همه ایستگاهها بجز یکی از رقابت کنار بکشند. در نهایت ایستگاه باقیمانده کانال را در اختیار می‌گیرد.

مثلثاً اگر ایستگاههای A و B و C و D، با آدرس‌های داده شده، سعی در تصالح کانال نمایند. در مرحله اول ایستگاههای A و D از چرخه رقابت خارج می‌شوند و ایستگاههای B و C به رقابت ادامه می‌دهند. این کار تا بازه زمانی چهارم ادامه می‌یابد تا در نهایت ایستگاه C کانال را در دست بگیرد.

A: 0010 B: 1010 C: 1011 D: 0100

ز- روش ردوبدل کردن نشانه (Token Passing)

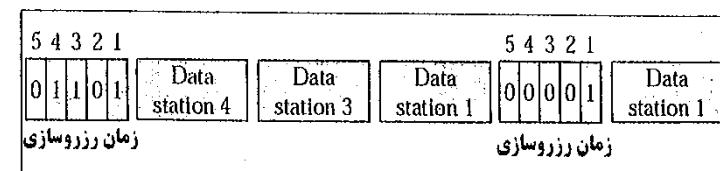
این روش در شبکه‌های با توپولوژی حلقوی مانند Token ring استفاده می‌شود. در این روش بسته کوچکی به نام نشانه (Token) مسدام در حال چرخش در داخل حلقه می‌باشد. هر کدام از ایستگاهها تنها در صورتی می‌خواهد اطلاعات خواهد بود که ابتدا Token را در اختیار بگیرند. به دلیل اینکه در هر لحظه Token فقط در اختیار یکی از ایستگاههاست، احتمال وقوع برخورد وجود ندارد.



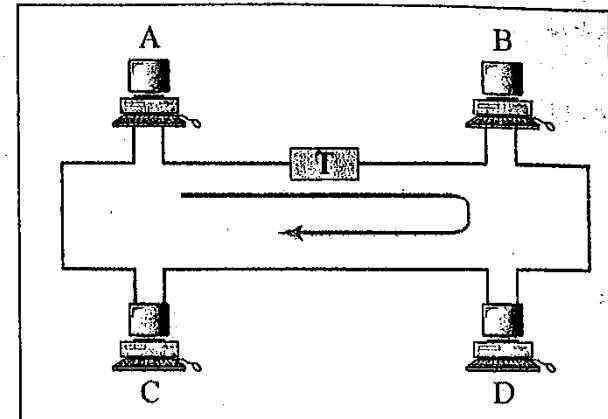
شکل(۲۷-۳)- الگوریتم Back-off

Bitmap

این روش یکی از روش‌های بدون برخورد بوده و در آن هر ایستگاه کاری قبل از ارسال باید جای خود را رزرو نماید. در این روش آرایه‌ای به تعداد کامپیوترهای شبکه، وجود دارد. در زمان رزروسازی هر کامپیوتر که بخواهد اطلاعاتی را ارسال نماید، بیت مربوط به خود را در آرایه مذکور Set می‌کند. پس از پایان زمان رزروسازی، فقط کامپیوترهایی مجاز به ارسال هستند که قبل از مریبوط به خود را Set کرده باشند. مثلاً در شکل(۲۸-۳)، در زمان رزروسازی اول، ایستگاههای ۱ و ۳ و ۴ بیتها مربوط به خود را Set کرده‌اند و سپس اقدام به ارسال نموده‌اند. در زمان رزروسازی بعدی، تنها ایستگاه شماره ۱ جای خود را رزرو کرده و سپس داده مربوطه را ارسال نموده است.



شکل(۲۸-۳)- روش رزروسازی برای دسترسی به رسانه

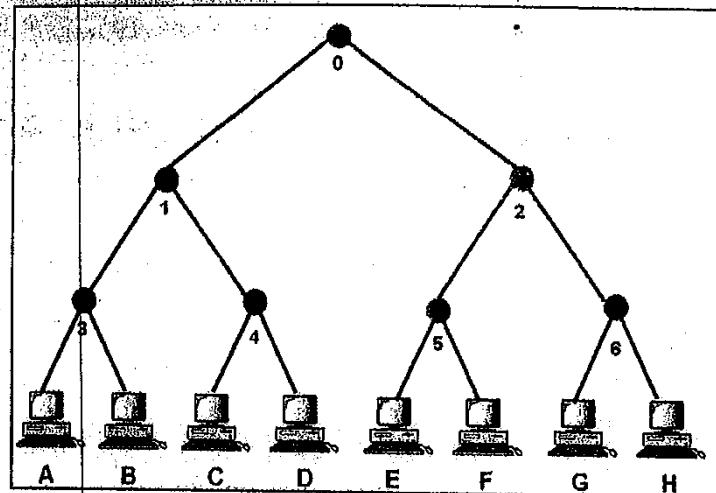


شکل (۲۹-۳)- روش استفاده از نشانه برای دسترسی به رسانه

ح - روش درخت وفقی

در این روش از یک درخت دودویی برای رفع مشکل تخصیص کانال استفاده می‌شود. به طوری که ایستگاهها به عنوان برگهای درخت در پایین‌ترین سطح در نظر گرفته می‌شوند. روش کار بدین ترتیب است که در ابتدا و در زمان رقابت اول، تمام ایستگاه‌ها حق تصاحب کانال را دارند. اگر یکی از آنها با موفقیت این کار را انجام داد که مقصود حاصل است؛ در غیر این صورت اگر برخورد اتفاق بیفتد، در زمان رقابت دوم تنها ایستگاه‌هایی که در زیرشاخه سمت چپ قرار دارند مجاز به رقابت هستند به طوری که درخت از بالا به پایین پیمایش شده به طوری که با هر بار برخورد، یک سطح در درخت پایین می‌آییم تا زمانی که فقط یک ایستگاه در داخل زیردرخت وجود داشته باشد، فرض کنید در شبکه‌ای که به روش فوق کار می‌کند، هشت ایستگاه کاری A تا H مطابق شکل (۳۰-۳) وجود داشته باشند و ایستگاه‌های A و C و F و همزمان درخواست تخصیص کانال را داشته باشند. در بازه زمانی اول به دلیل اینکه هر سه در داخل درخت صفر قرار دارند، برخورد صورت می‌گیرد. سپس در بازه زمانی دوم، ایستگاه‌هایی Zیر درخت ۱ حق رقابت دارند که باز به دلیل اینکه A و C در داخل این درخت هستند، برخورد اتفاق می‌افتد. در بازه زمانی سوم، ایستگاه A که در زیر درخت ۳ قرار دارد موفق به ارسال می‌گردد.

در این روش، در بار کم در سطوح بالای درخت، تخصیص کانال و ارسال صورت می‌گیرد و در بار زیاد باید سطوح بیشتری به پایین پیموده شود.



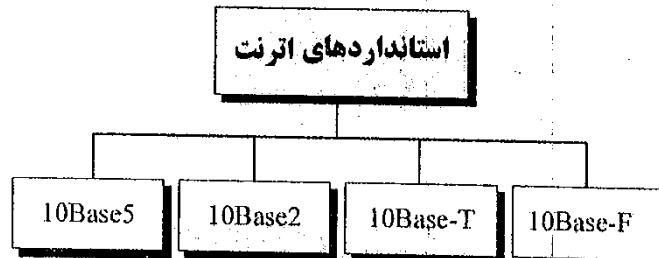
شکل (۳۰-۳)- روش درخت وفقی برای دسترسی به رسانه

برای این روش از یک درخت دودویی برای رفع مشکل تخصیص کانال استفاده می‌شود. به طوری که ایستگاهها به عنوان برگهای درخت در پایین‌ترین سطح در نظر گرفته می‌شوند. روش کار بدین ترتیب است که در ابتدا و در زمان رقابت اول، تمام ایستگاه‌ها حق تصاحب کانال را دارند. اگر یکی از آنها با موفقیت این کار را انجام داد که مقصود حاصل است؛ در غیر این صورت اگر برخورد اتفاق بیفتد، در زمان رقابت دوم تنها ایستگاه‌هایی که در زیرشاخه سمت چپ قرار دارند مجاز به رقابت هستند به طوری که درخت از بالا به پایین پیمایش شده به طوری که با هر بار برخورد، یک سطح در درخت پایین می‌آییم تا زمانی که فقط یک ایستگاه در داخل زیردرخت وجود داشته باشد، فرض کنید در شبکه‌ای که به روش فوق کار می‌کند، هشت ایستگاه کاری A تا H مطابق شکل (۳۰-۳) وجود داشته باشند و ایستگاه‌های A و C و F و همزمان درخواست تخصیص کانال را داشته باشند. در بازه زمانی اول به دلیل اینکه هر سه در داخل درخت صفر قرار دارند، برخورد صورت می‌گیرد. سپس در بازه زمانی دوم، ایستگاه‌هایی Zیر درخت ۱ حق رقابت دارند که باز به دلیل اینکه A و C در داخل این درخت هستند، برخورد اتفاق می‌افتد. در بازه زمانی سوم، ایستگاه A که در زیر درخت ۳ قرار دارد موفق به ارسال می‌گردد.

در این روش، در بار کم در سطوح بالای درخت، تخصیص کانال و ارسال صورت می‌گیرد و در بار زیاد باید سطوح بیشتری به پایین پیموده شود.

کابل انجام می گرفت که توسط تمام دستگاهها به اشتراک گذاشته می شد. مکانیزم انتخاب شده برای دسترسی به کanal مشترک توسط ایستگاهها، CSMA/CD می باشد.

دلیل موفقیت اترنت، سازگاری آن با انواع محیطهای ارتباطی مختلف و همچنین پشتیبانی سرعتهای مختلف می باشد. در شکل (۳-۱) انواع استانداردهای اترنت آورده شده است. عدد ۱۰ به معنای سرعت ده مگابیت بر ثانیه، کلمه Base به معنای ارسال Baseband و حرف یا عدد آخر، نشان دهنده محیط انتقال می باشد به طوری که اعداد ۵ و ۲ نمایانگر استفاده از کابل هم محور، حرف T نمایانگر استفاده از زوج به هم تابیده و حرف F نمایانگر استفاده از فیبرنوری در شبکه می باشد.



شکل (۳-۱)- انواع استانداردهای اترنت

10Base5
این استاندارد به معنای شبکه ای است که در آن از کابل هم محور ضخیم استفاده شده و طول یک سگمنت در این شبکه حداقل ۵۰۰ متر است که برای افزایش طول می توان از تکرارگر استفاده نمود. این کار را تا ۴ مرتبه می توان انجام داد که در نهایت طول کل شبکه به ۲۵۰۰ متر خواهد رسید. در هر قطعه کابل حداقل ۱۰۰ کامپیوتر می تواند قرار گیرد. دقت کنید که از ۵ قطعه متصل شده توسط تکرارگر، دو قطعه باید به صورت یک در میان خالی باشد. سرعت این شبکه ۱۰ مگابیت بر ثانیه و روش انتقال Baseband است. برای اتصال کامپیوتر به کابل از یک کابل کشی بین دستگاههای متصل بهم در اترنت ارائه نمود. اترنت در مدت زمان کوتاهی به عنوان یکی از تکنولوژیهای رایج برای برپاسازی شبکه در سطح دنیا مطرح گردید. با توجه به تغییرات و اصلاحات انجام شده در شبکه اترنت، عملکرد و نحوه کار آن نسبت به شبکه های اولیه تفاوت چندانی نکرده است. در اترنت اولیه، ارتباط تمام دستگاه های موجود در شبکه از طریق یک

۶- استانداردهای IEEE برای شبکه های محلی

در اوائل سال ۱۹۸۰، اولین گروه رسمی انجمن جهانی مهندسین برق و الکترونیک (IEEE) در رابطه با ایجاد استانداردهای واحد در زمینه شبکه های اطلاعاتی شکل گرفت و نام آن گروه ۸۰۲ نهاده شد. عدد ۸۰۲ نشان دهنده سال و ماه تشکیل گروه استانداردسازی است. گروه فوق از چندین گروه جانی دیگر تشکیل شده بود. هر یک از گروه های فرعی نیز مسئول بررسی جنبه های خاصی از شبکه گردیدند. موسسه IEEE برای تمایز هر یک از گروه های جانی از روش نامگذاری ۸۰۲.x استفاده کرد. x یک عدد منحصر بفرد بود که برای هر یک از گروه ها در نظر گرفته شده بود. تعدادی از استانداردهای تهیه شده توسط گروه ۸۰۲ در زیر توضیح داده شده است:

۸۰۲.۱: پروتکلهای لایه های بالاتر در LAN

۸۰۲.۲: زیر لایه LLC از لایه پیوند داده.

۸۰۲.۳: شبکه محلی

۸۰۲.۴: شبکه محلی Token Bus

۸۰۲.۵: شبکه محلی Token Ring

۸۰۲.۱۱: شبکه محلی بی سیم

لازم به توضیح است که IEEE لایه پیوند داده را به دو زیر لایه به نامهای MAC و LLC تقسیم کرده است. در مورد زیر لایه MAC در قسمت تخصیص کanal توضیح دادیم.

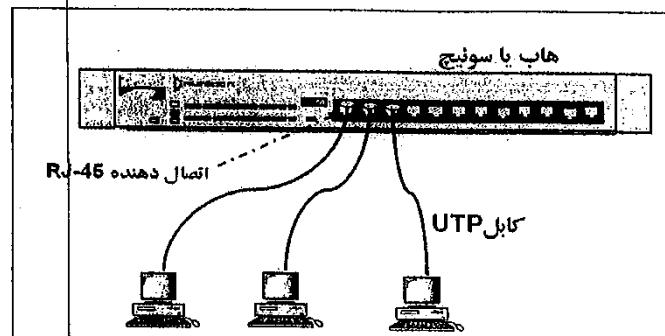
در ادامه به توضیح مفصلتر استانداردهای مربوط به شبکه های محلی خواهیم پرداخت.

الف- استاندارد اترنت (802.3)

در سال ۱۹۷۳ پژوهشگری با نام Metcalfe در مرکز تحقیقات شرکت Ziraksن، اولین شبکه اترنت را بوجود آورد. هدف وی ارتباط کامپیوتر به یک چاپگر بود. وی روشی فیزیکی به منظور کابل کشی بین دستگاههای متصل بهم در اترنت ارائه نمود. اترنت در مدت زمان کوتاهی به عنوان یکی از تکنولوژیهای رایج برای برپاسازی شبکه در سطح دنیا مطرح گردید. با توجه به تغییرات و اصلاحات انجام شده در شبکه اترنت، عملکرد و نحوه کار آن نسبت به شبکه های اولیه تفاوت چندانی نکرده است. در اترنت اولیه، ارتباط تمام دستگاه های موجود در شبکه از طریق یک

10BaseT

ین استاندارد به معنی شبکه‌ای است که در آن از کابل UTP استفاده شده و برای اتصال کامپیوترها از هاب یا سوینج استفاده می‌گردد. حداکثر فاصله کامپیوتر از هاب یا سوینج ۱۰۰ متر است. سرعت در آن ۱۰ مگابیت بر ثانية و روش انتقال Baseband است. در دو انتهای کابل برای اتصال به کارت شبکه و هاب، از کانکتور RJ-45 استفاده می‌شود. نوع توبولوژي استفاده شده، همانطور که در شکل (۳۴-۳) دیده می‌شود، ستاره‌ای است.

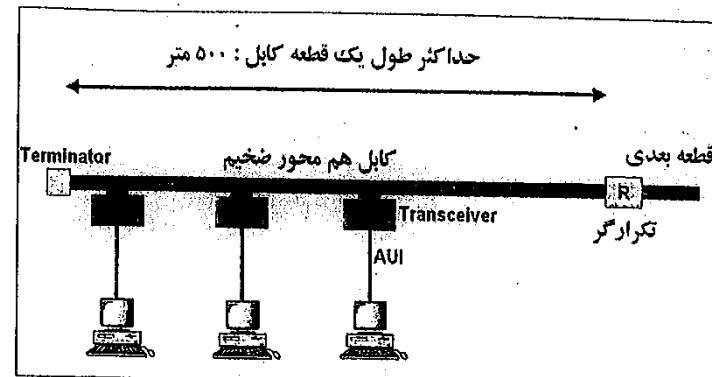


شکل (۳۴-۳)- اترنت 10BaseT

10BaseF

ین استاندارد از فیبرنوری استفاده می‌کند. حداکثر مسافت، بسته به نوع فیبر بکار رفته دو کیلومتر (برای فیبر تک‌حالته) و سه کیلومتر (برای فیبر چند‌حالته) است. سرعت در آن ۱۰ مگابیت بر ثانية و روش انتقال Baseband است. در این شبکه از یک زوج فیبر مطابق شکل (۳۵-۳) یکی برای ارسال و دیگری برای دریافت داده استفاده می‌شود. کانکتورهای ST و SC در دو انتهای فیبر استفاده می‌گردند.

حداکثر طول یک قطعه کابل: ۵۰۰ متر

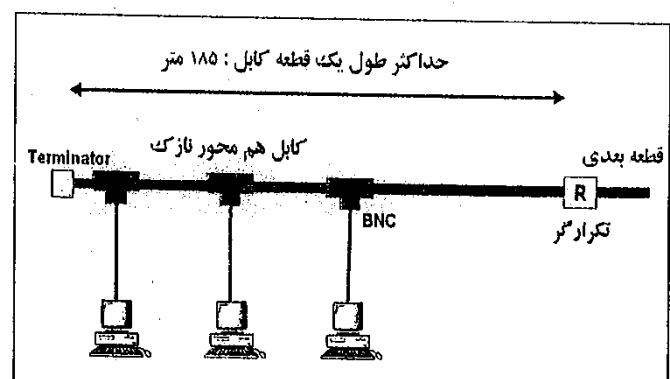


شکل (۳۲-۳)- اترنت 10Base5

10Base2

در این استاندارد از کابل هم محور نازک استفاده شده و طول یک قطعه کابل در این شبکه حداکثر ۱۸۵ متر است که برای افزایش طول می‌توان از تکرارگر استفاده نمود. این کار را تا ۴ بار می‌توان انجام داد گه در نهایت طول کل شبکه به ۹۶۵ متر خواهد رسید. در هر قطعه کابل حداکثر ۳۰ کامپیوتر می‌تواند قرار گیرد. در این استاندارد نیز مانند حالت قبل، از ۵ قطعه متصل شده توسط تکرارگر، دو قطعه باید به صورت یک در میان خالی باشد. سرعت این شبکه ۱۰ مگابیت بر ثانية و روش انتقال Baseband است. برای اتصال کامپیوتر به کابل از اتصال دهنده T شکل BNC مطابق شکل (۳۳-۳) استفاده می‌شود. نوع توبولوژي استفاده شده، گذرگاهی (Bus) می‌باشد. انتهای کابل توسط Terminator برای جلوگیری از برگشت سیگنال، بسته می‌شود.

حداکثر طول یک قطعه کابل: ۱۸۵ متر



شکل (۳۳-۳)- اترنت 10Base2

آدرس مقصده: آدرس MAC گیرنده را مشخص می‌کند. این آدرس که به آن آدرس فیزیکی هم گفته می‌شود، یک آدرس ۴۸ بیتی بوده که در داخل کارت شبکه توسط کارخانه سازنده نوشته شده است. آدرس MAC را برای سهولت در خواندن و نوشتگر به صورت HEX نشان می‌دهند که سه بایت سمت چپ، مشخص کننده کارخانه سازنده و سه بایت سمت راست، شماره سریال کارت را مشخص می‌نماید:

نمونه‌ای از آدرس MAC بدین صورت است: **00-0D-61-54-25-2B**

اگر آدرس MAC مقصده به صورت تمام یک (FF-FF-FF-FF-FF-FF) نوشته شود، فریم مورد نظر توسط تمامی کامپیوترهای داخل این سگمنت دریافت می‌شود. به عبارت دیگر به صورت پخش همگانی خواهد بود.

آدرس مبدأ: آدرس MAC فرستنده را مشخص می‌نماید.

طول فریم: دو بایت نشان دهنده طول فریم می‌باشد.

داده: در این قسمت اطلاعات قرار می‌گیرد که شامل Header لایه‌های بالاتر نیز خواهد بود.

PAD: برای اینکه در صورت بروز برخورد بتوان آن را تشخیص داد، طول فریم حداقل باید

۶۴ بایت (بدون ۸ بایت اول) باشد. به عبارت دیگر فیلد داده باید حداقل ۴۶ بایت را شامل شود.

اگر محتویات داده کمتر از این مقدار باشد، فیلد PAD این کسری را جبران خواهد نمود.

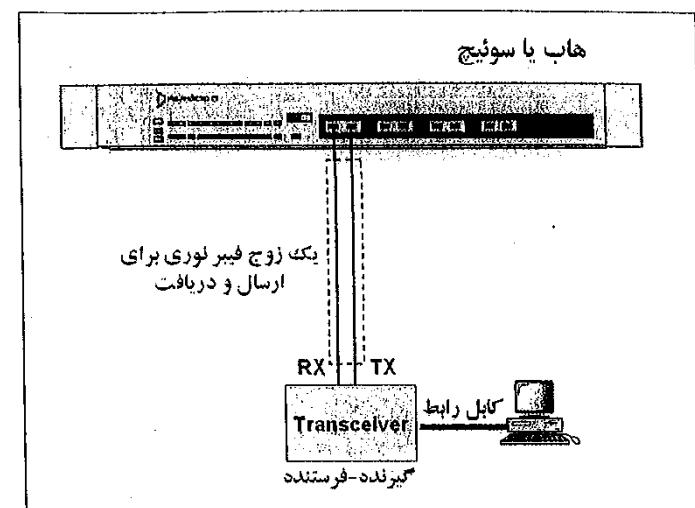
CRC: چهار بایت برای کنترل خطای روش

7	1	6	6	2	0-1500	0-46	4
Preamble	Start of frame	Destination Address	Source Address	Length	Data	PAD	CRC

شکل (۳۶-۳)= قالب یک فریم Ethernet

ب- گذرگاه نشانه یا **(802.4) Token Bus**

در این استاندارد همانطور که در شکل (۳۷-۳) نشان داده شده است، کامپیوترها از نظر فیزیکی بصورت خطی و یا اضطراباً با توبولوژی Bus به هم‌دیگر متصل شده اند اما از دید منطقی در داخل یک حلقه قرار گرفته‌اند. ورود و خروج از حلقه تحت نظر از کامپیوترها به نام

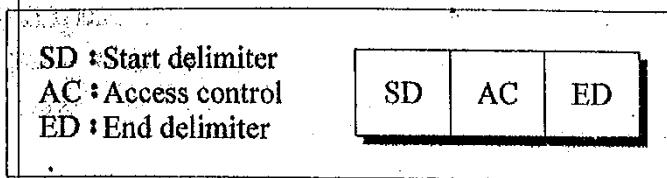


شکل (۳)- اترنت 10BaseT

- **100BaseTX:** یعنی شبکه‌ای که در آن از کابل UTP نوع Cat5 استفاده شده و عملاً دو جفت سیم در انتقال دیتا دارند (دو جفت دیگر بیکار می‌مانند)، سرعت در آن ۱۰۰ مگابیت بر ثانیه و روش انتقال Baseband است.
- **100BaseFX:** یعنی شبکه‌ای که در آن از کابل فیبرنوری استفاده شده است. سرعت در آن ۱۰۰ مگابیت بر ثانیه و روش انتقال Baseband است.
- **100BaseT4:** تنها تفاوت آن با نوع بالا این است که هر چهار جفت سیم در آن بکار گرفته می‌شوند.

ساختار فریم در اترنت

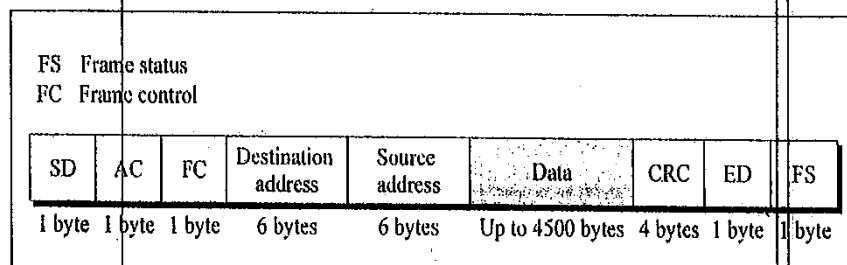
- یک فریم اترنت دارای هشت فیلد مطابق شکل (۳۶-۳) به شرح زیر می‌باشد:
- **Preamble:** ۷ بایت به صورت ۱۰۱۰۱۰۱۰ می‌باشد؛ که در حقیقت یک موج مربعی بوده و برای هماهنگی فرستنده و گیرنده استفاده می‌گردد.
- **SOF:** یک بایت نشان دهنده شروع فریم بوده و محتویات آن ۱۰۱۰۱۱۱ می‌باشد.



شکل(۳۹-۳)- ساختار Token در استاندارد حلقه نشانه

ایستگاههای موجود در حلقه می توانند در دو وضعیت شنود و یا صحبت کردن باشند. وضعیت شنود جلتی است که یا Token از جلوی ایستگاه عبور می کند و آن ایستگاه اطلاعاتی برای ارسال ندارد و یا اینکه یک فریم از جلوی آن عبور می کند و آدرس مقصد مربوط به وی نیست. در این حالت فقط یک بیت تاخیر به اطلاعات می دهد. وضعیت صحبت هنگامی است که بخواهد Token را در اختیار بگیرد و اطلاعات اضافی را به آن پچسباند و تبدیل به فریم کند.

ساختار فریم در این استاندارد مطابق شکل (۴۰-۳) می باشد. همانطور که در شکل مشخص است فریم دارای همان سه فیلد Token همراه با چند فیلد اضافی است که مشخص کننده آدرسهای مبدأ و مقصد، داده ارسالی، کنترل خطأ و وضعیت فریم هستند. در فیلد FS دو بیت به نامهای A و C (Address recognized) و (frame Copied) وجود دارد که به ترتیب به معنای تشخیص داده شدن آدرس مقصد و کپی شدن فریم می باشند.

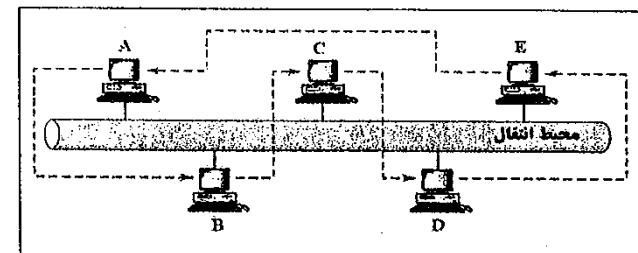


شکل(۴۰-۳)- ساختار فریم در استاندارد حلقه نشانه

در شکل (۳۸-۳)، فرض کنید کامپیوتر شماره ۲ بخواهد یک بسته اطلاعاتی برای کامپیوتر شماره ۵ ارسال نماید. ابتدا باید صبر کند تا Token به آن برسد. سپس با یک کردن بیت T در فیلد C، تصاحب Token را اعلام نموده فیلدهای اضافی را به آن می جسباند و آن را تبدیل به فریم می نماید. سپس فریم ایجاد شده را در حلقه رها می کند. کامپیوترهای میانی، معنی شماره

مدیر حلقه انجام می گیرد. در این شکل به طور مثال اگر کامپیوتر A بخواهد اطلاعاتی برای کامپیوتر C نفرستد، مستقیماً نمی تواند این کار را بکند بلکه باید ابتدا آنرا تحویل کامپیوتر B داده و سپس کامپیوتر B آنرا تحویل کامپیوتر C خواهد داد. بدیهی است که ارسال اطلاعات از طریق گذرگاه مشترک صورت خواهد گرفت

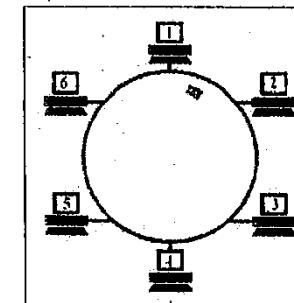
به علت این که این استاندارد دیگر استفاده نمی شود و منسخ شده است، از شرح بیشتر آن خودداری می کنیم.



شکل(۳۷-۳)- استاندارد (IEEE 802.4) Token Bus

ج- حلقه نشانه یا (802.5)Token Ring

در این استاندارد همانطور که در شکل (۳۸-۳) نشان داده شده است، کامپیوتراها به صورت حلقه ای به همیگر متصل هستند. این استاندارد توسط شرکت IBM در سال ۱۹۸۲ ابداع گردید. در این استاندارد یک بسته کوچک سه بایتی به نام Token که در شکل (۳۹-۳) نشان داده شده است، مدام در حلقه در حال چرخش است. کامپیوترا که بخواهد اطلاعاتی ارسال کند باید اول Token را در اختیار بگیرد سپس اقدام به ارسال نماید. در داخل فیلد AC بیتی به نام T وجود دارد که یک بودن آن به این معنی است که کسی Token را در اختیار دارد.



شکل(۳۸-۳)- استاندارد حلقه نشانه (IEEE 802.5)

های ۳ و ۴ عکس العملی نشان نمی‌دهند و در وضعیت شنود قرار می‌گیرند زیرا آدرس مقصود اولویت به آنها نیست. کامپیوتر شماره ۵ یک کپی از فریم گرفته، بیتهاي A و C را یک می‌کند و سپس فریم را دوباره در حلقه رها می‌نماید. فرستنده یعنی کامپیوتر شماره ۲ پس از چک کردن پیتهاي A و C، بعد از اطمینان حاصل کردن از اینکه کامپیوتر مقصد اطلاعات را برداشته است، فریم را از بین برده و Token را در حلقه رها می‌نماید. سرعت ارسال اطلاعات در این نوع شبکه‌ها چهار یا شانزده مگابیت بر ثانیه است.

در این استاندارد، هر کامپیوتر باید آدرس نزدیکترین همسایه فعال فوکانی یا به اصطلاح NAUN خود را بداند. کلمه "فوکانی" به جهت خلاف حرکت فریم اشاره می‌کند. به عنوان مثال در شکل (۳-۸) کامپیوتر شماره ۲ به عنوان NAUN برای کامپیوتر شماره ۳ محسوب می‌شود. این اطلاعات برای بازسازی حلقه پس از ورود و یا خروج یک کامپیوتر از حلقه لازم است. در شبکه Token Ring یکی از کامپیوتراها نقش مدیر حلقه و یا به اصطلاح "ناظر فعال" را بر عهده دارد. در هنگام شروع بکار حلقه، تمام کامپیوتراها در یک رقابت وارد می‌شوند تا تعیین کنند که کدامیک به عنوان ناظر فعال انتخاب گردد. در این حالت، کامپیوتری که بالاترین آدرس MAC را داشته باشد، این مسئولیت را به عهده می‌گیرد. از جمله وظایف ناظر فعال می‌توان به موارد زیر اشاره کرد:

- اطمینان از وجود تاخیر مناسب در حلقه
- نظرات بر انتقال Token و فریم
- ردیابی فریمهای Token گم شده (با استفاده از Timer)
- از بین بردن حلقه در صورت بروز مشکل
- ایجاد همزمانی بین ایستگاههای موجود در حلقه
- بازسازی مجدد حلقه پس از رفع خرابی یا خطأ
- انجام عمل سرشماری در حلقه به صورت هر هفت ثانیه یک بار برای اینکه هر کامپیوتر داخل حلقه از NAUN خود باخبر شود.

متلا وضعیتی را در نظر بگیرید که در آن کامپیوتری که در انتخاب دارد از کار بیفتند. در این حالت وظیفه ناظر فعال است که پس از مدت زمان معینی (زمان به سر رسیدن Timer) مجدداً Token را ساخته و در حلقه رها کند.

این استاندارد اجازه تعریف هشت سطح اولویت را به کاربر می‌دهد؛ به طوری که کاربر می‌تواند یک یا چند ایستگاه را به صورت اولویت بالا تعریف کند به صورتی که بتواند دفعات بیشتری Token را در اختیار بگیرند و در نتیجه بیشتر از شبکه استفاده کنند. این کار از طریق سه بیت

۵- استاندارد شبکه‌های محلی بی‌سیم (802.11)

چند سال است که استفاده از شبکه‌سازی بی‌سیم در دنیا آغاز گردیده است. تا همین اواخر یک LAN بی‌سیم با سرعت انتقال پایین و خدمات غیرقابل اعتماد متراوف بود، اما هم اکنون تکنولوژی‌های LAN بی‌سیم خدمات قابل قبولی را با سرعتی که حداقل برای کاربران معمولی شبکه کابلی پذیرفته شده می‌پاشد، فراهم می‌کنند. کاربرد یک شبکه بی‌سیم در محیط‌هایی است که کاربران متوجه باشند مانند بیمارستانها و یا جاهایی که اجازه کابل کشی نداشته باشند و یا اینکه کابل کشی مقرون به صرفه نباشد. در حالت کلی به دلیل امنیت پایینتر شبکه‌های بی‌سیم نسبت به شبکه‌های باسیم، اگر تحرک کاربران چندان اهمیتی نداشته باشد، بهتر است شبکه به صورت باسیم پیاده‌سازی گردد.

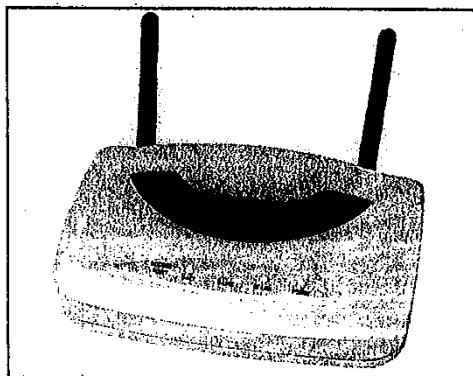
شبکه‌های محلی بی‌سیم (WLAN) از امواج الکترومغناطیسی (رادیویی یا مادون قرمز) برای انتقال اطلاعات از یک نقطه به دیگر استفاده می‌کنند. همانطور که می‌دانیم، امواج رادیویی در تمام جهات پخش می‌گردند و نیازی به دید مستقیم فرستنده و گیرنده نیست؛ اما در ارسال به روش مادون قرمز، حتماً باید فرستنده و گیرنده دید مستقیم داشته باشند چراکه امواج در یک جهت منتشر می‌گردند.

انواع مختلف استاندارد 802.11 به ترتیب تاریخ پیدایش عبارتند از 802.11b، 802.11a و 802.11g که خصوصیات آنها در زیر نشان داده شده است:

نام استاندارد	باند فرکانسی	نرخ ارسال داده
802.11b	۲/۴ GHz	۱۱ مگابیت بر ثانیه
802.11a	۵ GHz	۶,۹,۱۲,۱۸,۲۴,۳۶,۴۸,۵۴ مگابیت بر ثانیه
802.11g	۲/۴ GHz	۵۴ مگابیت بر ثانیه

• نقطه دسترسی (Access Point)

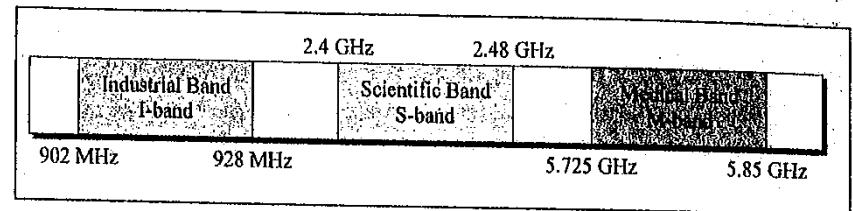
نقطه دسترسی در شبکه‌های بی‌سیم، سخت افزارهای فعالی هستند که عملآ نوش سویچ در شبکه‌های باسیم را بازی می‌کنند. AP محدوده خاصی را پوشش می‌دهد که بسته به اینکه در فضای باز (Outdoor) یا فضای بسته (Indoor) کار کند، این محدوده متفاوت است. بدیهی است که هرچه فاصله کامپیوتر بی‌پار از AP بیشتر باشد، سیگنال ضعیفتر شده و سرعت انتقال پایینتر خواهد آمد. در شکل (۴۳-۳) یک نوع AP نشان داده شده است.



شکل (۴۳-۳)- نقطه دسترسی (AP)

در واقع در حکم پلی است که ارتباط ایستگاه‌های بی‌سیم را با سیستم توزیع یا شبکه سیمی برقرار می‌سازد. کوچکترین عنصر ساختمانی شبکه‌های محلی بی‌سیم در استاندارد 802.11 مجموعه سرویس پایه یا (Basic Service Set)BSS نامیده می‌شود. در واقع BSS مجموعه‌ای از ایستگاه‌های بی‌سیم است، به مجموعه چند BSS یک مجموعه سرویس توسعه یافته یا (Extended Service Set)ESS گفته می‌شود. همانطور که در شکل (۴۴-۳) مشاهده می‌گردد، برای اینکه یک کامپیوتر سیار بتواند از یک BSS به BSS دیگر بدون قطع ارتباط حرکت نماید، باید BSS‌ها دارای ناحیه همپوشانی باشند.

همانطور که از جدول مشخص است این شبکه‌ها در باند ISM کار می‌کنند. این باند شامل سه محدوده فرکانسی است که برای مقاصد صنعتی و علمی و پزشکی استفاده می‌شوند که احتیاج به گرفتن مجوز برای کار در این باندها نیست. در شکل (۴۱-۳) باند ISM و سه محدوده فرکانسی آن نشان داده است.

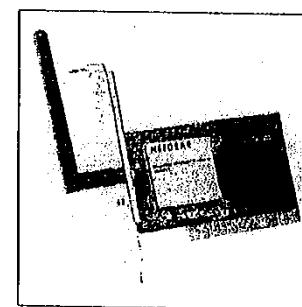


شکل (۴۱-۳)- باند ISM

اجراء اصلی یک شبکه محلی بی‌سیم در شبکه‌های محلی بی‌سیم دو جزء اصلی وجود دارد:

• ایستگاه بی‌سیم

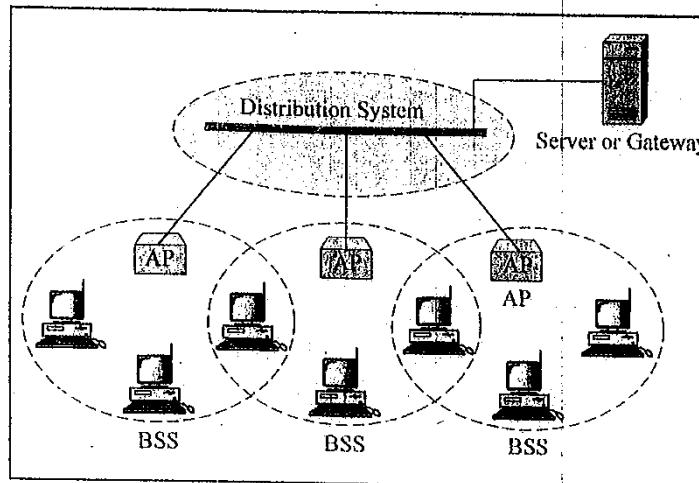
ایستگاه یا سرویس گیرنده بی‌سیم معمولاً یک کامپیوتر Laptop یا یک ایستگاه کاری ثابت است که توسط یک کارت شبکه بی‌سیم به شبکه محلی متصل می‌شود. در حال حاضر اکثر کامپیوترهای Laptop موجود در بازار به این امکان به صورت سرخود مجهز هستند و نیازی به اضافه کردن یک کارت شبکه بی‌سیم نیست. در شکل (۴۲-۳) نمونه‌ای از یک کارت شبکه بی‌سیم را مشاهده می‌نمایید.



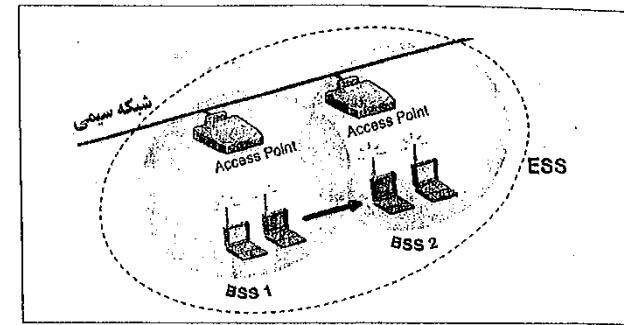
شکل (۴۲-۳)- کارت شبکه بی‌سیم

• زیرساختار (Infrastructure)

همیندی دیگر زیرساختار است. در این همیندی، ایستگاه‌های موجود در یک شبکه بی‌سیم از طریق AP به ساختار باسیم متصل می‌گردند. در این حالت تمام ایستگاه‌ها با AP مربوطه تماس می‌گیرند و اتصال مستقیم بین ایستگاه‌ها وجود ندارد در واقع AP وظیفه دارد فریم‌ها را بین ایستگاه‌ها توزیع و پخش کند. شکل (۴۶-۳) همیندی زیرساختار را نشان می‌دهد.



شکل (۴۶-۳)- همیندی زیرساختار



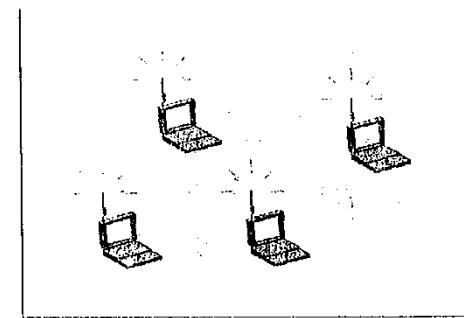
شکل (۴۴-۳)- همیندی BSS‌ها

• همیندیهای شبکه‌های محلی بی‌سیم

در یک تقسیم‌بندی کلی می‌توان دو همیندی را برای شبکه‌های محلی بی‌سیم در نظر گرفت:

• فی‌البداهه (Ad Hoc)

در این همیندی ایستگاه‌ها از طریق رسانه بی‌سیم به صورت نظری به نظری با یکدیگر در ارتباط هستند و برای تبادل داده از تجهیزات یا ایستگاه واسطی استفاده نمی‌کنند. واضح است که در این همیندی به سبب محدودیت‌های فاصله، هر ایستگاه ضرورتاً نمی‌تواند با تمام ایستگاه‌های دیگر در تماس باشد. به این ترتیب شرط اتصال مستقیم در این همیندی آن است که ایستگاه‌ها در محدوده عملیاتی بی‌سیم یا همان برد شبکه بی‌سیم قرار داشته باشند. شکل (۴۵-۳) همیندی Ad Hoc را نشان می‌دهد.



شکل (۴۵-۳)- همیندی فی‌البداهه یا Ad hoc

لایه فیزیکی در 802.11

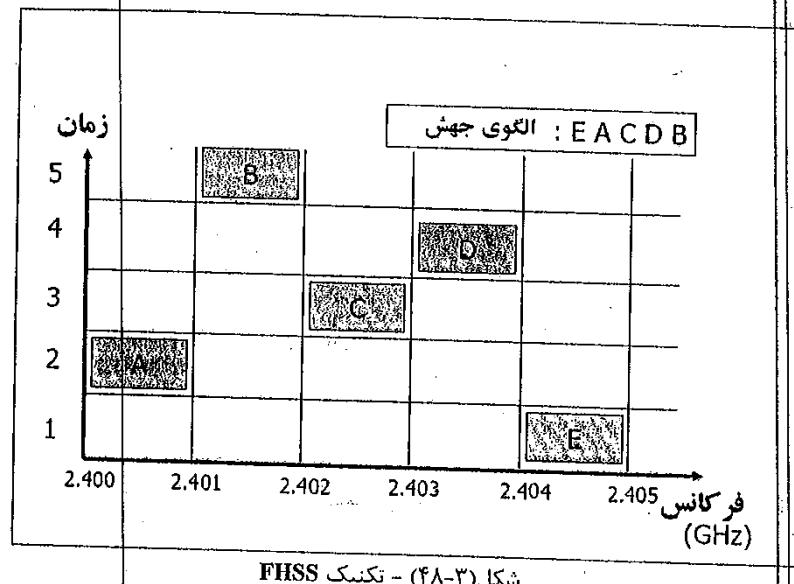
همانطور که قبلاً گفته شد، شبکه‌های محلی بی‌سیم می‌توانند هم به صورت مادون قرمز و هم با امواج رادیویی پیاده‌سازی اشوند.

در ارتباطات مادون قرمز از فرکانس‌های بالا (دقیقاً زیر طیف نور مرئی) استفاده می‌شود. در این روش، سیگنالها نمی‌توانند از اشیاء و دیوارها عبور کنند. این امر بکارگیری تکنولوژی مادون قرمز را محدود می‌سازد. در فناوری مادون قرمز ارسال کننده و دریافت کننده باید یکدیگر را ببینند (در خط دید یکدیگر باشند) همانند یک کنترل کننده راه دور دستگاه تلویزیون.

در ادامه دو تکنیک پیاده‌سازی طیف گستردگی را توضیح می‌دهیم:

• ارسال طیف گستردگی با جهش فرکانسی (FHSS)

در یک سیستم مبتنی بر جهش فرکانسی، فرکانس سیگنال حامل به شکلی شبیه تصادفی و تحت کنترل یک الگوی جهش تغییر می‌کند. شکل (۴۸-۳) این تکنیک را نشان می‌دهد.



همانطور که از شکل مشخص است، در هر محدوده زمانی، ارسال در یک باند فرکانسی انجام می‌گردد. این عمل به صورت شبیه تصادفی و از روی الگوی جهش انجام می‌گردد. فرستنده و گیرنده هر دو باید از الگوی جهش یکسانی استفاده کنند. در تکنیک FHSS، از ۷۹ کانال با پهنای باند ۱ مگاهرتز استفاده می‌شود که کانال اول از فرکانس $\frac{2}{4}$ گیگاهرتز شروع می‌گردد. دقت کنید که به دلیل محرومانه بودن الگوی جهش و شبیه تصادفی بودن جهشها، امکان استراق سمع بسیار پایین می‌آید و استراق سمع کننده نمی‌تواند تشخیص دهد که بازه فرکانسی بعدی کدام است.

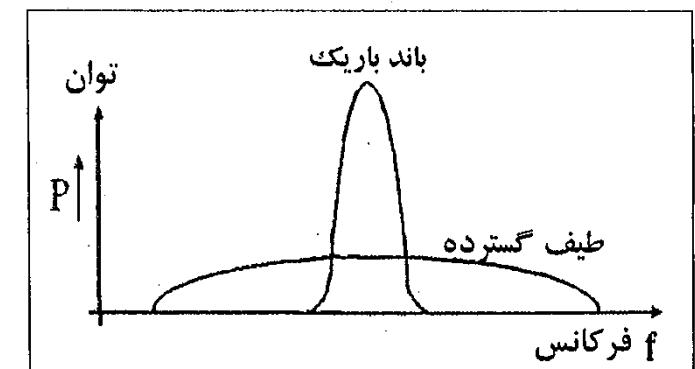
امواج رادیویی بخاطر برد، پهنای باند و پوشش مکانی بیشتر، از نور مادون قرمز کاربرد بیشتری دارند. در این حالت ارسال به صورت طیف گستردگی (Spread Spectrum) انجام می‌گردد که در ادامه بحث خواهد شد.

ویژگی‌های سیگنال‌های طیف گستردگی

عبارت طیف گستردگی به هر تکنیکی اطلاق می‌شود که با استفاده از آن پهنای باند سیگنال ارسالی بسیار بزرگ‌تر از پهنای باند سیگنال اطلاعات باشد. یکی از سوالات مهمی که با در نظر گرفتن این تکنیک مطرح می‌شود آن است که با توجه به نیاز روز افزون به پهنای باند و اهمیت آن به عنوان یک منبع با ارزش، چه دلیلی برای گسترش طیف سیگنال و مصرف پهنای باند بیشتر وجود دارد. پاسخ به این سوال در ویژگی‌های جالب ارسال به شیوه طیف گستردگی نهفته است. این ویژگی‌های عبارتند از:

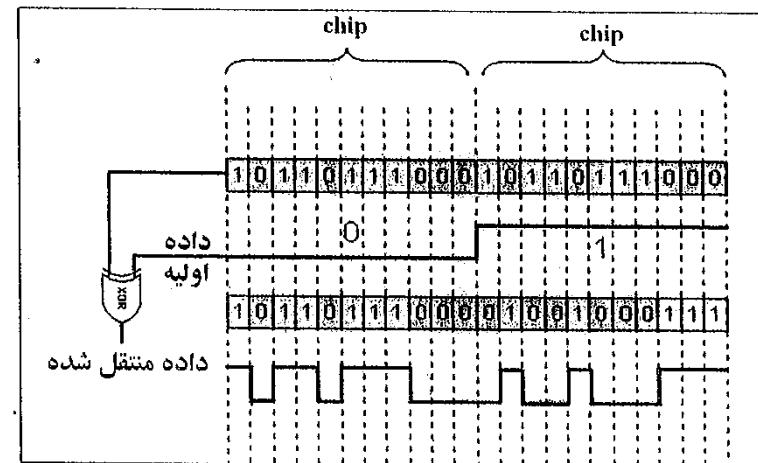
- پایین بودن توان چگالی طیف به طوری که سیگنال اطلاعات برای شنود غیر مجاز و نیز در مقایسه با سایر امواج به شکل اعوجاج و پارازیت به نظر می‌رسد.
- مصونیت بالا در مقابل پارازیت و تداخل
- رسایی با تفکیک پذیری و دقت بالا

در شکل (۴۷-۳) روش طیف گستردگی با روش باند باریک مقایسه شده است. همانطور که مشاهده می‌گردد، در روش طیف گستردگی سیگنال در محدوده فرکانسی وسیعتر ولی با توان کمتری ارسال می‌گردد.



• تکنیک توالی مستقیم (DSSS)

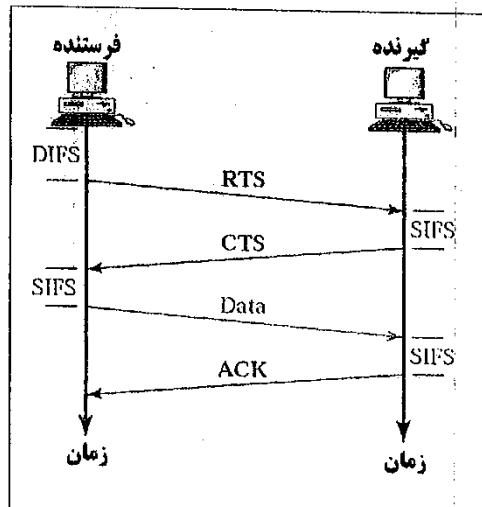
در این روش، سیگنال برروی یک باند فرکانسی بزرگتر از طریق تسهیم آن با یک امضاء یا کد درسته می‌گردد. برای پخش کردن سیگنال، هر بیت واحد با یک ۱۱ بیتی موسوم به دنباله (Barker Sequence) تسهیم می‌شود. در گیرنده نیز سیگنال اولیه با استفاده از همان کد بازسازی می‌شود. بنابراین اگر داده اصلی ۴ بیتی باشد، ۴۴ بیت ارسال می‌گردد. به دنباله بارگرد Chip هم گفته می‌شود. در شکل (۴۹-۳) مشاهده می‌گردد که هر بیت داده با ۱۱ بیت XOR شده است. مشخص است که نرخ تغییرات داده منتقل شده از داده اصلی بالاتر بوده و به پهنای باند بالاتری نیاز دارد. در این روش حتی اگر ۴۰٪ داده ارسالی خراب شود، گیرنده می‌تواند داده اولیه را تشخیص دهد.



شکل (۴۹-۳) تکنیک DSSS

روش دسترسی به رسانه در ۸۰۲.۱۱

روش دسترسی به رسانه در این استاندارد CSMA/CA است که تاحدودی مشابه روش دسترسی به رسانه در این استاندارد CSMA/CD است. CA مخفف Collision Avoidance به معنی اجتناب از برخورد می‌باشد. به دلیل اینکه یک ایستگاه بی‌سیم در هنگام ارسال نمی‌تواند به کانال گوش دهد، مکانیزم تشخیص برخورد همانند CSMA/CD امکانپذیر نیست. در این روش ایستگاه فرستنده ابتدا کانال را کنترل کرده و در صورتی که رسانه به مدت خاصی موسوم به DIFS آزاد باشد، بسته کنترلی به



شکل (۵۰-۳)- دسترسی به رسانه در ۸۰۲.۱۱

دلیل استفاده از بسته‌های کنترلی RTS و CTS، مشکل ایستگاههای پنهان و آشکار است که در ادامه توضیح داده خواهند شد.

فرض کنید که در شکل (۵۱-۳) ندهای A و C هر دو می‌خواهند داده‌ای را برای ند B ارسال کنند. از آنجا که در برده هم‌دیگر قرار ندارند، نمی‌توانند از طریق شنود تشخیص دهند که دیگری مشغول ارسال است. به عبارت دیگر ندهای A و C از دید هم‌دیگر پنهان هستند و نمی‌توانند در شبکه یکدیگر را ردیابی نمایند. استفاده از بسته‌های RTS این مشکل را رفع می‌کند. مطابق

خود آژهای:

۱- در روش فریم‌بندی بیت گرا در طرف فرستنده بعد از چند بیت ۱ متوالی یک بیت ۰ درج می‌شود؟

- (۱) ۷ بیت (۲) ۶ بیت (۳) ۵ بیت (۴) ۴ بیت (۵) ۳ بیت

۲- در نظر گرفتن چند جمله ای مولد $G(x) = x^3 + x + 1$ ، چه بیت‌هایی باید به داده $D = 111011$

- (۱) ۱۰۰ (۲) ۱۱ (۳) ۱۱۰ (۴) ۱۰۱ (۵) ۱۰۰

۳- های زیر که به روش CRC کد شده‌اند، توسط گیرنده دریافت شده‌اند. با فرض

ابینه چند جمله‌ای مولد $1 + x^3 + G(x)$ باشد، گدامیک بدون خطاست؟

- (۱) ۱۰۱۰۱۰۱۱ (۲) ۱۰۱۱۱۰۱۱ (۳) ۱۱۰۱۰۰۱۱۰ (۴) ۱۰۱۱۱۰۱۱۱ (۵) ۱۱۰۱۰۰۱۱۰

۴- گیرنده‌ای پس از گرفتن codeword زیر که به روش hamming کد شده است متوجه وجود

خطا در آن می‌شود. مشخص کنید که خطای کدام بیت اتفاق افتاده است. (با فرض توازن فرد)

- (۱) ۱۰۰۱۰۱۰ (۲) ۱۰۰۱۰۰۱ (۳) ۱۰۰۱۰۱۱ (۴) ۱۰۰۱۰۰۰ (۵) ۱۰۰۱۰۰۱

الف) بیت ششم ب) بیت سوم ج) بیت هفتم د) بیت هشتم

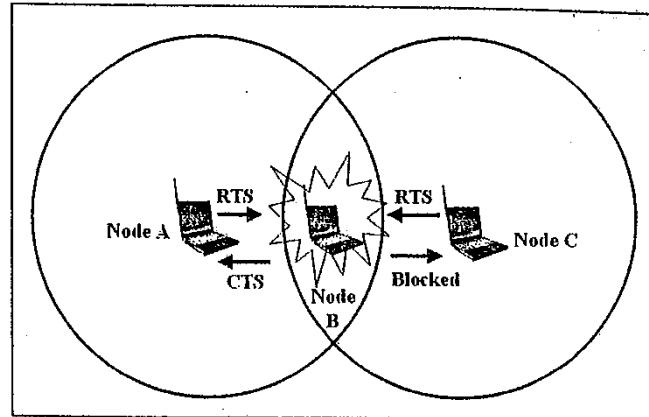
۵- کد شده داده هفت بیتی زیر به روش hamming کدام است؟ (با فرض توازن زوج)

- (۱) ۱۰۰۱۱۰۱۰ (۲) ۱۰۰۱۱۱۰۱ (۳) ۱۰۰۱۱۱۰۱۰ (۴) ۱۰۰۱۱۱۰۱۱ (۵) ۱۰۰۱۱۱۰۱۰

۶- در روش کنترل جریان اگر سیگنال NAK دریافت شود، فقط بسته خراب شده

- مجدداً ارسال می‌گردد.
 (۱) Go-Back-N (۲) Stop & Wait (۳) Selective Repeat

شکل اگر بسته RTS همزمان به یک ایستگاه برسد، بسته CTS تنها برای یکی از درخواست گذنده‌گان (مثلان A) ارسال خواهد شد و بدین ترتیب از خرایی داده‌ها جلوگیری به عمل می‌آید.



شکل (۵۱-۳)-مشکل ایستگاه‌های پنهان

مشکل دیگری که ممکن است بروز کند، مشکل ایستگاه‌های آشکار است که در شکل (۵۲-۳)

نشان داده شده است. فرض کنید که ندهای A و C در محدوده پوشش ند B باشند و ند D خارج از این محدوده باشد. همچنین فرض کنید که ندهای B و D در محدوده پوشش ند C باشند و ند A خارج از برد این محدوده باشد.

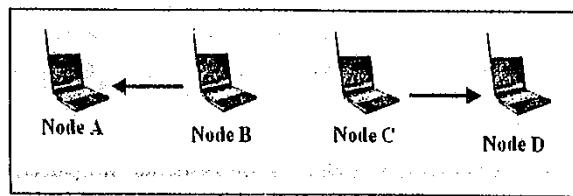
ند C می‌خواهد اطلاعاتی را برای ند D ارسال کند و ند B نیز می‌خواهد با ند A تبادل داده

نماید. قاعده‌تا هر دوی این انتقالات همزمان می‌توانند انجام گردد؛ چراکه مقصد هر کدام خارج از برد دیگری است. با این وجود هنگامی که ند B اطلاعاتی را برای ند A ارسال می‌کند، ند C نیز از

این انتقال باخبر می‌گردد زیرا در برده B قرار دارد. در این حالت ند C به تصور اینکه در صورت

ادامه انتقال با مشکل برخورد یا collision مواجه می‌گردد، از ادامه ارسال به ند D دست می‌کشد. این مشکل را نیز می‌توان با ارسال بسته RTS حل کرد. بدین ترتیب که ند C با دیدن آدرس ند A در بسته RTS، متوجه می‌گردد که این ند در برد وی قرار ندارد و می‌تواند بدون خطر به انتقال

خود به ند D ادامه دهد.

شکل (۵۲-۳)-مشکل ایستگاه‌های آشکار
ایستگاه‌های آشکار

- ۱۴- نرخ انتقال داده در نموده های متفاوت اینترنت چه میزان است؟
 ب) ۱۰۰ مگابیت بر ثانیه
 الف) ۱۰۰ مگابیت بر ثانیه
 ج) ۱۰۰۰ مگابیت بر ثانیه
 د) تمامی موارد

- ۱۵- نام دیگر کدامیک از استانداردهای زیر است؟ Thin-net
 ب) 10Base5
 الف) 10Base2
 ج) هیچکدام

- ۱۶- حداقل طول کابلی که می توان در شبکه های اینترنت 10BaseT استفاده نمود، چه میزان است؟
 ب) ۱۰۰ متر
 الف) ۱۰ متر
 ج) ۱۰۰۰ متر
 د) ۱۸۵ متر

- ۱۷- آدرس اینترنت به چه نام دیگری شناخته می شود؟
 ب) آدرس MAC
 الف) آدرس IP
 ج) آدرس مجازی
 د) هیچکدام

- ۱۸- یک آدرس MAC چند بایت است؟
 ب) شش بایت
 الف) چهار بایت
 ج) هشت بایت
 د) ده بایت

- ۱۹- یک فریم اینترنت حداقل دارای چه اندازه ای است؟
 ب) ۱۰۰۰ بایت
 الف) ۵۱۸ بایت
 ج) ۱۵۰۰ بایت
 د) ۱۵۱۸ بایت

- ۲۰- از preamble فریم اینترنت به چه منظوری استفاده می شود؟
 ب) استفاده به منظور کنترل خط
 الف) تراز اندازه فریم به صورت مضربی از سی و دو
 ج) همزمانی فرستنده و گیرنده
 د) اعلان طول واقعی فریم

- ۷- در روش کنترل جریان Stop & Wait برای n پسته ارسالی، Ack دریافت می گردد.
 n+1 (د) n-1 (ج) 2n (ب) n (الف)

- ۸- کدامیک از روش های کنترل دسترسی به کانال بدون برخورد است؟
 ب) Slotted Aloha
 الف) CSMA/CD
 ج) Adaptive Tree
 د) Token Passing

- ۹- کارایی پروتکل Aloha چند درصد است؟
 ب) ۷۳۶٪
 الف) ۷۴۰٪
 ج) ۷۲۵٪
 د) ۷۱۸٪

۱۰- روش در اینترنت سنتی به عنوان پروتکل دسترسی به رسانه استفاده می شود.

- ب) CSMA
 الف) CSMA/CA
 ج) ALOHA
 د) CSMA/CD

۱۱- یک ایستگاه کاری در یک شبکه اینترنت سه بار اقدام به ارسال یک فریم نموده و هر بار با Collision مواجه شده است. در زمان تاخیر محاسبه شده از طریق $\text{Collision} \times \text{Backoff}_{\text{item}}$ ، چه بازه های زمانی برای سعی مجدد در اختیار دارد؟

- ب) [1..8]
 الف) [0..7]
 ج) [1..16]
 د) [0..15]

- ۱۲- استاندارد Token Ring با چه عددی شناخته می شود؟
 ب) 802.4
 الف) 802.3
 ج) 802.5
 د) 802.11

- ۱۳- ابداع اینترنت به کدامیک از افراد زیر نسبت داده می شود؟
 ب) Bob Metcalfe
 الف) Vinton Cerf
 ج) Berners-Lee
 د) Amdhal

۲۱- از چه کلماتی اختباس شده است؟ CSMA/CD

- (الف) Carrier Sense Multiple Access with Collision Detection
(ب) Collision Sense Multiple Access with Carrier Detection
(ج) Carrier Single-Multiple Access with Collision Detection
(د) Collision Single-Multiple Access with Carrier Detection

۲۲- کدامیک از کانکتورهای زیر در اترنت 10Base2 استفاده می‌گردد؟

- (د) هیچکدام RJ-45 (ج) BNC (ب) AUI (الف)

فصل چهارم

لایه شبکه

۲۳- حداقل طول یک قطعه کابل در شبکه 10Base5 چند متر است؟

- (الف) ۲۰۰ متر (ب) ۵۰۰ متر (ج) ۱۰۰ متر (د) ۱۸۵ متر

۲۴- در کدامیک از شبکه‌های زیر از فیبر نوری به عنوان رسانه انتقال استفاده می‌شود؟

- (الف) 100BaseTX (ب) 100BaseFX (ج) 100BaseT4 (د) الف و ج

۲۵- استاندارد 802.11a کدامیک از نرخهای ارسال داده زیر را پشتیبانی می‌کند؟

- (الف) ۹ مگابیت بر ثانیه (ب) ۳۶ مگابیت بر ثانیه (ج) ۵۴ مگابیت بر ثانیه (د) همه موارد

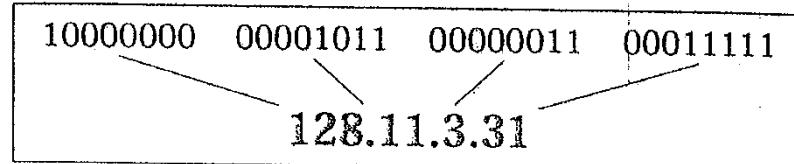
۲۶- کدامیک از گزینه‌های زیر روش‌های ارسال به صورت طیف گستردگ را بیان می‌کند؟

- (الف) DHSS و FHSS (ب) DHSS و FSSS (ج) DSSS و FHSS (د) DSSS و FSSS

۴- آدرس IP

چنانچه قبل از وظایف لایه شبکه، آدرسدهی منطقی است. یکی از مشهورترین روش‌های آدرسدهی منطقی که در پروتکل TCP/IP استفاده می‌شود، آدرس IP است. آدرس IP یک آدرس ۳۲ بیتی (چهار بایتی) است که برای سهولت در خواندن و نوشت، معادل اعشار باشتها را می‌توانیم که به صورت چهار عدد دهدهی که با نقطه از هم جدا شده‌اند، نوشتند می‌شود.

در شکل (۴-۲) یک آدرس IP به فرم دو دویی و معادل دهدهی آن نشان داده شده است. آدرس‌های IP منحصر به فرد و جهانی هستند. به عبارت دیگر هیچ دو دستگاهی در اینترنت دارای آدرس IP یکسانی نیستند.



شکل (۴-۲)- آدرس IP

فضای آدرسدهی آدرس‌های IP شامل ۲^{۳۲} آدرس است که این آدرسها به دسته‌های مختلفی به نام کلاس‌های آدرسدهی به نامهای A, B, C, D, E و F تقسیم‌بندی شده‌اند. اینکه یک آدرس IP به چه کلاسی تعلق دارد، از روی بیت‌های اول (سمت چپ) آن مشخص می‌گردد؛ به طوری که اگر آدرس IP را به صورت دو دویی بنویسیم، و بیت سمت چپ آن صفر باشد، آدرس مذکور متعلق به کلاس A بوده و اگر دو بیت سمت چپ آن به صورت 10 باشد، متعلق به کلاس B می‌باشد.

شکل (۴-۳) نحوه تشخیص کلاس‌های مختلف را نشان داده است.

	بایت اول	بایت دوم	بایت سوم	بایت چهارم
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

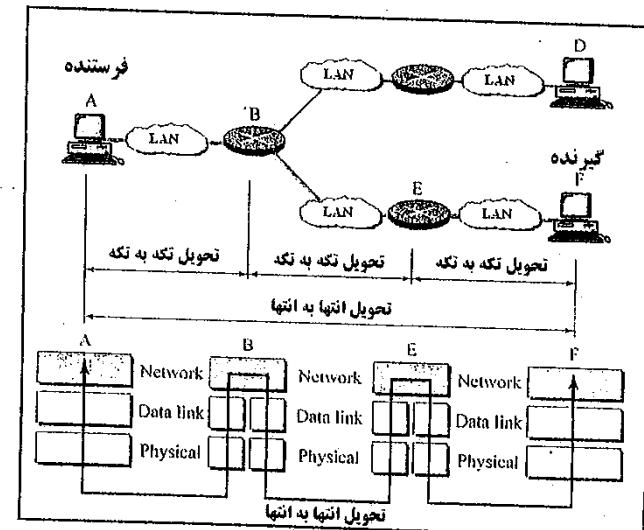
شکل (۴-۳)-
کلاس‌های آدرس IP

لایه شبکه وظیفه دارد که به مقصد نهایی برساند. این لایه سرویسهایی را از لایه پیوند داده دریافت کرده و سرویسهایی به لایه انتقال می‌دهد. اصلی‌ترین سرویسی که از لایه پیوند داده دریافت می‌کند، انتقال داده به صورت نقطه به نقطه است. اگر بین مبدأ و مقصد چند نقطه میانی وجود داشته باشد، برای تحويل داده از مبدأ به مقصد، نیاز به چند بار تحويل به صورت تکه به تکه می‌باشیم.

برای رسیدن به این مقصود، لایه شبکه لازم است توبیلوژی زیر شبکه‌های ارتباطی را بداند تا بتواند مناسب‌ترین مسیر را برای تحويل داده انتخاب نماید. انتخاب مناسب‌ترین مسیر (مسیریابی) از

بین مبدأ و مقصد ممکن است چندین شبکه با پروتکلهای مختلف و اندازه فریم‌های متفاوت وجود داشته باشد. یکی دیگر از وظایف این لایه رفع این مشکلات است.

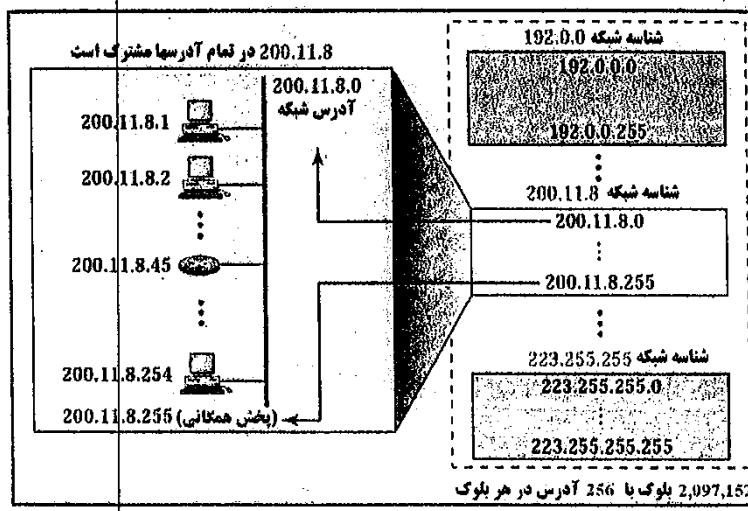
در شکل (۴-۱)، تحويل انتها به انتها در مقایسه با تحويل تکه به تکه یا جهش به جهش (تحويل دریک جهش) نشان داده شده است.



شکل (۴-۱)- تحويل انتها به انتها

همانطور که احتمالاً متوجه شده باشید، از کلاس A برای شبکه‌های بزرگ استفاده می‌شود؛ چون در این کلاس سه بایت مشخص کننده کامپیووترهای داخل یک شبکه می‌باشد. کلاس B برای شبکه‌های متوسط و کلاس C برای شبکه‌های کوچک مناسب است.

همانطور که در شکل (۴-۵) مشاهده می‌کنید تعداد زیادی شبکه کلاس C وجود دارد که در داخل هر کدام ۲۵۶ آدرس IP قرار دارد. از این تعداد، ۲۵۴ آدرس برای کامپیووترهای داخل شبکه استفاده می‌شود. آدرس اول یعنی X.X.X.0، برای نشان دادن آدرس شبکه و آدرس X.X.X.255 برای پخش همگانی در کل شبکه استفاده می‌شود.



شکل (۴-۵)- شبکه کلاس C

در این شکل، آدرس‌های داخل شبکه 200.11.8.0 نشان داده شده است. سه عدد اول برای تمام کامپیووترهای داخل این شبکه یکسان است زیرا این شبکه متعلق به کلاس C می‌باشد. بسته‌ای که آدرس مقصد آن 200.11.8.255 باشد، توسط همه کامپیووترهای داخل شبکه دریافت می‌گردد. در مورد شبکه‌های کلاس B، آدرس شبکه به صورت X.X.0.0 و آدرس پخش همگانی به صورت X.X.255.255 خواهد بود. آدرس شبکه در شبکه‌های کلاس A، به صورت 0.0.0.0 و آدرس پخش همگانی در این نوع شبکه‌ها به صورت X.255.255.255 می‌باشد.

کلاس آدرسدهی را می‌توان از روی معادل مبنای ده آدرس با توجه به عدد سمت چپ، به صورت زیر تشخیص داد:

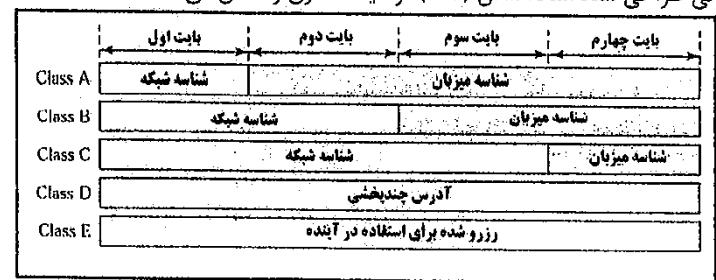
- ۰ تا ۱۲۷، کلاس A
- ۱۲۸ تا ۱۹۱، کلاس B
- ۱۹۲ تا ۲۲۳، کلاس C
- ۲۲۴ تا ۲۳۹، کلاس D
- ۲۴۰ تا ۲۵۵، کلاس E

به عنوان مثال آدرس‌های زیر متعلق به کلاس‌های ذکر شده می‌باشند:

- C: 195.29.81.212 کلاس A: 28.213.87.12
- D: 232.67.102.17 کلاس B: 167.210.8.51

آدرس 127.0.0.1 (در حالت کلی 127.X.X.X) در کلاس A به عنوان loopback استفاده شده و بسته ارسالی به این آدرس به خود کامپیوتر برمی‌گردد. این کار جهت تست کردن پروتکل انجام می‌شود.

آدرس IP یک آدرس دوسری است که در آن شناسه شبکه و شناسه میزبان داخل شبکه مشخص شده است. در کلاس A، بایت سمت چپ مشخص کننده شبکه و سه بایت دیگر مشخص کننده کامپیووتری داخل آن شبکه می‌باشد. در کلاس B، دو بایت سمت چپ مشخص کننده شبکه و دو بایت دیگر، کامپیووتری داخل آن شبکه را مشخص می‌نماید. در کلاس C، سه بایت سمت چپ بیانگر یک شبکه و بایت باقیمانده، کامپیووتری داخل آن شبکه را مشخص می‌کند. کلاس D برای مقاصد چندپیشی (Multicast) استفاده می‌شود. چند پخشی حالتی بین تک پخشی (Unicast) و پخش همگانی (Broadcast) می‌باشد که در آن، پخش برای گروهی از کاربران صورت می‌گیرد. در این حالت آدرس گروه مذکور همه چهار بایت را دربر می‌گیرد. از کلاس E استفاده نمی‌شود و برای مقاصد آتی طراحی شده است. شکل (۴-۴) توضیحات فوق را نشان می‌دهد.



شکل (۴-۴)- شناش شبکه و میزبان در آدرس IP

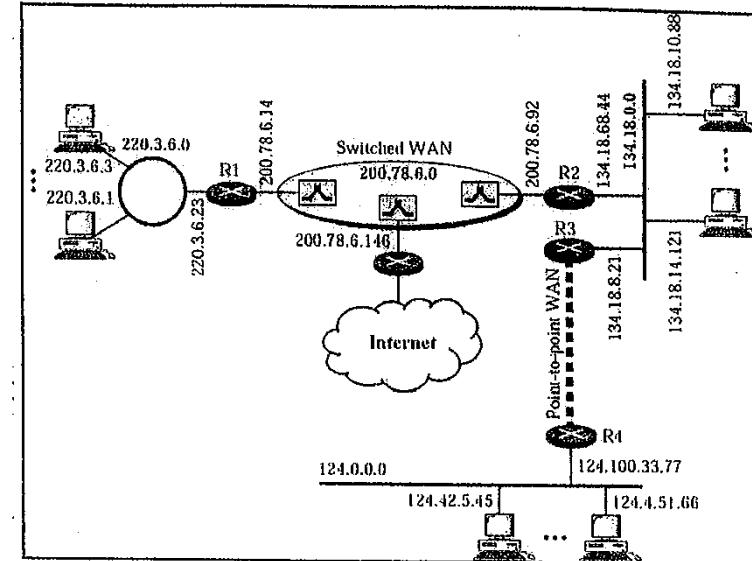
۳- هفهوم Mask یا پوشش شبکه

هنگامی که یک مسیریاب بسته‌ای را با آدرس مقصد مشخصی دریافت می‌کند، احتیاج دارد که آنرا به یکی از پورتهای خروجیش منتقل کند تا به سمت مقصد هدایت شود. این کار بر اساس آدرس شبکه بسته انجام می‌گردد تا مشخص شود که آیا متعلق به شبکه داخلی بوده یا اینکه باید خارج شود. ممکن است بپرسید که مسیریاب آدرس شبکه را چگونه تشخیص می‌دهد؟ این کار توسط مفهومی به نام Mask انجام می‌گردد. Mask یک رشته ۳۲ بیتی است که به صورت تعدادی ۱ پشت سرهم و سپس تعدادی ۰ پشت سرهم نوشته می‌شود. این رشته بیت، اگر بیت به بیت با آدرس IP AND منطبق شود، آدرس شبکه به دست می‌آید.

مثال برای آدرس IP 128.11.3.31 که معادل باینری آن به صورت زیر است خواهیم داشت:
 $IP = 10000000\ 00001011\ 00000011\ 00011111$
 $Mask = 11111111\ 11111111\ 00000000\ 00000000 = 255.255.0.0$
 $IP \text{ AND } Mask = 10000000\ 00001011\ 00000000\ 00000000 = 128.11.0.0$

مشاهده می‌کنید که نتیجه عمل AND، آدرس 128.11.0.0 بوده که همان آدرس شبکه است. بنابراین پوشش به صورت پیش فرض برای شبکه‌های کلاس A به صورت 255.0.0.0 برای شبکه‌های کلاس B به صورت 255.255.0.0 برای شبکه‌های کلاس C به صورت 255.255.255.0 می‌باشد. دقت کنید که در هر حالت، تعداد بیت‌های ۱، برابر با تعداد بیت‌های شناسه شبکه در کلاس مربوطه است.

در شکل (۶-۴)، ترکیبی از شبکه‌های مختلف که با مسیریاب به همدیگر متصل شده‌اند را مشاهده می‌کنید. سعی کنید از روی آدرس شبکه، تشخیص دهید که هر کدام متعلق به چه کلاسی هستند. هر مسیریاب به تعداد پورتهایی احتیاج به آدرس IP دارد.



شکل (۶-۴)- اتصال شبکه‌های مختلف توسط مسیریاب

برای درک بهتر آدرس زیرشبکه ها، دو بایت سمت چپ را به صورت مبنای دو و دو بایت سمت راست را به صورت مبنای دو نوشته ایم:

137.12.00	100000.00000000
137.12.32.0	يا

137.12.01	000000.00000000
137.12.64.0	يا

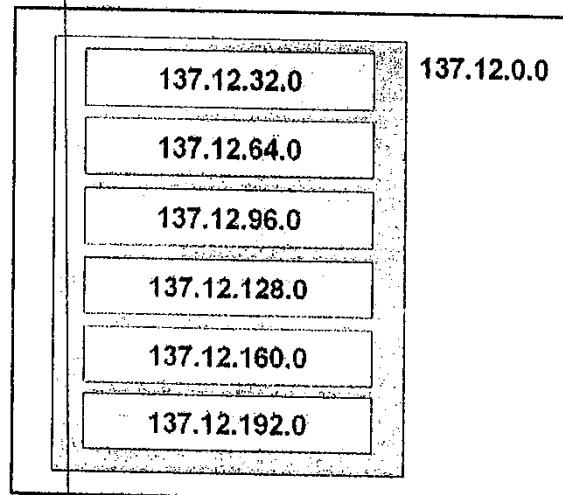
137.12.01	100000.00000000
137.12.96.0	يا

137.12.10	000000.00000000
137.12.128.0	يا

137.12.10	100000.00000000
137.12.160.0	يا

137.12.11	000000.00000000
137.12.192.0	يا

شبکه 137.12.0.0 و زیرشبکه های آن در شکل (۴-۸) نشان داده شده اند.



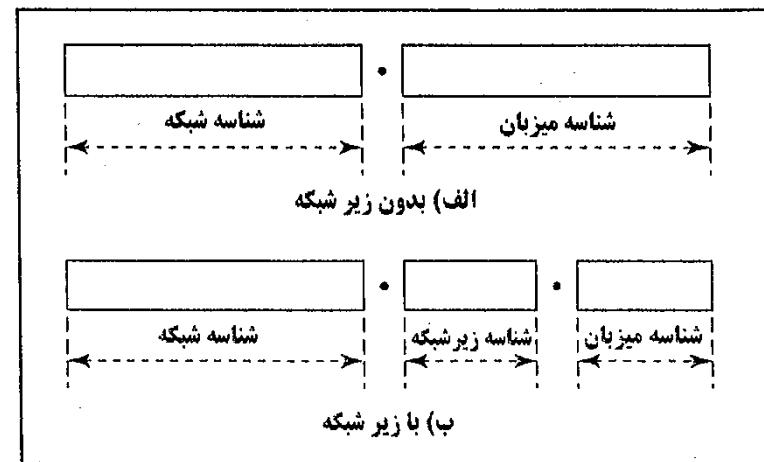
شکل (۴-۸)-آدرس زیرشبکه

از روی آدرس IP یک کامپیوتر می توان فهمید که متعلق به کدام زیرشبکه است؛ مثلاً کامپیوتر با آدرس 137.12.41.27 در زیرشبکه اول، و کامپیوتر با آدرس 137.12.139.12 در زیرشبکه چهارم قرار دارد.

پوشش برای زیرشبکه مشابه پوشش شبکه است با این تفاوت که این بار علاوه بر بیتهاي شناسه شبکه، بیتهاي شناسه زیرشبکه هم باید برابر با ۱ باشند. مثلاً پوشش زیرشبکه برای

۴- زیرشبکه سازی

همانطور که قبله گفته شد آدرس IP یک آدرس دو سطحی است. اگر بخواهیم یک شبکه را به تعدادی زیرشبکه تقسیم کنیم، از تکنیکی به نام زیرشبکه سازی (Subnetting) استفاده می کنیم. این کار به دلایل زیادی ممکن است انجام گردد. مثلاً اگر بخواهیم در اداره ای قسمتهای مختلف مثلاً حسابداری، کارگزینی و غیره را از هم تفکیک کنیم، به طوری که ترافیک شبکه در هر قسمت به کامپیوترهای همان قسمت محدود شود، از تکنیک زیرشبکه سازی استفاده می کنیم. برای این کار از قسمت شناسه میزبان تعدادی بیت قرض گرفته و یک آدرس سه سطحی مطابق شکل (۷-۴) می سازیم.



شکل (۷-۴)-زیرشبکه سازی

فرض کنید بخواهیم شبکه کلاس B، 137.12.0.0، را به شش زیرشبکه تقسیم کنیم. برای این کار سه بیت از شناسه میزبان فرض گرفته و در نتیجه ۱۳ بیت برای شناسه میزبان باقی می ماند. بنابراین یک آدرس سه سطحی شامل ۱۶ بیت شناسه شبکه، ۳ بیت شناسه زیرشبکه و ۱۳ بیت شناسه میزبان حاصل می گردد.

دقت کنید که با ۳ بیت می توان ۶ (۲^۳-۲) زیرشبکه را مشخص نمود. زیرا در این حالت نیز دو وضعیت ۰۰۰ و ۱۱۱، قابل قبول نیست.

زیرشبکه‌های فوق برابر با 255.255.224.0 می‌باشد. شکل(۹-۴) نحوه بدست آوردن پوشش زیرشبکه را برای مثال فوق نشان می‌دهد.

255.255.0.0	
پوشش پیش فرض	11111111 11111111 00000000 00000000
16	
255.255.224.0	
پوشش زیرشبکه	11111111 11111111 111 00000 00000000
3	13

شکل(۹-۴)- پوشش زیرشبکه

با استفاده از روش آدرسدهی به صورت کلاس‌های A، B و C، فضای آدرس‌های IP به صورت زیر تقسیم می‌گردد:

- تعداد ۱۲۶ شبکه کلاس A که هر کدام تا ۱۶۷۷۷۲۱۴ میزبان می‌تواند داشته باشد.
- تعداد حدود ۶۵۰۰ شبکه کلاس B که هر کدام تا ۸۵۳۴ میزبان می‌تواند داشته باشد.
- تعداد بیش از دو میلیون شبکه کلاس C که هر کدام تا ۲۵۴ میزبان می‌تواند داشته باشد.

همانطور که مشاهده می‌کنید، این روش تقسیم بندي بسیار ناهمگون است به طوری که فضای آدرسدهی IP به سه قسمت با اندازه‌های بسیار متفاوت تقسیم شده است؛ به طوری که اگر سازمانی به ۱۰۰ آدرس IP احتیاج داشته باشد، یک شبکه کلاس C به آن اختصاص داده خواهد شد که در این حالت تعداد ۱۵۴ آدرس بلاستفاده خواهد ماند. این مساله در کلاس‌های A و B بسیار حادتر است. همچنین برای بسیاری از ارگانها یک کلاس C بسیار کوچک و یک کلاس B بسیار بزرگ است.

روش آدرسدهی بدون کلاس، یک راه حل برای استفاده بهینه از فضای آدرس‌های IP است. همانطور که در بخش ۲ گفته شد، در کلاس‌های آدرسدهی A، B و C به ترتیب ۸، ۱۶ و ۲۴ بیت برای شناسه شبکه استفاده می‌شود. در روش آدرسدهی بدون کلاس، این محدودیت وجود ندارد و هر تعداد بیت را می‌توان به عنوان شناسه شبکه تعیین نمود. تعداد بیتهاي مشخص شده به عنوان شناسه شبکه پس از علامت "/" و در انتهای آدرس IP نوشته می‌شود. به عنوان مثال در آدرس نوشته شده به فرم 25.13.12.48/25، قسمت "25" مشخص می‌کند که ۲۵ بیت برای شناسه شبکه استفاده شده است. دقت کنید که در این حالت تعداد ۷ بیت برای شناسه میزبان باقی می‌ماند که در نتیجه تعداد ۱۲۶ میزبان در این شبکه می‌تواند وجود داشته باشد. همچنین در شبکه 192.168.12.0/23، تعداد ۲۳ بیت برای شناسه شبکه و ۹ بیت برای شناسه میزبان استفاده می‌شود. دقت کنید که این شبکه معادل دو شبکه کلاس C، 192.168.12.0/24 و 192.168.13.0/24 می‌باشد.

ایده پشت آدرسدهی بدون کلاس، مسیریابی بین حوزه‌ای بدون کلاس یا CIDR است که در آن مسیریابها بدون توجه به کلاس IP و تنها از روی منطبق‌ترین آدرس (طولانی‌ترین انتظام) پورت مناسب جهت خروج بستدها را پیدا می‌کنند.

۶- ترجمه آدرس شبکه (NAT)

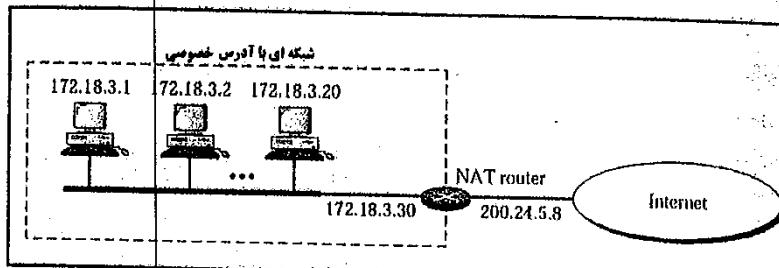
تعداد کاربران و شبکه‌های کوچک استفاده کننده از اینترنت روز به روز در حال افزایش است. همانطور که می‌دانیم هر کامپیوتر یا دستگاهی که بخواهد به اینترنت وصل شود احتیاج به یک آدرس IP دارد. در اوایل که آدرس دهی توسط IP مطرح گردید، کمتر کسی به این فکر می‌افتد که ممکن است خواسته‌ای مطرح شود که نتوان به آن یک آدرس را نسبت داد. با استفاده از سیستم آدرس دهی IP می‌توان (2^{32}) آدرس را تولید کرد. تعداد واقعی آدرس‌های قابل استفاده کمتر از مقدار فوق است (بین $\frac{3}{2}$ میلیارد و $\frac{3}{3}$ میلیارد). علت این امر، تفکیک آدرسها به کلاسها و اتفاف تعداد زیادی آدرس IP بخصوص در کلاس‌های A و B و همچنین رزرو بودن برخی از آدرس‌ها برای چندپخشی، تست و موارد خاص دیگر است.

با انفجار اینترنت و افزایش شبکه‌های کامپیوترا، تعداد آدرس‌های IP موجود، پاسخگوی نیازها نبود. منطقی ترین روش، طراحی مجدد سیستم آدرس دهی IP است تا امکان استفاده از آدرس‌های IP بیشتری فراهم گردد. موضوع فوق در حال پیاده‌سازی بوده و نسخه شماره شش IPv6، راهکاری در این زمینه است. چندین سال طول خواهد کشید تا سیستم فوق پیاده‌سازی گردد، چراکه می‌بایست تمامی زیرساخت‌های اینترنت تغییر و اصلاح گرددند. NAT با هدف کمک به مشکل فوق طراحی شده است.

NAT این امکان را فراهم می‌کند که تعداد زیادی آدرس داخلی توسط یک یا چند آدرس خارجی از بیرون قابل شناسایی باشند. برای جداسازی آدرس‌های داخلی یک موسسه و یا یک کاربر با آدرس‌های اینترنت، سه مجموعه از آدرسها به عنوان آدرس‌های خصوصی، به این کار اختصاص داده شده‌اند، به طوری که هر سازمان یا اداره‌ای می‌تواند از این آدرسها استفاده نماید. این بدین معنی است که هر کدام از این آدرسها ممکن است توسط هزاران شبکه در سراسر جهان استفاده شده باشند. جدول زیر محدوده آدرس‌های خصوصی را نشان می‌دهد.

تعداد آدرسها	محدوده آدرس‌های خصوصی
2^{24}	از ۱۰.۰.۰.۰ تا ۱۰.۲۵۵.۲۵۵.۲۵۵
2^{20}	از ۱۷۲.۳۱.۰.۰ تا ۱۷۲.۳۱.۲۵۵.۲۵۵
2^{16}	از ۱۹۲.۱۶۸.۰.۰ تا ۱۹۲.۱۶۸.۲۵۵.۲۵۵

محدوده آدرس‌های فوق را گاهی اوقات آدرس‌های نامعتبر نیز می‌نامند؛ زیرا مسیریابها بسته‌ای که حاوی چنین آدرسی باشد عبور نمی‌دهند. واضح است که کاربرانی که ازین آدرسها استفاده می‌کنند نمی‌توانند به اینترنت وصل شوند مگر اینکه قبل از آدرس آنها به یک آدرس معتبر ترجمه شود. این کار توسط مسیریابی که حداقل دارای یک آدرس معتبر و منحصر بفرد در اینترنت باشد شود. این شکل (۴-۱۰) یک شبکه کلاس B که دارای آدرس خصوصی می‌باشد و توسط یک مسیریاب با آدرس معتبر به اینترنت وصل می‌شود، نشان داده است.



شکل (۴-۱۰)-مفهوم NAT

همانطور که مشاهده می‌کنید، مسیریاب دارای یک آدرس معتبر در طرف اینترنت و یک آدرس خصوصی در سمت شبکه مذکور می‌باشد. تمام بسته‌هایی که از شبکه مذکور به طرف اینترنت خارج می‌شوند، آدرس 200.24.5.8 را به عنوان آدرس مبدا حمل می‌کنند. به عبارت دیگر این شبکه از دید کاربران دیگر اینترنت به صورت یک آدرس IP دیده می‌شود. ممکن است پرسید که مسیریاب از کجا می‌فهمد که بسته‌های دریافتی از اینترنت هر کدام متعلق به کدام کامپیوتر داخل شبکه است؟

این کار توسط جدولی موسوم به جدول ترجمه در داخل مسیریاب صورت می‌گیرد. مسیریاب هر کامپیوتر داخل شبکه یک شماره پورت نسبت می‌دهد و در داخل جدول ترجمه، آدرس خصوصی کامپیوترها و شماره پورت آنها را یادداشت می‌کند. این کار مسیریاب را در یافتن کامپیوتر مورد نظر هنگام دریافت یک بسته از اینترنت کمک می‌کند.

۷- پروتکل‌های لایه شبکه

پروتکل IP

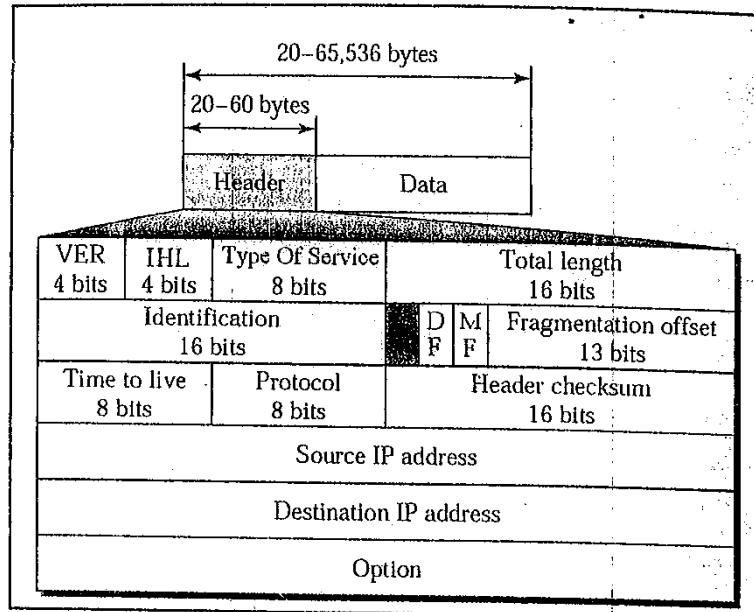
این پروتکل که به IP نسخه چهار (IPV4) نیز معروف است، پروتکلی است که مسئولیت ارسال انتها به انتهای میزبان به میزبان را در لایه شبکه به عهده دارد و مهمترین پروتکل لایه شبکه است. IP یک پروتکل غیرقابل اعتماد و غیر اتصالگرایست که تلاش خود را برای رساندن بسته‌های اطلاعاتی به مقصد می‌کند ولی کنترل روی خطاب و یا جریان داده ندارد. ممکن است یک بسته اطلاعاتی در زمان ارسال، گرفتار مسائل متعددی نظیر گم شدن، خرابی، عدم توزیع با اولویت مناسب، تکرار در ارسال و یا تاخیر گردد. در چنین مواردی، پروتکل IP تلاشی به منظور حل مشکلات فوق نخواهد کرد و داده‌های مورد نظر باید مجدداً ارسال شوند. آگاهی از وصول بسته اطلاعاتی در مقصد و بازیافت بسته‌های اطلاعاتی گم شده، مسئولیتی است که بر عهده پروتکلهای لایه بالاتر نظیر TCP و یا برنامه ارسال کننده اطلاعات، واگذار می‌گردد.

IP را می‌توان همانند سیستم پست در نظر گرفت. اداره پست حداقل تلاش خود را برای رساندن نامه‌ها به مقصد می‌نماید ولی همیشه موفق نمی‌شود. اگر بنا به دلایلی نامه‌ای گم شود، این وظیفه فرستنده نامه است که آن را مجدد ارسال نماید.

بسته‌های IP را داده‌نگار (Datagram) هم می‌گویند. این پروتکل در صورت لزوم می‌تواند یک داده‌نگار را به تکه‌های کوچکتری به نام fragment بشکند. مثلاً هنگامی که یک مسیریاب بین یک شبکه Token Ring با سایز بسته‌های بزرگتر و یک شبکه اترنت با سایز بسته‌های کوچکتر قرار می‌گیرد، مجبور به شکستن بسته‌ها خواهد بود. پروتکل IP مجبور است هنگام تکه کردن یک داده‌نگار، برای آن یک شماره مشخصه و برای هر تکه، یک شماره ترتیب قرار دهد تا گیرنده بتواند یک داده‌نگار را برای تحویل به لایه بالاتر بازسازی کند.

هر چند حداقل طول یک بسته IP می‌تواند تا ۶۴ کیلوبایت باشد، اما در عمل عموماً اندازه بسته‌ها چیزی حدود ۱۵۰۰ بایت است.

در شکل(۱۱-۴) قالب یک بسته IP نشان داده شده است. همانطور که مشاهده می‌کنید، سرآیندی که پروتکل IP در لایه شبکه به بسته اضافه می‌کند، بین ۲۰ تا ۶۰ بایت است. اگر اندازه داده صفر باشد، بسته فقط شامل سرآیند خواهد بود. سرآیند مذکور، دارای تعدادی فیلد مجزا می‌باشد که هر کدام حاوی اطلاعاتی هستند که در زمان مورد نیاز، این اطلاعات از داخل بسته‌ها استخراج شده مورد استفاده قرار می‌گیرد.



شکل(۱۱-۴)-قالب یک بسته IP

اینک به بررسی فیلدهای قالب بسته IP می‌پردازیم:

فیلد VER (version)

اولین فیلد در قسمت header نگاش پروتکل را تعیین می‌کند که می‌تواند ۴ یا ۶ باشد. در حال حاضر تمامی سیستم‌ها و شبکه‌ها از نسخه شماره ۴ پروتکل IP پشتیبانی می‌کنند. بنابراین، عددی که در این فیلد قرار می‌گیرد، همان (0100) با ۴ است.

فیلد IHL

این فیلد هم چهار بیتی است و طول کل سرآیند را بر مبنای کلمات ۳۲ بیتی بیان می‌نماید. پس اگر عنوان مثال در این فیلد عدد ۲۰ قرار گرفته باشد بدین معناست که کل سرآیند ۳۲۰ بیت معادل ۴۰ بایت خواهد بود. طول header حداقل ۲۰ بایت و حداقل ۶۰ بایت خواهد بود. به همین دلیل حداقل عددی که می‌تواند در این فیلد قرار گیرد ۵، و حداقل آن ۱۵ می‌باشد.

فیلد Fragmentation Offset

در این قسمت شماره ترتیب تکه های یک داده نگار شکسته شده قرار دارد و چون اندازه این فیلد ۱۳ بیت می باشد، یک داده نگار می تواند حداقل به ۸۱۹۲ تکه شکسته شوند. (اندازه هر تکه بیش از آخری باید ضربی از ۸ باشد).

فیلد (TTL) Time To Live

این فیلد ۸ بیتی عملان نقش یک شمارنده را بازی می کند که طول عمر بسته در آن قرار می گیرد. در این فیلد زمان سرگردانی بسته مشخص می شود و این بدين معنی است که این بسته می تواند از چند مسیر یا ب عبور کند تا به مقصد برسد؛ که حداقل آن ۲۵۵ می باشد.

فیلد Protocol

در این فیلد شماره پروتکلی که قرار است بسته به آن بررسد مشخص می شود. مثلاً این شماره برای پروتکل TCP برابر با ۶ و برای پروتکل UDP برابر با ۱۷ است.

فیلد Header Checksum

وظیفه کشف خطای احتمالی در header بسته را بر عهده دارد.

فیلد Source IP Address

در این فیلد آدرس IP مبدأ نوشته می شود.

فیلد Destination IP Address

در این فیلد آدرس IP مقصد نوشته می شود.

فیلد اختیاری Option

در این فیلد می تواند تا حداقل چهل بایت قرار بگیرد و محتوای آن اطلاعاتی است که می توان با آنها به مسیریابها در مورد یافتن مسیر مناسب کمک کرد.

:Type Of Service

در این فیلد نوع سرویس انتقال تعیین می شود: کم سرعت و مطمئن یا پرسرعت و نامطمئن. بنویان مثال ممکن است یک میزبان بخواهد صدا و یا تصویری را بصورت بلادرنگ برای مقصد مورد نظرش ارسال نماید؛ در چنین شرایطی تقاضای ارسال سریع و به موقع اطلاعاتش را دارد نه قابلیت اطمینان صد درصد. در برخی شرایط دیگر مانند ارسال Email یا ارسال فایل، موقع اطمینان صد درصد از شبکه وجود دارد و سرعت تاثیر چندانی بر کیفیت کار ندارد.

فیلد Total Length

در این فیلد اندازه کل بسته IP قرار دارد که شامل قسمت سرآیند و ناحیه داده می باشد. مبنای طول بر حسب بایت است. بنابراین همانطور که گفته شد، طول کل بسته می تواند ۶۴ کیلوبایت یا ۶۵۵۳۵ بایت باشد.

فیلد Identification

همانگونه که قبلاً اشاره شد، برخی از مسیریابها و حتی میزبانها مجبورند یک داده نگار را به تکه های کوچکتر بشکنند و سپس در مقصد آن را بازسازی کنند. بنابراین یک داده نگار واحد که باقیتی شکسته شود، به گونه ای باید مشخص گردد تا در هنگام بازسازی بتوان تکه هایش را از بقیه تشخیص داد. در این فیلد که ۱۶ بیتی است، عددی قرار می گیرد که یک داده نگار واحد را مشخص می کند.

فیلد Fragment Offset

این فیلد خود به سه بخش تقسیم می شود:

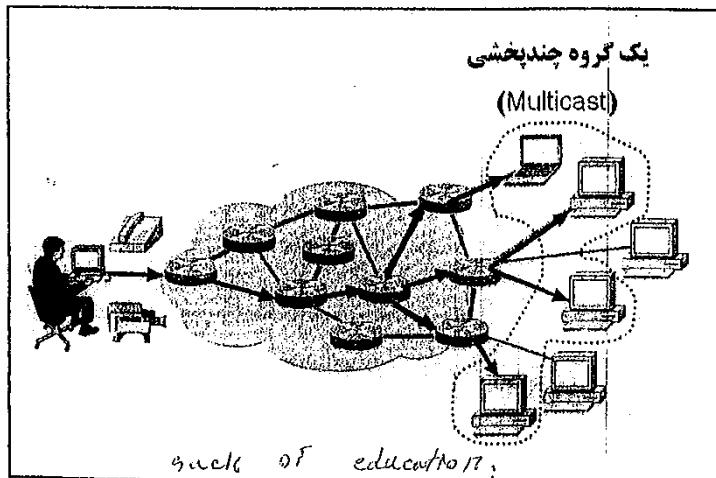
- بیت DF: مخفف Don't Fragment است. اگر این بیت ۱ باشد هیچ مسیریابی حق شکستن این بسته را ندارد زیرا مقصد قادر به بازسازی تکه ها نیست.
- بیت MF: مخفف More Fragment است. این بیت مشخص می کند که آیا بسته جاری آخرین تکه از یک داده نگار محسوب می شود یا باز هم تکه های بعدی وجود دارند. اگر این بیت ۰ بود به این معنی است که این تکه آخرین تکه ارسال شده می باشد.

۷- پروتکل IGMP - برگشتن ریدکت مسیر به آن دسته میزبان

این پروتکل مدیریت لیست اعضاء و گروهها را برای ارسال چندپخشی (Multicast) در یک شبکه مبتنی بر TCP/IP بر عهده دارد. چند پخشی فرآیندی است که بر اساس آن یک پیام برای گروهی انتخاب شده از گیرنده‌گان که گروه multicast نامیده می‌شود، ارسال می‌گردد. چندپخشی امروزه کاربردهای فراوانی دارد که از جمله می‌توان به آموزش از راه دور، ارتباطات چندرسانه‌ای و دسترسی به پایگاههای داده توزیع شده اشاره نمود. IGMP لیست اعضاء را نگهداری نموده، نحوه ورود و خروج اعضاء از گروه را کنترل می‌نماید. زمانی که چندین کامپیوتر نیازمند دستیابی به اطلاعات مشترکی باشند، یک آدرس IP را روزشده برای multicasting استفاده می‌گردد. مسیریابها نیز که به منظور پردازش چندپخشی پیکربندی می‌گردند، اطلاعات را انتخاب و آنها برای تمامی مشترکین گروه چندپخشی ارسال می‌نمایند. بنابراین هر یک از مسیریابهای موجود در مسیر ارتباطی می‌نایست قادر به حمایت از چندپخشی باشد.

IGMP از آدرس‌های کلاس D، یعنی از آدرس‌های 224.0.0.0 تا 239.255.255.255 برای این کار استفاده می‌کند.

تمامی اعضای یک گروه چندپخشی، به ترافیک هدایت شده برای آدرس آن گروه، گوش داده و بسته‌های اطلاعاتی ارسال شده به آن آدرس را دریافت می‌نمایند. در شکل (۱۲-۴)، مفهوم چندپخشی نشان داده شده است.



شکل (۱۲-۴)- چندپخشی در اینترنت

internet control message protocol ICMP

این پروتکل عهده‌دار گزارش دادن خطاهای و پیامهای مربوط به تحويل بسته‌های IP می‌باشد. همان پروتکلی است که وقتی میزبان مقصد غیر قابل دسترس است، به ما اخطار می‌دهد و با مدت زمانی که برای رسیدن به مقصد لازم است را اعلام می‌نماید. این پروتکل را می‌توان مشابه پلیس راهنمایی و رانندگی در شبکه راهها و جاده‌ها در نظر گرفت؛ چراکه مانند پلیس موالب عملیات شما بر روی اینترنت می‌باشد. پیامهای ICMP به دو دسته تقسیم می‌شوند:

الف) پیامهای گزارش دهنده خطأ شامل:

۱- مقصد غیرقابل دسترسی (Destination Unreachable). این خطأ هنگامی اتفاق می‌افتد که یک بسته IP به خارج فرستاده شده ولی یا آدرس مقصد پیدا نمی‌شود و یا اینکه کامپیوتر مقصد قرارداد تعیین شده را پشتیبانی نمی‌کند.

۲- تفییر دادن مسیر (Redirect). این پیغام توسط مسیریابها ارسال می‌شود. به طوری که اگر مسیریاب یک مسیر بهتر را به سوی یک مقصد ویژه تعیین کند، اولین بسته‌ای را که دریافت نموده به جلو میراند و یک پیغام تغییر مسیر به میزبان می‌فرستد تا جدول مسیریابی خود را بروز درآورد.

۳- آرام سازی منبع (Source Quench). گاهی اوقات به دلیل اینکه بسته‌های زیادی دریافت شده‌اند و نمی‌توان پردازش را بر روی تمام آنها انجام داد، این پیغام گزارش می‌شود و نشانگر این است که نیازمند آرامتر شدن مخابره از جانب منبع است.

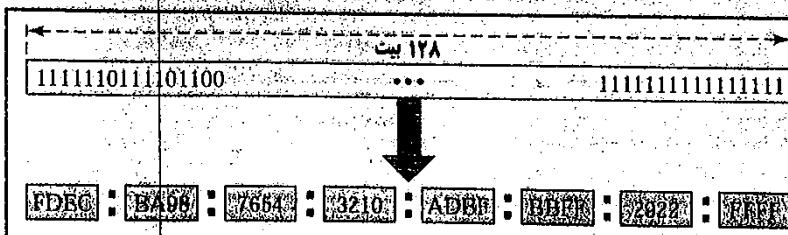
۴- به سرسیدن زمان (Time Exceeded). این پیغام زمانی صادر می‌شود که بسته IP به خاطر سپری شدن زمان TTL، حذف شود؛ و بدین ترتیب ماشین فرستنده را از وجود یک حلقه مسیریابی نامتناهی آگاه کند و یا از کم بودن TTL برای رسیدن به مقصد اخطار دهد.

ب) پیامهای ارسال پرسش مانند درخواست طنین (Echo Request) و پاسخ طنین (Echo Reply) که در برنامه Ping استفاده می‌شوند. از برنامه ping برای برای تست وضعیت ارتباط بین دو سیستم موجود در شبکه استفاده می‌شود. برای تست در دسترس بودن یک کامپیوتر در شبکه، آدرس IP و یا نام نمادین آن را جلوی دستور ping در Command Prompt تایپ می‌کنیم. بدین ترتیب یک پیغام درخواست طنین برای مقصد ارسال می‌شود. اگر مقصد در دسترس بود، با پیغام پاسخ طنین جواب می‌دهد. در غیر اینصورت پیغام خطأ توسط ICMP ظاهر می‌شود.

پروتکل IPv6

این پروتکل که به آن IP نسل بعد (IP Next Generation) هم گفته می‌شود برای حل مشکلات IP موجود ابداع شده است. ویژگیهای IPv6 طوری طراحی شده است که گذر آن را بسیار آسان کرده است. برای مثال آدرس‌های IPv6 بصورت اتوماتیک ایجاد سیاهی IPv4 استخراج می‌گردد. این پروتکل نسبت به نسخه قبلی آن دارای محاسبی به شرح زیر است:

(الف) فضای آدرس بزرگتر: آدرسها در IPv6 ۱۲۸ بیت طول دارند، بنابراین تعداد دستگاههایی که به این روش می‌توان آدرسدهی کرد عدد بسیار بزرگی (۳^{۱۲۸}) می‌باشد. این آدرسها به صورت ۸ عدد چهار رقمی (۳۲ رقم) در منای شانزده، که با علامت ":" از هم جدا شده‌اند، نوشته می‌شوند. در شکل (۱۴-۴) نمونه‌ای از یک آدرس IPv6 نشان داده شده است.



شکل (۱۴-۴)-آدرسدهی در IPv6

(ب) فرمت سرآیند بهتر: کاهش تعدادی از فیلدهای موجود در سرآیند IPv4 از سرآیند IPv6، مسیریابی روترا را آسان‌تر نموده و باعث بالا رفتن کارآبی روترهای نیز می‌شود. فرمت سرآیندها در IPv6 در مقایسه با IPv4 بسیار ساده‌تر است. این سرآیندها در جهت بهینه سازی مسیریابی طراحی شده‌اند. روترهای موجود در مسیر بسته‌ها نیازی به تکه کردن بسته‌ها ندارند. همچنین checksum بسته‌ها نیز ازین رفتار نیست. همچنین تعدادی از فیلدها را می‌توان به اختیار، فرارداد و یا حذف کرد.

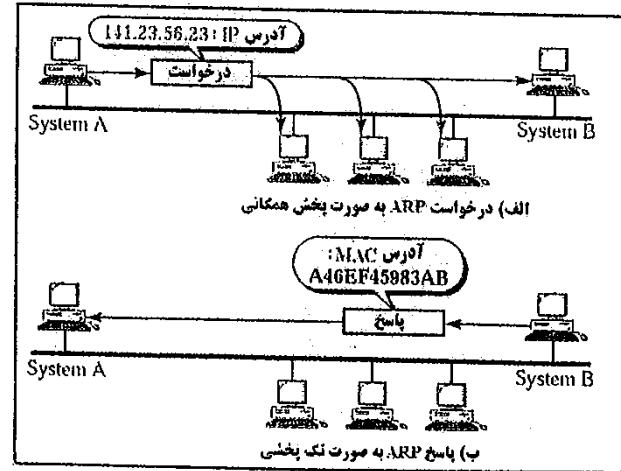
(ج) قابلیت توسعه بهتر: این پروتکل به گونه‌ای طراحی شده است که به راحتی با تکنولوژیها و کاربردهای جدید در صورت نیاز سازگار است.

پروتکل ARP

اینترنت ترکیبی از شبکه‌های فیزیکی مختلفی است که از طریق مسیریابها به هم‌دیگر متصل شده‌اند. بسته‌ای که از یک میزبان مبدأ سفر خود را شروع می‌کند، تا به میزبان مقصد برسد از شبکه‌های فیزیکی متعددی ممکن است عبور کند. میزبانها و مسیریابها در سطح شبکه با آدرس IP شناخته می‌شوند. آدرس IP یک آدرس بین شبکه‌ای بوده و قلمرو آن جهانی می‌باشد.

اما در داخل یک شبکه فیزیکی، میزبانها و مسیریابها توسط آدرس MAC شناخته می‌شوند. آدرس MAC یک آدرس محلی است و قلمرو آن در حد همان شبکه است. برای رسیدن یک بسته به مقصد، هم آدرس IP در لایه شبکه و هم آدرس MAC در لایه پیوند داده مورد نیاز است.

آدرس IP مقصد مشخص بوده ولی آدرس MAC آن برای فرستنده ناشناخته است. پروتکل ARP با داشتن آدرس IP یک میزبان یا یک پورت مسیریاب، آدرس MAC آن را بر می‌گرداند. نحوه کار آن بدین ترتیب است که برای به دست آوردن آدرس فیزیکی، ARP یک درخواست به صورت پخش همگانی برای تمام ایستگاههای موجود در آن شبکه فیزیکی ارسال می‌نماید و از ایستگاهی که آدرس IP آن را اعلام نموده درخواست می‌کند تا آدرس MAC خود را اعلام نماید. ایستگاهی که آدرس IP آن با آدرس اعلام شده موافقت داشته باشد، آدرس MAC خود را به صورت یک پاسخ تک پخشی برای ایستگاه درخواست کننده ارسال می‌کند. مراحل کار در شکل (۱۳-۴) نشان داده شده است.



شکل (۱۳-۴)- طرز کار پروتکل ARP

۸- مسیریابی (Routing)

همانطور که قبلاً گفته شد، در لایه شبکه از دید بالاتری به شبکه نگاه می‌شود. هنگامی که یک بسته از مبدأ به طرف مقصد ارسال می‌شود، ممکن است از تعداد زیادی مسیریاب عبور کند تا به مسیریابی که به شبکه مقصد متصل است برسد. مسیریابی به معنای انتخاب مناسبترین مسیر از مبدأ تا مقصد می‌باشد. ممکن است پرسید که منظور از مناسبترین مسیر چیست؟ در پاسخ باید گفت که معیارهای مختلفی برای انتخاب مناسبترین مسیر ممکن است در نظر گرفته شود. معیارهایی مانند: تعداد مسیریابها در یک مسیر (تعداد جهشها)، پهنای باند، تاخیر، قابلیت اطمینان و ... می‌توانند تأثیرگذار باشند. در عمل ثابت شده است که هیچ کدام از معیارهای فوق به تهایی نمی‌تواند ملاک باشد. بلکه برای انتخاب یک مسیر بهینه باید ترکیبی از معیارهای مذکور را با ضرایب مشخصی به کار برد.

Communication به مجموعه مسیریابها و کانالهای فیزیکی مابین آنها زیرساخت ارتباطی یا Subnet گفته می‌شود. برای نشان دادن زیرساخت ارتباطی از یک شبکه، تمامی ماشینهای میزبان خود را در یک فضای مجازی (Virtual Space) قرار می‌دهند که میزبان گفته شود. برای این ماشینها هیچ تاثیری در برقراری ارتباط و حمل ترافیک بسته ها نداشته و به عنوان استفاده کننده نهایی یا End user مطرح هستند. زیرساخت ارتباطی را به صورت یگ گراف نشان می‌دهند که در آن مسیریابها به عنوان گره (node) و شبکه‌های فیزیکی بین آنها، به صورت یالهای گراف در نظر گرفته می‌شوند.

هر مسیریاب دارای جدولی است موسوم به جدول مسیریابی که از روی آن می‌تواند بسته‌های دریافتی را یک جهش به جلو هدایت کند و یا به عبارت دیگر به مسیریاب بعدی تحويل دهد. به عنوان مثال جدول مسیریابی برای مسیریاب UOK در شکل(۴-۱۵) به صورت زیر است:

شبکه مقصد	پورت خروجی
132.34.0.0	S0
201.23.56.0	S1
194.34.6.0	E0

۵) پشتیبانی تخصیص منابع: در این پروتکل فیلد نوع سرویس (type of service) حذف شده و مکانیزمی به نام برچسب جریان (flow label) اضافه شده است که به منبع اجازه می‌دهد درخواست رفثار بخصوصی با یک بسته را بنماید. این مکانیزم را می‌توان برای پشتیبانی از ترافیکهای مانند ویدئو و صوت به صورت real time استفاده نمود.

۶) پشتیبانی از امنیت بالاتر: گزینه‌های مربوط به رمزگاری و تصدیق هویت که در این پروتکل تعبیه شده‌اند، محروم‌گاری و درستی بسته‌ها را تضمین می‌کنند.

IPV6 سه نوع پخش را پشتیبانی می‌کند:
Unicast: ارتباط بین یک فرستنده و یک گیرنده می‌باشد. بسته‌هایی که بدین صورت ارسال می‌شوند، فقط توسط یک استگاه دریافت می‌گردند.

Multicast: ارتباط بین یک فرستنده و چند گیرنده است. بسته‌هایی که بدین ترتیب ارسال می‌شوند توسط تمام اعضای یک گروه دریافت می‌شوند.

Anycast: ارتباط بین یک فرستنده و یک عضو از یک گروه می‌باشد. بسته‌هایی که بدین صورت ارسال می‌شوند اگر توسط یکی از اعضای گروه دریافت شوند، کافی است.

۷) دقت کنید که IPV6 از پخش همگانی پشتیبانی نمی‌کند و آن را با چندپخشی پیاده‌سازی می‌نماید.

الگوریتمهای مسیریابی

بر اساس اینکه مسیریابها چگونه اطلاعاتی در مورد زیرساخت ارتباطی شبکه جمع آوری می‌نمایند و نیز چگونگی تحلیل آنها از اطلاعات برای تعیین بهترین مسیر، الگوریتمهای مسیریابی می‌توان به دو دسته مت مرکز و غیر مت مرکز تقسیم بندی کرد.

در الگوریتمهای مت مرکز هر مسیریاب باید اطلاعات کاملی از زیرساخت ارتباطی شبکه داشته باشد یعنی هر مسیریاب باید تمامی مسیریابهای دیگر، ارتباطات بین آنها و هزینه هر خط را دقیقاً شناسایی نماید؛ سپس با جمع آوری این اطلاعات، "ساختمان داده" مربوط به گراف زیرساخت شبکه تشکیل پدهد.

در چنین شرایطی برای یافتن بهترین مسیر بین هر دو مسیریاب، از الگوریتمهای کوتاهترین مسیر نظری "الگوریتم دایکسترا (Dijkstra)" استفاده می‌شود. به چنین الگوریتمهایی که برای مسیریابی به اطلاعات کاملی از زیرساخت شبکه و هزینه ارتباط بین هر دو مسیریاب نیازمندند، اصطلاحاً الگوریتمهای وضعیت پیوند (Link State) گفته می‌شود که در مسیریابهای مدرن و جدید استفاده می‌گردد.

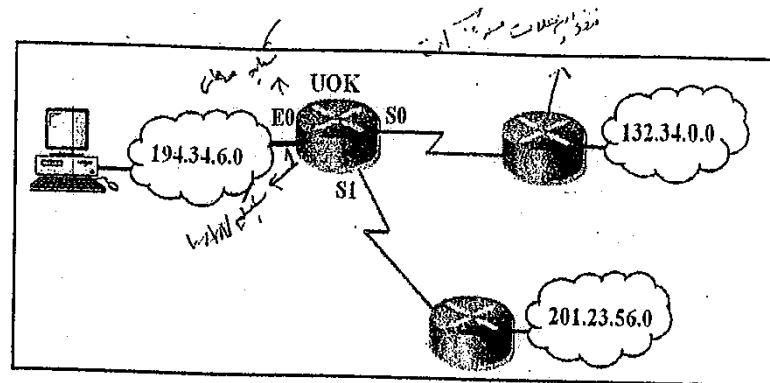
در الگوریتم های مسیریابی غیر مت مرکز، مسیریابها اطلاعات کاملی در مورد زیرساخت ارتباطی شبکه ندارند و هر مسیریاب اطلاعاتی در مورد مسیریابهایی که مستقیماً به آن متصل شده است در اختیار دارد. این الگوریتمها به بردار فاصله (Distance Vector) معروف هستند. اکنون به شرح مفصل این دو روش می‌پردازیم.

الگوریتمهای بردار فاصله یا DV

در الگوریتمهای بردار فاصله که به نامهای Bellman-Ford و Ford-Fulkerson نیز معروف هستند، هر مسیریاب دارای یک جدول مسیریابی می‌باشد که بهترین مسیر تا هر مقصد را نشان می‌دهد. در این جدول هر رکورد دارای سه فیلد مجزا است:

- آدرس شبکه مقصد.
- کوتاهترین فاصله برای رسیدن به آن بر حسب تعداد جهش.
- مسیریاب بعدی که باید بسته تحويل آن گردد.

در شکل (۱۶-۴) تعدادی مسیریاب و شبکه‌های فیزیکی بین آنها را مشاهده می‌کنید. جداول مسیریابی اولیه برای هر مسیریاب در شکل نشان داده شده است. برای سهولت، هر شبکه با یک شماره شناسایی مشخص شده است. همانطور که مشخص است، در لحظه اولیه هر مسیریاب فقط



شکل (۱۵-۴)- اتصال شبکه‌ها از طریق مسیریاب

جدول مسیریابی به دو صورت قابل تنظیم است:

• به صورت ایستا (Static)

در این روش، جدول مسیریابی توسط مدیر شبکه و به صورت دستی تنظیم می‌شود. بدینهی است که در صورت خراب شدن یک مسیر و یا تغییر پیکربندی زیرساخت ارتباطی شبکه، مجدداً باید تغییرات به صورت دستی وارد شوند. این روش هیچ اعتنایی به شرایط توپولوژیکی و ترافیک لحظه‌ای شبکه نمی‌کند.

• به صورت پویا (Dynamic)

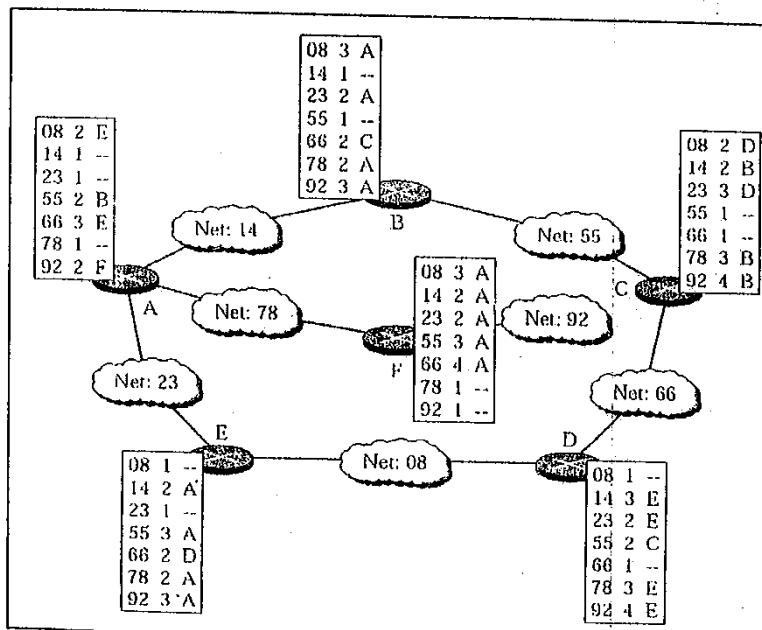
در روش پویا، جدول مسیریابی توسط الگوریتمهای مسیریابی و بر اساس آخرین وضعیت توپولوژیکی و ترافیک شبکه، هر T ثانیه بکار به هنگام می‌شود. این الگوریتمها براساس وضعیت فعلی شبکه تصمیم گیری می‌نمایند ولی ممکن است پیچیدگی این الگوریتمها به قدری زیاد باشد که زمان تصمیم گیری برای انتخاب بهترین مسیر، طولانی شده و منجر به تاخیرهای بحرانی گردد و نهایتاً به ازدحام (Congestion) بینجامد. به همین دلیل در مسیریابهای سریع از تکنیکهای چندپردازنده‌ای و پردازش موازی استفاده می‌شود.

بحث را روی الگوریتمهای مسیریابی برای به هنگام کردن جدول مسیریابی در روش پویا متمرکز می‌کنیم.

این کار را بقیه مسیریابها نیز انجام می‌دهند. در نهایت همه مسیریابها از وضعیت بقیه شبکه‌ها و نحوه رسیدن به آنها باخبر می‌شوند. در شکل (۱۸-۴) جدول مسیریابی نهایی برای همه مسیریابها نشان داده شده است.

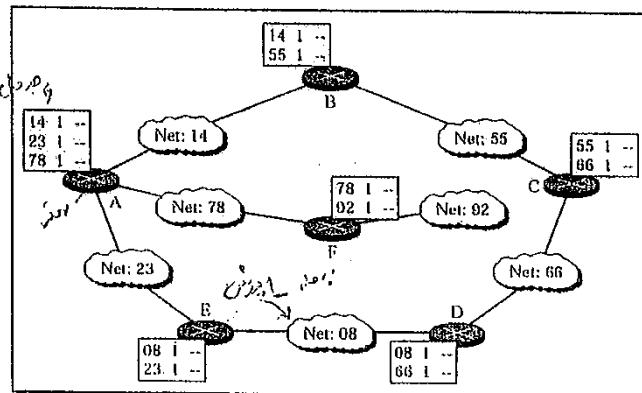
- می‌توان خصوصیات الگوریتم DV را به صورت زیر خلاصه کرد:
- مسیریابها اطلاعاتی را که در اختیار دارند به اشتراک می‌گذارند. اگرچه در آغاز ممکن است این اطلاعات پراکنده و ناقص باشد ولی به تدریج کاملتر می‌شود.
- مسیریابها اطلاعاتشان را فقط با همسایه‌های خود در میان می‌گذارند.
- اطلاعات در فواصل زمانی منظمی (مثلث هر ۳۰ ثانیه یک بار) ارسال می‌گردد.

یکی از مشهورترین پروتکلهایی که به این روش کار می‌کند، پروتکل RIP است. این پروتکل تا ۱۵ چesh را پشتیبانی می‌کند. به عبارت دیگر بسته‌ها تا ۱۵ مسیریاب به جلو رانده می‌شوند. در جدول مسیریابی نیز فاصله بینهایت و یا لینکهای قطع شده با هزینه ۱۶ نشان داده می‌شود.



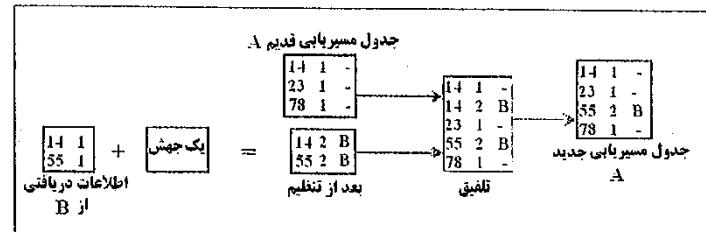
شکل (۱۸-۴)- جدولهای مسیریابی نهایی

اطلاعات مربوط به شبکه‌هایی که مستقیماً به آنها متصل است را می‌داند. فرض شده که هزینه رسیدن به این شبکه‌ها برابر با یک چesh باشد. از آنجا که برای رسیدن به این شبکه‌ها لازم نیست مسیریاب دیگری طی شود، فیلد مربوط به مسیریاب بعدی خالی گذاشته شده است. در روش مسیریابی بردار فاصله، هر مسیریاب فقط با مسیریابهای همسایه در ارتباط است و تمام اطلاعاتی را که در مورد شبکه در اختیار دارد، به آنها خبر می‌دهد. مسیریاب همسایه اصطلاحاً به مسیریابی گفته می‌شود که با یک چesh می‌توان به آن رسید. مسیریابها به محض روشن شدن شروع به شناسایی مسیریابهای همسایه می‌نمایند. این کار از طریق ارسال بسته‌های مخصوصی به نام بسته‌های Hello صورت می‌گیرد.



شکل (۱۶-۴)- مسیریابی به روش بردار فاصله

همانطور که ملاحظه می‌کنید، مسیریاب A اطلاعی در مورد شبکه ۵۵ ندارد. پس از اینکه مسیریاب B اطلاعات خود را در اختیار مسیریاب A قرار داد، مسیریاب A پس از تنظیم اطلاعات و تلقیق آن با اطلاعات قبلی خویش، درمی‌باید که از طریق مسیریاب B می‌توان با دو چesh به شبکه شماره ۵۵ رسید. مراحل کار در شکل شماره (۱۷-۴) نشان داده شده است.



شکل (۱۷-۴)- بروز رسانی جدول مسیریابی

پیوند خود تا A را از ۱ به ۳ تغییر داده است، بنابراین جدول خود را بروز نموده و وزن پیوند خود تا A را به ۴ تغییر می دهد. این پروسه به همین ترتیب تکرار می شود. این وضعیت در جدول نشان داده شده است.

D	C	B	
3,C	2,B	∞ ,A	هزینه رسیدن به A پس از قطع مسیر
3,C	2,B	3,C	هزینه رسیدن به A پس از اولین update
3,C	4,B	3,C	هزینه رسیدن به A پس از دومین update
5,C	4,B	5,C	هزینه رسیدن به A پس از سومین update
5,C	6,B	5,C	هزینه رسیدن به A پس از چهارمین update
7,C	6,B	7,C	هزینه رسیدن به A پس از پنجمین update

راه حل های مختلفی برای این مساله پیشنهاد شده که عمدها پیچیده‌اند به مقرن به صرفه نستند.

ساده ترین راه حل آن است که وقتی یک مسیریاب می خواهد اطلاعاتی را به همسایه هایش بدهد هزینه رسیدن به آنها را که قطعاً باید از همان مسیریاب بگذرند، اعلام نمی کند (یا بینهایت اعلام می کند).

به عنوان مثال چون C می داند که مسیر A از B می گذرد، هنگامی که بخواهد جدول مسیریابی خود را به B اعلام کند هزینه رسیدن به A را بینهایت اعلام می کند. این راه حل را روش شکاف افق (Split Horizon) می گویند.

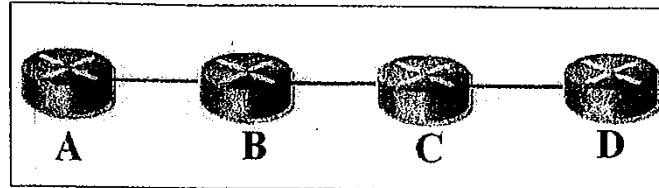
به طور کلی الگوریتم های بردار فاصله برای شبکه های بزرگ مناسب نیستند.

الگوریتم های وضعیت حالت یا LS

در این نوع الگوریتم ها که به الگوریتم Dijkstra نیز معروف هستند، هر مسیریاب اطلاعات کاملی از تپولوژی شبکه کسب می کند. برخلاف روش قبل که در آن هر مسیریاب فقط همسایه هایش را می شناخت و اطلاعی در مورد شبکه ها و یا مسیریاب های دورتر نداشت، در این روش هر مسیریاب اطلاع کاملی از سایر مسیریاب های دیگر و نحوه اتصالات آنها دارد. بدین ترتیب تمام مسیریابها نقشه یکسانی از شبکه در اختیار خواهند داشت.

یکی از مهم ترین مشکلات هنگام کار با الگوریتم های DV، مشکل شمارش تا بینهایت (Count to infinity) است. این اشکال زمانی پیش خواهد آمد که یکی از مسیریابها دچار خرابی شود یا آنکه مسیر ارتباطی او با دیگران قطع شود. اجازه بدھید. این مشکل را با ذکر یک مثال توضیح دهیم.

در شکل (۱۹-۴) چهار مسیریاب A تا D وجود دارد که هر کدام فقط از یک مسیر می تواند به دیگری برسد.



شکل (۱۹-۴)- مشکل شمارش تا بینهایت

جدول زیر فاصله مسیریابها و نحوه دسترسی آنها به هم دیگر را نشان می دهد. مثلاً مسیریاب A سه جهش تا مسیریاب D فاصله دارد.

	A	B	C	D
A	0,-	1,A	2,B	3,C
B	1,B	0,-	1,B	2,C
C	2,B	1,C	0,-	1,C
D	3,B	2,C	1,D	0,-

اگر یکی از مسیریابها جدول خود را بروز نموده و قطع شود. در این هنگام، B جدول خود را تصحیح می کند و هزینه رسیدن به A را مقدار بینهایت در نظر می گیرد. بعد از یک مدت زمان خاص، مسیریابها جداول خود را مبادله نموده و بنابراین B جدول مسیریابی C را دریافت می کند. از آنجایی که C نمی داند چه اتفاقی برای پیوند بین A و B رخ داده است، مقدار قبل از خرابی را گزارش می دهد و اعلام می کند که مسیری با هزینه ۲ به سمت A وجود دارد. B این جدول را دریافت نموده و تصور می کند که یک پیوند جداگانه بین C و A وجود دارد، بنابراین جدول خود را تصحیح نموده مقدار بینهایت را به ۳ تغییر می دهد. به همین شکل دوباره مسیریابها جداول خود را مبادله می کنند. هنگامی که C جدول مسیریابی B را دریافت می نماید، مشاهده می کند که B وزن

(۴) بسته LSA ساخته شده را به روش "سیل آسا" برای تمامی مسیریابهای شبکه ارسال نماید و همچنین بسته‌هایی را که از مسیریابهای دیگر می‌رسند دریافت و ذخیره کند. در روش سیل آسا هر مسیریاب بسته دریافتی را بر روی تمام پورتهای خود به غیر از پورتی که بسته از آن وارد شده است، ارسال می‌کند.

(۵) با استفاده از الگوریتم مناسب، بهینه‌ترین مسیر را بین هر دو مسیریاب در شبکه، پیدا نماید. بعد از آنکه همه مسیریابها بسته‌های LSA همیگر را دریافت کردند، از روی آنها می‌توانند اطلاعات کاملی در مورد توپولوژی شبکه و وضعیت سایر مسیریابها به دست آورند. مسیریابها زیرساخت ارتباطی را به صورت یک گراف در نظر می‌گیرند. سپس می‌توانند از الگوریتم یافتن کوتاهترین مسیر در گراف، مانند الگوریتم دایجکسترا، مناسبت‌ترین مسیر بین خود و سایر مسیریابها را پیدا کنند. در حقیقت با استفاده از الگوریتم دایجکسترا می‌توان یک درخت پوشای مینیمال از گراف به دست آورد. این درخت که ریشه آن همان مسیریاب سازنده است، تمام مسیریابهای دیگر را شامل بوده و ضمناً کم هزینه‌ترین درخت است.

قبل از اینکه به ادامه بحث پردازیم، اجازه دهید در مورد الگوریتم دایجکسترا کمی بیشتر توضیح دهیم.

همانطور که گفته‌یم، برای یافتن کوتاهترین مسیر بین دو ند در یک گراف جهت دار می‌توان از الگوریتم دایجکسترا استفاده کرد.

شیوه کد این الگوریتم در زیر نشان داده شده است که راهنمای آن به صورت زیر است:

- N مجموعه ندهای گراف
- (i,j) هزینه یا وزن لبه‌ای که ند i را به ند j وصل می‌کند
- S ند جاری
- M مجموعه ندهایی که تاکنون متصل شده‌اند
- C(n) هزینه مسیر از ند S به ند n

فرض کنید می‌خواهیم کوتاهترین مسیر از ند S به سایر ندهای گراف را در نشان (۲۱-۴) پیدا کنیم. ابتدا در مجموعه M فقط ند جاری قرار دارد. سپس هزینه بقیه ندها نا S را حساب نموده و مجموعه M را طوری گسترش می‌دهیم که هزینه رسیدن S با ندهای داخل آن کمترین باشد. این کار را تا پیوستن تمام ندهای گراف به M ادامه می‌دهیم.

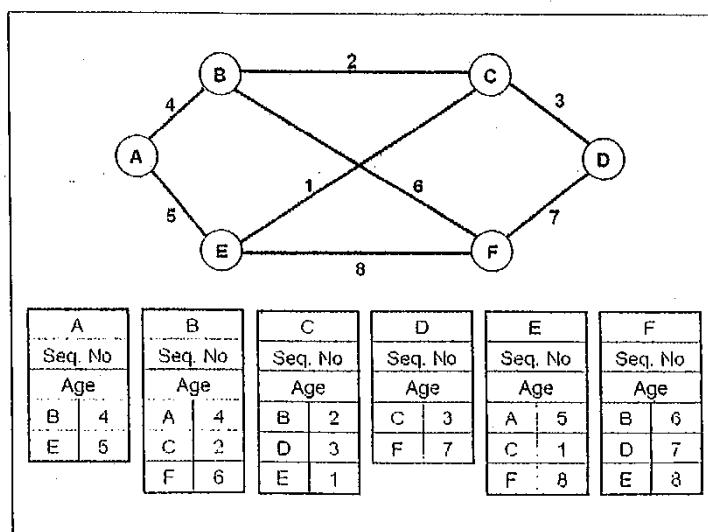
برای اینکه این اطلاعات بدست آید باید هر مسیریاب مرحل زیر را طی کند:

(۱) مسیریابهای مجاور خود را که بصورت فیزیکی به آنها متصل است شناسایی کرده و آدرس آنها را بدست آورده. برای شناسایی مسیریابهای مجاور، چنانکه در قسمت قبل نیز گفته شد، هر مسیریاب بسته‌های مخصوصی به نام بسته‌های Hello روی تمام خروجیهای خود ارسال می‌نماید. مسیریابهایی که مستقیماً به آن متصل هستند، ضمن پاسخ به این بسته، آدرس IP خود را نیز اعلام می‌نمایند.

(۲) تاخیر یا بطور کلی هزینه مسیریابهای مجاور خود را اندازه گیری نماید. محاسبه تاخیر از روی ارسال بسته‌های echo صورت می‌گیرد. مسیریابهای مجاور به این بسته‌ها پاسخ می‌دهند. برای محاسبه تاخیر بین دو مسیریاب، زمان رفت و برگشت این بسته‌ها تقسیم بر دو می‌گردد.

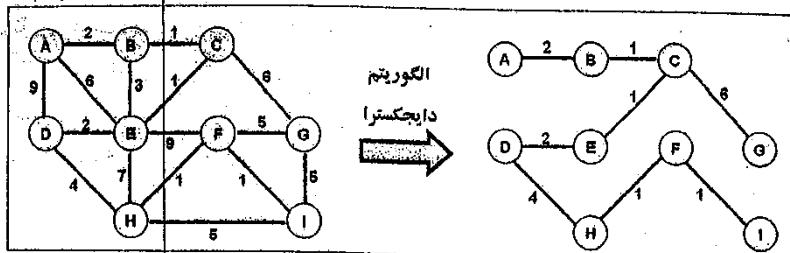
(۳) یک بسته بسازد و تمام اطلاعاتی که از مسیریابهای مجاور خود دارد در آن قرار بدهد. این بسته‌ها که LSA نامیده می‌شوند، شامل آدرس IP مسیریاب تولید‌کننده آن، شماره ترتیب، طول عمر بسته و آدرس IP مسیریابهای مجاور و هزینه تخمینی برای رسیدن به آنها می‌باشد.

در نشان (۲۰-۴)، یک زیرساخت ارتباطی مشکل از مسیریابهای A تا F و هزینه اتصالات بین آنها به صورت یک گراف وزن دار نشان داده است. بسته‌های LSA مربوط به هر کدام از مسیریابها نیز نشان داده شده‌اند.



نشان (۲۰-۴)- بسته‌های LSA

در شکل (۲۲-۴) یک گراف و درخت پوشای مینیمال برای گره A، نشان داده شده است.



شکل (۲۲-۴)- درخت پوشای مینیمال

بدین ترتیب کوتاهترین فاصله از گره A تا سایر گره‌ها به صورت زیر است:

	A	B	C	D	E	F	G	H	I
A	0	2	3	6	4	11	9	10	12

مسیریاب از روی این درخت می‌تواند جدول مسیریابی خود را بسازد. پروتکل OSPF از این روش برای مسیریابی استفاده می‌کند.

در پایان می‌توان خصوصیات الگوریتم LS را به صورت زیر خلاصه کرد:

- مسیریابها فقط اطلاعاتی را که از آن مطمئن هستند (در مورد مسیریابهای مجاور) به اشتراک می‌گذارند.
- مسیریابها اطلاعاتشان را برای تمام مسیریابهای دیگر به روش سیل آپا ارسال می‌کنند.
- اطلاعات، هنگامی که تغییراتی در زیرساخت ارتباطی اتفاق می‌افتد، ارسال می‌گردد.

مسیریابی سلسله مراتبی (SPT)

همانطور که در بخش قبل دیدیم، در هر دو الگوریتم LS و DV، هر مسیریاب مجبور به ذخیره نمودن اطلاعات مربوط به مسیریابهای دیگر می‌باشد. هنگامی که اندازه شبکه رشد می‌کند، تعداد مسیریابهای شبکه افزایش می‌یابد؛ در نتیجه اندازه جداول مسیریابی نیز افزایش یافته و مسیریابها می‌توانند ترافیک شبکه را به طور موثر کنترل کنند. مسیریابی سلسله مراتبی روشی برای برطرف کردن این مشکل است.

$$M = \{s\}$$

for each n in $N - \{s\}$

$$C(n) = l(s, n)$$

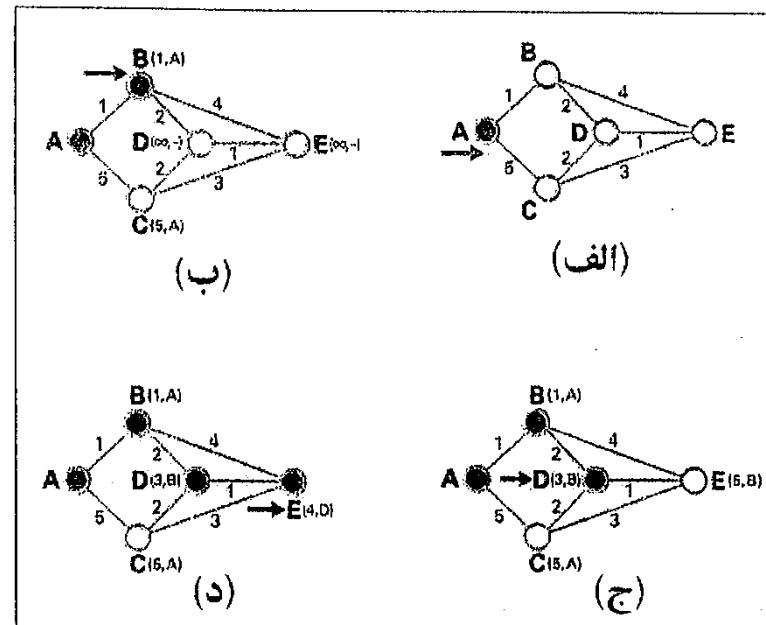
while ($N \neq M$)

$$M = M \cup \{w\} \text{ such that } C(w) \text{ is the minimum for all } w \text{ in } (N - M)$$

for each n in $(N - M)$

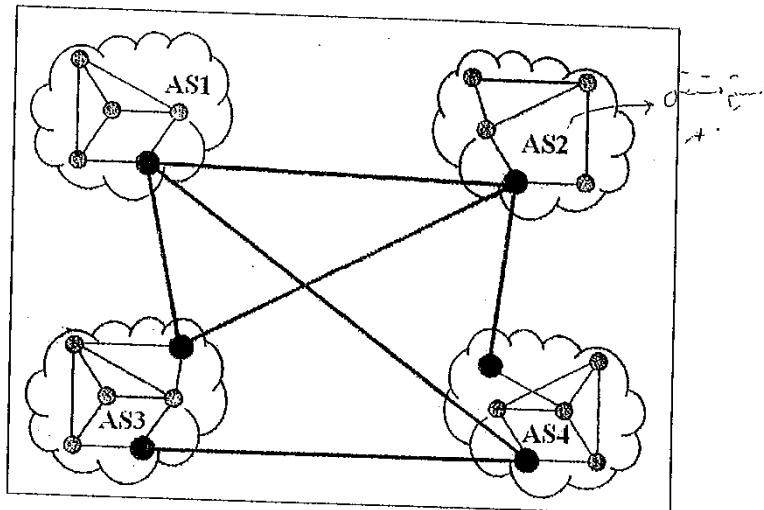
$$C(n) = \min(C(n), C(w) + l(w, n))$$

شکل (۲۱-۴)، مراحل اجرای الگوریتم دایجکسترا را برای یک گراف وزن دار نشان می‌دهد. ندهایی که توزیر هستند متعلق به مجموعه M و ندهای توخالی به مجموعه $N - M$ تعلق دارند. با اضافه شدن هر ند جدید به M تست می‌شود که آیا با در نظر گرفتن این ند، مسیر کوتاهتری تا ندهایی دیگر وجود دارد یا خیر. مثلاً بعد از مرحله (ب) کوتاهترین فاصله A تا E پنج واحد و از طریق ند B بوده است (E(5,B)). با اضافه شدن D به مجموعه M ، بعد از مرحله (ج) مشاهده می‌کنید که این فاصله به چهار واحد و از طریق D کاهش یافته است. در نهایت کوتاهترین فاصله از A تا بقیه ندهای گراف محاسبه شده است.



شکل (۲۱-۴) - الگوریتم دایجکسترا برای یافتن کوتاهترین مسیر در یک گراف وزن دار

قبل از اینکه بحث را در مورد مسیریابی سلسله مرتبی ادامه دهیم، اجازه دهید در مورد مفهومی به نام سیستم خودمختار و یا AS مختصری توضیح دهیم.
به مجموعه مسیریابهای تحت کنترل یک مدیریت واحد یک سیستم خودمختار گفته می‌شود.
در حقیقت اینترنت مجموعه‌ای از تعداد زیادی (حدود ۱۷۰۰۰) سیستم خودمختار است. هر سیستم خودمختار می‌تواند قوانین و پروتکلهای مسیریابی مربوط به خود را داشته باشد. مسئول شبکه خودمختار می‌تواند بر روی شبکه تحت نظرات خود کنترل کامل داشته باشد؛ یعنی می‌تواند در مورد تک‌نج اجزای شبکه، توبولوژی کل شبکه، سیستم عامل، طراحی زیرساخت ارتباطی و طریقه اتصال شبکه‌های محلی و نوع پروتکل مسیریابی تصمیم گیری نماید.
هر AS دارای یک شماره منحصر به فرد ۱۶ بیتی است که آن را از سایر AS‌ها متمایز می‌کند.
در شکل (۴-۲۳) چهار AS را که توسط خطوط ارتباطی به هم‌دیگر متصل شده‌اند، مشاهده می‌کنید.



شکل (۴-۲۳)- اتصال سیستمهای خودمختار

بدین ترتیب مسأله مسیریابی به دو مرحله شکسته می‌شود:

- مسیریابی داخل AS‌ها یا Intra-Domain Routing
- مسیریابی بین AS‌ها یا Inter-Domain Routing

هر AS دارای دو دسته مسیریاب است: مسیریابهای داخلی و مسیریابهای مرزی.

مسیریابهای داخلی که در شکل کوچکتر و کم رنگتر نشان داده شده‌اند، مسئول هدایت بسته‌ها در داخل یک AS می‌باشند و پروتکلهای مسیریابی داخل AS را اجرا می‌کنند. همانطور که قبلاً گفته شد، هر AS می‌تواند از پروتکل مسیریابی مخصوص به خود استفاده کند. به طوری که امکان دارد در یک AS از پروتکل RIP برای مسیریابی استفاده شود و در AS دیگر از پروتکل مسیریابی OSPF استفاده گردد.

پروتکل داخلی AS‌ها هر چه باشد، یک AS برای ارتباط با آن AS‌های دیگر باید از پروتکل واحدی استفاده کند. این پروتکل که توسط مسیریابهای مرزی (که در شکل پررنگتر نشان داده شده‌اند) اجرا می‌شود، پروتکل BGP نام دارد.

در مثال فوق اگر یک ماشین میزبان در AS1 بخواهد بسته‌ای برای ماشین دیگر در AS4 بفرستد سه مرحله مسیریابی لازم است:

□ مسیریابی در درون AS1 تا رسیدن بسته به مسیریاب مرزی با استفاده از یکی از پروتکلهای مسیریابی داخلی (IGRP, RIP, OSPF, ...).

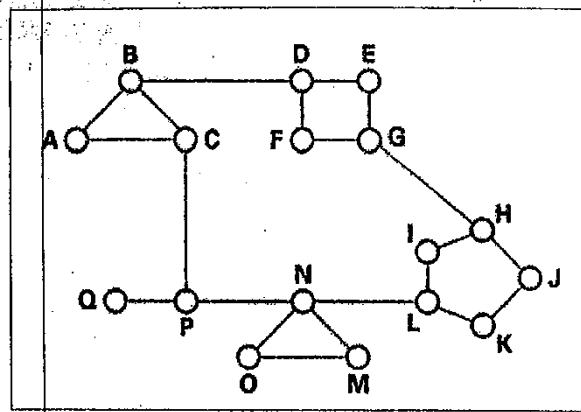
□ مسیریابی روی خطوط ارتباطی بین AS‌ها تا رسیدن به AS4 با استفاده از پروتکل BGP.

□ مسیریابی درون AS4 تا رسیدن به ماشین مقصد با استفاده از یکی از پروتکلهای مسیریابی داخلی.

مسیریابی سلسله‌مراتبی را می‌توان مشابه سفرهای داخلی و سفرهای بین‌المللی فرض نمود. مثلاً یک فرد ایرانی وقتی می‌خواهد از نقطه‌ای به نقطه دیگر سفر کند با یک ارزیابی ساده از میزان هزینه و زمان، مسیر خود را انتخاب و بر اساس آن سفرش را آغاز می‌نماید. یک ایرانی مشکل خاصی برای سفر آزادانه در درون کشور خود ندارد و براحتی می‌تواند بین هر دو نقطه سفر کند. ضوابط حاکم بر راههای هوایی و زمینی کشور نیز توسط دولت تبیین می‌شود.

حال فرض کنید یک ایرانی از ستدج بخواهد به شهر کلن در آلمان سفر کند. برای انتخاب مسیر خود اولاً نیاز به اخذ مجوزهای لازم از کشور مبدأ و مقصد دارد؛ ثانیاً چون پرواز مستقیم بین این دو شهر وجود ندارد؛ باید با یک پرواز داخلی خود را به یک فرودگاه بین‌المللی (مثلاً مهرآباد تهران) رسانده و از طریق یک پرواز خارجی به یکی از شهرهای آلمان (برلین یا فرانکفورت) سفر کند و پس از ورود به آلمان طبق ضوابط دولت آلمان و از یک مسیر مناسب به کلن آلمان سفر کند.

تفاوت‌های ویژه در پروازهای داخلی و پروازهای خارجی از لحاظ سطح کنترل مدارک، اخذ هزینه و مسائل امنیتی وجود دارد. یک پرواز خارجی ممکن است در طول مسیر از کشورهای ثالثی عبور



شکل (۲۵-۴)- مسیریابی در شبکه های بزرگتر

به عنوان مثال جدول مسیریابی برای مسیریاب A به صورت زیر است:

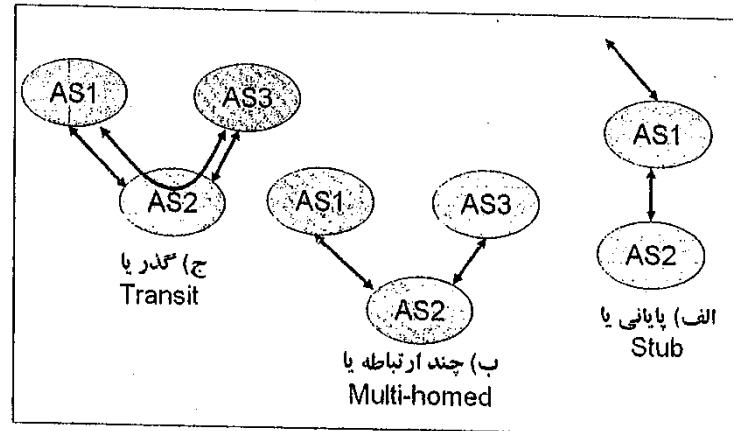
هزینه	از طریق	مقصد
-	-	A
1	B	B
1	C	C
2	B	D
3	B	E
3	B	F
4	B	G
5	B	H
5	C	I
6	C	J
5	C	K
4	C	L
4	C	M
3	C	N
4	C	O
2	C	P
3	C	Q

کند و این کشورها بر اساس تعریفهایی برای عبور یک پرواز خارجی اخذ هزینه کنند یا آنکه بدلا این ممکنی اصلاً اجازه عبور صادر نکنند.

سیستمهای خودمختار را می‌توان بر اساس نحوه اتصال آنها به مسیریابهای BGP به سه دسته تقسیم نمود:

- ۱- AS های پایانی یا Stub: فقط به یک مسیریاب BGP و به عبارتی فقط به یک AS دیگر متصل هستند و نقشی در ستون فقرات اینترنت و انتقال ترافیک اینترنت ایفا نمی‌کنند.
- ۲- AS های چند ارتباطه یا Multi-Homed: بین مسیریابهای BGP قرار دارند یعنی به دو یا چند AS دیگر متصل هستند ولی ترافیک اینترنت را انتقال نمی‌دهند.
- ۳- AS های گذر یا Transit: بین مسیریابهای BGP قرار دارند و نقش اصلی در انتقال ترافیک اینترنت دارند؛ به عبارت دیگر، جزء ستون فقرات اینترنت به شمار می‌روند.

شکل (۲۴-۴) سه نوع AS مذکور را نشان می‌دهد.

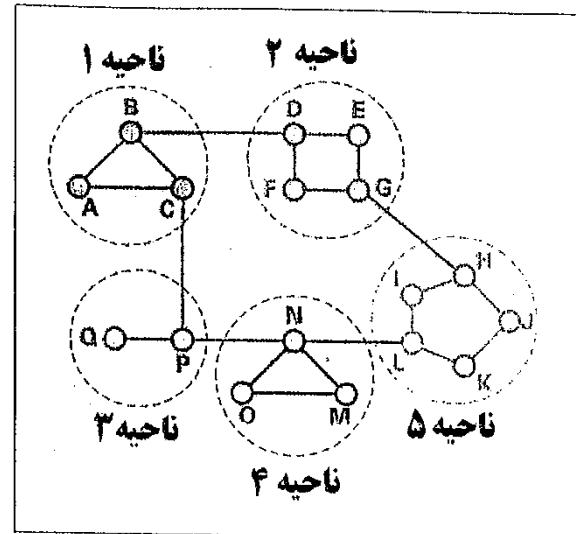


شکل (۲۴-۴) - انواع شبکه های خودمختار یا AS

بحث مسیریابی سلسله مراتبی را با یک مثال ادامه می‌دهیم. فرض کنید در شبکه شکل (۴-۲۵) مسیریابها از روش DV برای ساختن جدول مسیریابی و یافتن بهترین مسیر بین هم‌دیگر استفاده کنند. در وضعیت نشان داده در شکل، هر گره از شبکه مجبور به نگهداری یک جدول مسیریابی با ۱۷ رکورد می‌باشد.

همانطور که ملاحظه می‌کنید، با این کار جدول مسیریابی بسیار کوچکتر شده است و در نتیجه اطلاعات کمتری برای مبادله لازم بوده و راندمان الگوریتم افزایش خواهد یافت. این کار را می‌توان تعمیم داد و مسیریابی را به صورت چند سطحی تعریف نمود.

حال اگر مسیریابها را به صورت تعدادی ناحیه دسته‌بندی کنیم شکل (۲۶-۴) حاصل می‌گردد. در این مثال شبکه را به پنج ناحیه تقسیم کردیم. اگر A بخواهد بسته‌ای را به هر کدام از روترهای ناحیه ۲ ارسال کند، آن را به B می‌دهد و الى آخر، ناحیه‌ها را می‌توان همان سیستمهای خودمختار فرض نمود.



شکل (۲۶-۴)- مسیریابی سلسله مرتبی

با این توضیحات جدول مسیریابی برای مسیریاب A به صورت زیر درخواهد آمد:

هزینه	از طریق	مقصد
-	-	A
1	B	B
1	C	C
2	B	ناحیه ۲
2	C	ناحیه ۳
3	C	ناحیه ۴
4	C	ناحیه ۵

خود آزمایش:

- ۷- طول هدر IP من تواند چا توجه به گزینه های استفاده شده، متغیر باشد، حداقل الازه هدر IP چند بایت است؟
- (الف) ۲۰ بایت (ب) ۱۶ بایت (ج) ۶ بایت
- ۸- آدرس مبدأ در دیتاگرام IPv4 در چه مکانی از هدر ذخیره می گردد؟
- (الف) بایت های ۵ تا ۸ (ب) بایت های ۹ تا ۱۳ (ج) بایت های ۱۳ تا ۲۰ (د) بایت های ۱۷ تا ۲۰
- ۹- آدرس مقصد در دیتاگرام IPv4 در چه مکانی از هدر ذخیره می گردد؟
- (الف) بایت های ۵ تا ۸ (ب) بایت های ۹ تا ۱۳ (ج) بایت های ۱۳ تا ۲۰ (د) بایت های ۱۷ تا ۲۰
- ۱۰- کدامیک از محدوده آدرس های IP زیر مخصوص شبکه های کلاس A می باشد؟
- (الف) ۰.۰.۰ - ۱۲۷.۲۵۵.۲۵۵.۲۵۵ (ب) ۰.۰.۰ - ۱۲۶.۲۵۵.۲۵۵.۲۵۵ (ج) ۰.۰.۰ - ۱۲۷.۲۵۵.۲۵۵.۲۵۵ (د) ۱.۰.۰.۰ - ۱۲۶.۲۵۵.۲۵۵.۲۵۵
- ۱۱- کدامیک از محدوده آدرس های IP زیر بخشی از پک شبکه کلاس B می باشد؟
- (الف) ۱۲۸.۰.۰.۰ - ۱۵۹.۲۵۵.۲۵۵.۲۵۵ (ب) ۱۲۸.۰.۰.۰ - ۱۷۵.۲۵۵.۲۵۵.۲۵۵ (ج) ۱۲۸.۰.۰.۰ - ۲۰۷.۲۵۵.۲۵۵.۲۵۵ (د) ۱۲۸.۰.۰.۰ - ۱۹۱.۲۵۵.۲۵۵.۲۵۵
- ۱۲- کدامیک از محدوده آدرس های IP زیر مخصوص شبکه های کلاس C می باشد؟
- (الف) ۱۹۲.۰.۰.۰ - ۲۱۹.۲۵۵.۲۵۵.۲۵۵ (ب) ۱۹۲.۰.۰.۰ - ۲۲۳.۲۵۵.۲۵۵.۲۵۵ (ج) ۱۹۲.۰.۰.۰ - ۲۱۱.۲۵۵.۲۵۵.۲۵۵ (د) ۱۹۲.۰.۰.۰ - ۲۱۵.۲۵۵.۲۵۵.۲۵۵
- ۱۳- در IPv6، ویژگی Anycast امکان انجام چه عملیاتی را فراهم می نماید؟
- (الف) ارسال پسته های اطلاعاتی برای تمامی اعضای یک گروه (ب) ارسال پسته های اطلاعاتی برای یکی از اعضای یک گروه (ج) گوش دادن به هر پسته اطلاعاتی ارسال شده در شبکه توسط دریافت کنندگان

- ۱- الازه نسل جدید آدرس های IP (IPv6) چقدر است؟
- (الف) ۳۲ بیت (ب) ۹۶ بیت (ج) ۱۲۰ بیت
- ۲- پروتکل IP متعلق به کدام لایه مدل مرجع OSI است؟
- (Transport) (Session) (Data link) (Network)
- ۳- آدرس Loopback در IPv4 چیست؟
- (الف) 0.0.0.0 (ب) 10.0.0.1 (ج) 127.0.0.1
- ۴- پروتکل Address Resolution Protocol: ARP چه عملیاتی را انجام می دهد؟
- (الف) پیدا کردن آدرس IP از روی آدرس MAC (ب) اختصاص اتوماتیک آدرس IP به کامپیوتر
 (ج) پیشگیری از اختصاص یک IP مشابه به دو کامپیوتر متفاوت (د) هیچ کدام
- ۵- محدوده شبکه کلاس D برای چه عملیاتی بر روی اینترنت رزرو شده است؟
- (الف) Broadcast (ب) Multicast (ج) Unicast (د) Anycast
- ۶- پیش فرض برای آدرس های IP کلاس C کدامیک از موارد زیر است؟
- (الف) 255.255.0.0 (ب) 255.255.255.0 (ج) 255.255.255.255 (د) 255.255.0.0

۲۰- کدامیک از برنامه های زیر برای نسبت برقراری اتصال با یکه کامپیوتر در شبکه استفاده می شود؟

- | | | | |
|-------------|-------------|----------|------------------|
| netstat (د) | nbtstat (ج) | ping (ب) | traceroute (الف) |
|-------------|-------------|----------|------------------|

۲۱- کدامیک از پروتکل های زیر مدیریت گروه های چند پخش (Multicast) را بر عهده دارد؟

- | | | | |
|--------|---------|----------|------------|
| IP (د) | ARP (ج) | ICMP (ب) | IGMP (الف) |
|--------|---------|----------|------------|

۲۲- آدرس IP 194.19.256.89 متعلق به کدام کلاس آدرسدهن است؟

- | | | | |
|----------------|-------|-------|---------|
| د) نامعتبر (د) | C (ج) | A (ب) | B (الف) |
|----------------|-------|-------|---------|

۲۳- فیلد طول هدر IP TTL در چه کاربردی دارد؟

- | | | | |
|----------------------------|----------------------------------|---------------------------------|------------------------------------|
| ب) طول هدر را مشخص می کند. | الف) شماره تکه ها در یک دیتاگرام | د) طول عمر بسته را مشخص می کند. | ج) برای کنترل خطای استفاده می شود. |
|----------------------------|----------------------------------|---------------------------------|------------------------------------|

۲۴- برای اینکه یک شبکه را به هشت زیر شبکه تقسیم کنیم، چند بیت باید از قسمت شاخص میزبان جدا کنیم؟

- | | | | |
|----------------|--------------|--------------|---------------------------|
| الف) ۳ بیت (د) | ب) ۴ بیت (ج) | ج) ۵ بیت (ب) | د) بستگی به کلاس IP دارد. |
|----------------|--------------|--------------|---------------------------|

۲۵- دریافت کنندگان از آن به منظور معرفی حضور خود در شبکه برای فرستنده ای استفاده می نمایند.

۲۶- کدامیک از محدوده آدرس های زیر برای استفاده بر روی شبکه های خصوصی را زیر نموده اند؟

- | | | | |
|---------------------------------|---------------------------------|-----------------------------------|-----------------|
| 172.16.0.0 - 172.31.255.255 (ب) | 10.0.0.0 - 10.255.255.255 (الف) | 192.168.0.0 - 192.168.255.255 (ج) | تمامی موارد (د) |
|---------------------------------|---------------------------------|-----------------------------------|-----------------|

۲۷- فیلد طول هدر در دیتاگرام IPv4 که اندازه هدر IP را مشخص می نماید، با چه واحدی اندازه گیری می گردد؟

- | | | | |
|-----------|------------|---------------------------|-------------|
| Bytes (ب) | Bits (الف) | longwords (چهار بایت) (ج) | هیچکدام (د) |
|-----------|------------|---------------------------|-------------|

۲۸- فیلد طول دیتاگرام در دیتاگرام IPv4 چه چیزی را در خود ذخیره می نماید؟

- | | | | |
|--|---|--|---|
| الف) مجموع بایت های موجود در دیتاگرام به اضافه هدر | ب) مجموع بایت های موجود در دیتاگرام منهای هدر | ج) مجموع longword موجود در دیتاگرام به اضافه هدر | د) مجموع longword موجود در دیتاگرام منهای هدر |
|--|---|--|---|

۲۹- حداقل اندازه یک دیتاگرام IP (شامل هدر) چه میزان است؟

- | | | |
|---------------|---------------|-----------------|
| ۵۰۹۶ بایت (ج) | ۱۵۰۰ بایت (ب) | ۱۰۲۴ بایت (الف) |
|---------------|---------------|-----------------|

۳۰- پروتکل IGMP چه کاربردی دارد؟

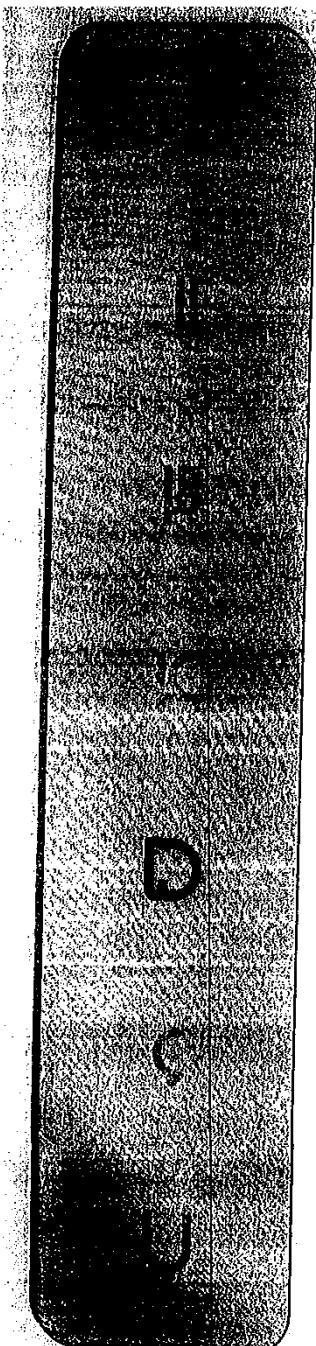
- | | | | |
|----------------------------|----------------|------------|----------------------------|
| ب) مدیریت گروه های چند پخش | الف) گزارش خطا | د) هیچکدام | ج) یک پروتکل مسیر یابی است |
|----------------------------|----------------|------------|----------------------------|

۳۱- کدام جمله در مورد مسیر یابی به روشهای LS و DV صحیح است؟

- | | | | |
|--|--|--|---|
| الف) در مسیر یابی به روش بردار فاصله (DV) هر مسیر یاب نقشه کامل شبکه را می داند. | ب) مشکل شمارش تا بینهایت در الگوریتم های مسیر یابی نوع LS اتفاق می افتد. | ج) در مسیر یابی به روش LS مسیر یابها اطلاعات شان را فقط با همسایه های خود در میان می گذارند. | د) در مسیر یابی به روش DV، اطلاعات در فواصل زمانی منظمی ارسال می گردند. |
|--|--|--|---|

فصل پنجم

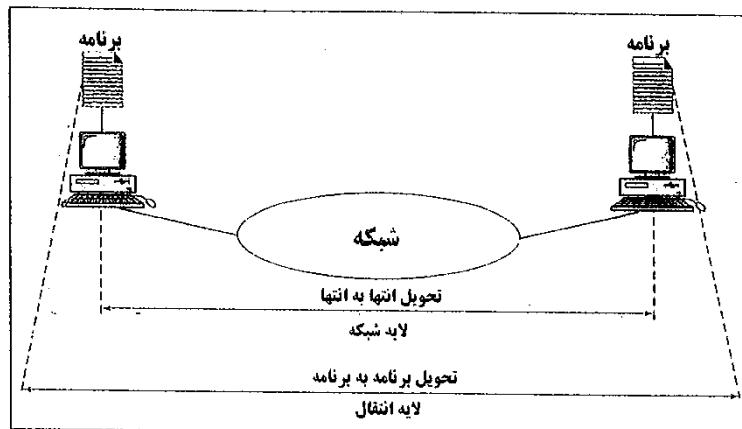
لایه انتقال



۱- مقدمه

لایه انتقال با استفاده از سرویسی که لایه شبکه برایش فراهم می‌کند، می‌تواند یک ارتباط قابل اطمینان بین دو برنامه فراهم نماید. همانطور که در فصل قبل اشاره شد، پروتکلهای لایه شبکه (مثل IP) هیچ تضمینی برای ارسال صحیح اطلاعات ندارند. در لایه شبکه حداکثر تلاش برای رسیدن بسته‌ها می‌شود اما با این وجود، ممکن است بسته‌ای توسط یک مسیریاب دور اندخته شود (به دلیل ازدحام و یا به سر رسیدن طول عمر) و یا اینکه بسته‌ها خارج از ترتیب به کامپیوتر مقصود برند. هدف لایه انتقال برطرف کردن این کاستی‌هاست.

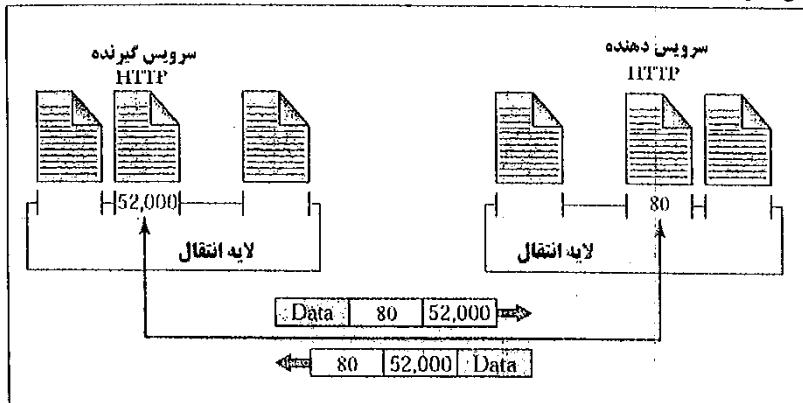
همچنین در لایه انتقال، این برنامه‌ها هستند که با همدیگر ارتباط دارند. به عبارت دیگر در این لایه از سطح بالاتری به ارتباط نگاه می‌شود. شکل (۱-۵) مفهوم تحويل برنامه به برنامه و مقایسه آن با تحويل انتهای به انتهای در لایه شبکه نشان داده شده است.



شکل (۱-۵)- تحويل برنامه به برنامه

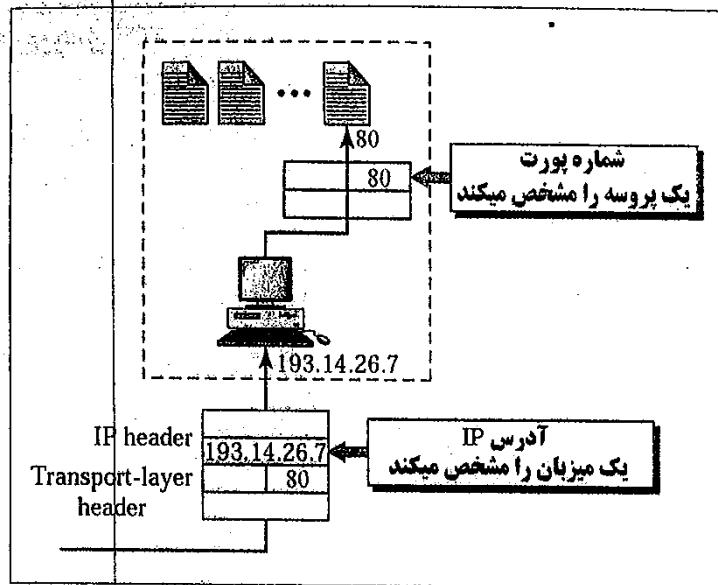
همانطور که در بخش قبل گفته شد، در لایه انتقال، ارتباط بین یک برنامه از کامپیوتر مبدأ و یک برنامه از کامپیوتر مقصد صورت می‌گیرد. از آنجا که ممکن است در آن واحد چندین برنامه روی هر کامپیوتر در حال اجرا باشند، احتیاج داریم که به نحوی بین این برنامه‌ها تمایز قابل شویم. در لایه انتقال از عددی به نام شماره پورت برای این کار استفاده می‌شود. پورت یک عدد ۱۶ بیتی (از صفر تا ۶۵۵۳۵^۶) است که مشخص کننده یک برنامه منحصر به فرد روی کامپیوتر سرویس گیرنده با کامپیوتر سرویس دهنده می‌باشد. همانطور که در لایه شبکه آدرس‌های IP فرستنده و گیرنده به بسته چسبانده می‌شود، در لایه انتقال نیز باید شماره پورت برنامه سرویس گیرنده و شماره پورت برنامه سرویس دهنده به آن چسبانده شود.

شماره پورت برنامه‌های سرویس دهنده مشخص و از پیش تعیین شده است. به عنوان مثال سرویس دهنده Http از طریق پورت شماره ۸۰ به درخواستهای وب پاسخ می‌دهد. این شماره را تمام برنامه‌هایی که درخواست Http داشته باشند می‌دانند. در شکل (۲-۵) ارتباط بین یک برنامه سرویس گیرنده و یک برنامه سرویس دهنده در لایه انتقال نشان داده شده است.



شکل (۲-۵)- ارتباط در لایه انتقال

به طور کلی شماره پورتهای زیر ۲۴، برای برنامه‌های سرویس دهنده مختلف در نظر گرفته شده و به عنوان پورتهای مشهور (well known) شناخته می‌شوند. جدول زیر تعدادی از پورتهای مشهور و برنامه‌های سرویس دهنده معادل آنها را نشان می‌دهد.



شکل (۳-۵)- ارتباط منحصر بفرد از طریق سوکت

توصیف	نام پروتکل	شماره پورت
سرвис تاریخ و زمان	Daytime	۱۳
کانال داده برای پروتکل انتقال فایل	FTP, Data	۲۰
کانال کنترل برای پروتکل انتقال فایل	FTP, Control	۲۱
ورود به یک سیستم از راه دور	TELNET	۲۳
پروتکل انتقال Email	SMTP	۲۵
سرвис نامگذاری دامنه	DNS	۵۳
پروتکل انتقال صفحات وب	HTTP	۸۰
پروتکل دریافت Email	POP3	۱۱۰

دقیقت کنید که برای تحويل برنامه به برنامه احتیاج به دو شناسه داریم؛ آدرس IP و شماره پورت. به عبارت دیگر هم باید بدانیم که با کدام کامپیوتر ارتباط برقرار کنیم و هم اینکه با کدام برنامه از آن کامپیوتر، بنابراین تنها با داشتن آدرس IP یا شماره پورت نمی‌توان ارتباط را برقرار نمود. به ترکیب آدرس IP و شماره پورت که یک ارتباط منحصر به فرد را مشخص می‌نماید، آدرس سوکت گفته می‌شود. برای برقراری ارتباط در لایه انتقال به یک جفت آدرس سوکت احتیاج داریم؛ آدرس سوکت سرویس گیرنده و آدرس سوکت سرویس دهنده. آدرس سوکت را به صورت زیر نشان می‌دهیم:

IP Address : Port Number = Socket Address

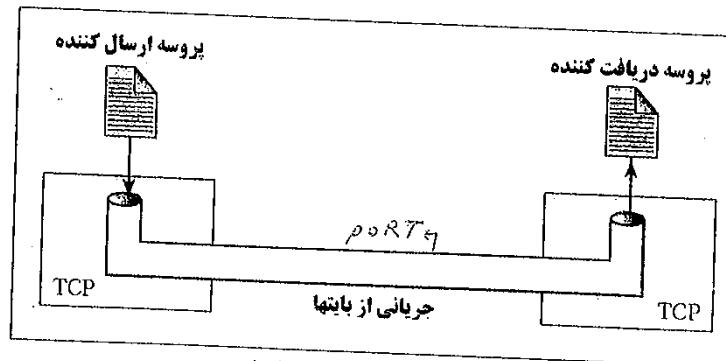
مثال آدرس سوکت 193.14.26.7:80 مشخص کننده سرویس دهنده Http روی کامپیوتری با آدرس 193.14.26.7 می‌باشد. در شکل (۳-۵) نحوه مشخص نمودن یک برنامه منحصر بفرد بر روی یک کامپیوتر با استفاده از آدرس سوکت نشان داده شده است.

۴- پروتکل TCP

در این پروتکل قبل از ارسال داده‌ها، بین فرستنده و گیرنده یک ارتباط مجازی ایجاد می‌گردد. به عبارت دیگر TCP یک پروتکل اتصالگرایست. همچنین در این پروتکل، هر بسته داده دارای یک شماره سریال بوده که از روی آن مقصد از دریافت تمامی بسته‌ها و ترتیب درست آنها اطمینان حاصل می‌کند. مقصد پس از دریافت هر بسته شماره بسته بعدی را به مبدأ اعلام می‌کند. مبدأ در صورتی که پاسخ مناسبی از مقصد در مدت زمان معینی دریافت نکند، بسته قبلی را مجدداً ارسال خواهد کرد. بدین ترتیب بسته‌ها با اطمینان کامل (از دریافت در مقصد) در شبکه منتقل می‌شوند و از این رو این پروتکل را قابل اعتماد می‌گویند.

TCP یک پروتکل جریان‌گراست. بدین معنی که این پروتکل به پروسه ارسال کننده اجازه می‌دهد که داده را به صورت یک جریان از بایتها تحولی دهد. همچنین پروسه دریافت کننده نیز این اطلاعات را به صورت جریانی از بایتها تحولی می‌گیرد. TCP محيطی را فراهم می‌آورد که گویی دو پروسه به وسیله یک لوله فرضی به هم‌دیگر متصل شده‌اند. این لوله، داده را از طریق اینترنت عبور می‌دهد.

در شکل (۴-۵) مفهوم لوله فرضی و ارتباط پروسه‌ها از طریق پروتکل TCP نشان داده شده است.



شکل (۴-۵)- اتصال TCP و لوله فرضی

۲- سرآیند TCP
پروتکل TCP در لایه انتقال سرآیندی به داده می‌چسباند. این سرآیند دارای فیلدۀای برای انجام وظایف ذکر شده می‌باشد. شکل (۴-۵) ساختار سرآیند پروتکل TCP را نشان می‌دهد.

اطلاعات استفاده می‌گردد. مکانیسمی که برای کنترل جریان در این پروتکل انجام می‌شود به صورت "پنجه نفزان با تکرار انتخابی" می‌باشد. این روش در فصل سوم توضیح داده شده است. در پروتکل TCP هر بایت دارای یک شماره می‌باشد. این شماره گذاری برای هر طرف مستقل است. هنگامی که پروتکل TCP بایتهاي از داده را از لایه بالاتر تحويل می‌گيرد، ضمن اينها را در بافر فرستنده ذخیره می‌گند، شماره گذاري نيز می‌نماید. شماره گذاري لزوماً از عدد صفر شروع نمی‌شود بلکه با عددی تصادفی که هنگام برقراری اتصال انتخاب می‌شود، آغاز می‌گردد. به عنوان مثال اگر عدد انتخابی برای شروع شماره گذاري ۰۰۵۷ و تعداد بایتهاي ارسالی ۶۰۰۰ بایت باشد، این بایتها از عدد ۰۰۵۷ تا ۰۵۶ شماره گذاري می‌گردد.

پروتکل TCP مجموعه‌ای از بایتها را در قالب یک قطعه (Segment) ارسال می‌کند. بعد از اینکه بایتها شماره گذاري شدند، TCP برای هر قطعه از اطلاعات که ارسال می‌کند یک شماره ترتیب قرار می‌دهد. شماره ترتیب هر قطعه، شماره اولین بایتی است که جمل می‌گند. مثلاً اگر قطعه‌ای با بایت به شماره ۱۲۵۳ شروع گردد و تعداد بایتهاي داخل این قطعه ۱۰۰۰ بایت باشد، شماره ترتیب این قطعه ۱۲۵۳ و شماره ترتیب قطعه بعدی ۲۲۵۳ خواهد بود.

یک ارتباط TCP به صورت دوطرفه است. هنگامی که ارتباط برقرار شد هر دو طرف می‌توانند داده را ارسال و دریافت نمایند. هر کدام از طرفین صحت دریافت اطلاعات را به دیگری خبر می‌دهند. این کار توسط عددی به نام شماره تصدیق (Acknowledge Number) (Acknowledge Number) انجام می‌گردد. این عدد در واقع شماره بایت بعدی را که انتظار دارد دریافت نماید، مشخص می‌کند.

به دلیل اینکه فرستنده و گیرنده ممکن است داده را با سرعت یکسانی تولید و مصرف نکنند، هر دو طرف دارای بافرهایی برای ذخیره موقعت اطلاعات هستند. از این بافرها برای کنترل جریان

فیلد Acknowledgment Number

این فیلد ۳۲ بیتی نیز شماره ترتیب باشی که منتظر دریافت آن است را تعیین می‌کند. عنوان مثال اگر در این فیلد عدد باینری معادل ۳۴۲۳۱۱ قرار گرفته باشد، بدین معناست که از رشته داده‌ها (که مشخص نیست چند بایت است)، تا شماره ۳۴۲۳۱۰ صحیح و کامل دریافت شده است و منتظر باشتهای از ۳۴۲۳۱۱ به بعد می‌باشد.

فیلد (Header Length) HLEN

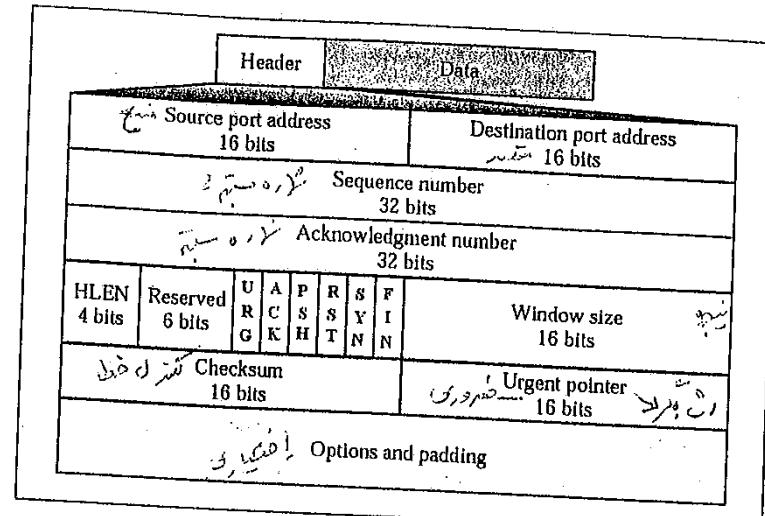
در این فیلد نیز عددی وجود دارد که طول سرآیند را بر مبنای کلمات ۴ باشی تعیین می‌کند و در واقع مرز بین داده‌ها و سرآیند پسته را مشخص می‌نماید. به عنوان مثال اگر در این فیلد عدد ۸ قرار گیرد، طول سرآیند برابر با ۳۲ بایت خواهد بود. وقت کنید که قسمت ثابت سرآیند TCP ۲۰ بایت است ولی به دلیل اینکه در قسمت option می‌توان اطلاعات اضافی نوشت، وجود این فیلد برای تعیین مرز بین داده و سرآیند لازم است.

فیلد Windows size

همانگونه که قبلاً نیز اشاره شد، پروتکل TCP از مکانیزم پنجه لفزان برای کنترل جریان اطلاعات استفاده می‌کند. بنابراین گیرنده، اطلاعات دریافتی را بافر می‌کند تا آنکه ترتیب داده‌های دریافتی صحیح بوده و سپس تحویل برنامه کاربردی خود شود. مقدار قرار گرفته در این فیلد مشخص می‌کند که بافر گیرنده چند بایت دیگر ظرفیت دارد. کاربرد این فیلد به این صورت است که مقداری که در این فیلد قرار دارد (مقدار فضای خالی بافر گیرنده) با مقدار داده‌ای که برای ارسال آمده است مقایسه می‌شود اگر بافر گیرنده فضای کافی داشته باشد، داده‌ها ارسال می‌شوند و در غیر اینصورت منتظر می‌ماند تا بافر گیرنده خالی شود و بعد اقدام به ارسال داده‌ها می‌کند.

فیلد Checksum

این فیلد که فضای ۱۶ بیتی را اشغال می‌کند حاوی کدی برای کنترل و کشف خطاهای احتمالی می‌باشد.



شکل (۵-۵)- سرآیند Header

در ادامه هر کدام از فیلدهای داخل آن را توضیح می‌دهیم:

فیلدهای Source port و Destination port: عنوان آدرس پورت مبدأ که این سگمنت را جهت ارسال تولید کرده و پورت این دو آدرس عنوان آدرس پورت مبدأ که این سگمنت را جهت ارسال تولید کرده و پورت مقصد که آنرا تحویل خواهد گرفت تعیین خواهد شد. در مبحث پورت و سوکت اشاره کردیم که این آدرس مشخص می‌کنند که رشته داده ارسالی از چه برنامه کاربردی در لایه بالاتر گرفته شده و تحویل چه برنامه‌ای باید بشود.

فیلد Sequence number

این فیلد ۳۲ بیتی نشان می‌دهد شماره ترتیب آخرین باشی که در قسمت Data از سگمنت جاری قرار دارد چند است. عنوان مثال اگر در این فیلد عدد باینری معادل ۱۹۳۴۱ قرار گیرد به این معناست که داده‌ها تا بایت ۱۹۳۴۱ درون فیلد داده قرار دارد. وقت کنید که این عدد به معنای آن نیست که ۱۹۳۴۱ بایت درون فیلد Payload قرار دارد بلکه همیشه به شماره ترتیب آخرین بایت داده اشاره می‌کند.

آن به برنامه Telnet سریعاً پاسخ لازم را روی صفحه نمایشش ببیند. ولی نرم افزار TCP معمولاً در هنگام دریافت بسته‌های کوچک، آنها را بافر کرده تا وقتی حجم بافر به اندازه مشخصی پر شد، آنرا یکجا تحویل برنامه کاربردی بدهد. در چنین حالتی فرستنده بسته با ۱ کردن بیت PSH، از گیرنده آن می‌خواهد که آنرا بافر نکند.

بیت RST:

اگر در این بیت مقدار ۱ قرار بگیرد ارتباط کاملاً Reset خواهد شد. بدین معنا که به هر دلیلی (اعم از نقص سخت افزاری یا نرم افزاری) اشکالی بوجود آمده است که یکی از طرفین ارتباط، مجبور به خاتمه ارتباط فعلی و برقراری ارتباط مجدد در صورت امکان می‌باشد. همچنین بیت RST می‌تواند بعنوان علامت عدم پذیرش برقراری ارتباط بکار رود.

بیت SYN:

این بیت یکی از مهمترین قسمتهای بسته TCP می‌باشد؛ زیرا در برقراری ارتباط نقش دارد که در قسمت بعد بدان خواهیم پرداخت.

بیت FIN:

این بیت تقریباً به معنای خداحافظی می‌باشد. اگر یکی از طرفین ارتباط داده دیگری برای ارسال نداشته باشد در آخرین بسته این بیت را ۱ می‌کند و در حقیقت ارسال اطلاعات خودش را یک طرفه قطع می‌کند.

برقراری و قطع ارتباط

برقراری یک ارتباط TCP شامل رویداد کردن سه قطعه توسط طرفین بوده که به "دست دادن سه طرفه" مشهور است. مراحل انجام این کار به شرح زیر است:

- ۱- سرویس گیرنده اولین قطعه را ارسال می‌کند. در این قطعه سرآیند شامل یک شماره ترتیب اولیه تصادفی (مثل ۱۲۰۰) و همچنین شماره پورت مبدأ و مقصد می‌باشد. شماره پورت مقصد در حقیقت سرویس دهندگان را که می‌خواهیم به آن متصل شویم مشخص می‌کند. مثلاً اگر شماره پورت مقصد ۲۳ باشد، منظور این است که برنامه سرویس گیرنده می‌خواهد با سرویس

فیلد Urgent pointer:
در این فیلد یک عدد به عنوان اشاره‌گر قرار می‌گیرد که موقعیت داده‌های اضطراری یا Urgent در این سگمنت معین می‌کند. این داده‌ها زمانی اتفاق می‌افتد و ارسال می‌شوند که عملی شبیه وقوع وقفه‌ها در هنگام اجرای برنامه رخ بدهد. بدون آنکه ارتباط قطع بشود داده‌های لازم در همین سگمنت جاری ارسال خواهد شد.

فیلد Option:
در موقعی که حجم بسته ضربی از چهار نشود، این فیلد با داده‌های بی‌ارزش برو می‌شود به تحویل که طول بسته ضربی از چهار باقی بماند.

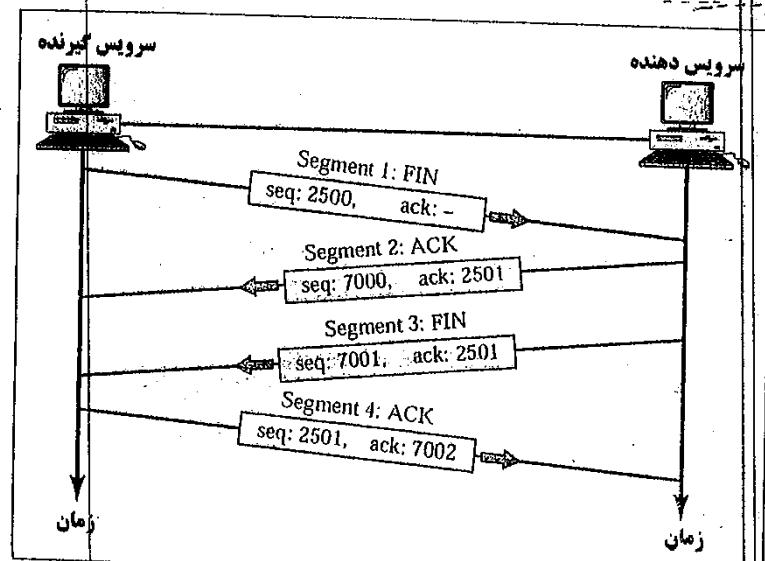
بیت URG:
در صورتی که این بیت مقدار ۱ داشته باشد معین می‌کند که در فیلد Urgent Pointer که قبله آن اشاره شد، مقداری قابل استناد و معتبر قرار دارد و باستی مورد پردازش قرار گیرد.

بیت ACK:
اگر در این بیت مقدار ۱ قرار گرفته باشد، نشان می‌دهد که عددی که در فیلد Acknowledgement Number قرار گرفته است دارای مقدار معتبر و قابل استناد است. بیتهاي SYN دیگری نیز دارند که در ادامه بدان اشاره خواهد شد.

بیت PSH (Push):
اگر در این بیت مقدار یک قرار گرفته باشد فرستنده اطلاعات از گیرنده تقاضا می‌کند که داده‌های موجود در این سگمنت را بافر نکند و در اسرع وقت آنرا جهت پردازش‌های مشابه Telnet ضروری است؛ بعنوان مثال برنامه کاربردی دهد. این عمل گاهی برای برنامه‌هایی مشابه IBM به کامپیوتری در فاصله هزاران فرض کنید یک کاربر با کامپیوتر شخصی خود از نوع سازگار با IBM به کامپیوتری که می‌خواهد ارتباط برقرار کرده و دستورات سیستم عامل UNIX را تمرین نماید. فرض کنید کاربر دستور ls (معادل Dir در DOS) را اجرا می‌کند و بالطبع موقعیت دارد پس از ارسال این دو کاراکتر و تحويل

- ۱- سرویس گیرنده قطعه اول را ارسال می‌نماید که در آن بیت FIN به نشانه درخواست بایان ارتباط یک شده است.
- ۲- سرویس گیرنده قطعه دوم را ارسال می‌کند که در آن بیت ACK به نشانه تصدیق دریافت قطعه اول، برابر با یک است. همچنین شماره ack برابر است با شماره ترتیب قطعه قبل بعلاوه یک.
- ۳- سرویس گیرنده می‌تواند به ارسال اطلاعات ادامه دهد. اما اگر داده دیگری برای ارسال نداشته باشد، یک قطعه که در آن بیت FIN برابر با یک قرار گرفته است را برای طرف مقابل ارسال می‌کند.
- ۴- سرویس گیرنده نیز با ارسال یک قطعه که در آن بیت ACK برابر با یک است، به آن پاسخ می‌دهد.

مراحل خاتمه اتصال TCP در شکل (۷-۵) نشان داده شده است.

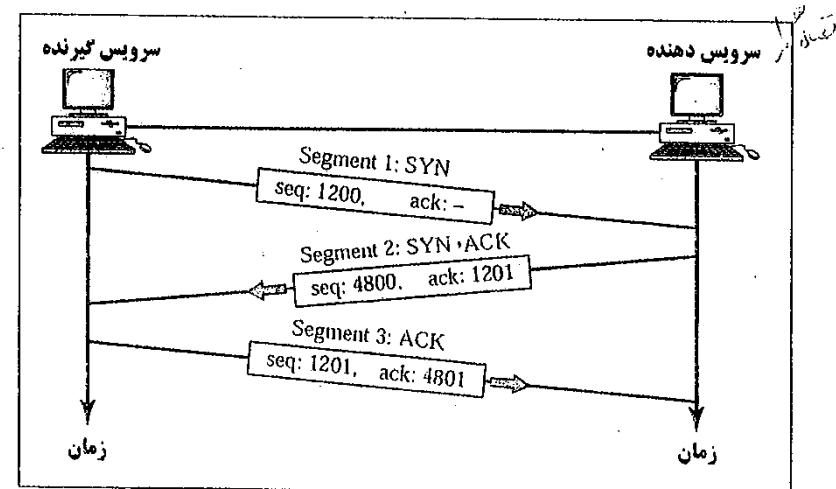


شکل (۷-۵)- نحوه قطع اتصال TCP

۶۱ بیت آن

- ۱- ارتباط برقرار نماید. همچنین در این قطعه بیت SYN به نشانه درخواست برقراری اتصال برابر با یک می‌گردد.
- ۲- سرویس گیرنده قطعه دوم را به نشانه پاسخ ارسال می‌کند. در سرآیند این قطعه بیتهاي SYN و ACK برابر با یک قرار می‌گیرند. در حقیقت این قطعه دومنظوره است یعنی هم صحت دریافت قطعه اول را نشان می‌دهد و هم شماره ترتیب را برای طرف سرویس گیرنده مشخص می‌نماید. دقت کنید که این بار نیز شماره ترتیب یک عدد تصادفی است(مثالاً ۴۸۰۰). شماره ack در این قطعه برابر است با شماره ترتیب قطعه قبل بعلاوه یک، زیرا این قطعه حاوی داده نیست.
- ۳- سرویس گیرنده قطعه سوم را ارسال می‌کند. در این قطعه، بیت ACK به نشانه تصدیق دریافت قطعه دوم، برابر با یک قرار گرفته و در این قطعه نیز شماره ack برابر با شماره ترتیب قطعه قبل بعلاوه یک می‌باشد.

در شکل (۶-۵) روش دست دادن سه طرفه برای برقراری ارتباط نشان داده شده است.



شکل (۶-۵)- روش دست دادن سه طرفه

قطع ارتباط نیز روشنی مشابه برقراری اتصال دارد. هر کدام از طرفین که مایل باشند می‌توانند اقدام به قطع ارتباط نمایند. اگر اتصال در یک جهت قطع گردید، طرف دیگر می‌تواند به ارسال ادامه دهد. اما اگر دو طرف بخواهند به ارتباط خاتمه دهند، چهار قطعه باید به صورت زیر رد و بدل شود:

۴- پروتکل UDP پروتکل درایور میکرتری اچپ

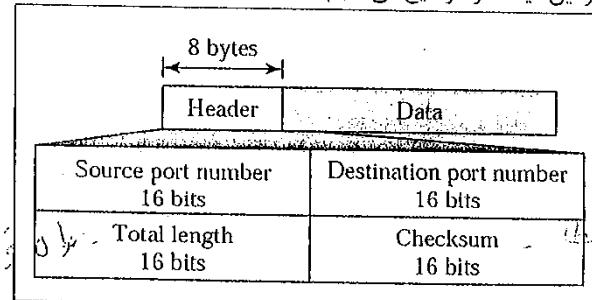
UDP یک پروتکل غیر اتصالگرا و غیر قابل اطمینان است. بدین معنی که قبلاً از ارسال داده نیازی به برقراری ارتباط نیست. همچنین اگرچه این پروتکل حداکثر تلاش خود را خواهد کرد ولی اطمینانی از نظر صحت تحويل بسته‌ها وجود ندارد.

سرآیند UDP ساده و کم حجم بوده و دارای پارامترهایی مانند شماره سریال و یا تایید دریافت بسته نمی‌باشد. در این پروتکل به دلیل اینکه عملیات‌هایی مانند ردیابی توالی شماره بسته‌ها، پیامهای تصدیق و ارسال مجدد بسته‌ها وجود ندارد و همچنین زمانی برای برقراری اتصال صرف نمی‌شود، از پروتکل TCP سریعتر است و بنابراین برای ارسال داده‌های بلاذرنگ (انتقال مکالمه صوتی بلاذرنگ) و یا اختلال‌های عمومی (پیامهای ICMP) کاربرد دارد.

برای اینکه کاربرد این پروتکل را بهتر درک کنید مثالی را مطرح می‌کنیم، فرض کنید بخواهیم یک مکالمه صوتی را به صورت بلاذرنگ از طریق شبکه منتقل کنیم، واضح است که برای این کار سرعت بر دقت ارجحیت دارد. به عبارت دیگر انتظار داریم کلمات سریعاً و بدون تاخیر به طرف مقابله برستند. خرایی مقداری از داده، ممکن است اصلاً برای گوش محسوس نباشد و یا نهایتاً مر کدام از طرفین با گفتن عبارت "متوجه نشدم لطفاً دوباره تکرار کن" می‌توانند آن را تصحیح کنند. ولی اگر پروتکل طوری طراحی شده بود که سعی در صحت ارسال داده‌ها داشت، برای این مورد قابل استفاده نبود.

بنابراین به طور خلاصه هرگاه سرعت اهمیت بیشتری داشته باشد از پروتکل UDP و هرگاه صحت اهمیت بیشتری داشته باشد از پروتکل TCP استفاده می‌کنیم.
مطابق شکل (۸-۵)، سرآیند UDP شامل ۸ بایت بوده که به صورت چهار فیلد دوباره است.

در ادامه هر کدام از این فیلدها را توضیح می‌دهیم.



شکل (۸-۵)- سرآیند UDP

: Source port و Destination port

این دو فیلد بعنوان آدرس پورت مبدأ که این قطعه را جهت ارسال تولید کرده و پورت مقصد که آنرا تحويل خواهد گرفت در نظر گرفته می‌شود. در مبحث پورت و سوکت اشاره کردیم که این دو آدرس مشخص می‌کند که داده ارسالی از چه برنامه کاربردی در لایه بالاتر گرفته شده و تحويل چه برنامه‌ای باید بشود.

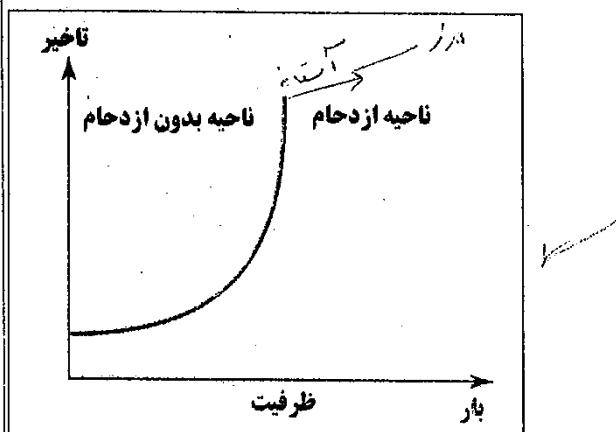
فیلد :Total Length

در این فیلد نیز عددی وجود دارد که طول سرآیند و داده را تعیین می‌کند.

فیلد :Checksum

این فیلد که فضایی ۱۶ بیتی را اشغال می‌کند حاوی کدی برای کنترل و کشف خطاهای احتمالی می‌باشد.

ترکیبی از تاخیر انتشار و تاخیر پردازش است که در این حالت هر دو قابل صرفنظر نگرفتن هستند. هنگامی که بار شبکه به ظرفیت شبکه نزدیک می‌شود، تاخیر به یکباره افزایش می‌یابد؛ زیرا در این حالت زمان انتظار در صفها را نیز باید در نظر بگیریم. هنگامی که بار بیش از ظرفیت می‌گردد، تاخیر به سمت بینهایت می‌رود. در این حالت بسته‌ها به مقصد نمی‌رسند و صفها طولانی و طولانی‌تر خواهند شد. از طرف دیگر، فرستنده بسته‌ها نیز به دلیل اینکه پیام تصدیقی از جانب گیترنده دریافت نمی‌کند، اقدام به ارسال مجدد بسته‌ها نموده و به بدر شدن شرایط کمک می‌نماید.



شکل (۱۰-۵)- ارتباط بین تاخیر بسته‌ها و بارکاری شبکه

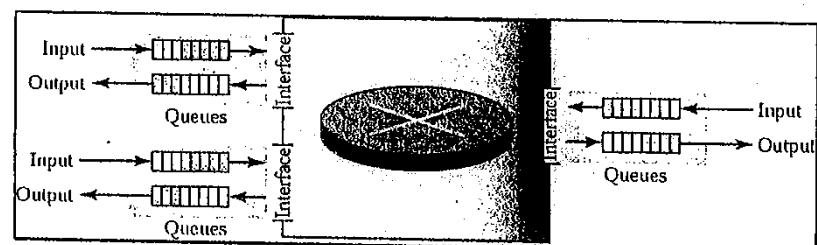
توان عملیاتی را می‌توان به صورت تعداد بسته‌هایی که در واحد زمان از شبکه می‌گذرند، تعریف نمود. رابطه بین توان عملیاتی شبکه و تاخیر در شکل (۱۱-۵) نشان داده شده است. در این شکل هنگامی که بار شبکه کمتر از ظرفیت آن است، توان عملیاتی به صورت متناسب با بار شبکه افزایش می‌یابد. انتظار داریم بعد از اینکه بار کاری به ظرفیت شبکه رسید، توان عملیاتی ثابت بماند اما مشاهده می‌کنید که به شدت کاهش می‌یابد. دلیل آن است که در این حالت صفها پر شده و بسته‌ها توسط مسیریابها دورانداخته می‌شوند. این کار به کاهش تعداد بسته‌ها در شبکه منجر نمی‌شود؛ زیرا فرستنده مجدداً آنها را ارسال می‌نماید.

۵- کنترل ازدحام

یکی از مهمترین مباحث در شبکه‌هایی که بر اساس راه‌گزینی بسته‌ای کار می‌کنند، بحث ازدحام (Congestion) است. مشکل ازدحام هنگامی بوجود می‌آید که تعداد بسته‌هایی که به یک شبکه وارد می‌شود از ظرفیت آن بیشتر باشد.

یک مسیریاب دارای بافرهایی به صورت صف است که بسته‌ها را قبل و بعد از پردازش در داخل خود نگه می‌دارند. هر مسیریاب برای هر کدام از پورتهای خود یک صف ورودی و یک صف خروجی دارد(شکل (۹-۵)). هنگامی که بسته‌ای به یکی از پورتها وارد می‌شود، باید سه مرحله را پشت سر گذارد:

- ۱- بسته در انتهای صف ورودی قرار گرفته و منتظر پردازش می‌ماند.
- ۲- هنگامی که بسته به ابتدای صف رسید، پردازنده مسیریاب، آن را از صف ورودی برداشته و با استفاده از آدرس مقصد آن و جدول مسیریابی، پورت خروجی را پیدا می‌کند.
- ۳- بسته در صف خروجی پورت مذکور قرار گرفته، منتظر خروج از مسیریاب می‌ماند. ما باید از دو حالت اجتناب کنیم. اول هنگامی است که نرخ ورودی بسته‌ها، از سرعت پردازش بسته‌ها در داخل مسیریاب بیشتر باشد؛ که در این حالت صفهای ورودی طولانی خواهند شد. دوم هنگامی است که نرخ حرکت بسته‌ها در صفهای خروجی کمتر از نرخ پردازش آنها باشد؛ که در این وضعیت، صفهای خروجی طولانی خواهند شد.



شکل (۹-۵)- صفحه‌ای ورودی و خروجی در مسیریاب

برای کنترل ازدحام دو فاکتور را که به کارایی شبکه مربوط می‌شوند، باید مد نظر قرار دهیم: تاخیر و توان عملیاتی.

در شکل (۱۰-۵) رابطه بین تاخیر بسته‌ها و بارکاری شبکه نشان داده شده است. دقت کنید هنگامی که بار شبکه بسیار کمتر از ظرفیت آن است، تاخیر حداقل مقدار را دارد. این تاخیر

باشد ممکن است مجبور به دور زیختن آنها گردد که این کار منجر به ارسال مجدد بسته‌ها از طرف فرستنده و بدتر شدن وضعیت ازدحام خواهد شد. پروتکل TCP فرض می‌کند که گم شدن بسته‌ها به دلیل ازدحام صورت می‌گیرد.

گفته‌یم که پروتکل TCP برای کنترل جریان از روش پنجه لزان استفاده می‌کند، گیرنده می‌تواند به فرستنده اطلاع دهد تا اندازه پنجه خویش را افزایش داده و یا کاهش دهد. اما در یک ارتباط تنها فرستنده و گیرنده دخیل نیستند؛ بلکه شبکه ارتباطی نیز نقش اساسی دارد. اگر شبکه نتواند داده را به همان سرعتی که فرستنده آماده می‌کند ارسال نماید، باید سرعت فرستنده پایین آورده شود.

در پروتکل TCP، اندازه پنجه فرستنده هم به وسیله گیرنده و هم توسط ازدحام در شبکه مشخص می‌گردد. فرستنده با استفاده از اندازه پنجه اعلام شده توسط گیرنده و همچنین اندازه پنجه ازدحام، می‌تواند اندازه پنجه خود را تعیین کند که حداقل دو مقدار فوق است:

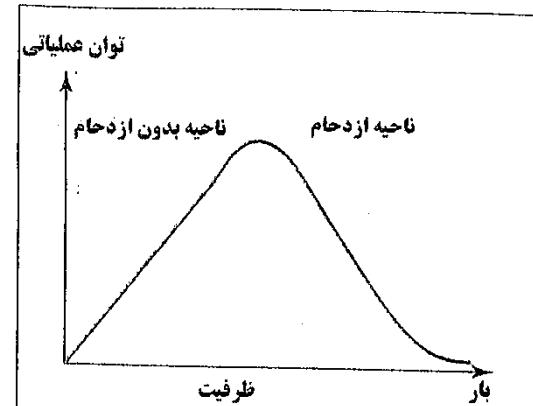
(اندازه پنجه ازدحام ، اندازه اعلام شده از طرف گیرنده) $\text{Min} = \text{اندازه پنجه فرستنده}$

برای اجتناب از ازدحام، پروتکل TCP از دو استراتژی استفاده می‌کند؛ اولی شروع آرام (Slow Start) و افزایش به صورت خطی (Start) و دومی استراتژی کاهش به صورت تصاعدی (Multiplicative Decrease) است.

در ادامه هر کدام از این اصطلاحات را توضیح می‌دهیم:

Slow Start: شروع آرام

در آغاز اتصال، TCP اندازه پنجه ازدحام را برابر با حداقل اندازه یک قطعه قرار می‌دهد. برای هر پیام تصدیق از طرف گیرنده، TCP اندازه پنجه ازدحام را یکی افزایش می‌دهد. این کار تا زمانی ادامه می‌یابد که اندازه پنجه ازدحام به یک سطح آستانه برسد. البته این پروسه برخلاف اسمش، اصلاً شروع آرامی محسوب نمی‌شود؛ چراکه چنانچه در شکل (۱۲-۵) نیز مشاهده می‌کنید، تا قبل از رسیدن به آستانه، افزایش پنجه ازدحام به صورت تصاعدی است. علت این امر این است که وقتی فرستنده یک قطعه را ارسال می‌کند، یک پیام تصدیق نیز دریافت نموده و اندازه پنجه را یک واحد افزایش می‌دهد. سپس دو قطعه را ارسال می‌کند، دو پیام تصدیق نیز دریافت می‌نماید و اندازه پنجه را دو واحد افزایش می‌دهد (یک واحد برای هر پیام تصدیق). سپس چهار قطعه را ارسال می‌نماید و این کار تا رسیدن به سطح آستانه به همین ترتیب ادامه می‌یابد. شکل (۱۲-۵) ایده شروع آرام را شناسان می‌دهد.



شکل (۱۱-۵)- ارتباط بین توان عملیاتی و بارکاری شبکه

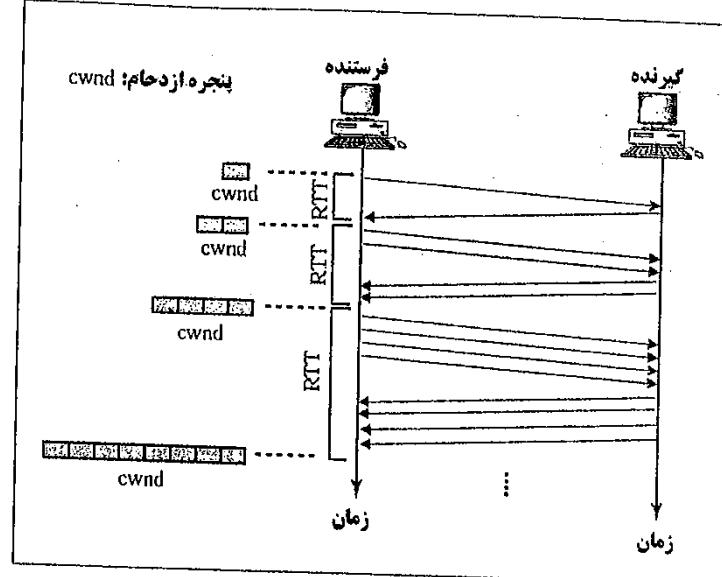
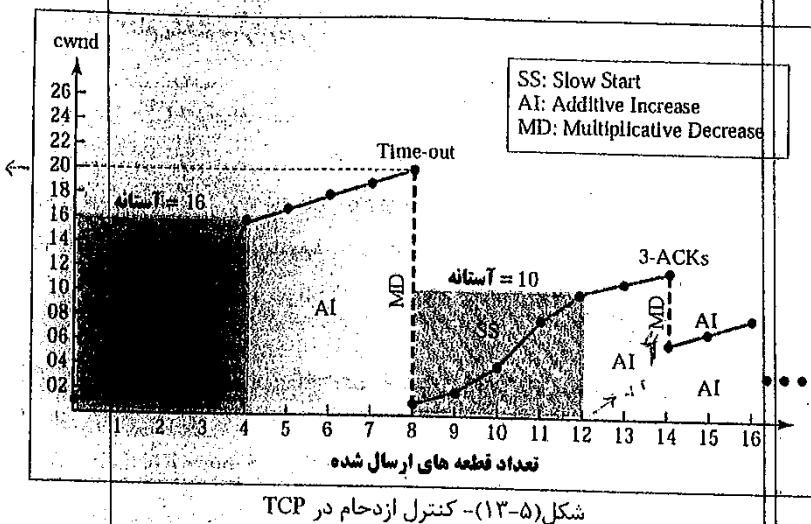
کنترل ازدحام به تکنیک‌هایی گفته می‌شود که یا از وقوع ازدحام جلوگیری می‌کنند (پیشگیری) و یا بعد از وقوع ازدحام، آن را رفع می‌کنند (درمان). به طور کلی روش‌های کنترل ازدحام را می‌توان به دو دسته تقسیم نمود: کنترل ازدحام به صورت حلقه باز و کنترل ازدحام به صورت حلقه پسته.

- کنترل ازدحام به صورت حلقه باز: در این روشها تدبیری اتخاذ می‌شود تا از بروز ازدحام قبل از وقوع جلوگیری شود. در این حالت باید سیاستهای ارسال مجدد، نحوه انتخاب پنجه (تکرار انتخابی یا برگشت ایابی به عقب)، نحوه ارسال پیام تصدیق و همچنین دور انداختن بسته‌ها توسط مسیریاب به طور مناسب انتخاب شود.

- کنترل ازدحام به صورت حلقه پسته: این روشها سعی می‌کنند پس از بروز ازدحام آن را برطرف نمایند. در این حالت روش‌هایی مانند فشار به عقب (یک مسیریاب به مسیریاب قبلی اعلام می‌کند که نرخ بسته‌های خروجی را کاهش دهد) یا سیگنالینگ به عقب یا جلو بکار گرفته می‌شود.

کنترل ازدحام در پروتکل TCP
همانطور که می‌دانیم، یک بسته هنگامی که از طرف فرستنده ارسال می‌شود تا به دست گیرنده برسد، ممکن است از مسیریابهای بسیاری عبور کند. مسیریاب دارای بافرهایی است که بسته‌ها را ذخیره نموده، پردازش کرده و سپس روانه مقصد می‌نماید. اگر نرخ بسته‌های ورودی زیاد

Reno در حالتی که سه ACK تکراری دریافت شود، مرحله شروع آرام تغییر نمی‌شود و افزایش پنجه ازدحام به صورت Additive Increase خواهد بود. (شکل(۱۳-۵))



شکل(۱۲-۵)- مکانیزم Slow start

Additive Increase

برای اجتناب از ازدحام قبل از آنکه انفاق بیفتند، باید این افزایش تصاعدی به نحوی آرام شود. پس از رسیدن پنجه ازدحام به سطح آستانه، افزایش به صورت یک واحدی (خطی) خواهد بود. این کار تا زمانی که صورت گیرد و یا سه ACK تکراری دریافت شود ادامه می‌باید. ACK تکراری به معنای رسیدن یک قطعه به صورت خارج از ترتیب است. (شکل(۱۳-۵))

Multiplicative Decrease

با بروز ازدحام، باید اندازه پنجه ازدحام کاهش یابد. تنها راه برای اینکه فرستنده حدم بزند که ازدحام انفاق افتاده است، از روی گم شدن قطعه‌هاست. برای اینکه در شبکه‌های امروزی احتمال گم شدن یک قطعه بیشتر از خراب شدن آن است، اگر در زمان تعیین شده، هیچ پیام تصدیقی از طرف گیرنده دریافت نشود، فرستنده فرض را بر بروز ازدحام می‌گذارد. در این حالت مقدار آستانه، نصف آخرین اندازه پنجه ازدحام می‌گردد و سپس پنجه ازدحام دوباره با مکانیسم شروع آرام از مقدار یک شروع به افزایش می‌نماید. در نسخه‌های جدیدتر پرونکل TCP مانند

- ۷- گدامپک از عبارت‌های زیر در موردن TCP و UDP صحیح است؟
- الف) TCP یک پروتکل اتصالگرا و غیرقابل اعتماد و UDP یک پروتکل غیراتصالگرا و قابل اعتماد است.
 - ب) TCP یک پروتکل غیر اتصالگرا و قابل اعتماد و UDP یک پروتکل اتصالگرا و غیرقابل اعتماد است.
 - ج) TCP یک پروتکل اتصالگرا و قابل اعتماد و UDP یک پروتکل غیراتصالگرا و قابل اعتماد است.
 - د) TCP یک پروتکل اتصالگرا و قابل اعتماد و UDP یک پروتکل غیراتصالگرا و غیرقابل اعتماد است.

۸- شماره پورت چیست؟

- الف) یک عدد ۱۶ بیتی است که مشخص کننده یک برنامه در حال اجرا بر روی یک کامپیوتر است.
- ب) یک عدد ۳۲ بیتی است که مشخص کننده یک برنامه در حال اجرا بر روی یک کامپیوتر است.
- ج) یک عدد ۱۶ بیتی است که مشخص کننده یک کامپیوتر سرویس دهنده است.
- د) یک عدد ۱۶ بیتی است که مشخص کننده یک برنامه سرویس گیرنده است.

۹- TCP از مکانیزم‌های و برای افزایش اندازه پنجره ازدحام استفاده می‌کند.

- الف) Multiplicative Decrease و Additive Increase
- ب) Multiplicative Increase و Slow start
- ج) Additive Decrease و Slow start
- د) Additive Increase و Slow start

۱۰- چون یک سرآیند UDP چند بایت است؟

- الف) ۱۶ بایت
- ب) ۴ بایت
- ج) ۲۰ بایت
- د) ۸ بایت

- ۱۱- در یک ارتباط TCP، اندازه پنجره فرستنده از روی چه عاملی مشخص می‌شود؟
- الف) گیرنده
 - ب) فرستنده
 - ج) وضعیت ازدحام
 - د) الف و ج

خود آزمایی:

۱- UDP کدام پک از موارد زیر را تضمین می‌کند؟

- الف) کنترل جریان
- ب) به ترتیب رسیدن قطعه‌ها
- ج) ارسال ACK برای فرستنده
- د) هیچکدام

۲- برای بدست آوردن تعداد کل پایتهای موجود در سرآیند TCP عدد موجود در فیلد Header را در چند ضرب می‌کنیم؟

- الف) ۲
- ج) ۴
- ب) ۶
- د) ۸

۳- فیلد برای تشخیص خطأ استفاده می‌شود.

- الف) Checksum
- ب) Urgent Pointer
- ج) Sequence Number
- د) Acknowledge Number

۴- یک میزبان از طریق و یک برنامه در حال اجرا بر روی آن از روی مشخص می‌شود.

- الف) آدرس IP - شماره پورت
- ب) شماره پورت - آدرس IP
- ج) آدرس IP - آدرس MAC
- د) آدرس MAC - آدرس IP

۵- شماره ACK برابر با ۱۰۰ به چه معنایست؟

- الف) ۹۹۹ بایت به طور موقتی آمیز دریافت شده است.
- ب) ۱۰۰ بایت به طور موقتی آمیز دریافت شده است.
- ج) رشته‌ای از بایتها نا شماره ۹۹۹ به طور موقتی آمیز دریافت شده‌اند.
- د) هیچکدام

۶- برای برقراری ارتباط از کدام flag‌ها استفاده می‌کند؟

- الف) فقط SYN
- ب) ACK و SYN
- ج) FIN و SYN
- د) FIN و ACK

فصل ششم

لایه کاربرد

۱- مقدمه

لایه کاربرد مستقیماً با کاربر (برنامه‌ها یا اشخاص) در ارتباط است. این لایه از طریق پروتکلهای مختلفی که در اختیار دارد، خدمات مورد نیاز کاربران را فراهم می‌آورد. هر کدام از پروتکلهای این لایه بسته به نوع و ماهیت آنها از یکی از پروتکلهای TCP یا UDP در لایه پایینتر استفاده می‌کنند. برخی از این پروتکلهای عبارتند از:

FTP: پروتکلی برای انتقال فایل

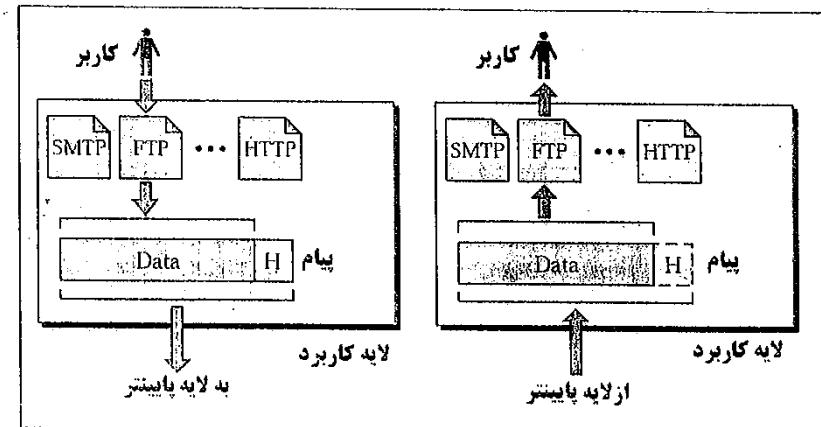
HTTP: پروتکلی برای دسترسی به صفحات وب

DNS: پروتکلی برای ترجمه نامهای نمادین به آدرس‌های IP

Telnet: پروتکلی برای ورود به سیستم از راه دور

E-mail: پروتکلهایی برای ارسال و دریافت POP3 و SMTP

در شکل(۶) نحوه ارتباط لایه کاربرد با کاربر نشان داده شده است.



شکل(۶)- ارتباط لایه کاربرد با کاربر

۴- مدل سرویس گیرنده- سرویس دهنده

قبل از اینکه به توضیح پروتکلهای لایه کاربرد بپردازیم، اجازه بدھید در مورد مفاهیم سرویس دهنده و سرویس گیرنده بیشتر توضیح دهیم. تمام پروتکلهای لایه کاربرد داری دو طرف هستند: سرویس دهنده و سرویس گیرنده.

سرویس گیرنده برنامه‌ایست که در ماشین محلی اجرا شده و درخواست سرویسی را از یک برنامه سرویس دهنده می‌نماید. این برنامه توسط کاربر (یا توسط برنامه دیگری) شروع شده و با دریافت سرویس مورد نظر، خاتمه می‌یابد. طرف سرویس گیرنده با استفاده از آدرس IP یک ماشین راه دور و یک شماره پورت مشهور (کمتر از ۱۰۲۴) مربوط به یک سرویس خاص، کانال ارتباطی را برقرار کرده و ارتباط را آغاز می‌کند. پس از برقراری کانال ارتباطی درخواست خود را مطرح می‌نماید.

برخی از برنامه‌های سرویس گیرنده در داخل نرم‌افزارهای خاصی قرار دارند؛ مثلاً برنامه سرویس گیرنده Http در داخل مرورگر تعییه شده است.

سرویس دهنده عموماً در یک ماشین راه دور اجرا شده و از پورت مربوطه منتظر درخواست‌های برنامه‌های سرویس گیرنده می‌ماند. این برنامه تا زمانی که سرویسی درخواست نشده باشد، خود اقدام به دادن سرویس نمی‌کند.

۳- سیستم نامگذاری حوزه (DNS)

همانطور که می‌دانیم در اینترنت از آدرس IP برای شناسایی یک میزبان استفاده می‌گردد. اما آنچه مسلم است این است که برای کاربران کار با اسمی بسیار آسانتر از کار با اعداد است. به عنوان مثال به خاطر سپاری آدرس به فرم www.google.com بسیار راحت‌تر از به خاطر سپاری همان آدرس به فرم 64.233.169.99 می‌باشد. بنابراین احتیاج به سیستمی داریم که بتواند یک نام را به آدرس IP آن تبدیل نماید.

در اولین سالهای راه اندازی شبکه اینترنت، راه حل بسیار ساده‌ای برای ترجمه نامهای نامادین hosts.txt به آدرس IP وجود داشت و آن تعریف تمام نامها و آدرس‌های IP معادل، در یک فایل بنام hosts.txt بود. این فایل دارای دو ستون بود که در یک طرف آدرس نامادین و در طرف دیگر آدرس IP معادل آن نوشته شده بود. به دلیل اینکه در آن تاریخ تعداد آدرسها زیاد نبود، حجم چنین فایلی چندان بزرگ نمی‌شد و هر ماشین میزبان می‌توانست یک نسخه از این فایل را در اختیار داشته باشد و ساعت ۲۴ هر شب این فایل را از روی فایل مرجع تازه‌سازی و به روز می‌کرد تا هر گونه تغییر احتمالی و تعریف آدرس‌های جدید اعمال شود. بدیهی است که امروزه با حجم میلیونی آدرسها در اینترنت، داشتن یک فایل متاخر و قرار دادن تمام آدرسها و معادل آدرس IP در آن، امکان پذیر نیست.

راه حل این است که آن حجم عظیم اطلاعات را به قطعات کوچکتری تقسیم نموده و هر قسمت را روی یک کامپیوتر ذخیره نمود. در این روش، میزبان برای ترجمه آدرس به نزدیکترین کامپیوترا که اطلاعات مربوطه را در اختیار دارد مراجعه می‌کند. این روش، سیستم نامگذاری حوزه یا DNS نام دارد. DNS یک روش سلسه مراتبی است که بانک اطلاعاتی مربوط به نامهای نامادین و معادل IP آنها را روی کل شبکه اینترنت توزیع کرده است.

همانطور که آدرس‌های IP منحصر به فرد هستند، نامهای نامادین نیز باید منحصر به فرد باشند تا یک رابطه یک به یک بین آنها برقرار باشد. همه ماشینهای میزبان، حداقل باید آدرس IP یک سرویس دهنده DNS را در اختیار داشته باشند. این سرویس دهنده را که کامپیوترا میزبان با آن مستقیماً در ارتباط است، "سرویس دهنده محلی" می‌نامند.

بارها و بارها با آدرس‌های نامادین به فرم زیر روبرو شده‌اید:

www.uok.ac.ir
www.yale.edu
www.yahoo.com

بدیهی است که این نامها بگونه مسمی نیستند و بدلیل انتخاب نامی شوند، بلکه حاوی اطلاعاتی هستند که از روی آن جستجو در بانک اطلاعاتی آسانتر می‌گردد. همانطور که مشاهده می‌کنید یک آدرس نامادین (نام حوزه) از چند بخش مجزا که با علامت ". " از هم تفکیک شده‌اند، تشکیل می‌شود. هر کدام از این بخشها که "سطح" نام دارد به یک قسمت از بانک اطلاعاتی توزیع شده این‌روه می‌نماید که به محدودتر شدن فضای جستجو کمک می‌کند.

برای تحلیل یک نام حوزه، سطوح از سمت راست به چه تفکیک می‌شوند و در یک روند سلسه مراتبی، سرویس دهنده متناظر با آن سطح پیدا می‌شود. فعل از بالاترین سطح که در سمت راست نام حوزه قرار می‌گیرد (مثل .com، .ir ...) شروع می‌کنیم.

نامهای حوزه به هفت منطقه عمومی و حدود صد و چند منطقه کشوری تقسیم‌نشده‌اند. منظور از حوزه این است که شما با یک نگاه ساده به انتهای آدرس نامادین، می‌توانید ماهیت آن نام و سرویس دهنده متناظر با آن را حدس بزنید یعنی اگر انتهای نامهای حوزه متفاوت باشد منطقه جستجو برای یافتن آدرس IP معادل نیز متفاوت خواهد بود. هفت حوزه عمومی وجود دارند که عبارتند از:

حوزه com (commercial): برای موسسات اقتصادی و تجاری. مانند: www.sony.com

حوزه edu (educational): برای موسسات علمی یا دانشگاهی. مانند: www.yale.edu

حوزه gov (government): برای آژانس‌های دولتی آمریکا مانند: www.whitehouse.gov

حوزه int (international): برای سازمانهای بین‌المللی (مثل یونسکو، یونیسف، فانو ...). مانند:

www.unicef.int

حوزه mil (military): برای سازمانهای نظامی دنیا. مانند: www.usarmy.mil

حوزه net (Network Service Provider): برای ارائه‌دهندگان خدمات شبکه. مانند:

www.pegah.net

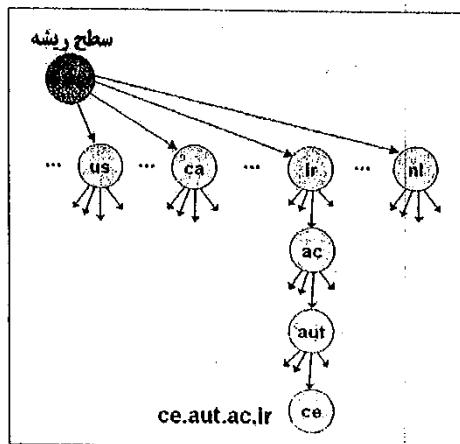
حوزه org (organization): برای سازمانهای عام‌المنفعه و غیرانتفاعی. مانند: www.ieee.org

احتمالاً تاکنون به آدرس‌های زیادی در اینترنت برخورد کرده‌اید که هیچ کدام از حوزه‌های هفتگانه فوق را در انتهای آنها نمی‌بینید. معمولاً در انتهای این آدرسها یک رشته دو حرفی مثل ir یا .in قرار گرفته است. این رشته مخفف نام کشوری است که آن آدرس و ماشین صاحب آن نام،

در آن کشور واقع است.

مثل ir برای ایران یا jp برای ژاپن.

در شکل (۴-۶) چگونگی شکسته شدن یک آدرس به زیرحوزه‌های کوچکتر نشان داده شده است. با این ساختار برای ترجمه یک نام حوزه مثل `ce.aut.ac.ir`, عملیات از سطح ریشه شروع می‌شود. سپس آدرس سرویس دهنده حوزه `ir` بدست می‌آید. با مراجعه به این سرویس دهنده، آدرس ماسنی که سرویس دهنده `ac.ir` در آنجا قرار دارد به دست می‌آید؛ این روند تا رسیدن به آدرس IP معادل ادامه می‌یابد. این عملیات در چند مرحله تکرار می‌شود و با توجه به آنکه از پروتکل UDP استفاده می‌شود، تأخیر زیادی نخواهد داشت.

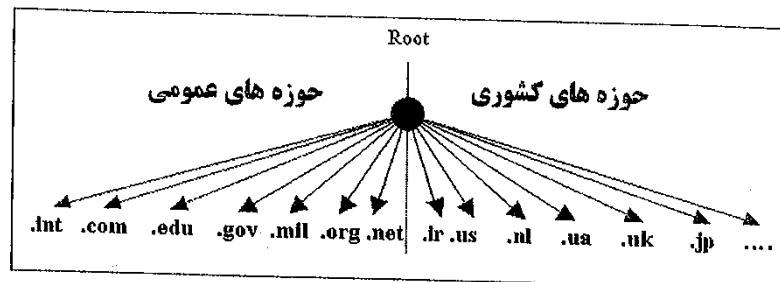


شکل (۴-۶)- زیرحوزه‌ها

دقت کنید شما نمی‌توانید هر نام دلخواه را برای شرکت یا سازمان خود انتخاب نمایید بلکه برای اینکار باید نام مورد نظر را ثبت نمایید؛ در غیر این صورت چنین آدرسی در اینترنت هویت خواهد داشت. برای ثبت آدرس باید به سایتهای ثبت کننده نام حوزه مراجعه کرده و تقاضای ثبت آدرس نمایید. سایتهای ثبت نام، حوزه، متعددند ولی مشهورترین آنها `www.internic.net` می‌باشد که هزینه‌ای را نیز بابت این کار دریافت می‌کند.

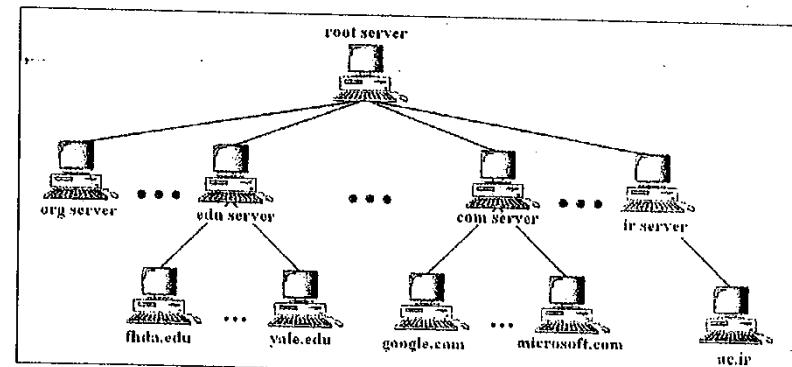
همانطور که قبل ذیقتیم، آدرس IP معادل اسمی نمادین در شبکه اینترنت، در یک فایل مستمر کز ذخیره نمی‌شوند بلکه روی کل شبکه توزیع شده‌اند؛ به همین دلیل برای ترجمه یک نام به آدرس IP ممکن است چندین مرحله "پرس و جو" صورت بگیرد. طبیعی است که یک پرس و جو شود یا حتی ممکن است یک آدرس نمادین اشتباہ باشد و هیچ معادل IP نداشته باشد.

هر حوزه می‌تواند به زیرحوزه‌های کوچکتری تقسیم شود. بنویس مثال نامهای مربوط دو حوزه کوچکتر مربوط به حوزه ایران با مخفف `ir` را در نظر بگیرید: `.co.ir` و `.ac.ir`، که اولی یک موسسه علمی و دانشگاهی و دوضی یک موسسه بازرگانی با تجاری را در ایران تعیین می‌نماید. در شکل (۲-۶) حوزه‌های عمومی و حوزه‌های کشورها نشان داده شده است.



شکل (۲-۶)- حوزه‌های عمومی و کشوری

هر کدام از حوزه‌های فوق دارای سرویس دهنده مخصوص به خود می‌باشد. سرویس دهنده‌های دیگری به نام سرویس دهنده ریشه (Root Server) وجود دارند که آدرس بقیه سرویس دهنده‌های حوزه را می‌دانند. تعداد ۱۳ سرویس دهنده ریشه در اینترنت وجود دارد. در شکل (۳-۶) موقعیت یک سرویس دهنده ریشه و سرویس دهنده‌های حوزه نشان داده شده است.



شکل (۳-۶)- سرویس دهنده ریشه و سرویس دهنده‌های حوزه

- سه روش برای پرس و جوی نام در سرویس دهنده‌های نام وجود دارد:
- روش پرس و جوی تکراری (Iterative Query)
- روش پرس و جوی بازگشتی (Recursive Query)
- روش پرس و جوی معکوس (Reverse Query)

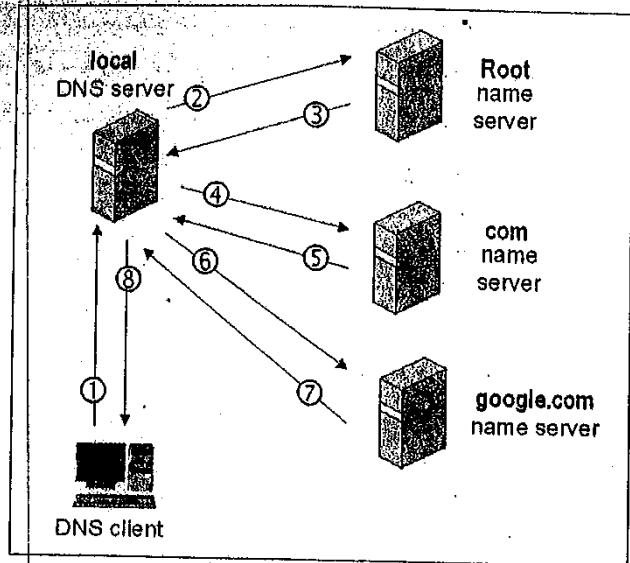
اکنون به بررسی این سه روش می‌پردازیم:

روش پرس و جوی تکراری

گفتیم که یک سرویس گیرنده DNS باید حداقل آدرس IP یک سرویس دهنده DNS که مستقیماً با آن در ارتباط است را در اختیار داشته باشد. این سرویس دهنده را سرویس دهنده محلی می‌نامند.

هنگامی که درخواستی برای ترجمه نام از طرف یک برنامه (مثلًا مرورگر وب) داده می‌شود، سرویس گیرنده DNS یک ارتباط UDP با سرویس دهنده DNS محلی (پورت ۵۳) برقرار می‌نماید.

در پرس و جوهای تکراری، قسمت اعظم تلاش برای تبدیل یک نام بر عهده سرویس دهنده محلی است. این DNS حداقل به آدرس ماشین Root، به عنوان نقطه شروع نیاز دارد. وقتی یک تقاضای ترجمه آدرس به سرویس دهنده محلی ارسال می‌شود، در صورتی که قادر به ترجمه باشد، معادل آدرس IP نام مورد نظر را به تقاضاً کننده برمی‌گرداند؛ این حالت وقتی است که سرویس دهنده محلی قبل از نام را ترجمه و در یک فایل ذخیره کرده باشد. در غیر این صورت سرویس دهنده محلی خودش یک تقاضاً برای DNS سطح بالا (سرویس دهنده ریشه) ارسال می‌کند. این سرویس دهنده، آدرس ماشینی را که می‌تواند برای ترجمه نام مورد نظر مفید باشد، به سرویس دهنده محلی معرفی می‌کند. سرویس دهنده محلی مجدداً یک تقاضاً به ماشین معرفی شده در مرحله قبل ارسال می‌کند. در این حالت هم سرویس دهنده نام می‌تواند در صورت یافتن آدرس IP معادل با آن نام حوزه، آنرا ترجمه کند و یا آنکه آدرس سرویس دهنده سطح پایینتری را به او برگرداند. این روند ادامه می‌یابد تا DNS نهایی نام مورد نظر را به آدرس IP ترجمه نماید. دقت کنید که در این روش بار کاری بر دوش DNS محلی است و این سرویس دهنده مسئولیت نهایی پیدا کردن آدرس IP و تحويل آن به سرویس گیرنده را بر عهده دارد. برای درک بهتر از روند کار، به شکل (۶-۵) دقت کنید.



شکل (۶-۵)- پرس و جوی تکراری

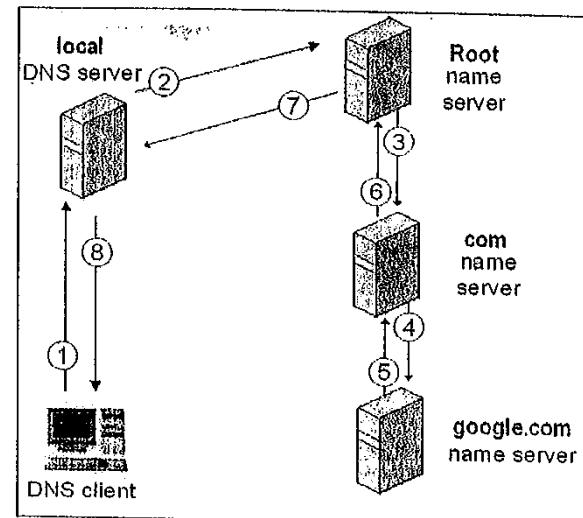
در این مثال فرض شده است که یک برنامه سرویس گیرنده DNS، از سرویس دهنده محلی تقاضای ترجمه نام www.google.com را نموده است.

روش پرس و جوی بازگشتی

در این روش نیز سرویس گیرنده برای دریافت آدرس مورد نیاز، ابتدا به سرویس دهنده محلی مراجعه می‌نماید. بعد از این کار اگر در بانک اطلاعاتی مربوط به سرویس دهنده محلی، آدرس معادل با آن نام از قبیل وجود داشته باشد، به سرعت مقدار معادل IP آن برمی‌گردد و تحويل سرویس گیرنده می‌شود. اما اگر در بانک اطلاعاتی سرویس دهنده محلی، معادل IP آن نام وجود نداشته باشد، سرویس دهنده محلی موظف است بدون آنکه به تقاضاً دهنده خبر بدده، خودش راساً به سرویس دهنده سطح بالاتر تقاضای ترجمه آدرس بدهد. در این حالت هم DNS سطح بالاتر بهمین نحو ترجمه آدرس را پیگیری می‌کند؛ یعنی اگر معادل IP آن نام را داشته باشد آنرا برمی‌گردد و در غیر اینصورت خودش از سرویس دهنده سطح پایینتر تقاضای ترجمه آن نام را این مراحل تکرار می‌شود. در روش پرس و جوی بازگشتی ماشین سرویس دهنده محلی می‌نماید و این مراحل تکرار می‌شود. در روش پرس و جوی بازگشتی ماشین سرویس دهنده محلی این مراحل متوالی را نمی‌بیند و هیچ کاری جز ارسال تقاضای ترجمه یک آدرس بر عهده ندارد و پس از ارسال تقاضاً برای سرویس دهنده سطح بالا منتظر خواهد ماند. در این حالت برخلاف حالت

بعنوان مثال آدرس 138.14.7.13 را در نظر بگیرید. آدرس کلاس B و مشخصه آن 138.14.0.0 است. زمانیکه موسسه‌ای یک کلاس IP ثبت می‌کند یک سرویس‌دهنده DNS، متناظر با شبکه خود ایجاد کرده و آنرا نیز معرفی می‌کند. سرویس‌دهنده محلی باقیتی آدرس DNS متناظر با شبکه 138.14.0.0 را پیدا کرده و سپس برای آن یک تقاضا ارسال کند. DNS مربوط به این شبکه براساس زیرشیوه‌هایی که دارد این سؤال را از طریق سرویس‌دهنده‌های متناظر با هر زیرشبکه پیگیری می‌کند. چون هر زیرشبکه یک سرویس‌دهنده DNS مخصوص به خود دارد، نهایتاً یک نام نمادین حوزه معادل با آن آدرس IP برخواهد گشت.

قبل همه مسئولیت بر دوش سرویس‌دهنده محلی نیست و هر سرویس‌دهنده آدرس را از سرویس‌دهنده دیگری به صورت بازگشته تقاضا می‌کند. شکل (۶-۴) روش پرس و جوی بازگشته را نشان می‌دهد.



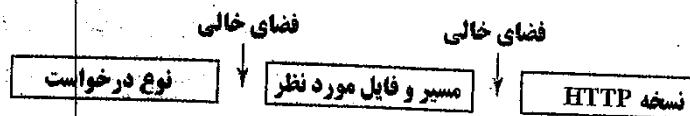
شکل (۶-۴)- پرس و جوی بازگشته

پرس و جوهای محکوس

فرض کنید حالتی بوجود بیاید که یک سرویس‌دهنده DNS، آدرس IP یک ماشین را بداند ولی نام نمادین معادل با آن را نداند. بعنوان مثال DNS مایل است بداند که چه نامی در شبکه اینترنت معادل با 195.13.42.7 می‌باشد در چنین حالتی مسئله کمی حادتر به نظر می‌رسد؛ چرا که برای ترجمه نامهای نمادین، چون این نامها دارای حوزه و زیرحوزه هستند، تحلیل آدرسها ساده است ولی ترجمه آدرس [P] به معادل نام حوزه، از چنین روابطی تبعیت نمی‌کند. به عبارت بهتر هیچ ارتباط مستقیم و متناظری بین آدرس‌های IP و اسمی انتخاب شده در اینترنت وجود ندارد. برای یافتن نامهای متناظر با یک آدرس IP باید یک جستجوی کامل و در عین حال وقتی‌گیر انجام شود.

روش کاربردین صورت است که سرویس‌دهنده محلی یک تقاضا برای DNS متناظر با شبکه‌ای که مشخصه آن در آدرس IP، مشخص شده (یعنی فیلد NetID در آدرس IP)، ارسال می‌کند.

مهمترین فیلد در پیغام درخواست همان خط درخواست است که یک سطر به فرمی زیر می باشد:



نوع درخواست یا متد، مشخص کننده سرویسی است که این پیغام درخواست می کند. ذیلا برخی از سرویسهای پرکاربردتر را توضیح می دهیم:
GET: این درخواست هنگامی استفاده می شود که سرویس گیرنده بخواهد یک صفحه وب را از سرویس دهنده دریافت نماید. آدرس صفحه مورد نظر بر روی این سرویس دهنده در فیلد بعدی داده می شود. GET متداولترین درخواست است. سرویس دهنده با قرار دادن محتویات صفحه مورد نظر در فیلد بدن پیغام پاسخ به آن جواب می دهد.

HEAD: این درخواست برای دریافت سرآیند یک صفحه وب است نه خود آن صفحه. مشابه درخواست GET است با این تفاوت که در اینجا پاسخ حاوی فیلد بدن نمی باشد.

PUT: از طرف سرویس گیرنده و برای ذخیره نمودن یک صفحه وب بر روی سرویس دهنده استفاده می شود. محتویات صفحه مورد نظر در بدن پیغام درخواست نوشته می شود. COPY: این درخواست برای کپی کردن فایلی در محل دیگری استفاده می شود. محل فایل مبدأ در فیلد دوم خط درخواست و آدرس فایل مقصد در فیلد سرآیند پیغام درخواست مشخص می گردد.

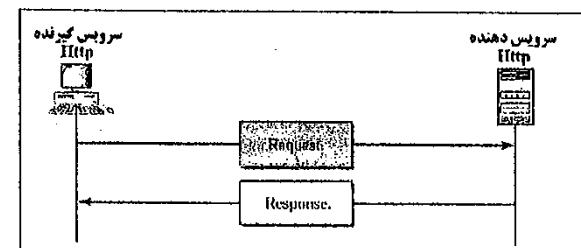
DELETE: این درخواست برای حذف یک صفحه وب بر روی سرویس دهنده بکار می رود. با این درخواست سرویس گیرنده از سرویس دهنده تقاضا می کند که داده هایی را به یک منبع موجود (مثل یک صفحه وب یا یک فایل) اضافه نماید.

به عنوان مثال خط "GET /Help/Doc.htm Http/1.1" در پیغام درخواست، اولاً مشخص می کند که نوع درخواست GET بوده و ثانیاً اطلاعات درخواستی، محتویات فایل Doc.htm در Help می باشد. ثالثاً نسخه Http که این سرویس گیرنده پشتیبانی می کند، ۱.۱ است.

شاید Help می باشد. لذا نسخه 1.0 پروتکل Http یک اتصال غیرماندگار بین سرویس گیرنده و سرویس دهنده برقرار می نماید. به عبارت دیگر اگر یک صفحه وب مثلًا شامل N تصویر باشد، اتصال بین سرویس دهنده و سرویس گیرنده باید N بار برقرار گردد و قطع شود. اما نسخه 1.1

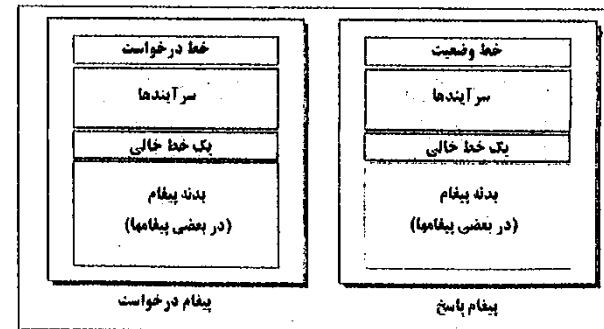
HTTP -۴

این پروتکل را می توان پرکاربردترین پروتکل لایه کاربرد به شمار آورد. با استفاده از این پروتکل می توان داده را به صورتهای مختلف ابرمن، صدا، تصویر، ویدئو وغیره منتقل نمود. این پروتکل از ارتباط TCP و پورت ۸۰ استفاده می کند. همانند سایر پروتکلهای لایه کاربرد، این پروتکل نیز دارای یک طرف سرویس گیرنده و یک طرف سرویس دهنده می باشد. سرویس گیرنده پس از برقراری اتصال، تقاضای خود را به صورت یک پیغام درخواست (Request) مطرح می کند. پس از بررسی تقاضا، سرویس دهنده جواب را به صورت یک پیغام پاسخ (Response) برمی گرداند (شکل ۶-۷). در مورد ساختار پیامهای درخواست و پاسخ در ادامه صحبت می کنیم.



شکل (۶-۷)- پیامهای درخواست و پاسخ HTTP

قالب پیامهای درخواست و پاسخ در شکل (۶-۸) نشان داده شده است. همانطور که ملاحظه می کنید تقریباً دارای ساختار مشابهی هستند.



شکل (۶-۸)- ساختار پیامهای درخواست و پاسخ

در این مثال در پیغام درخواست، سرویس گیرنده از متدها GET برای دریافت یک فایل تصویری استفاده کرده است. برآیندهای Accept، مشخص کننده نوع فرمت قابل قبول می‌باشند. همانطور که مشخص است در پیغام درخواست، فیلد بدن وجود ندارد.

در پیغام پاسخ، ابتدا خط وضعیت را مشاهده می‌کنید که نسخه HTTP و همچنین موقیت آمیز بودن درخواست را کد ۲۰۰ و عبارت OK نشان داده است. سپس خطوط سرآیند را مشاهده می‌کنید که دارای اطلاعاتی در مورد تاریخ و زمان و همچنین نوع سرویس دهنده می‌باشند. در ادامه یک خط خالی و سپس محتويات فایل درخواست شده به فرمت مشخصی آورده شده است. در پایان برای درک بهتر مطلب مراحل بارشدن یک صفحه وب را در قالب یک مثال توضیح می‌دهیم:

فرض کنید کاربر، آدرس زیر را در مرورگر خود وارد می‌کند:
<http://www.w3.org/hyper/www/project.html>

مرورگر با تحلیل آدرس استوجه می‌شود که باید تقاضای فایلی را طبق پروتکل HTTP به سمت

سرویس دهنده بفرستد. مراحلی که اتفاق می‌افتد به شرح زیر خواهد بود:

(۱) مرورگر آدرس را تحلیل کرده و قسمتهای پروتکل، آدرس نام حوزه، شاخه و نام فایل را از آن استخراج می‌کند.

(۲) مرورگر یک اتصال UDP با پورت ۵۳ سرویس دهنده DNS برقرار نموده و تقاضای ترجمه آدرس نام حوزه را به آن ارسال می‌نماید تا آدرس IP ماشین سرویس دهنده بدست آید. در این مثال

مرورگر تقاضای ترجمه نام www.w3.org DNS را به آدرس IP ارسال می‌کند.

(۳) در پاسخ، آدرس IP معادل با نام حوزه را برمی‌گرداند. فرض کنید در این مثال DNS IP را ۱۲۸.۳۰.۵۲.۳۱ برگردانده است.

(۴) مرورگر یک ارتباط TCP با آدرس ۱۲۸.۳۰.۵۲.۳۱ و پورت ۸۰ برقرار می‌کند.

(۵) پس از برقراری ارتباط، یک پیغام درخواست به صورت زیر به سمت سرویس دهنده ارسال می‌شود:

“GET /hyper/www/project.html http/1.1”

(۶) سرویس دهنده این رشتہ را دریافت و پس از پردازش آن، فایل project.html را از شاخه

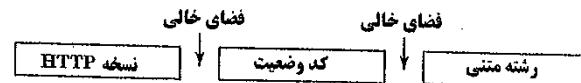
/hyper/www/ استخراج کرده و برای مرورگر ارسال می‌نماید.

(۷) مرورگر فایل را دریافت کرده و پس از خاتمه دریافت ارتباط TCP را قطع می‌کند.

(۸) مرورگر فایل ابرمتنی را تفسیر کرده و آنرا روی خروجی نمایش می‌دهد.

پروتکل Http یک اتصال ماندگار برقرار می‌سازد به طوری که در مثال قبل پس از برقراری اتصال هر N تصویر می‌توانند از همان اتصال منتقل شوند و نیازی به اتصال مجدد نیست و در نتیجه این نسخه سریعتر است.

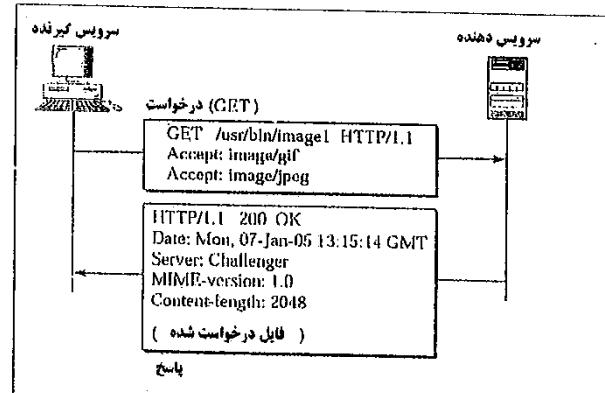
فیلد سرآیند در پیغامهای درخواست و پاسخ، برای مبالغه اطلاعات اضافی بین سرویس گیرنده و سرویس دهنده بکار می‌رود. این اطلاعات می‌تواند شامل اطلاعات عمومی در مورد پیام، اطلاعاتی در مورد نوع فرمت داده‌های قابل قبول توسط سرویس گیرنده و یا وضعیت سرویس دهنده و یا اطلاعاتی در مورد بدن پیغام باشد. این فیلد می‌تواند شامل یک یا چند سطر باشد. فیلد خط وضعیت در پیغام پاسخ شامل نسخه HTTP، کد وضعیت و یک رشته متنی می‌باشد:



کد وضعیت یک عدد سه رقمی بوده که مشخص کننده وضعیت فرمان ارسالی است. مثلاً عدد ۲۰۰ در این فیلد به معنای موقیت آمیز بودن درخواست یا عدد ۴۰۰ به معنای وجود اشتباه در پیغام درخواست است.

فیلد رشته متنی در انتهای خط وضعیت، متن کوتاهی است که وضعیت اجرای فرمان را توصیف می‌کند.

در شکل (۹-۶) یک پیغام درخواست که از طرف سرویس گیرنده ارسال شده است و پیغام پاسخ آن از طرف سرویس دهنده را مشاهده می‌کنید.



شکل (۹-۶)- مثالی از درخواست و پاسخ Http

(۹) اگر فایل ابرمتنی در جایی دارای صدا یا تصویر باشد به ازای تک تک آنها مراحل ۱ تا ۸ را تکرار نموده و آنها را بترتیب دریافت می‌کند.
دقیق کنید که درون فایلهای ابرمتنی، داده‌های مربوط به فایلهای صدا یا تصویر وجود ندارد بلکه فقط نام و محل قرار گرفتن فایل تصویر یا صدا درون آن درج شده است.

۵- پروتکل Telnet

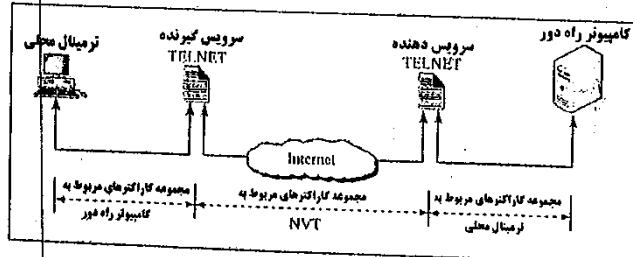
این پروتکل کاربر را قادر می‌سازد که با استفاده از یک ترمینال، از هر مکانی و با استفاده از یک خط ارتباطی همانند خط تلفن با یک سیستم راه دور ارتباط برقرار کرده و وارد سیستم شده، از آن سرویس پنگیرد. با این قابلیت، تفاوتی بین یک کاربر که در کنار کامپیوتر مرکزی نشسته و یک کاربر راه دور وجود نخواهد داشت.

به عنوان مثال فرض کنید که شما یک کامپیوتر شخصی پنتیوم با سیستم عامل Windows در اختیار دارید ولی دانشگاه شما دارای یک سیستم مینی کامپیوتر SUN با سیستم عامل یونیکس است؛ شما برنامه‌های کاربردی خود را در محیط یونیکس نوشته‌اید و همانجا ذخیره کرده‌اید. حال به فرض اگر خواستید در منزل خود همانند کسی که در مرکز کامپیوتر نشسته است به محیط یونیکس وارد شده و برنامه‌های خود را ویرایش یا اجرا نمایید، نیازمند یک ترمینال سازگار با یونیکس هستید. ولی تنها چیزی که در اختیار شماست یک کامپیوتر شخصی است. در اینجا برایم Telnet راه‌گشایست.

برنامه Telnet یک ترمینال مجازی و سازگار با ترمینالهای حقیقی از سیستم سرویس دهنده، بر روی کامپیوتر شما شبیه‌سازی می‌کند و اجازه می‌دهد به سیستم یونیکس وارد شده و با آن محاوره نمایید.

برنامه Telnet فرامینی را که صادر می‌کنید به نحو مناسبی به سمت کامپیوتر راه دور هدایت می‌کند و پس از تفسیر و اجرای فرمان صادره بر روی آن کامپیوتر، نتیجه به برنامه Telnet بر روی کامپیوتر شما باز خواهد گشت.

بنابراین در یک تعریف ساده، برنامه Telnet موظف است برروی ماشین کاربر، مشخصه‌های ترمینال حقیقی سرویس دهنده را شبیه سازی نماید. این ترمینال شبیه‌سازی شده را NVT می‌نامید. (شکل (۱۰-۶))



شکل (۱۰-۶)- پروتکل Telnet

۶- پروتکلهای POP3 و SMTP

یکی از پرطرفدارترین سرویسهای موجود در اینترنت، سرویس پست الکترونیکی یا همان E-Mail می‌باشد. از این سرویس می‌توان برای ارسال پیامهایی که حاوی متن، صوت، تصویر و یا هر چیز دیگر به فرم الصاق شده باشند، استفاده نمود. مشابه سرویس پست سنتی که هر سرویس گیرنده دارای یک آدرس منحصر بفرد است، در سیستم E-mail هم باید سرویس گیرنده‌گان دارای آدرس منحصر بفرد و مشخصی باشند. این آدرسها به فرم زیر هستند:

نام و حوزه سرویس دهنده @ شناسه سرویس گیرنده

مثال آدرس Abdollahpour@uok.ac.ir مشخص کننده نام سرویس گیرنده و همچنین موسسه سرویس دهنده E-mail (دانشگاه کردستان) می‌باشد.

مشابه نامهای عادی، یک نامه الکترونیکی باید علاوه بر متن نامه، حاوی اطلاعات دیگری مانند آدرسها فرستنده و گیرنده نامه نیز باشد.

سرویس Email از برخی نکات با سایر سرویسهای ارائه شده در اینترنت متفاوت است. اصلیترین ویژگی سیستم Email این است که ماهیت Offline دارد. به عبارت دیگر لزومی ندارد در همان لحظه‌ای که نامه ارسال می‌شود، طرف مقابل آماده دریافت باشد. بلکه ممکن است گیرنده مانند چند روز بعد به جعبه پستی خود سر برزند و آنرا مشاهده نماید. سیستم Email از دو پروتکل مختلف برای ارسال و دریافت نامهای الکترونیکی استفاده می‌کند. یکی از این پروتکلاها مسئولیت دریافت نامه‌ها را بر عهده دارد، می‌تواند یکی از دو پروتکل POP3 یا IMAP باشد.

سرویس دهنده SMTP ابه پورت ۲۵، سرویس دهنده POP3 به پورت ۱۱۰ و سرویس دهنده IMAP به پورت ۱۴۳ گوش می‌دهند.

سرویس دهنده SMTP

زمینکه از طریق سرویس گیرنده خود (مثال از طریق برنامه Outlook) اقدام به ارسال نامه الکترونیکی می‌نمایید، برنامه سرویس گیرنده SMTP با سرویس دهنده SMTP به منظور ارسال آن نامه، ارتباط برقرار می‌نماید. سرویس دهنده فوق، بر حسب نیاز ممکن است با سایر سرویس دهنده‌گان SMTP جهت ارسال آن نامه ارتباط برقرار نماید. شکل (۱۱-۶) نحوه عملکرد سرویس دهنده و سرویس گیرنده SMTP را نشان می‌دهد. از آنجا که مسئولیت SMTP به جلو راندن و

از مهمترین وظایف پروتکل Telnet این است که باید خود را با ترمینالهای متفاوت تطبیق دهد. به عنوان مثال فرض کنید یک کاربر از کامپیوتری با کدهای ASCII استفاده می‌کند (مثلاً یک سیستم PC) در حالی که تمایل دارد به سیستمی وارد شود که استاندارد آن کدهای EBCDIC است (مثلاً یک کامپیوتر Mainframe). آگاهی از این موضوع و تبدیل این کدها به عهده Telnet است.

سرویس دهنده Telnet

این برنامه که بر روی کامپیوتر سرویس دهنده نصب و اجرا می‌شود، موظف است تقاضاهای ورودی برقراری یک نشست Telnet را پذیرد و پس از هماهنگی‌های لازم با برنامه مشتری، به او سرویس بدهد.

سرویس گیرنده Telnet

این برنامه که بر روی کامپیوتر کاربران نصب می‌شود و منطبق بر سخت افزار و سیستم عامل ماشین کاربراست، وظیفه دارد تا مراحل برقراری یک نشست Telnet را برقرار کرده و یک ترمینال مجازی را به گونه‌ای شیوه‌سازی نماید که فرامین صادره از کاربر، منطبق و سازگار با ماشین سرویس دهنده باشد.

یک اتصال Telnet پس از برقراری ارتباط TCP بین برنامه سرویس گیرنده و پورت ۲۲ برنامه سرویس دهنده آغاز می‌شود.

برای برقراری یک نشست Telnet کاربر احتیاج به شناسه و رمز عبور دارد:

```
Telnet varmint
Trying 194.5.30.68 ...
Connected to varmint.
Escape character is '^]'.
SunOS UNIX (varmint)
login: Jones
Password:*****
varmint%
```

مثال زیر نحوه ارسال یک نامه الکترونیکی را از طریق دستورات SMTP نشان می‌دهد:

```
C:\> telnet www.uok.ac.ir 25
Connecting to www.uok.ac.ir ...
```

```
برقراری اتصال
220 PARSDATA Mail Server (IMail 8.00 2586-5) NT-ESMTP Server X1
HELO PARSDATA
250 hello PARSDATA Mail Server
_____ بوشن نامه
MAILFROM: Abdollahpour@uok.ac.ir
250 ok
RCPT TO: Abdollahpour@uok.ac.ir
250 ok deliver to alternate
_____ سرآیند و بدن نامه
DATA
354 ok, send it; end with <CRLF>.<CRLF>
FROM: Abdollahpour
TO: myself
```

Hi this is a sample e-mail to show SMTP in action.

```
خاتمه اتصال
250 Message queued
QUIT
221 Goodbye
Connection to host lost.
```

سرویس دهنده POP3

همگامی که با استفاده از یک برنامه سرویس گیرنده (مانند Outlook)، می‌خواهید جهت بررسی صندوق پستی خود وارد آن شوید، برنامه فوق با سرویس دهنده POP3 از طریق پورت 110 ارتباط برقرار می‌نماید. سرویس دهنده POP3 به یک نام کاربری و رمز عبور نیاز دارد. پس از تایید اعتبار و مجوز شما، سرویس دهنده POP3 امکان دستیابی شما به جعبه پستی را فراهم می‌نماید.

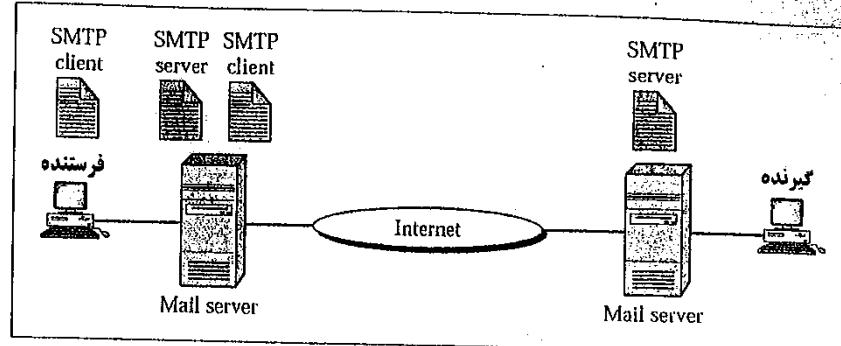
سرویس دهنده POP3 نیز از دستورات متین ساده، استفاده می‌نماید که تعدادی از آنها عبارتند از:

- USER ID: برای ورود شناسه کاربر استفاده می‌شود.

- PASS: برای ورود رمز عبور استفاده می‌شود.

- QUIT: برای قطع ارتباط با سرویس دهنده POP3 استفاده می‌گردد.

وارد کردن نامه‌ها در جعبه پستی گیرنده است، گاهی از آن به عنوان یک پروتکل Push یاد می‌شود.



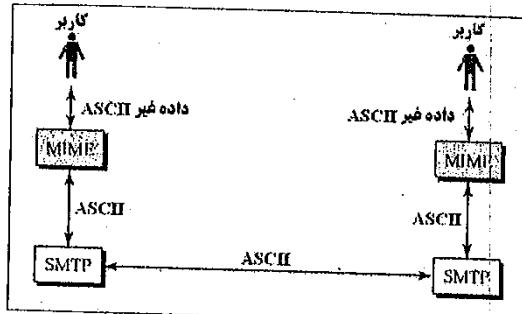
شکل (۱۱-۶)- پروتکل SMTP

اگر صندوق پستی گیرنده پیام بر روی همان سرویس دهنده باشد، سرویس دهنده SMTP پیام دریافت شده را در اختیار سرویس دهنده POP3 قرار خواهد داد؛ ولی اگر گیرنده پیام بر روی حوزه‌ای دیگر باشد، سرویس دهنده SMTP نیازمند برقراری ارتباط با حوزه مربوطه است. برنامه‌های سرویس گیرنده و سرویس دهنده SMTP با استفاده از یک زبان ساده متین، با یکدیگر ارتباط برقرار می‌نمایند. در ابتدا برنامه سرویس گیرنده خود را معرفی، آدرس فرستنده و گیرنده و محتويات پیام را مشخص خواهد کرد. در ادامه تعدادی از دستوراتی را که سرویس دهنده SMTP استفاده می‌کند توضیح می‌دهیم:

- HELO: برنامه سرویس گیرنده را معرفی می‌کند.
- MAIL FROM: فرستنده پیام را مشخص می‌کند.
- RCPT TO: گیرنده را مشخص می‌کند.
- DATA: بدن نامه را مشخص می‌کند.
- QUIT: ارتباط را قطع می‌نماید.
- HELP: در رابطه با دستورات توضیحات لازم را ارائه می‌نماید.

با استفاده از برنامه Telnet نیز می‌توان با سرویس دهنده پست الکترونیکی و از طریق پورت 25 ارتباط برقرار کرد.

ارسال نامه نمی‌باشد بلکه توسعه‌ای برای پروتکل SMTP محسوب می‌شود. می‌توان MIME را به صورت برنامه‌ای تصور نمود که داده غیر ASCII را به داده ASCII و بالعکس ترجمه می‌کند. شکل (۱۲-۶) نحوه کار MIME را نشان می‌دهد.

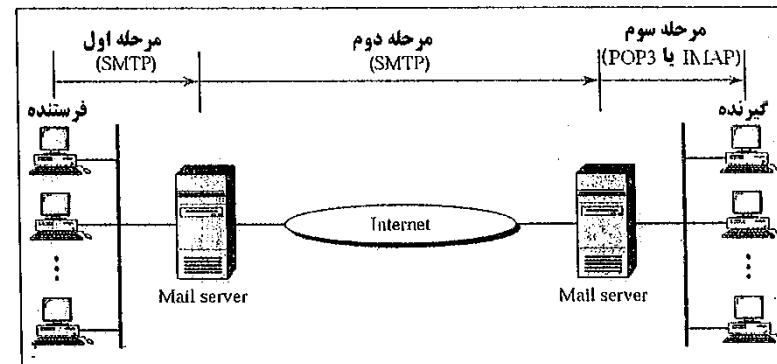


شکل (۱۲-۶)- پروتکل MIME

- LIST: لیست پیامها بهمراه اندازه آنها را نشان خواهد داد.
- RETR: برای بازبینی یک پیام استفاده می‌شود.
- DELE: برای حذف یک پیام استفاده می‌گردد.

برنامه سرویس گیرنده پست الکترونیکی با سرویس دهنده POP3 ارتباط برقرار کرده و مجموعه‌ای از دستورات فوق را بمنظور انتقال نسخه‌هایی از پیامهای الکترونیکی بر روی ماشین شما، انجام می‌دهد.

از آنجا که مسئولیت پروتکل POP3 خواندن و خارج کردن نامه‌ها از جعبه پستی گیرنده است، گاهی از آن به عنوان یک پروتکل Pop (مقابل Push) یاد می‌شود. در شکل (۱۲-۶) مراحل ارسال یک نامه الکترونیکی و استفاده از پروتکلهای POP3 یا SMTP در هر مرحله نشان داده شده است.



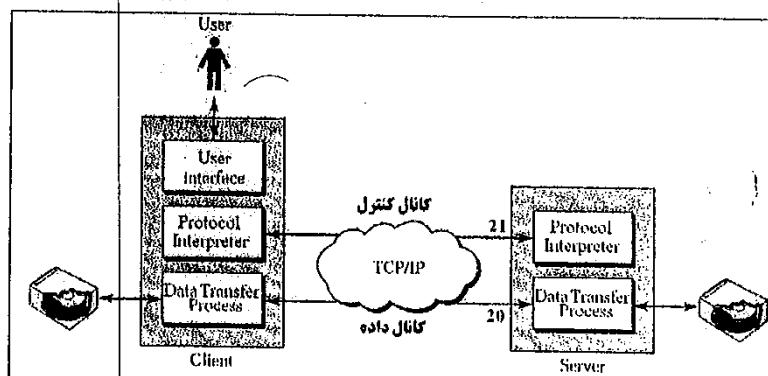
شکل (۱۲-۶)- مراحل ارسال و دریافت یک Email

MIME

پروتکل SMTP تنها قادر به ارسال پیامهایی به فرمت ASCII می‌باشد. به عبارت دیگر نمی‌توان از طریق آن کاراکترهای غیر ASCII زبانهای دیگر (فارسی- زبانی- روسی و ...) را ارسال کرد. همچنین نمی‌توان از آن برای ارسال فایل‌های باینری و تصویر و صدا استفاده نمود. MIME یک پروتکل تکمیلی است که اجزه می‌دهد کاراکترهای غیر ASCII نیز از طریق SMTP منتقل شوند. دقت کنید که MIME یک پروتکل جایگزین برای SMTP نیست و قادر به

دلیل لزوم برقراری دو کانال مجزا بین سرویس دهنده و سرویس گیرنده آن است که بتوان بدون قطع جریان داده‌ها، فرامین را بطور همزمان مبادله کرد. بعضی امثله در حین انتقال یک فایل می‌توان روی کانال فرمان، دستور لغو عمل انتقال یا تغییر مود انتقال را صادر کرد. هر کدام از طرفین در یک اجلان FTP باید دو پروسه ایجاد نمایند که یکی وظیفه مدیریت ارتباط روی کانال فرمان را به عهده داشته و اصطلاحاً "مسن پروتکل" یا پروسه PI نامیده می‌شود و دیگری وظیفه مدیریت انتقال داده‌ها را انجام می‌دهد و به "پروسه انتقال داده" یا DTP معروف است.

در طرف سرویس دهنده، پروسه PI به پورت شماره ۲۱ و پروسه DTP به پورت شماره ۲۰ گوش می‌ذند. در شکل (۱۴-۶) کانال‌های داده و کنترل بین پروسه‌های PI و DTP نشان داده شده است.



شکل (۱۴-۶) - کانال‌های کنترل و داده در پروتکل FTP

بروتکل FTP تقریباً پروتکل پیچیده‌ای است؛ زیرا از یک کانال کنترل (کانال اولیه) و یک کانال داده (کانال ثانویه) استفاده می‌کند. نحوه ایجاد کانال داده به مد یا روش برقراری کانال کنترل بستگی دارد. این کار به دو روش امکان پذیر است:

- روش معمولی یا فعال (Active Mode)
- روش غیرفعال (Passive Mode)

۷- پروتکل انتقال فایل (FTP)

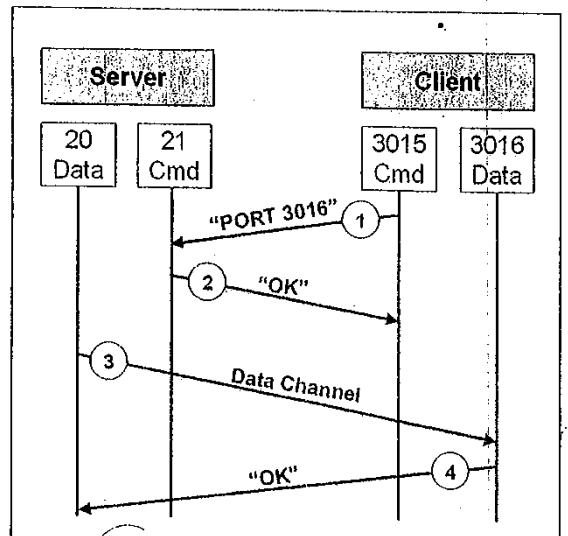
پروتکل انتقال فایل با FTP، ساده‌ترین و مطمئن‌ترین راه برای انتقال فایل بین کامپیوترهای متصل در اینترنت است. شما چه با این پروتکل آشنا باشید و چه آشنا نباشید، تاکنون بارها از آن استفاده کرده‌اید. متداول‌ترین مورد استفاده FTP برای Download کردن فایلها از اینترنت می‌باشد. برخی از سرویس‌هایی که این پروتکل ارائه می‌کند عبارتند از:

- تهیه لیستی از فایل‌های موجود در یک کامپیوتر راه دور
- حذف، تغییر نام و جایجا کردن فایل‌های کامپیوتر راه دور
- جستجو در دایرکتوریهای کامپیوتر راه دور
- ایجاد یا حذف شاخه روی کامپیوتر راه دور
- انتقال فایل از کامپیوتر میزبان به کامپیوتر راه دور (Uploading)
- انتقال فایل و ذخیره آن از کامپیوتر میزبان به کامپیوتر راه دور (Downlading)

همانطور که احتمالاً متوجه شده باشید، با قابلیتهایی که این پروتکل ارائه می‌کند به راحتی می‌توان اعمال خرابکارانه‌ای را بر روی سیستم سرویس دهنده انجام داد؛ از این‌روه کاربرانی که از این سرویس استفاده می‌کنند باید قبل از این‌کار از این‌نوع احتیاط نمایند و کلمه عبور خود را وارد نمایند و سرویس دهنده پس از شناسایی و تایید اتصالت کاربر، سطح دسترسی و عملیات مجاز را برای وی تعیین می‌کند و یک نشست FTP آغاز می‌شود.

اکنون ارتباط بین سرویس دهنده و سرویس گیرنده FTP را تشریح می‌نماییم؛ پروتکل FTP برخلاف سایر پروتکلهای لایه کاربرد، برای شروع یک نشست بین برنامه سرویس دهنده و برنامه سرویس گیرنده از دو ارتباط همزمان از نوع TCP استفاده می‌کند. به هر کدام از این ارتباطات یک "کانال" گفته می‌شود. این دو کانال عبارتند از:

- کانال فرمان: این کانال که به کانال اولیه نیز مشهور است، یک ارتباط از نوع TCP با پورت شماره ۲۱ سرویس دهنده بوده که روی آن فرامین لازم برای نحوه انتقال فایلها ارسال می‌گردد. این کانال در تمام طول اجلاس FTP باز می‌باشد.
- کانال داده: این کانال که به آن کانال ثانویه نیز گفته می‌شود، یک ارتباط از نوع TCP با پورت شماره ۲۰ سرویس دهنده می‌باشد که روی آن داده‌ها مبادله می‌شود. این کانال فقط ۸ می‌باشد که داده‌ای برای مبادله موجود باشد، باز است.



شکل(۱۵-۶)- برقراری نشست FTP به روش فعال

در ادامه به یک مثال عملی از نحوه ارتباط با یک سرویس دهنده FTP توجه کنید:

```
$ ftp eng.uok.ac.ir
Connected to eng.uok.ac.ir
220 Server ready
Name: Abdollahpour
331 Password required for Abdollahpour
Password: xxxxxxxx
230 User Abdollahpour logged in
ftp > ls /user/report
200 OK
150 Opening ASCII mode
.....
.....
226 transfer complete
ftp > close
221 Goodbye
ftp > bye
```

در ادامه به بررسی هر یک از روش‌های Passive و Active FTP در بروتکل خواهیم پرداخت.
روش فعال، روش سنتی ارتباط بین یک سرویس گیرنده FTP و یک سرویس دهنده می‌باشد که عملکرد آن بر اساس مراحل زیر است:

الف- سرویس گیرنده دو پورت با شماره تصادفی بالای ۱۰۲۴ را به صورت پشت سر هم فعال می‌نماید (مثلاً پورتهای ۳۰۱۵ و ۳۰۱۶).

ب- سرویس گیرنده یک ارتباط با پورت ۲۱ سرویس دهنده FTP برقرار می‌نماید. همانطور که قبلاً گفته شد، پورت ۲۱، پورتی است که سرویس دهنده از طریق پروسه PI به آن گوش فرا می‌دهد تا از صدور فرامین آگاه و آنان را به تنظیب پاسخ دهد. سرویس گیرنده برای برقراری ارتباط با سرویس دهنده از پورت با شماره کوچکتر مرحله قبل استفاده می‌نماید (پورت ۳۰۱۵). تا این لحظه کانال کنترل بین دو پروسه PI برقرار شده است.

ج- سرویس گیرنده شماره پورت دوم برای برقراری کانال داده بین سرویس دهنده با خود را از طریق صدور دستور PORT N+1 به وی اطلاع می‌دهد که N شماره پورت پروسه PI در سرویس گیرنده است.

د- سرویس دهنده یک ارتباط را از طریق پورت ۲۰ خود با پورت مشخص شده سرویس گیرنده (پورت ۳۰۱۶) برقرار می‌نماید؛ به عبارت دیگر کانال داده بین پروسه‌های DTP برقرار می‌گردد.

در شکل(۱۵-۶) نحوه برقراری یک نشست FTP از نوع فعال نشان داده شده است. در فرآیند فوق، ارتباط توسط سرویس گیرنده آغاز شده و پس از برقراری کانال کنترل، پاسخ به آن توسط سرویس دهنده و از طریق پورت ۳۰۱۶ که توسط سرویس گیرنده مشخص شده است، انجام می‌شود. در صورتی که سرویس گیرنده از سیستم‌ها و دستگاه‌های امنیتی خاصی نظریه فایروال استفاده کند، باید تمهیمات لازم به منظور ارتباط کامپیوترهای راه دور را پیش بینی کند تا آنان بتوانند به هر پورت بالاتر از ۱۰۲۴ سرویس گیرنده دستیابی داشته باشند. بدین منظور لازم است که پورت‌های اشاره شده بر روی ماشین سرویس گیرنده باز باشند. این موضوع می‌تواند خطرات امنیتی متعددی را برای سرویس گیرنده‌گان به دنبال داشته باشد.

مثال زیر نحوه استفاده از پروتکل FTP به روش غیرفعال را نشان می‌دهد:

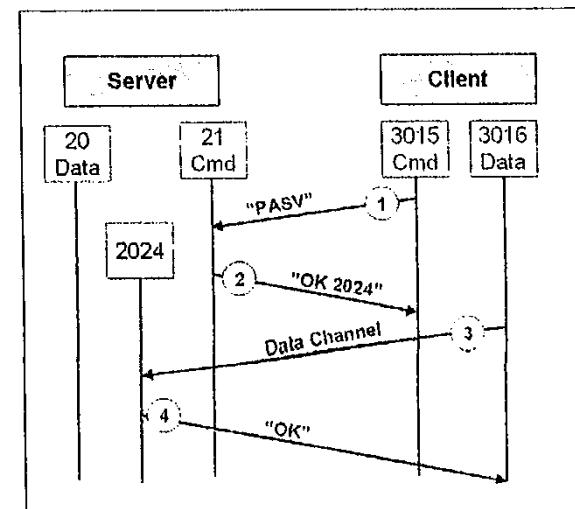
```
$ ftp eng.uok.ac.ir
Connected to eng.uok.ac.ir
220 Server ready
Name: Abdollahpour
331 Password required for Abdollahpour
Password: xxxxxxxx
230 User Abdollahpour logged in
ftp> passive
Passive mode on.
ftp> ls
ftp: setsockopt (ignored): Permission denied
ftp> PASV
227 Entering Passive Mode (192,168,150,90,195,149).
ftp > ls
200 OK
150 Opening ASCII mode<
.....
.....
226 transfer complete
ftp > close
221 Goodbye
ftp > bye
```

با توجه به مستندات درج شده در RFC 1579، استفاده از روش غیرفعال به دلایل متعددی به روش فعال ترجیح داده می‌شود.

- در روش غیرفعال مراحل برقراری یک نشست به صورت زیر است:
- الف- سرویس گیرنده دو پورت با شماره تصادفی بالای ۱۰۲۴ را فعال می‌نماید (مثلاً ۳۰۱۵ و ۳۰۱۶)
- (۳۰۱۶) ب- ارتباط اولیه از طریق پورت ۳۰۱۵ سرویس گیرنده با پورت ۲۱ سرویس دهنده آغاز می‌شود. بدین ترتیب کانال فرمان برقرار می‌گردد.
- ج- سرویس دهنده یک پورت دیگر با شماره تصادفی بالای ۱۰۲۴ را فعال کرده (مثلاً ۲۰۲۴) و به سرویس گیرنده شماره پورت را اعلام می‌نماید.
- د- در ادامه، سرویس گیرنده کانال داده را با استفاده از یک اتصال از طریق پورت ۳۰۱۶ با پورت ۲۰۲۴ سرویس دهنده برقرار می‌نماید.

در فرآیند فوق، سرویس گیرنده دارای نقش محوری است و فایروال موجود بر روی آن می‌تواند درخواست‌های دریافتی غیرمجاز به پورت‌های بالاتر از ۱۰۲۴ را به منظور افزایش امنیت رد کند.

شکل (۱۶-۶) مراحل برقراری یک نشست غیرفعال FTP را نشان می‌دهد. همانطور که ملاحظه می‌کنید، در این حالت در برقراری هر دو کانال، سرویس گیرنده شروع کننده ارتباط است.



شکل (۱۶-۶)- برقراری نشست FTP به روش غیرفعال

خود آزمایی:

۸- کدامیک از درخواستهای زیر برای ذخیره نمودن یک صفحه وب بر روی سرویس دهنده استفاده منشود؟

- | | | | |
|--------|----------|----------|-----------|
| PUT(د) | COPY (ج) | POST (ب) | GET (الف) |
|--------|----------|----------|-----------|

۹- برای برقراری یک نشست احتیاج به شناسه کاربر و رمز عبور داریم.
 (د) الف و ج
 (ج) FTP
 (ب) SMTP
 (الف) Telnet

۱۰- کدامیک از پروتکل‌های زیر قابلیت ارسال کاراکترهای غیر ASCII را از طریق Email فراهم می‌نماید؟

- | | | | |
|---------|---------|----------|-----------|
| IMAP(د) | POP3(ج) | MIME (ب) | SMTP(الف) |
|---------|---------|----------|-----------|

۱۱- کدامیک از پروتکل‌های زیر از پورت ۱۱ استفاده می‌کند؟
 (د) Telnet
 (ج) DNS
 (ب) SMTP
 (الف) POP3

۱- کدامیک از پروتکل‌های زیر از دو کانال همزمان هنگام برقراری ارتباط استفاده می‌کند؟

- | | | | |
|-----------|--------|---------|-----------|
| Telnet(د) | FTP(ج) | HTTP(ب) | DNS (الف) |
|-----------|--------|---------|-----------|

۲- کدامیک از پروتکل‌های زیر از پورت ۸۰ استفاده می‌کند؟

- | | | | |
|---------|--------|---------|--------------|
| HTTP(د) | FTP(ج) | DNS (ب) | Telnet (الف) |
|---------|--------|---------|--------------|

۳- کدامیک از پروتکل‌های زیر برای ردوبلن کردن شناسه کاربر و رمز عبور هنگام دریافت Email استفاده منشود؟

- | | | | |
|--------|----------|----------|------------|
| FTP(د) | SNMP (ج) | POP3 (ب) | SMTP (الف) |
|--------|----------|----------|------------|

۴- کدامیک از پروتکل‌های زیر برای ورود به یک کامپیوتر از راه دور استفاده می‌شود؟

- | | | | |
|---------|-----------|--------|------------|
| SMTP(د) | Telnet(ج) | FTP(ب) | HTTP (الف) |
|---------|-----------|--------|------------|

۵- در کدامیک از نامهای زیر از حوزه کشوری برای ترجمه آدرس استفاده می‌شود؟

- | | |
|----------------------|--------------------------|
| gsfc.nasa.gov (ب) | www.atac.flida.edu (الف) |
| mac.eng.sony.com (د) | kenz.acct.sony.jp (ج) |

۶- کدامیک از عبارات زیر در مورد روش‌های پرس و جوی DNS صحیح است؟

- (الف) در روش پرس و جوی تکراری بیشتر بار کاری بر عهده سرویس دهنده محلی است.
 (ب) در روش پرس و جوی بازنگشتی بیشتر بار کاری بر عهده سرویس دهنده محلی است.
 (ج) برای پیدا کردن آدرس IP حتماً مراجعته به سرویس دهنده ریشه لازم است.
 (د) از روی آدرس IP نمی‌توان نام معادل آن را بدست آورد.

۷- در پیغامهای درخواست و پاسخ HTTP، کدامیک از موارد زیر هم در خط درخواست و هم در خط وضعیت قرار دارد؟

- | |
|---|
| ب) مسیر و فایل مورد نظر (الف) نسخه Http |
| د) الف و ج (ج) کد وضعیت |

