شبکه‌های کامپیوتری

Computer Networks

جزوه مهندس حمید رضا نیرومند
در دانشگاه جامع علمی-کاربردی
http://niroomand.ir

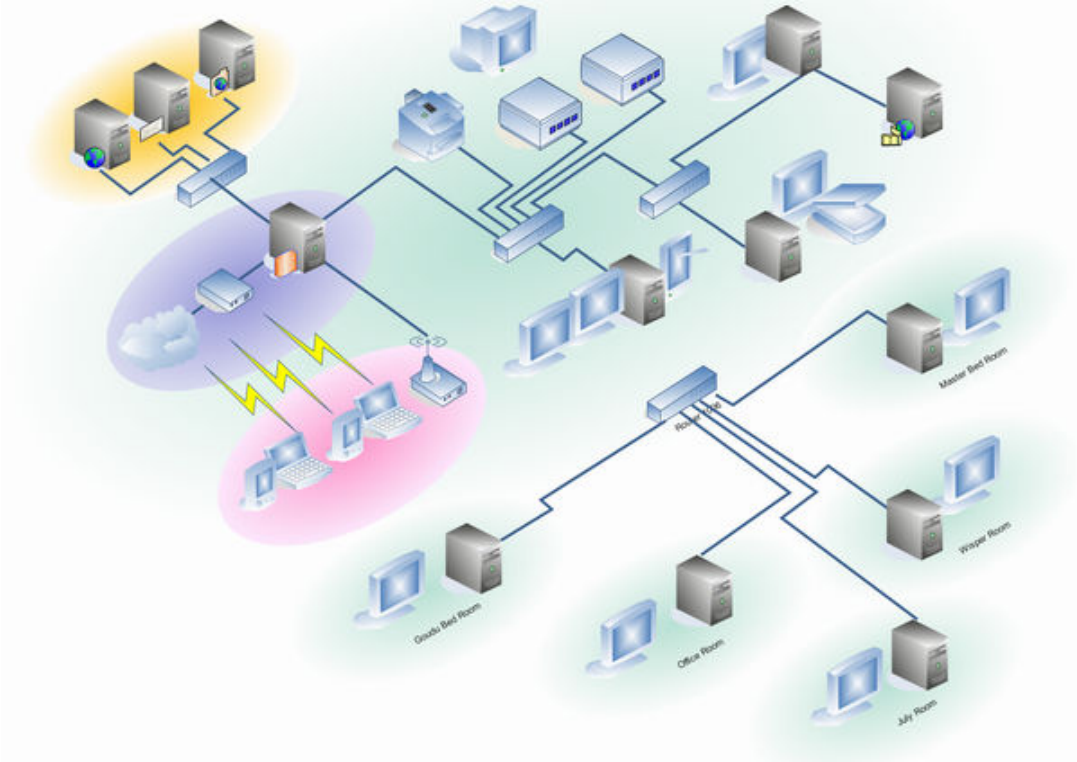
منابع:

- Network+ 2005 in Depth
  (Author: Tamara Dean) (http://st.aftab.cc/uni/network/network_resources)
- Teracom Video Courses (http://yourl.ir/teracom)
- TestOut Video Tutorials (Network 2009)
- TrainSignal Video Courses (Network)
- **Wikipedia.org**
- **http://aftab.cc**

توجه:

- استفاده از جزوه بدون حضور در کلاس‌ها پیشنهاد نمی‌شود.
- این یک انتشار غیررسمی از جزوه و ویژه دانشجویان مهندس نیرومند است.
- این، نسخه ۱.۱.۰ از جزوه است و به مرور غنی‌تر خواهد شد. (لطفاً اشتباهات سهوی که مشاهده می‌کنید را به ایمیل info@niroomand.ir ارسال نمایید.)

تعریف شبکه:



گروهی از کامپیوترها و دیگر قطعات (مانند پرینتر، منبع ذخیره‌سازی و ...) که به وسیله یک نوع رسانه انتقال به یکدیگر متصل شده‌اند.

Network:
A group of computers and other devices (such as printers) that are connected by some type of transmission media.

اجزای اصلی شبکه:

Computer systems:

- سیستم‌های کامپیوتری. (که اغلب به آن گره (node) یا میزبان (host) گفته می‌شود)

Transmission media:

- مسیری برای انتقال سیگنال‌ها بین دستگاه‌ها.

Network interface card (NIC):

- کارت واسط شبکه. (کارت شبکه)

Protocol:

- زبان صحبت (مانند زبان مکالمه در یک تماس تلفنی) که به آن در اصطلاح پروتکل گفته می‌شود.

تعریف پروتکل:

قواعد و استانداردهایی که نحوه ارتباط و تبادل داده بین میزبان‌ها (hosts) را تعیین می‌کنند. (تصور کنید دارید پشت تلفن با دوستتان صحبت می‌کنید. این صحبت باید طبق یک زبان مشترک و گرامرهای خاص باشد وگرنه صحبت‌های یکدیگر را متوجه نخواهید شد. پروتکل یعنی همان زبان و قوانین و گرامرهای مکالمه بین دو host)

Protocol:
Rules or standards that describe how hosts communicate and exchange data.

Standalone computer:

به کامپیوترهایی که به شبکه یا هیچ کامپیوتردیگری متصل نیستند و از برنامه‌ها و داده‌های روی حافظه خودشان استفاده می‌کنند standalone computer (کامپیوتر مستقل) می‌گویند.

سؤال: چرا از شبکه استفاده می‌کنیم؟

Why use network?

- **Sharing resources:**
  - مهم‌ترین دلیل استفاده از شبکه: اشتراک منابع مانند پرینترها و هارد دیسک‌ها.
  - اشتراک منابع، صرفه جویی در زمان و هزینه را در پی دارد. (به طور مثال در یک شبکه به جای چند پرینتر از یک پرینتر استفاده می‌شود.)
  - امکان مدیریت و نظارت بر روی چندین کامپیوتر از یک مکان مرکزی. (به طور مثال می‌توان از طریق اتاق server به عنوان مدیر، نرم افزارهای لازم را بر روی تمام کامپیوترها نصب کرد)

شبکه کفش کتانی (sneaker net):

- در صورت عدم وجود شبکه باید در اصطلاح کفش کتانی به پا کرد و بین کامپیوترهای مختلف حرکت کرد و یک به یک اطلاعات را در آن کپی کرد!! شبکه‌کارها به این وضعیت به شوخی sneaker net می‌گویند!

سؤال: شکی نیست که هزینه‌های راه‌اندازی شبکه بسیار زیاد است، اما چرا با وجود هزینه‌های زیاد راه‌اندازی شبکه، سازمان‌ها رغبت به راه‌اندازی آن دارند؟

پاسخ: زیرا شبکه‌ها بیش از هزینه‌هایی که دارند، موجب صرفه جویی می‌شوند.

انواع شبکه(Network Types):

شبکه‌ها را می‌توان از جنبه‌های مختلف بررسی کرد. اما دو تقسیم بندی مشهور عبارتند از:

انواع شبکه از نظر قرارگرفتن hostها نسبت به یکدیگر:

۱- شبکه‌های نظیر به نظیر(peer to peer = p2p):

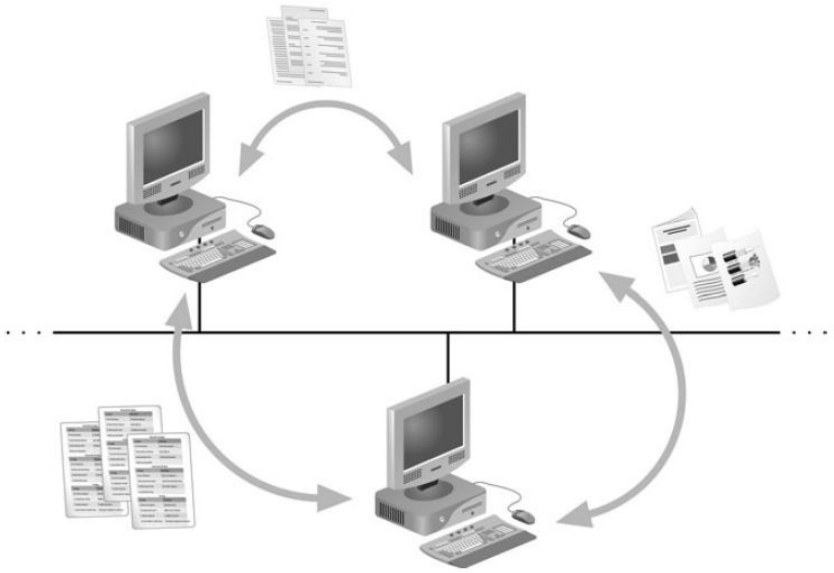


FIGURE 1-1 *Resource sharing on a simple peer-to-peer network*

در یک شبکه P2P:

- هرکامپیوتر به طور مستقیم با کامپیوتر دیگر ارتباط دارد.
- لزوماً هیچ کامپیوتری نسبت به دیگری قدرت و دسترسی مدیریتی بالاتری ندارد. در حقیقت هر کامپیوتر ممکن است هم از سرویس دیگران استفاده کند و هم به دیگران سرویس‌هایی بدهد. (به طور مثال یکی پرینترش را share کند و دیگری در حالی که از پرینتر اولی استفاده می‌کند، هارد دیسکش را به اشتراک بگذارد.)

مزایای شبکه P2P:

- پیاده‌سازی آسان
- ارزان‌تر بودن نسبت به نوع دیگر

معایب شبکه P2P:

- چندان قابل توسعه نیستند. (هرچه بزرگ‌تر، مدیریت آن‌ها سخت‌تر).
- امنیت ندارند و هر کامپیوتر به اطلاعات کامپیوتر دیگر دسترسی دارد در حالی که شاید شما بخواهید اطلاعات را برای اشخاص خاصی share کنید. (مثلاً یکی ممکن است تمام اطلاعات را پاک کند).
- منابع در یک جا متمرکز نیستند به خصوص حافظه ذخیره سازی که بر روی چندین کامپیوتر قرار دارد و این، کار گروهی را بسیار مشکل می‌کند.
- در کل پشتیبانی چنین شبکه‌هایی بسیار سخت است.

۲- شبکه‌های سرویس دهنده/سرویس گیرنده (Client/Server=C/S):

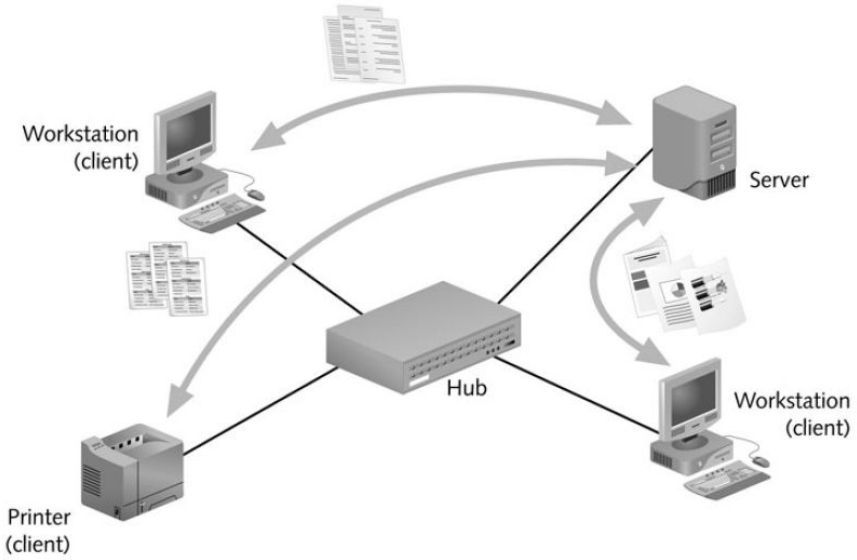


FIGURE 1-2 *Resource sharing on a client/server network*

در این نوع شبکه‌ها یک کامپیوتر مرکزی (که به نام server شناخته می‌شود) برای آسان‌سازی اشتراک منابع بین دیگر کامپیوترها (که به نام client شناخته می‌شوند)، به کار گرفته می‌شود.

نکته۱: clientها معمولاً در سطح کامپیوترهای شخصی (PCها) هستند وبه نام workstation (ایستگاه کاری) نیز شناخته می‌شود.

نکته۲: serverها ممکن است از لحاظ سخت افزاری هیچ تفاوتی با clientها نداشته باشند اما از نظر نرم افزاری حتماً متفاوت هستند و تفاوت آن‌ها در سیستم عاملی است که بر روی server نصب شده است.

نکته۳: در یک شبکه C/S، کلاینت‌ها به طور مستقیم به منابع یکدیگردسترسی ندارند بلکه از server به عنوان واسطه استفاده می‌کنند.

نکته٤: به سیستم عامل‌های شبکه در اصطلاح NOS (مخفف Network Operating System) می‌گویند که:

- وظیفه مدیریت داده‌ها و منابع دیگر را به عهده دارند.
- سطح دسترسی کاربران برای دسترسی به منابع شبکه را تعیین می‌کنند.
- تعیین می‌کنندکه چه فایل‌هایی فقط خواندنی و یا فقط نوشتنی باشند.
- تعیین می‌کنند که کاربران چه موقع و از چه مکانی به شبکه دسترسی داشته باشند.
- قواعد ارتباط کامپیوترها با یکدیگر را تعیین می‌کنند.
- و بسیاری امکانات دیگر را برای شبکه فراهم می‌کنند.

چند سیستم عامل شبکه مشهور:

1- Microsoft Windows Server
2- Linux
3- Unix
4- NetWare

نکته: serverها معمولاً فضای ذخیره‌سازی (Hard Disc) و قدرت پردازش (CPU) و حافظه (RAM) بیشتری نسبت به clientها دارند. حتی ممکن است مثلاً ۲ هارددیسک داشته باشند که با یک RAID به یکدیگر متصل شده‌اند تا اگر یکی از کار افتاد، دومی فعال می‌شود.

مزایای شبکه‌های Client/Server:

- از طریق server می‌توان مشکلات کل شبکه را زیر نظر داشت و عیب یابی کرد.
- امنیت بیشتری دارند.
- قابلیت توسعه در آن‌ها بیشتر و ساده‌تر است.
- serverها برای انجام کارهای سنگین بهینه شده‌اند، بنابراین زمان پاسخگویی (Response time) کمتری دارند.
- دسترسی به منابع مشترک می‌تواند به یک یا چند کاربر اجازه داده شده باشد.

نمونه‌ای از یک شبکه **Client/Server** گسترده:

سعی کنید کلمات و اشکالی که در تصویر زیر می‌بینید را مرور کنید تا در آینده بیشتر با آن‌ها آشنا شوید.

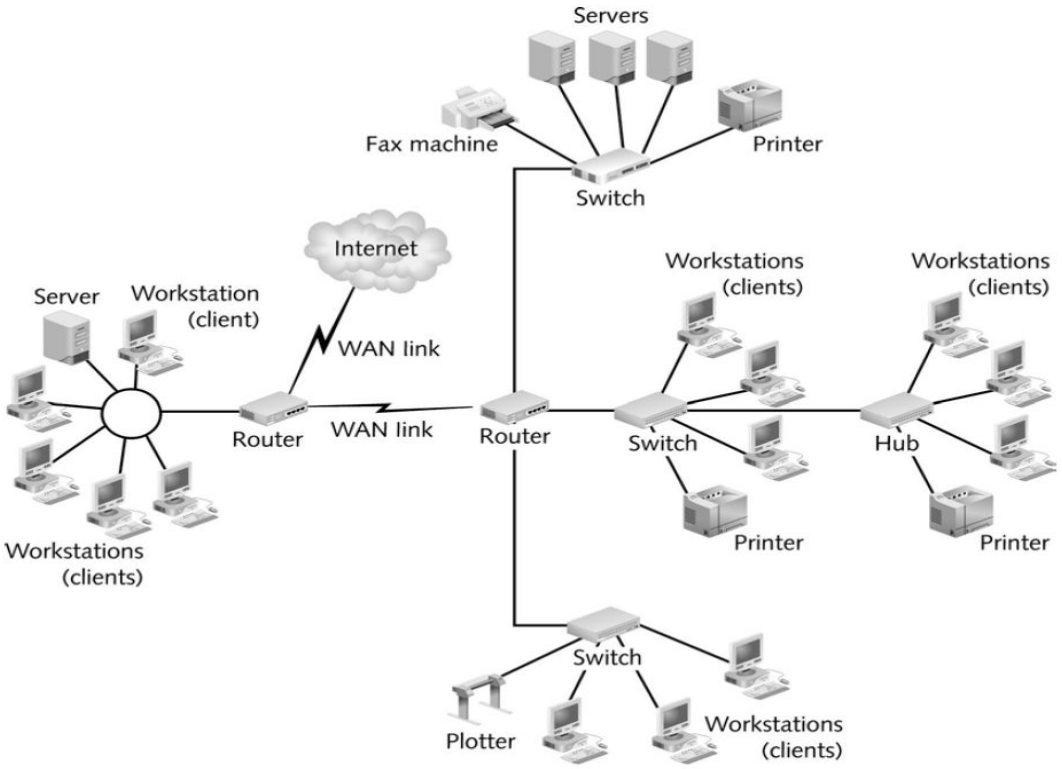


FIGURE 1-3 *A more complex client/server network*

انواع شبکه از نظر Size (وسعت جغرافیایی):

1- LAN (Local Area Network) (شبکه محلی)

2- MAN (Metroplitan Area Network) (شبکه شهری)

3- WAN (Wide Area Network) (شبکه گسترده)

♦ **LAN:**

شبکه‌ای از کامپیوترها و دستگاه‌ها در یک فضای نسبتاً کوچک مثل یک ساختمان یا یک دفتر کاری.

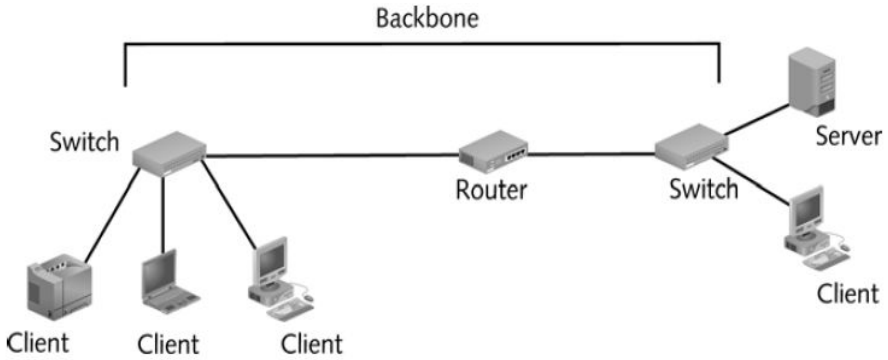


FIGURE 1-6 *A LAN backbone*

♦ **MAN:**

شبکه‌ای که چندین ساختمان در نقاط مختلف یک شهر یا استان را به هم متصل می‌کند. (به دلیل فاصله زیاد ممکن است از تکنولوژی‌های مختلفی برای اتصال استفاده شود)

♦ **WAN:**

شبکه‌ای که شبکه‌هایLAN و MAN در نقاط دور را به هم متصل می‌کند.

نکته: گاهی اوقات شبکه‌های MAN را جزءِ WANها به حساب می‌آورند و فقط دو نوع شبکه LAN و WAN را معرفی می‌کنند.

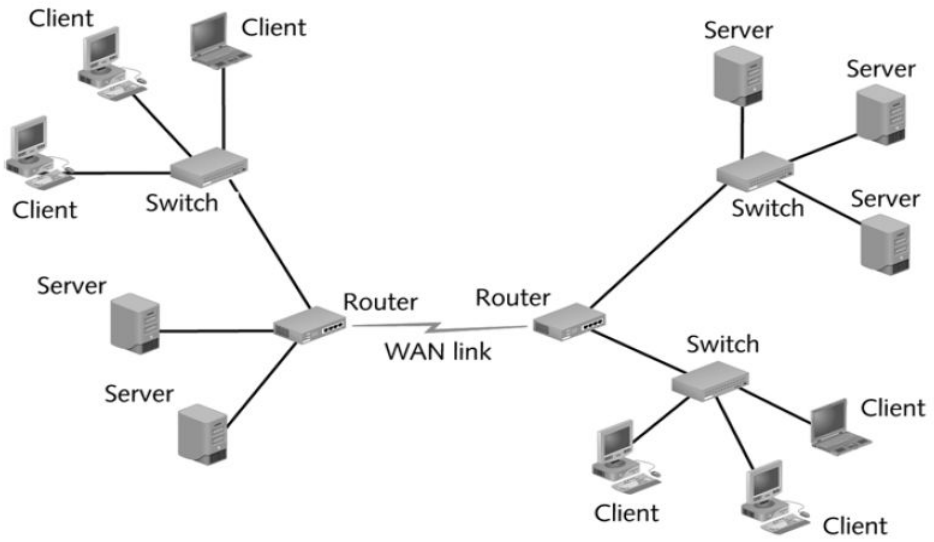


FIGURE 1-4 *A simple WAN*

Backbone (ستون فقرات شبکه) :

بخش اصلی در شبکه کابل‌ها و دستگاه‌های به اشتراک گذاشته شده (مثل Routerها و Switchها و Serverها) به آن متصل‌اند.

همبندی یا توپولوژی (Topology) :

آرایش فیزیکی یک شبکه کامپیوتری را در اصطلاح توپولوژی (یا تاپولوژی) می‌نامند.

توپولوژی هر شبکه نسبت به نیازهای سازمان یا سخت‌افزارهای در دسترس، متفاوت است.

رایج‌ترین توپولوژی‌های شبکه‌های LAN در تصویر زیر مشخص است:

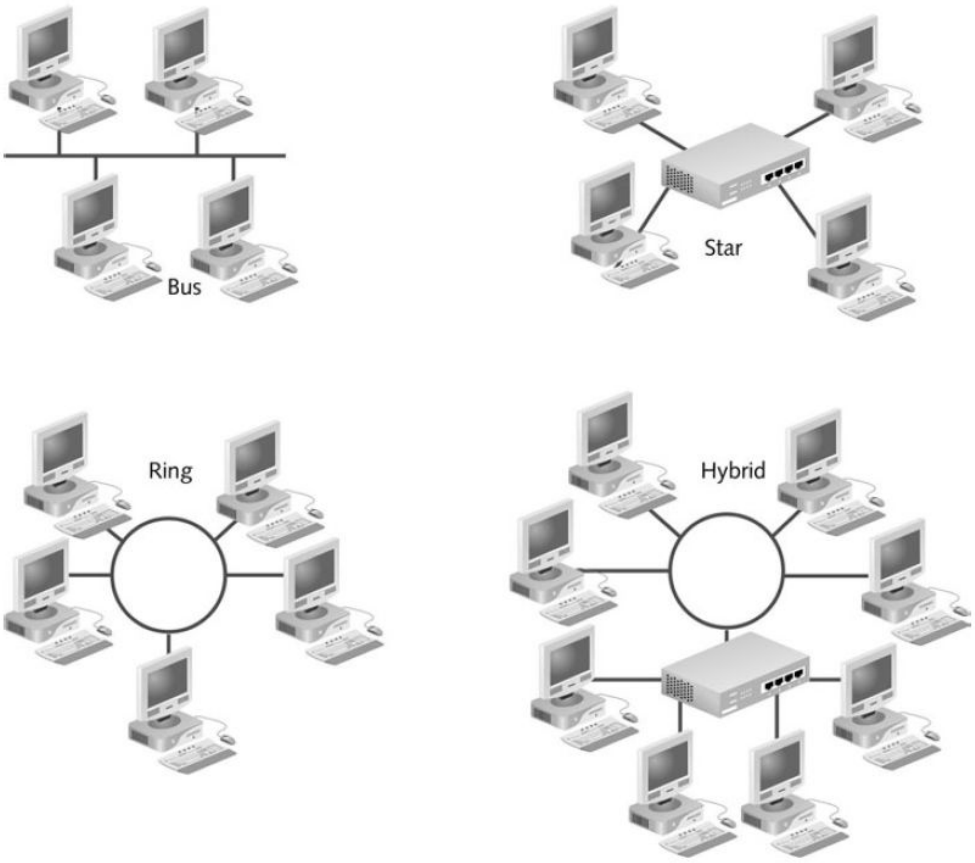
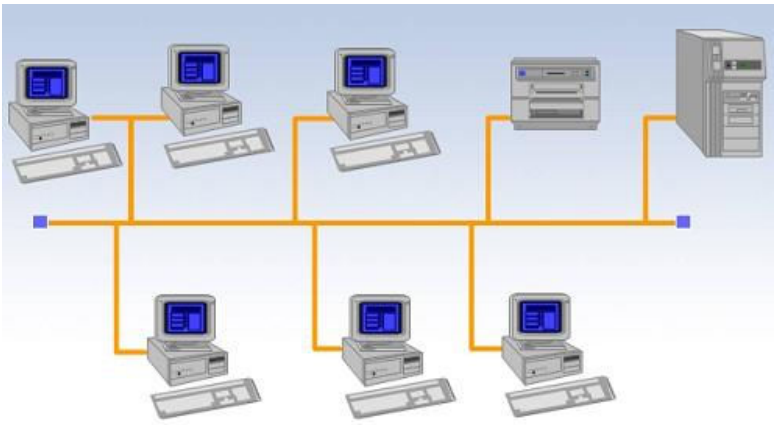


FIGURE 1-7 *Common network topologies*

توپولوژی خطی یا Bus:

نوعی پیکربندی برای یک شبکه محلی که در آن تمام گره‌ها به یک خط ارتباطی اصلی (گذرگاه) متصل می‌شوند. هر گره در یک شبکه خطی بر فعالیت خط نظارت دارد. پیام‌ها توسط تمامی گره‌ها آشکار می‌شوند اما تنها گره یا گره‌های مورد نظر آنها را می‌پذیرند گرهی که به درستی عمل نمی‌کند ارتباطش متوقف می‌شود اما وقفه‌ای در عملیات به وجود نمی‌آورد.

برای اجتناب از تصادفاتی که ممکن است در نتیجه اقدام همزمان دو یا بیشتر از دو گره برای استفاده از خط پیش آید شبکه‌های خطی عموماً برای تنظیم ترافیک بر آشکارسازی تصادف (Collision detection) یا ارسال نشانه (Token Passing) تکیه دارند.



مزایا:

- افزایش و کاهش سیستم‌ها به راحتی (تا حد مجاز) صورت می‌گیرد.
- در کل، ساده و کم‌هزینه است.

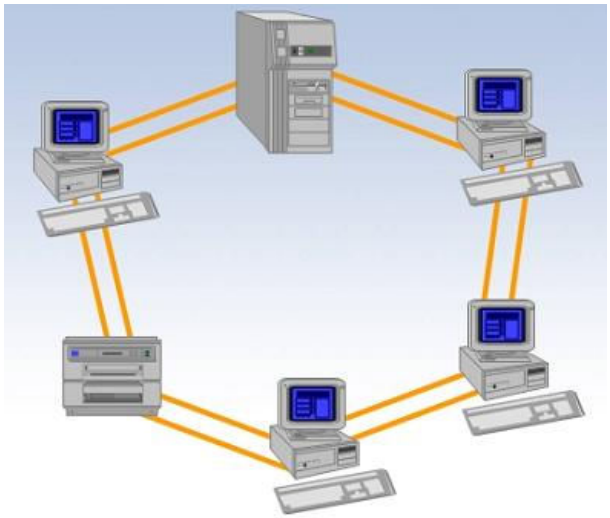
معایب:

- در صورت قطعی در یک قسمت از کابل اصلی، تمامی شبکه از کار می‌افتد.
- عیب‌یابی آن وقت‌گیر است.
- نیاز به نگهداری و مراقبت بیشتری نسبت به سایر توپولوژی‌های دیگر دارد.

توپولوژی حلقوی یا Ring:

نوعی شبکه محلی که وسایل (گره‌ها) در آن در یک حلقه بسته به یکدیگر متصل می‌شوند پیام ها در این نوع شبکه در یک جهت از گره‌ای به گره دیگر انتقال می‌یابند.

وقتی گره‌ای پیام را در یافت می‌کند ابتدا نشانی مقصد آن را بررسی می‌کند اگر نشانی پیام با نشانی گره یکسان باشد گره پیام را می‌پذیرد در غیر اینصورت سیگنال را از نو تولید و پیام را برای گره بعدی ارسال می‌کند. این تولید مجدد سیگنال به شبکه‌های حلقوی امکان می‌دهد که فواصل بزرگ‌تری را نسبت به شبکه‌های ستاره‌ای و خطی پوشش دهند این حلقه را می‌توان به گونه‌ای طراحی نمود تا گره‌های خراب یا ناقص نیز نادیده انگاشته شوند. اما افزودن گره‌های جدید به دلیل بسته بودن حلقه دشوار است.



مزایا:

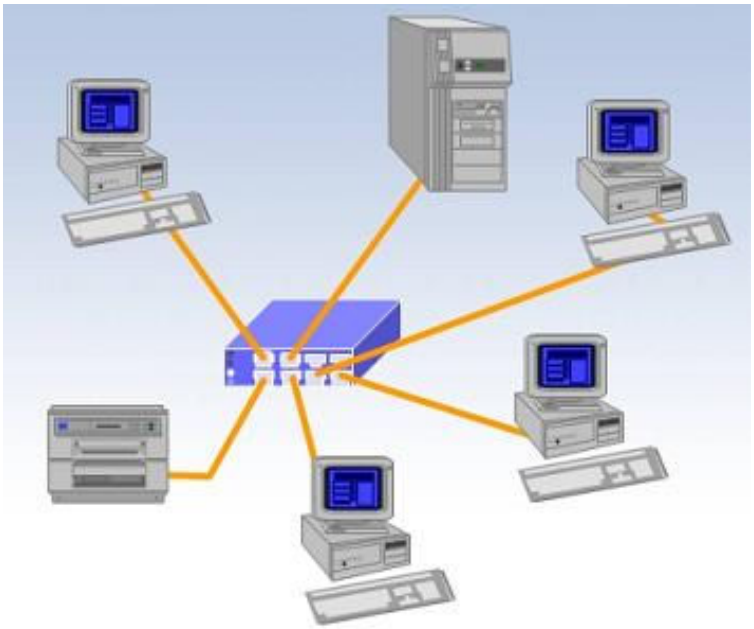
- نیاز به فضایی خاص جهت انشعابات در کابل‌کشی نخواهد بود. به دلیل استفاده از یک کابل جهت اتصال هر گره به گره همسایه‌اش، اختصاص محل‌هایی خاص به منظور کابل‌کشی ضرورتی نخواهد داشت.
- مناسب جهت فیبر نوری: استفاده از فیبر نوری باعث بالا رفتن نرخ سرعت انتقال اطلاعات در شبکه است. چون در توپولوژی Ring، ترافیک داده‌ها در یک جهت است، می‌توان از فیبر نوری به منظور محیط انتقال استفاده کرد. در صورت تمایل می‌توان در هر بخش از شبکه از یک نوع کابل به عنوان محیط انتقال استفاده کرد. مثلاً در محیط‌های ادرای از مدل‌های مسی و در محیط کارخانه از فیبر نوری استفاده کرد.

معایب:

- اشکال در یک گره باعث اشکال در تمام شبکه می‌گردد. در صورت بروز اشکال در یک گره، تمام شبکه با اشکال مواجه خواهد شد. و تا زمانی‌که گره معیوب از شبکه خارج نگردد، هیچگونه ترافیک اطلاعاتی را روی شبکه نمی‌توان داشت.
- اشکال‌زدایی مشکل است. بروز اشکال در یک گره می‌تواند روی تمام گره‌های دیگر تأثیر گذار باشد. به منظور عیب‌یابی می‌بایست چندین گره بررسی شود تا گره مورد نظر پیدا گردد.
- تغییر در ساختار شبکه مشکل است. در زمان گسترش و یا اصلاح حوزه جغرافیائی تحت پوشش شبکه، به دلیل ماهیت حلقوی شبکه مسائلی به وجود خواهد آمد.
- توپولوژی بر روی نوع دستیابی تاثیر می‌گذارد. هر گره در شبکه دارای مسؤولیت عبور دادن داده‌ای است که از گره مجاور دریافت داشته است.
- قبل از اینکه یک گره بتواند داده خود را ارسال نماید، می‌بایست به این اطمینان برسد که محیط انتقال برای استفاده قابل دستیابی است.

توپولوژی ستاره‌ای یا Star :

یک شبکه محلی که در آن هر وسیله (گره) به صورت پیکربندی ستاره‌ای شکل به یک کامپیوتر مرکزی متصل می‌شود. این شبکه عموماً از یک دستگاه مرکزی (هاب:Hub) که با پایانه‌هایی احاطه شده است تشکیل می‌شود.



مزایا:

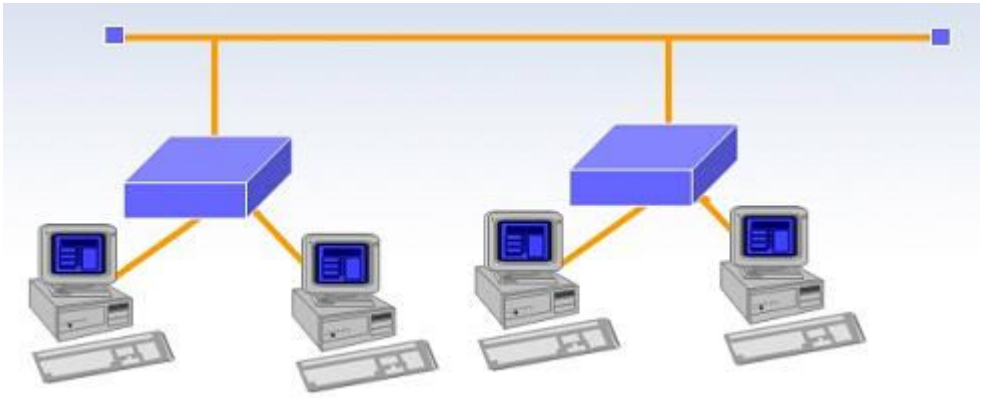
- قطع شدن یک خط به طور معمول بقیه شبکه را تحت تأثیر قرار نمی‌دهد.
- اگر از switch استفاده شود امکان تبادل اطلاعات دو به دو به صورت همزمان وجود دارد، در نتیجه حجم ترافیک بیشتری در واحد زمان می‌تواند انجام شود.

معایب:

- اگر به هر دلیلی «نقطه‌ی مرکزی» از کار بیفتد، کل شبکه از کار باز می‌ایستد، به‌همین دلیل معمولاً hub را از نظر فیزیکی در یک تابلوی مخصوص معروف به Rack نصب کرده و Rack را در یک مکان مطمئن و با شرایط محیطی مناسب قرار می‌دهند.
- مصرف کابل و به طور کلی هزینه پیاده‌سازی آن نسبت به خطی بیشتر است. البته در عوض هزینه نگهداری و رفع عیب پایین‌تر است. زیرا کمتر دچار مشکل شده و عیب‌یابی در آن ساده‌تر و سریع‌تر انجام می‌شود.

توپولوژی ترکیبی یا Hybrid :

شبکه‌ای که با همبندی‌های مختلفی چون حلقوی و ستاره‌ای ساخته می‌شود.



چند مفهوم مهم در شبکه:

- **اینترنت:**

یک شبکه عمومی بزرگ. شبکه‌ای از شبکه‌های LAN و WAN.

Internet : a large public network.

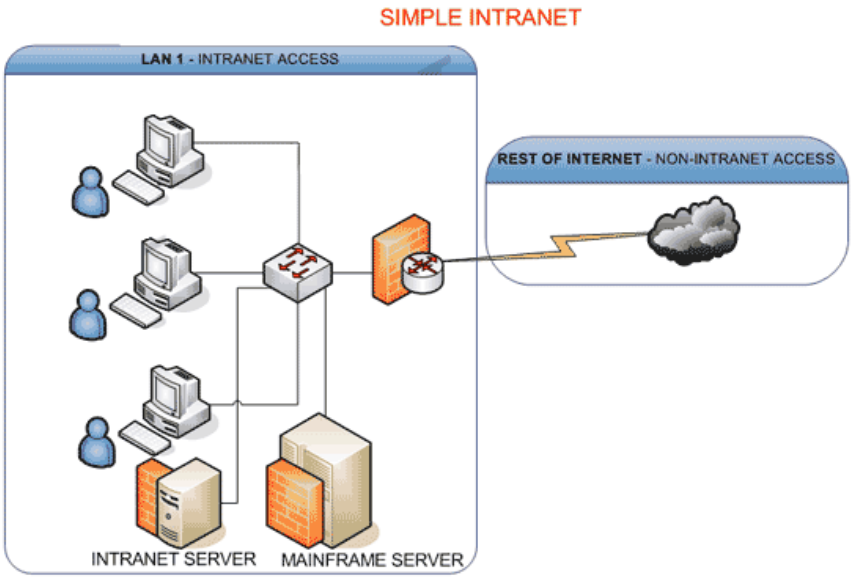
- **تار جهان‌گستر:** همان مفهوم اینترنت را دارد. WWW (World Wide Web)

- **اینترانت:**

یک شبکه خصوصی درون سازمانی که از تکنولوژی اینترنت استفاده می‌کند.

Intranet : a private network that uses internet technology.

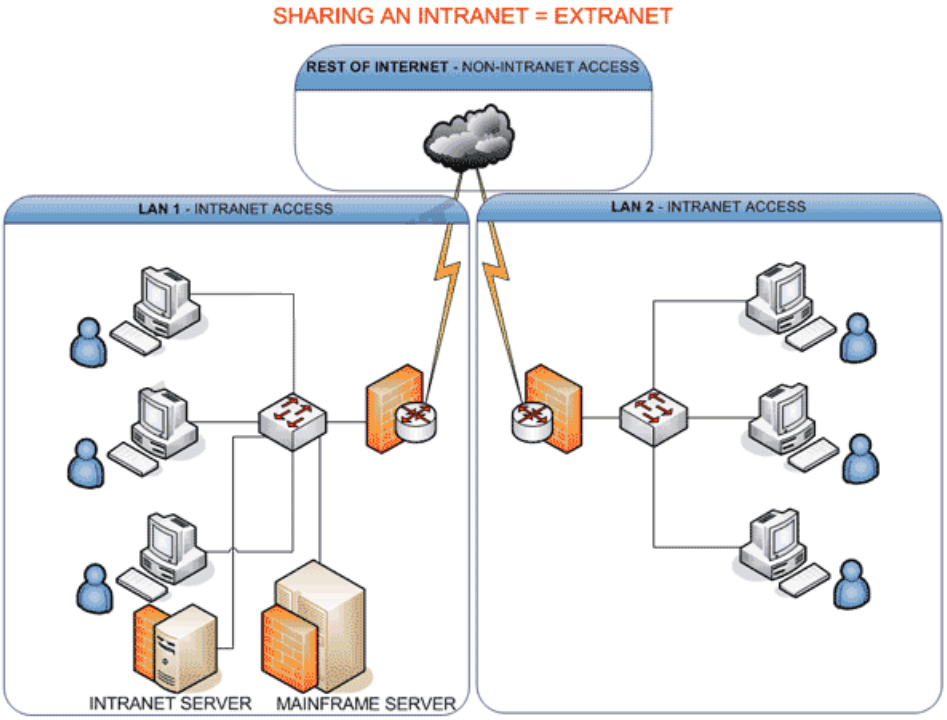
نکته: یک اینترانت ممکن است به اینترنت متصل باشد یا نباشد. (تشابه این دو کلمه شما را به اشتباه نیاندازد که اینترانت به اینترنت وصل است)



- **اکسترانت:**

یک شبکه خصوصی درون یک سازمان که برای کاربران خارجی از طریق اینترنت قابل دسترسی است **اما** فقط کاربرانی که اجازه داده شده باشند.

Extranet : a private network that is made available to external user but only authorized external users.



مهم‌ترین مؤسسات تعیین کننده استانداردهای شبکه:

بدون وجود استانداردها به مشکل بر می‌خورید چون مطمئن نیستید که آیا محصول یک شرکت با شرکت دیگر هماهنگ هست یا نه.

مثال: باید شرکت‌های پریز و دوشاخه تلفن هماهنگ باشند وگرنه...

نکته: تحت استاندارد بودن اجباری نیست ولی به نفع شرکت‌هاست.

- **ANSI:**
  (American Notional Standard Institute):

مؤسسه‌ای با هزاران نماینده و کارشناس که مسؤول تعیین استانداردهای مختلف از جمله استانداردهای شیمی و کامپیوتر و... هستند، هم در آمریکا و هم در سطح بین المللی.

- **EIA and TIA:**
  (Electronic Industries Alliance Telecommunication Industry Association) (TIA/EIA)

مسؤول تعیین استانداردهای IT، بی‌سیم، ماهواره، فیبر نوری و تجهیزات تلفن و...

مهم‌ترین استانداردهایی که توسط این مؤسسه تعیین شده است استاندارد کابل‌های شبکه است.

- **IEEE:**
  (Institute of Electrical & Electronics Engineers):

مؤسسه مهندسان الکترونیک و الکتریک

این مؤسسه بین المللی متشکل است از حرفه‌ای‌های رشته‌های مهندسی و هدف مؤسسه ارتقای سطح توسعه و تحصیلات در رشته‌های الکترونیک و کامپیوتر و بیشترین تمرکز مؤسسه تعیین استانداردهای شبکه‌های کامپیوتری است. مانند استانداردهای کارت‌های شبکه.

- **ISO or IOS:**
  (International Organization for Standardization):

ISO مخفف نام شرکت نیست بلکه یک کلمه یونانی است به معنی Equal (مساوی).

برخی از فعالیت‌های این شرکت:

تعیین استانداردهای پردازش اطلاعات، صنعت ارتباطات، صنعت بسته بندی، توزیع اجناس، تولید انرژی، سرویس‌های بانکی و ...

- کمتر از ۳۰۰ استاندارد از ۱۴۲۵۰ استانداردی که ISO دارد، مرتبط با محصولات کامپیوتری است.

- **ITU:**
  (International Telecommunication Union):

مسؤول تعیین استانداردهای فرکانس‌های تلویزیونی، تلفنی، ماهواره‌ای، بیشترین تمرکز بر روی سرویس‌های مرتبط با اینترنت.

- **IANA & ICANN**
  (Internet Assignment Number Authority & Internet Corporation for Assignment Names & Numbers):

مسؤول دادن اسم یا همان دامنه به شماره‌هاست. قبل از دامنه، برای ورود به سایت باید IP کامپیوتررا می‌زدند.

هر کامپیوتر در یک شبکه باید آدرسی واحد داشته باشد که به آن IP می‌گویند.درابتدا IANAمسؤول نگهداری و انتساب این آدرس‌ها به کامپیوتری که به اینترنت متصل شده است بود و بعدها این مؤسسه به ICANN تغییر نام داد.

مدل OSI

در بحث‌های علمی برای فهم بهتر مفاهیم بهتر است یک تصویر از آن در ذهن خود شکل دهید مثل تصویر کردن اتم‌های هیدروژن و اکسیژن در مولکول آب به صورت دایره (در حالی که به این معنی نیست که اتم، شکل دارد و شکل آن دایره است!)

برای تصویر کردن انتقال داده‌ها نیز برای اینکه که توضیح و فهم آن ساده‌تر شود، از مدل‌ها استفاده می‌شود.

در بحث شبکه نیز درست است که ارتباط بین Nodeها را نمی‌بینیم اما می‌توانیم از مدلی برای تجسم آنچه اتفاق می‌افتد، استفاده کنیم.

مدلی که بیش از همه برای توصیف ارتباطات شبکه استفاده می‌شود مدل مرجع یا OSI (Open System Interconnection) است.

در اوایل سال ۱۹۸۰ مؤسسه ISO کار بر روی یک مجموعه استاندارد را آغازکرد که کامپیوترهای سراسردنیا را قادر به اتصال به یکدیگر کند.

نتیجه، مدل موفق OSI شد که ارتباطات شبکه‌ای را به ۷ لایه تقسیم کند.

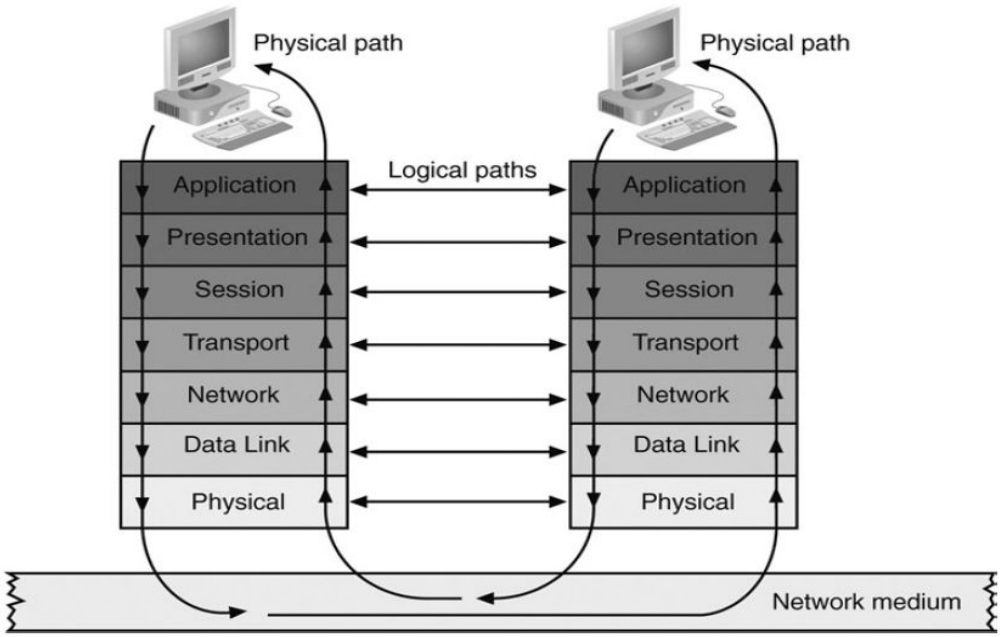


FIGURE 2-1 *Flow of data through the OSI Model*

مدل OSI یک نماد تئوری از آنچه بین Nodeها اتفاق می‌افتد، است نه اینکه نرم افزار یا سخت افزار خاصی است.

روند کلی: در ابتدا یک کاربر یا دستگاه یک مجموعه داده بر روی لایه Application قرار می‌دهد. این لایه آن مجموعه‌ها را به واحدهایی به نام (PDU یا Protocol Data Unit) تقسیم می‌کند. این واحدها، لایه‌ها را به سمت پایین طی می‌کنند و روی رسانه انتقال قرار می‌گیرند تا به کامپیوتر دوم برسند. همه این اتفاقات در طی چند میلی ثانیه اتفاق می‌افتد.

در مورد این مدل در آینده به طور مفصل صحبت خواهیم کرد، اما در حد آشنایی اجمالی مطالب زیر را مطالعه کنید:

لایه Application:

واسطی بین نرم افزارهایی مثل Word، Excel و... و لایه پایینی خود یعنی لایه Presentation است. در این لایه مسائلی مانند فرمت‌بندی، مسائل امنیتی (Security) و(Synchronization) و دیگر نیازمندی‌های شبکه در مورد نرم افزاری که قصد ارتباط با شبکه را دارد بررسی می‌شود.

مثال: وقتی یک صفحه وب را در مرورگر باز می‌کنید پروتکل http که مربوط به لایه APP است درخواست شما را فرمت بندی می‌کند و به سرور ارسال می‌کند. همچنین این پروتکل است که پاسخ سرور را به مروگر ارسال می‌کند.

لایه Presentation:

به عنوان یک مترجم عمل می‌کند، داده‌های لایه هفت را می‌گیرد و طوری آن‌ها را فرمت‌بندی می‌کند که شناسایی آن‌ها در کامپیوتر مقصد ممکن باشد.

مثال: وقتی یک عکس از لایه App دریافت می‌کند آن را طوری فرمت بندی می‌کند که کامپیوتر مقصد بتواند تشخیص دهد کـه ایـن داده‌ها مربوط به یک عکس است نه ویدئو.

یکی از مهم‌ترین وظایف این لایه Encryption یا رمزگذاری داده‌ها است.

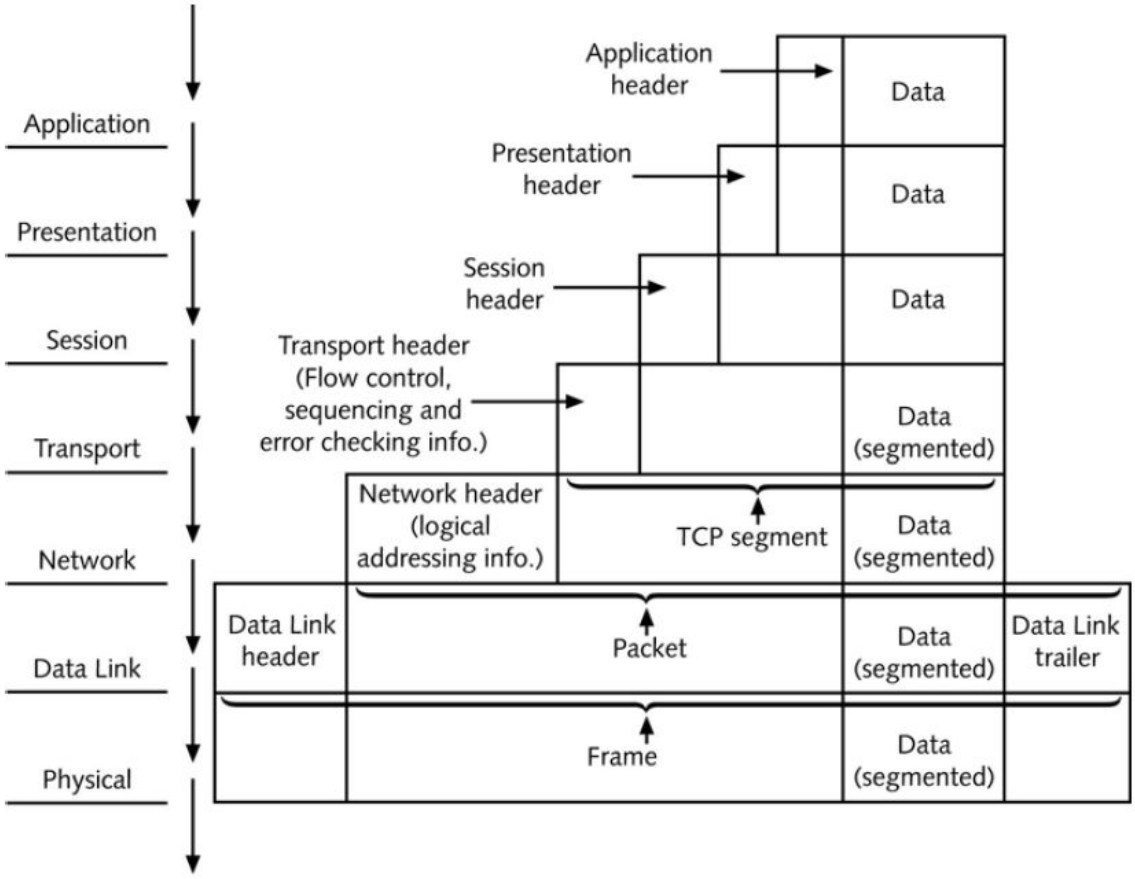


FIGURE 2-7 *Data transformation through the OSI Model*

وظایف لایه Session:

مسؤول برقراری ارتباط، حفظ ارتباط و قطع آن بین مبدأ و مقصد است و همچنین فقط به Nodeهایی اجازه ورود به جلسه (Session) را می‌دهد که اجازه دارند. در واقع، یکی از وظایف آن برقراری امنیت است.

مثال: وقتی ارتباط شما با ISP (Internet Service Provider) قطع بشود این لایه سریعا بـه Windows اطـلاع مـی‌دهـد و Windows آیکون کنار ساعت را تغییر می‌دهد یا دوباره قصد اتصال می‌کند.

لایه Transport:

این لایه مسؤول انتقال بسته‌ها به مقصد است.

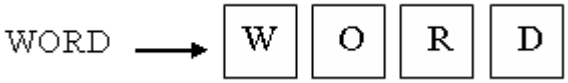
می‌تواند بفهمد که آیا یک بسته با موفقیت ارسال شده یا خیر؟

ده‌ها پروتکل برای این لایه نوشته شده که مهم‌ترین و جدیدترین آن TCP است. (Transmission Control Protocol)

یکی از مهم‌ترین وظایف این لایه این است که داده‌های بزرگی را که از لایه Session دریافت کرده است، به چندین واحد کوچک‌تر بـه نام قطعه (Segment) تبدیل کند. این پروسه به قطعه بندی (Segmentation) معروف است.

مثال: یک نوع از شبکه Ethernet بسته‌های بیش از ۱۵۰۰ بایتی را نمی‌تواند ارسال کند.

Segmentation مثل تبدیل کلمه به حروف است:



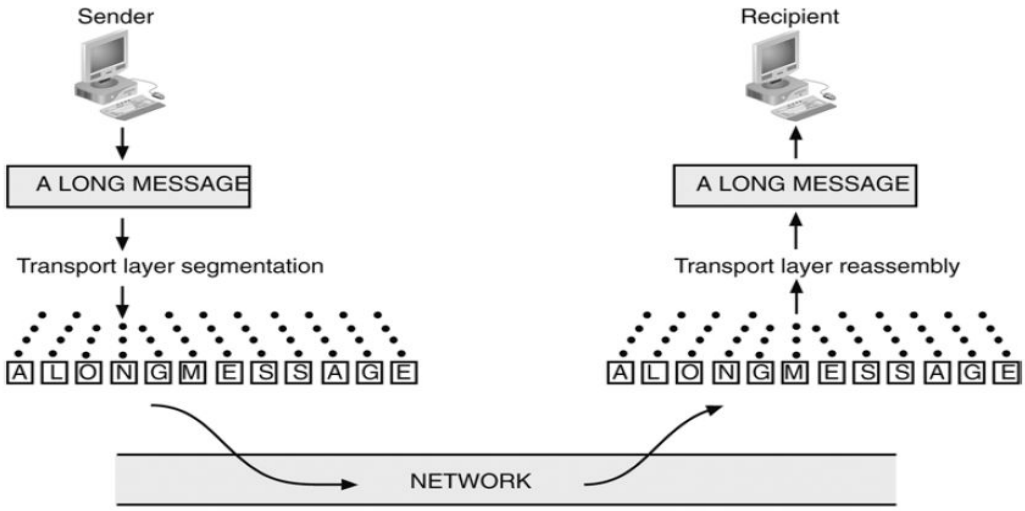


FIGURE 2-2 *Segmentation and reassembly*

نکته: Reassembly (دوباره سرهم کردن) عکسِ عمل Segmentation را گویند که در مقصد انجام می‌شود.

لایه Network:

مهم‌ترین وظیفه آن مسیریابی یاRouting است که این عمل با اتصال آدرس مبدأ و آدرس مقصد به هرSegment ممکن می‌شود.
یکی دیگر از وظایف این لایه تبدیل آدرس منطقی یا مجازی به آدرس فیزیکی است.

تعریف Packet:

به مجموعه Segment و آدرس مبدأ و آدرس مقصد، یک Packet یا بسته گفته می‌شود.

لایه Data link:

وظیفه اصلی این لایه این است که اطلاعاتی که از لایه Network دریافت کرده را در یک سری قاب (Frame) قرار دهد. این لایه اطلاعات را چک می‌کند که آیا اطلاعات به درستی به مقصد رسیده یا خیر؟ که این کار اصطلاحاً Error checking نامیده می‌شود.

تعریف Frame:

هر قاب شامل داده اولیه، آدرس فرستنده، آدرس گیرنده و اطلاعات مربوط به تست خطا (Error checking) می‌شود.

لایه Physical:

این لایه اطلاعات را به صفر و یک و سپس به سیگنال تبدیل می‌کند. پروتکل‌های این لایه اطلاعات دریافت شده از لایه Data link را به ولتاژهای مختلف تبدیل می‌کند تا سیگنال تولید شود و از طریق رسانه انتقال، قابل ارسال باشد. برخی از پروتکل‌های این لایه Cat 5e، V.35، Rj-45 می‌باشد.

نکته: مهم‌ترین وظیفه مدیران شبکه کار با لایه‌های Transport، Network، Data link و Physical است.

نکته: هر لایه پروتکل خاص خود را دارد.

پروتکل: پروتکل یا قانون چیزی نیست جز چند خط کد که یک برنامه نویس نوشته است تا طبق آن قوانین ارتباطات شکل گیرد.

مفاهیم پایه انتقال

انواع ارسال اطلاعات در شبکه:

۱- Analog

۲- Digital

تفاوت آنالوگ و دیجیتال: آنالوگ پیوسته است و دائماً بین مقادیر ولتاژ مختلف، متغیر است ولی دیجیتال گسسته است و به صورت پالس در هر لحظه یکی از دو مقدار مشخص را دارد. (مثلاً اگر ۵۰ ولت برق روی کابل بود می‌گیریم نماد 1 و اگر صفر ولت بود، می‌گیریم نماد 0)

توجه: کلمه «ولت» در انتقال کابلی کاربرد دارد و نه انتقال بی‌سیم. فعلاً برای فهم بهتر، از این کلمه استفاده می‌کنیم، اما بعداً در بحث انتقال بی‌سیم بیشتر توضیح خواهیم داد.

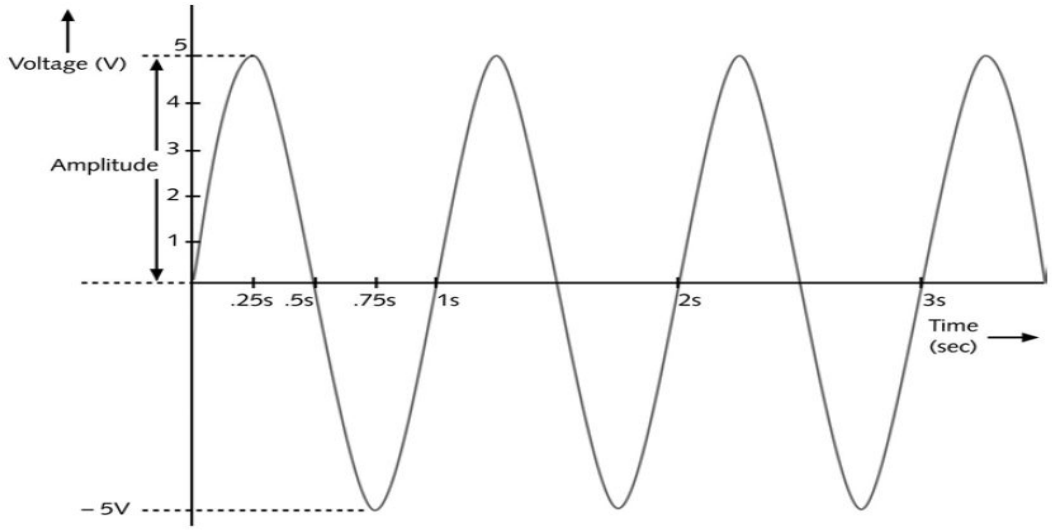


FIGURE 3-1 *An example of an analog signal*

نمایش نمادین یک سیگنال آنالوگ

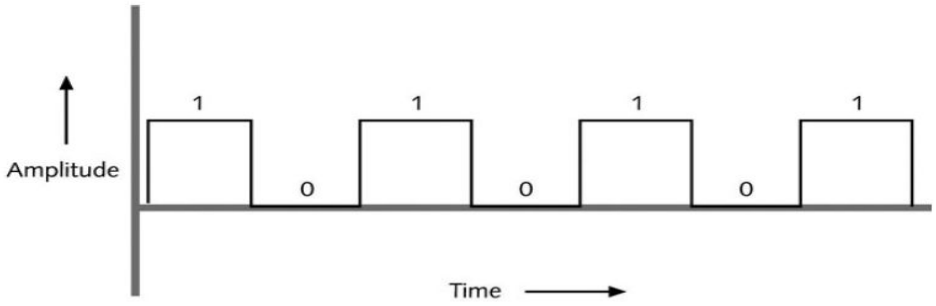


FIGURE 3-3 *An example of a digital signal*

نمایش نمادین یک سیگنال دیجیتال

تعریف میدان (Amplitude):

قدرت هر موج در هر نقطه از زمان را گویند.

تعریف فرکانس:

به تعداد تغییرات دامنه در یک واحد زمانی مشخص فرکانس گفته می‌شود.

Frequency:

The number of times that a signal's amplitude changes over a fixed period of time.
Expressed in cycle per second = (Hertz = Hz)

تعریف طول موج:

فاصله بین نقاط متناظر روی یک چرخه موج را طول موج می‌گویند و آن را با لاندا نمایش می‌دهند.

Wavelength:
The distance between corresponding points on a wave's cycle. (meter/feet)

نکته: هر قدر که فرکانس زیاد شود طول موج کم می‌شود.

مثال: یک موج رادیویی با فرکانس (Hz)۱۰۰۰۰۰۰ طول موجی معادل (M)۳۰۰ دارد. اگر فرکانس این موج به (Hz)۲۰۰۰۰۰۰ افزایش یابد، طول موج چقدر خواهد شد؟

پاسخ: ۱۵۰ متر

نکته: هر feet تقریبا ۳۰/۴۸ سانتی‌متر است.

نکته: چون سیگنال‌های Analog نسبت به سیگنال‌های Digital متغیرتر هستند می‌توانند ظرافت و کیفیت بالاتری ارائه دهند. مانند صدای انسان که آنالوگ است و صدای ضبط شده‌ای که روی کامپیوتر است.

سؤال: چرا از سیگنال Analog به صورت عمده استفاده نمی‌شود؟

پاسخ: زیرا ولتاژ دائما در سیگنال Analog تغییر می‌کند و این یعنی هزینه‌های بسیار برای تولید و دریافت این سیگنال‌ها. ضمن اینکه انتقال Analog به موانعی مثل نویز (Noise) و حتی باد و طوفان بسیار حساس است.

پالس‌های سیگنال Digital:

سیگنال Digital از دو پالس مختلف تشکیل شده است:

۱- پالس ولتاژ مثبت که نماد یک است.

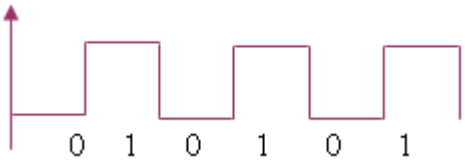
۲- پالس ولتاژ صفر(عدم حضور ولتاژ) که نماد صفر است.

تعریف سیستم‌های باینری (Binary) یا دودویی:

به سیستم‌هایی که کلاً بر اساس دو پالس صفر و یک هستند گفته می‌شوند.

نکته: به هر پالس یک بیت و به هر هشت بیت یک بایت گفته می‌شود.

مثال: موج زیر نمایانگر چه عدد ده‌دهی (Decimal) است؟



پاسخ: 010101 =16+4+1=21

نکته: برای ارسال اطلاعات، مثل یک ایمیل، این اطلاعات خیلی سریع به صفر و یک تبدیل می‌شوند.

ممکن است یک پیغام از میلیون‌ها صفر و یک تشکیل شده باشد.

مدولاسیون (Data Modulation):

مفهوم Data بیشتر با انتقال Digital مطرح می‌شود. اما گاهی نوع اتصال شما به یک شبکه طوری است که فقط می‌توانید از سیگنال Analog استفاده کنید. مثل اتصال به اینترنت از طریق خطوط تلفن قدیمی‌تر که آنالوگ بود (و نه ISDN) و یا امروزه، انتقال از طریق امواج رادیویی. (مثل شبکه‌های بی‌سیم، رادیو و تلویزیون)

بنابراین سیگنال‌های Digital که داخل کامپیوتر در جریان هستند، باید به Analog تبدیل شوند تا بتوان آن‌ها را از کامپیوتر خود به محیط انتقال واگذار کرد و ارسال کرد و در برگشت نیز سیگنال‌های Analog باید به Digital تبدیل شود تا برای کامپیوتر قابل فهم باشد.

این کار توسط Modem انجام می‌شود. واژه مودم مخفف کارهایی است که این دستگاه انجام می‌دهد:

Modem = Modulation /Demodulation

پس، «مدولاسیون داده» تکنولوژی‌ای است که **سیگنال‌های Analog** را طوری تغییر می‌دهد که برای انتقال **داده‌های Digital** روی یک مسیر ارتباطی آنالوگ مناسب باشند.

مدهای ارتباطی (Transmission Direction):

جهت‌های انتقال:

۱. Simplex (ساده و یک طرفه):

اگر بر روی یک مسیرِ انتقال، سیگنال‌ها فقط در یک جهت حرکت کنند، ارتباط را یک‌طرفه گویند؛ مانند: رادیو و تلویزیون.

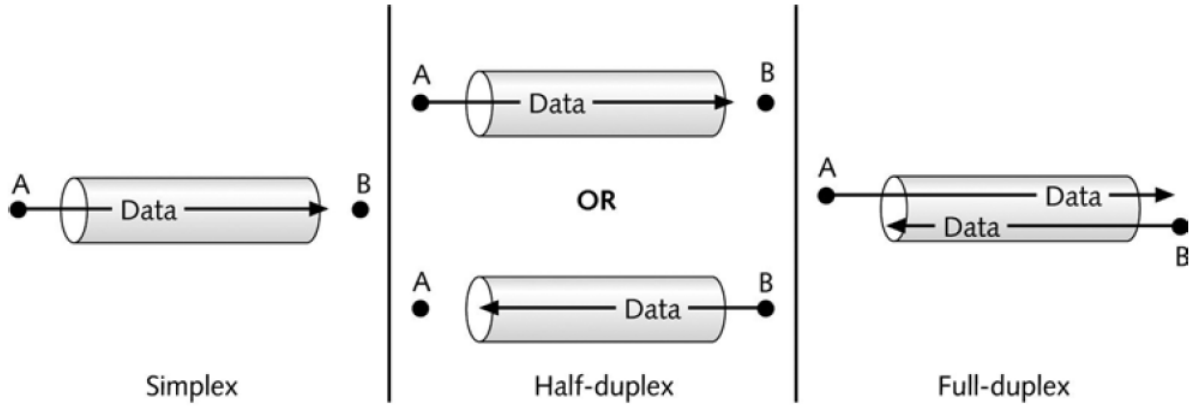
۲. Half-Duplex (نیمه-دوطرفه):

سیگنال‌ها در دو جهت حرکت می‌کنند اما در هر لحظه فقط در یک جهت؛ مانند: بی‌سیم‌های نظامی.

۳. Full-Duplex (دوطرفه):

سیگنال‌ها آزادند در هر لحظه در هر دو طرف حرکت کنند. (نام دیگرآن Bidirectional است)

معمولاً در شبکه‌ها Full-Duplex داریم (و گاهی اوقات هم Half-Duplex)



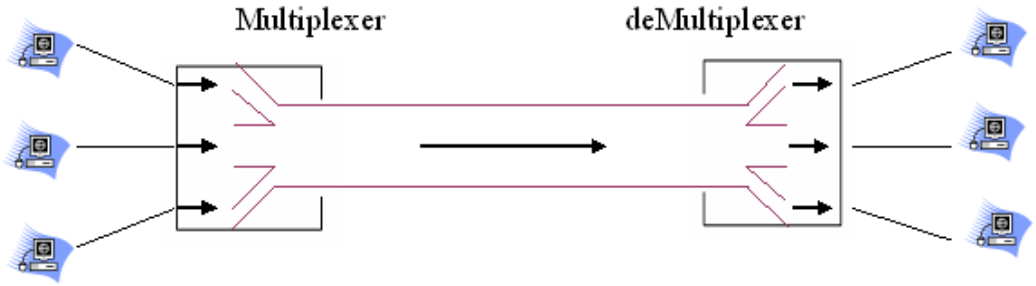
Multiplexing:

نوعی از انتقال است که اجازه حرکت چندین سیگنال را به صورت همزمان بر روی یک رسانه انتقال می‌دهد. سیم، هوا و فیبر نوری مهم‌ترین رسانه‌های انتقال هستند.

انواع مختلفی از Multiplex کردن وجود دارد که در هر نوع یک دستگاه به نام Multiplexer استفاده می‌شود. در طرف دریافت سیگنال از دستگاهی به نام DeMultiplexer استفاده می‌شود.

Multiplexer:

دستگاهی است که چندین سیگنال را ترکیب کرده و به طور همزمان در یک کانال ارتباطی ارسال می‌کند.



مشهورترین روش‌های Multiplex کردن:

1- TDM (Time Division Multiplexing)

مالتی پلکس کردن بر اساس تقسیم زمانی:

در این روش کانال ارتباطی به چندین شکاف زمانی (time-slot) تقسیم می‌شود و سپس هر slot به روش نوبت دهی چرخشی (Round-Robin(RR)) به یک کامپیوتر (node) نسبت داده می‌شود و در آن slot اطلاعات این node ارسال می‌شود.

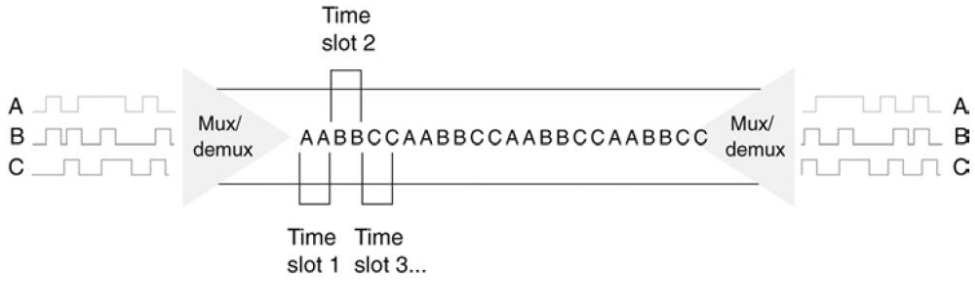
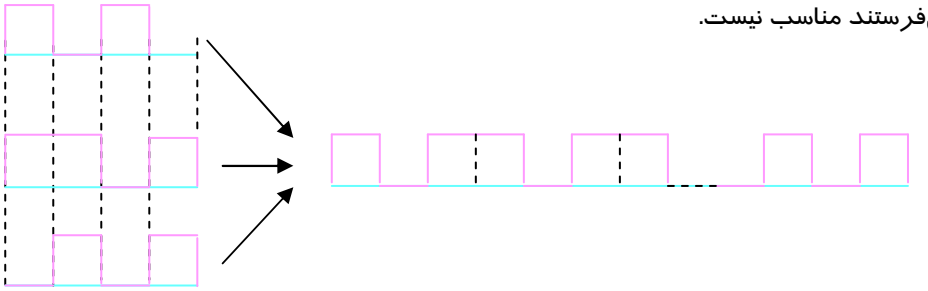


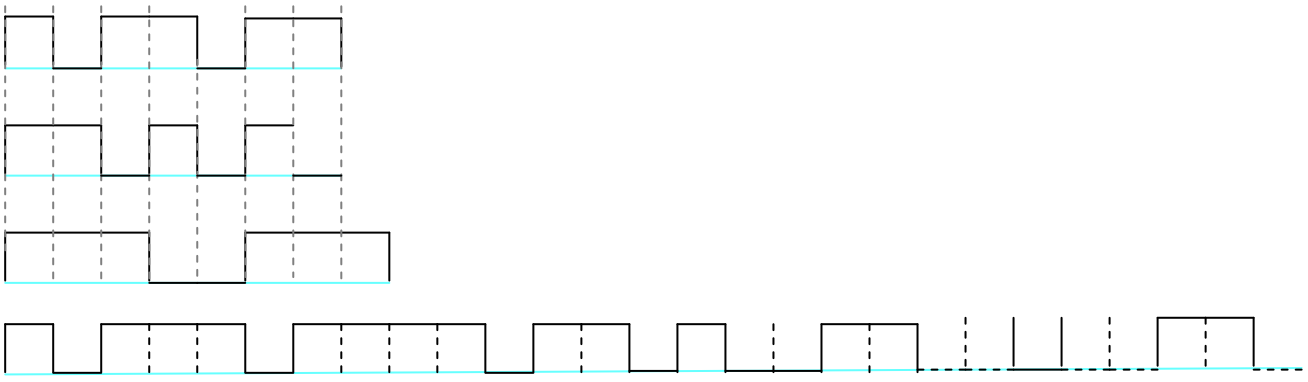
FIGURE 3-7 *Time division multiplexing*

اشکال TDM:

اگر یک node هیچ داده‌ای برای ارسال نداشته باشد در آن لحظه از کانال هیچ استفاده‌ای نمی‌شود پس برای شبکه‌ای که برخی nodeها به ندرت اطلاعات می‌فرستند مناسب نیست.



تمرین: سه سیگنال زیر قرار است به روش TDM از یک کانال ارتباطی عبور کنند. اگر برای هر سیگنال سه slot زمانی در نظرگرفته شود در کانال، شاهد چه سیگنالی خواهیم بود؟



پاسخ:

2- Statistical Multiplexing:

مالتی پلکس کردن به روش آماری:

این روش زیر مجموعه TDM است با این تفاوت که کانال را به برش‌های زمانی مساوی تقسیم نمی‌کنیم و پهنای ثابتی را برای هر کانال رزرو نمی‌کنیم بلکه بسته‌های داده‌ای (Data Packetهای) ایجاد شده توسط کاربران مختلف را که به صورت تصادفی ایجاد می‌شوند بر اساس اولویت و نیاز، بر روی خط قرار می‌دهیم. در شبکه‌های پیشرفته از این روش استفاده می‌شود.



FIGURE 3-8 *Statistical multiplexing*

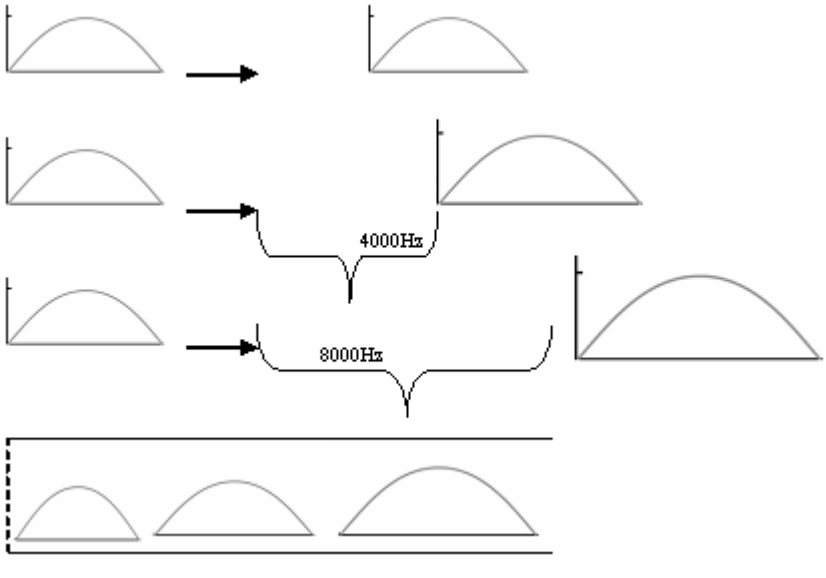
3- FDM (Frequency Division Multiplexing)

مالتی پلکس کردن بر اساس تقسیم فرکانسی:

در این روش ابتدا سیگنال‌های دیجیتال به آنالوگ تبدیل شده سپس فرکانس سیگنال‌هایی که همزمان بر روی یک رسانه انتقال قرار می‌گیرند با مقادیر مختلف (از ٤٠٠٠ به بعد) افزایش می‌یابند. مانند امواج رادیویی.

مقدار فاصله فرکانسی یا گاردباند (guard band) نیز برای جلوگیری از تداخل بین آن‌ها در نظر گرفته می‌شود.

در این حالت این سیگنال‌ها درحوزه فرکانس در باندهای فرکانسی جدا از یکدیگر و بدون مشکل در کنار هم قرار گرفته و ارسال می‌شوند و در مقصد به وسیله عمل Demodulation از یکدیگر جدا می‌شوند. دقیقاً مانند امواج رادیویی ایستگاه‌های مختلف که همگی در کنار یکدیگردر یک کانال ارتباطی (هوا) منتشر می‌شوند و بخش Tuner رادیوی شما قادر است موج دلخواه را از سایر امواج جدا کند.



4- WDM (Wavelength Division Multiplexing)

مالتی پلکس کردن بر اساس تقسیم طول موجی:

تکنولوژی‌ای است که در کابل‌های فیبر نوری استفاده می‌شود. با تغییر در فرکانسِ سیگنال‌ها، نورهای مختلف یعنی در حقیقت طول موج‌های مختلفی ایجاد می‌شود. روش WDM فیبرنوری را قادر می‌کند تا چندین نور با طول موج‌های متفاوت را به طور همزمان منتقل کند با استفاده از لیزر این نورها با هم ترکیب شده و در یک کانال ارسال می‌شوند. در مقصد، سیگنال‌ها از طریق طول موج‌های مختلف (رنگ‌های مختلف) از هم جدا می‌شوند. در روش‌های پیشرفته‌تر مانند DWDM یک کابل فیبرنوری می‌تواند به ۸۰ تا ۱۶۰ کانال تقسیم شود.

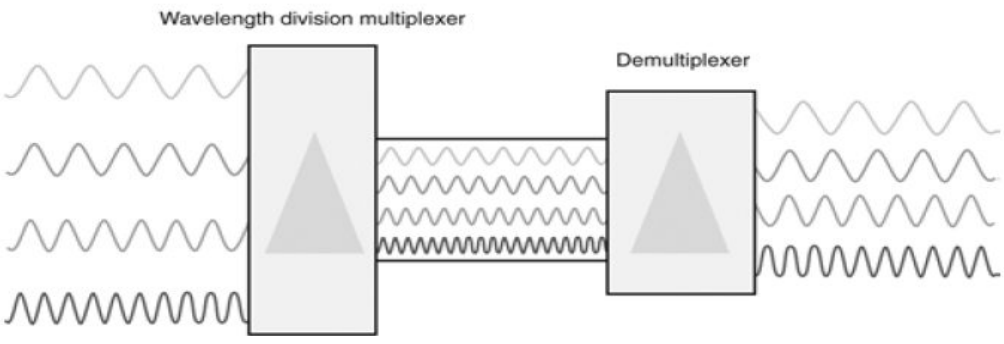


FIGURE 3-9 *Wavelength division multiplexing*

5- DWDM (Dense Wavelength Division Multiplexing)

نوع پیشرفته‌تر از WDM

انواع ارتباط بین Nodeها:

۱- Point-to-Point:

اگر در انتقال داده‌ها فقط یک ارسال کننده و یک دریافت کننده داشته باشیم گفته می‌شود نوع ارسال، نقطه به نقطه است. مانند اتصال مستقیم یک کامپیوتر به یک کامپیوتر دیگر و برداشت اطلاعات. که در این حالت ارسال کننده فقط اطلاعاتی را ارسال می‌کند که دریافت کننده نیاز دارد و از طرفی مهم است که آیا اطلاعات به مقصد رسید یا خیر!؟

۲- Broad Casting (انتشار گسترده):

در این نوع انتقال یک ارسال کننده و چندین دریافت کننده داریم. مانند ایستگاه TV که از طریق برج ارسال (Tower) به هزاران آنتن تلویزیون ارسال می‌کند بدون توجه به اینکه کدام دریافت کننده می‌تواند آن را دریافت کند. از این انتقال به دلیل سادگی و سرعت در شبکه‌های بسیاری استفاده می‌شود.

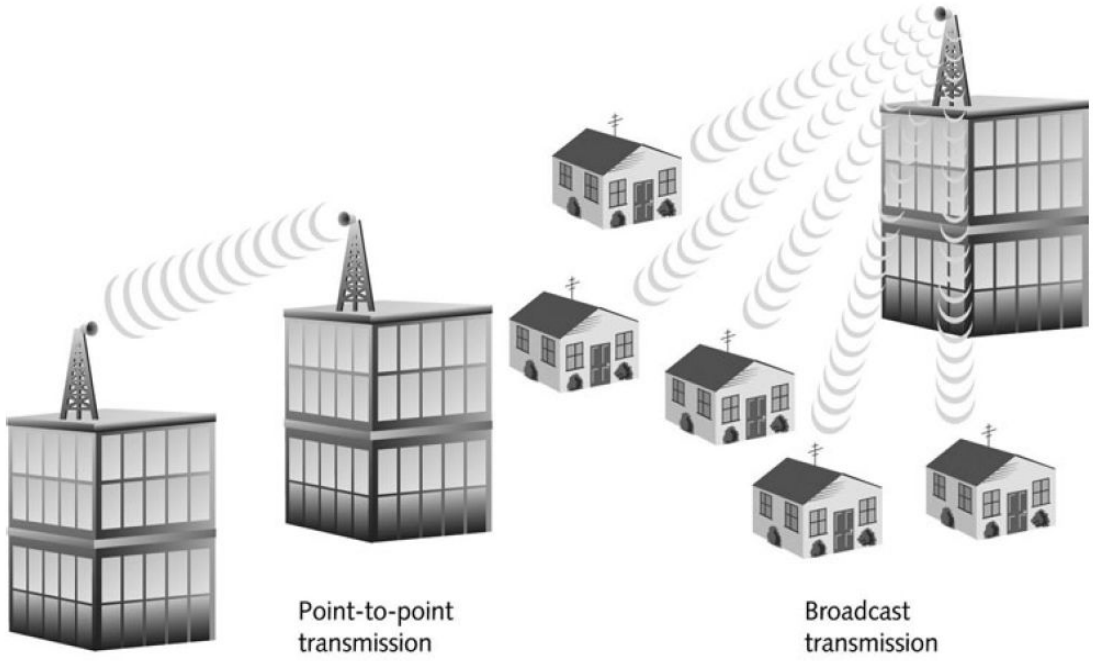


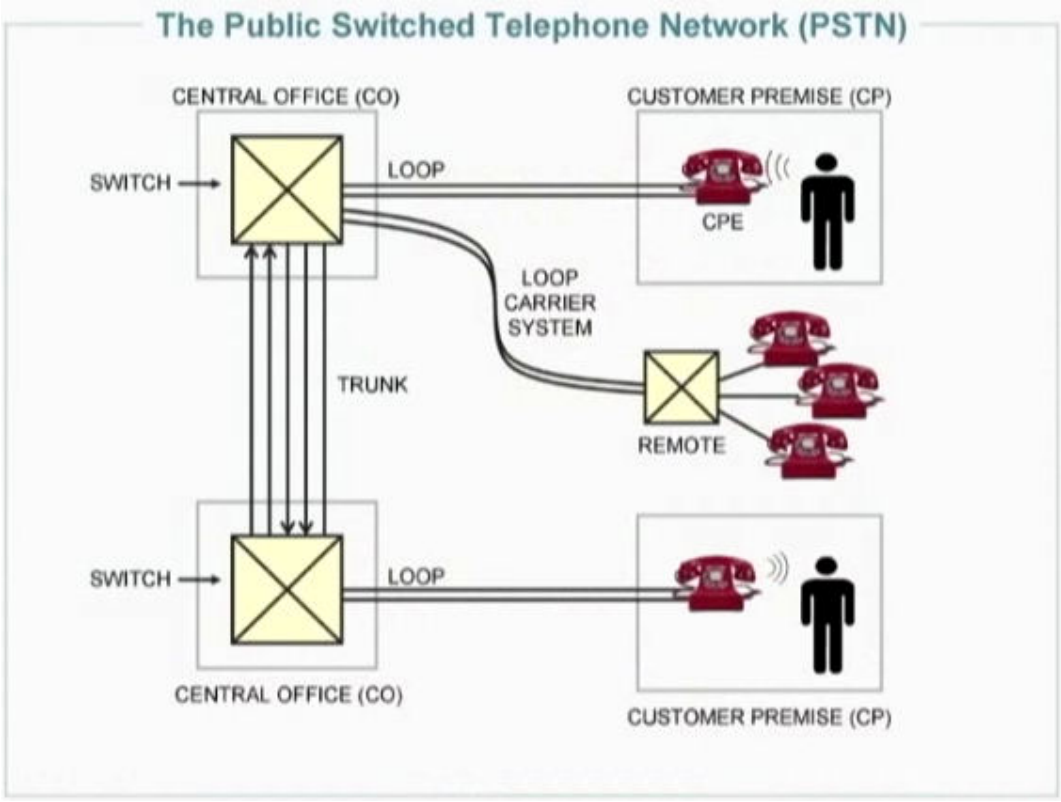
FIGURE 3-10 *Point-to-point versus broadcast transmission*

سوئیچینگ مداری
Circuit Switching

اتصالات بین تلفن‌ها به صورت سیستم مداری یا Circuit Switching است. یعنی قبل از اینکه کاربر شروع به تبادل داده کند، باید یک مدار اختصاصی (Dedicated Circuit) یا کانال برای او ایجاد شود.

شبکه PSNT یا شبکه تلفن سوئیچی عمومی (PSTN : Public Switched Telephone Network)

شکل کلی تماس کاربر و برقراری ارتباط با مخابرات:



تعریف Customer Premise (CP):

به محلی که تلفن کاربر قرار دارد در اصطلاح CP می‌گویند. (خانه یا اداره و...)

تعریف دفتر مرکزی (Central Office (CO)):

به محلی که سوئیچ‌های مخابرات قرار گرفته، دفتر مرکزی یا CO می‌گویند.

وقتی تماس برقرار می‌شود از طریق یک کابل به هم تابیده، اتصال کاربر با اداره مرکزی یا CO برقرار می‌شود. در CO یک سری سوئیچ وجود دارد که وظیفه شناسایی شما و مقصدتان را دارند.

تعریف حلقه (Loop):

کابلی که بین سوئیچ مخابراتی وCP کشیده شده است، تشکیل یک حلقه را می‌دهد. به این حلقه که با یک کابل به هم تابیده برقرار می‌شود Loop می‌گویند.

سؤال: چرا کلمه Loop ؟

چون وقتی کاربر گوشی تلفن را بر می‌دارید در حقیقت دو سر کابلی که بین خود و سوئیچ کشیده شده است را به یکدیگر متصل می‌کند و ولتاژهای مختلف روی آن ارسال می‌کند.

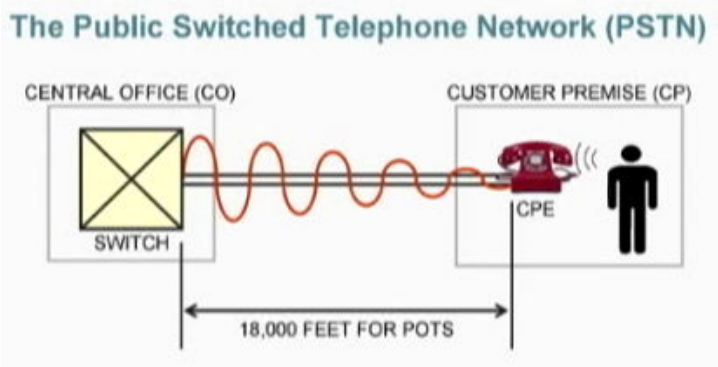
تعریف TRUNK :

حلقه‌ای که بین دو سوئیچ مختلف برقرار می‌شود در اصطلاح Trunk گفته می‌شود.

نکته: به این نوع مدارها که قبل از اینکه کاربر شروع به تبادل داده کند، باید یک مدار اختصاصی (Dedicated Circuit) یا کانال برای او ایجاد شود، در اصطلاح Circuit Switching گفته می‌شود.

تعریف POTS(Plain Ordinary Telephone Service):

سرویس تلفنی را که مخابرات به کاربران ارائه می‌دهد (سرویس تلفنی معمولی ساده) POTS گویند.



نکته: کابل اتصالات بین سوئیچ تا منزل یا جایگاه کاربر از جنس مس (Copper) است.

سؤال: چرا به جای مس از طلا یا نقره که رسانای بهتری است، استفاده نمی‌کنند؟

پاسخ: رسانایی طلا (Gold) خیلی قوی است اما گذشته از گران بودن آن، بسیار شکننده است و نمی‌توان آن را تغییر شکل داد و خمیده کرد. البته از طلا در ماهواره‌برها برای جاهای حساس استفاده می‌کنند.

نقره هم با اینکه رسانایی بالاتری نسبت به طلا دارد اما زود با اکسیژن هوا ترکیب شده و اکسید شده ودر نهایت سیاه می‌شود.

دلیل استفاده از مس:

مس اکسید نمی‌شود.

مس ارزان قیمت است.

مس حالت انعطاف‌پذیری دارد.

نقاط ضعف مس:

مس در مقابل عبور الکترون‌ها مقاومت دارد و حرارت تولید می‌کند. اگرجریان یا سیگنالی را از مس عبور دهیم، مس حرارت تولید کرده و داغ می‌شود و در نتیجه مسافتی که سیگنال را حمل می‌کند، کم می‌شود. یعنی سیگنال بعد از طی مسافتی در حدود 18000 feet یا ۳ مایل و یا ۵ کیلومتر (حداکثر طول یک کابل مس در تلفن شهری) افت پیدا کرده و ضعیف می‌گردد. به همین دلیل برای مسافت‌های طولانی از مس استفاده نمی‌کنند و از رسانه‌های جدید مثل فیبر نوری استفاده می‌کنند.

تعریف تضعیف سیگنال (Attenuation):

سیگنال ارسالی بر روی رسانه پس از مدتی به دلایل مختلف، از جمله: طی مسافت طولانی و یا تأثیر نویز بر روی رسانه، ضعیف شده و تغییر می‌کند. به این اتفاق در اصطلاح تضعیف گفته می‌شود.

ایده شرکت AT&T :

اختراع تلفن توسط آقای گراهامبل در سال ۱۸۷۶ بود. از آن زمان تاکنون محوطه‌های شهری (Suburb) کم کم پیشرفت کرد و مردم به اطراف شهر مهاجرت کرده و سکونت گزیدند. تا قبل از سکونت در محوطه‌های شهری، ایده آقای گراهامبل به این صورت بود که در هر محله به مسافت ۵ کیلومتر یک Central Office داشته باشیم تا مردم تلفن‌های ساده داشته و به CO محل خود متصل شوند و مثلاً کارمند CO، دو خانه را با کابل‌های ساده به هم متصل کند. در ۱۸۸۵ توسط ایده‌ای از شرکت AT&T (بزرگ‌ترین شرکت مخابراتی آمریکا که رئیس آن شخصی ایرانی است و در حدود 60 تا 70 درصد تلفن‌های آمریکا تحت نظر این شرکت است) این مراکز یعنی Local Central Office ها به هم متصل شدند. به طوری که فقط یک محله تلفن نداشته باشد بلکه همه COها به هم متصل شده و در نهایت کل یک شهر به هم متصل شوند.

اتصالات راه دور (Remote) :

سؤال: اگر بخواهیم مناطق دور شهر را به سوئیچ وصل کنیم چه کار باید کرد؟

می‌توان برای هر مشتری در دور دست، از کابل‌های ضخیم استفاده کردکه مقاومت کم گردد، که طبیعتاً مقرون به صرفه نیست. زیرا نمی‌توان کابل گران قیمت را فقط برای یک خانه و اتصال آن به مرکز مخابرات محلی، استفاده کرد.

در این حالت از Baby Switchها استفاده می‌کنند که شما آن‌ها را نقاط مختلف یک شهر در جعبه‌های بتنی در زیر زمین دیده‌اید. اگر درب آن‌ها را باز کنید داخل آن‌ها یک Box بتونی خیلی بزرگ و داخل Box هم یک سوئیچ بزرگ ولی کوچک‌تر از سوئیچ‌های CO هست.

در نهایت کابل‌ها از ضخیم کم‌کم نازک شده تا تبدیل به یک زوج سیم می‌شود و به منازل آورده می‌شود.

کم کم Baby Switch برداشته شده و از فیبر نوری استفاده می‌گردد.

فیبر نوری از نظر امکان صحبت تلفنی هیچ تفاوتی ندارد به هرحال کاربردارای تلفن خواهد بود ولی از نظر تکنولوژی‌های پیشرفته‌تر به مشکل برمی‌خوریم. به طور مثال روی فیبرنوری نمی‌توان DSL داشت.

مدارهای آنالوگ

(Analog Circuits)

آیا تا به حال از خود پرسیده‌اید که هنگام صحبت با تلفن، چگونه صدای من به همین صورت، به کیلومترها آن‌طرف‌تر منتقل می‌شود؟
برای آشنایی با آنچه در مخابرات و مدارهای آنالوگ می‌گذرد، باید با برخی مفاهیم آشنا شوید:

صدا یا Sound چیست؟

آیا تا به حال فکر کرده‌اید که تعریف صدا چیست؟

تا وقتی نتوانیم صدا را تعریف کنیم، نمی‌توانیم راهی برای انتقال آن بیابیم.

از نظر علمی، به فشرده شدن و باز شدن (جا به جا شدن و لرزیدن) مولکول‌های هوا **صدا** می‌گویند.

با این دیدگاه، اطراف ما پر است از Sound. از صدای پای یک مورچه بگیرید تا لرزشی که یک آنتن شبکه موبایلی در مولکول‌های هوا ایجاد می‌کند.

سؤال این است که چرا ما این نوع صداها را نمی‌شنویم؟

تعریف Audio یا Audible Sound:

گوش انسان فقط قادر به شنیدن Soundهایی است که فشرده شدن و باز شدن مولکول‌های هوا توسط آن‌ها، بین ۲۰ تا ۲۰۰۰۰ بار در ثانیه باشد. (این نوع Soundها را «صدای شنیدنی» یا Audible Sound می‌گویند).

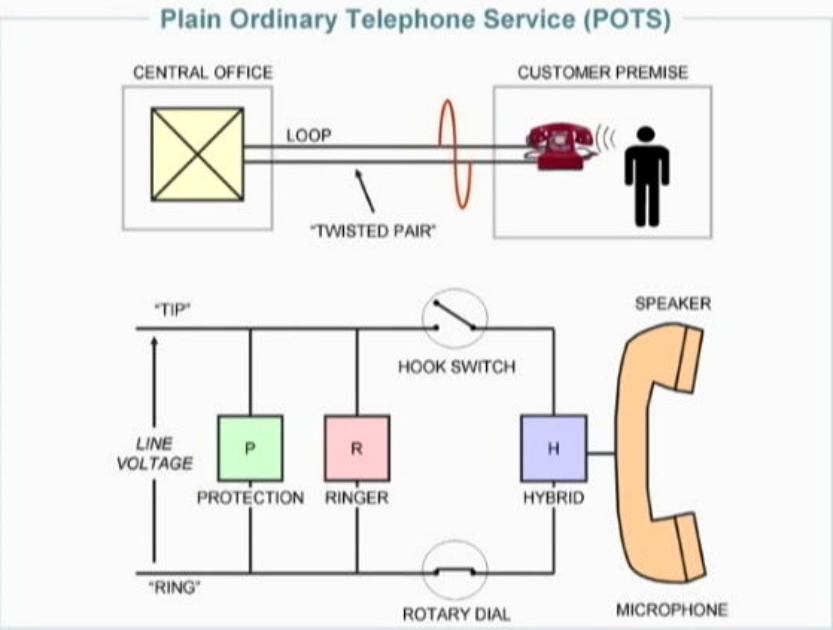
احتمالاً هنگام خرید، عبارت 20-20000Hz را بر روی کارتن ضبط صوت‌ها یا اسپیکرها دیده‌اید. حالا متوجه می‌شوید که این اعداد یعنی چه. (یعنی این بلندگو محدوده شنوایی گوش انسان را به طور کامل پشتیبانی می‌کند)

حالا می‌توانید بگویید چرا ما صدای تولیدی توسط یک آنتن موبایل را نمی‌شنویم! امواجی که یک آنتن به موبایل شما می‌فرستد، میلیون‌ها بار در ثانیه مولکول‌ها را جا به جا می‌کنند و همانطور که گفته شد، ما فقط ۲۰ تا ۲۰ هزار بار را می‌توانیم بشنویم.

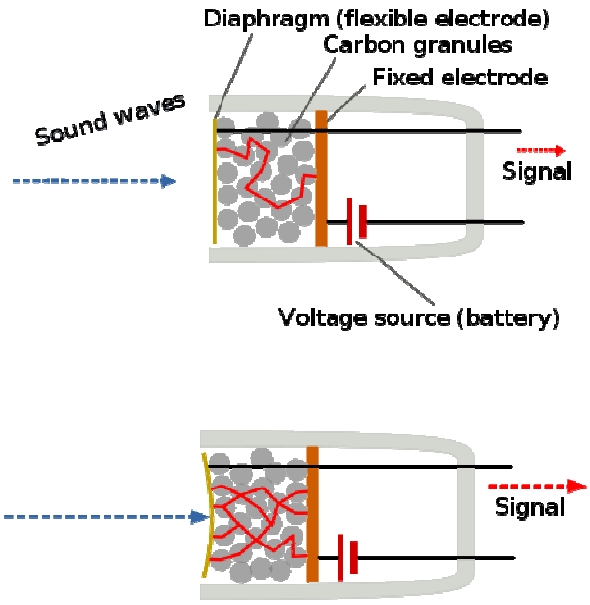
آزمایش: دست خود را کنار گوش خود بگیرید و خیلی آهسته (مثلاً ۲ بار در ثانیه) دستتان را بالا و پایین ببرید و خود را باد بزنید. طبیعتاً نباید صدایی از حرکت دست‌هاتان بشنوید. حرکت دست‌هاتان را تندتر کنید... خواهید دید که کم‌کم فشردگی و باز شدن مولکول‌های هوا به مرز شنوایی می‌رسد و شما صدای حرکت دست‌هاتان را می‌شنوید.

وقتی قبول کردید که صدا یعنی لرزش، حالا می‌توان راهی برای انتقال آن یافت:

اجزای تلفن:



تلفن دارای یک Speaker و یک Microphone است. آیا تا به حال به مکانیزم میکروفون و بلندگو فکر کرده‌اید؟



تصویری از یک میکروفون کربنی

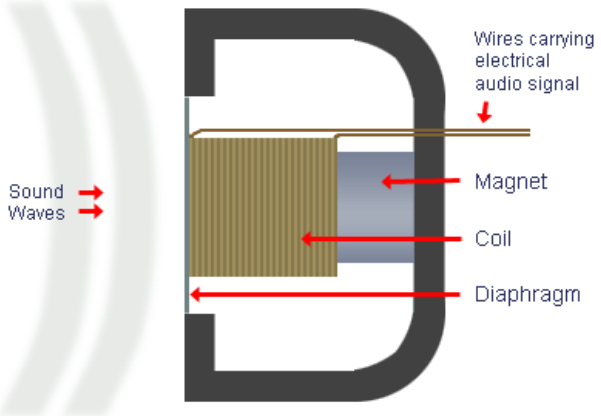
اگر به میکروفن‌های قدیمی‌تر (که به آن‌ها میکروفون کربنی یا Carbon Microphone گفته می‌شد) نگاه می‌کردید، می‌دیدید که این میکروفون دارای یک پرده کاغذی است که پشت آن قطعات ریز کربنی وجود دارد. وقتی شما صحبت می‌کنید، فشار صدای شما پرده را می‌لرزاند و این لرزش به قطعات کربن فشار وارد می‌کند. این فشار خاصیت‌های الکترونی کربن‌ها را بر اثر برخورد و نزدیکی به هم عوض می‌کند. مثلاً هرچه فشار وارده بیشتر باشد تغییر الکترون‌ها بیشتر و ولتاژی که به سیم متصل به میکروفون وارد می‌شود، بیشتر است. صداها و یا حرف‌های مختلف فشارهای مختلفی را ایجاد می‌کنند، پس در نتیجه ولتاژهای مختلفی را تولید می‌کنند.

اطلاعات بیشتر در مورد میکروفون‌های کربنی:

http://yourl.ir/carbon_mic
http://en.wikipedia.org/wiki/Carbon_microphone

توجه: همانطور که در تصویر زیر می‌بینید، در میکروفون‌های امروزی از یک آهن‌ربا و یک سیم‌پیچ برای تولید ولتاژ از روی صدا استفاده می‌شود.

Cross-Section of Dynamic Microphone



این ولتاژها به کابل منتقل شده و به تلفن مقصد می‌رسند. در تلفن مقصد، بلندگو کاری عکسِ کار میکروفون انجام می‌دهد. ولتاژهای مختلف دریافت شده و به قطعات کربنی و یا به سیم‌پیچ داده می‌شوند. هر چه ولتاژ بیشتر باشد، فشاری که این قطعات به پرده کاغذی درون بلندگو می‌آورند، بیشتر خواهد بود. بنابراین با ولتاژهای مختلف، میزان لرزش پرده نیز متفاوت است. (توجه کنید که به این نتیجه رسیدیم که صدا یعنی لرزش) و در نتیجه لرزش مولکول‌های هوا که در اطراف پرده هستند، متفاوت است. این لرزش‌ها به

تارهای صوتی داخل گوش ما رسیده و باعث لرزش آن‌ها می‌شود و مغز نیز هر نوع لرزشی را به کاراکتری تعبیر می‌کند. پس همان لرزشی که از صدای شما ایجاد می‌شد، در مقصد نیز همان لرزش ایجاد می‌شود، یعنی در حقیقت صدای شما بازتولید می‌شود.

تعریف فرکانس (Frequency):

در شبکه، بسیاری از کلمات هستند که در مباحث مختلف، معانی مختلفی دارند. فرکانس یکی از آن‌هاست.

فرکانس در مباحث مختلف تعاریف مختلفی دارد. اما در کل، تعریف عمومی آن Cycles Per Second یعنی تعداد تکرار یک چرخه در واحد زمان (معمولاً یک ثانیه) است.

در بحث صدا، به تعداد لرزش‌هایی که یک Sound در واحد زمان (ثانیه) در مولکول‌های هوا ایجاد می‌کند، فرکانس گفته می‌شود. واحد اندازه‌گیری فرکانس، Vibrations Per Second (تعداد لرزش در ثانیه) است که چون آقای هرتز آن را تعریف و ابداع کرد، به احترام وی واحد آن را هرتز گذاشتند و با Hz نمایش می‌دهند.

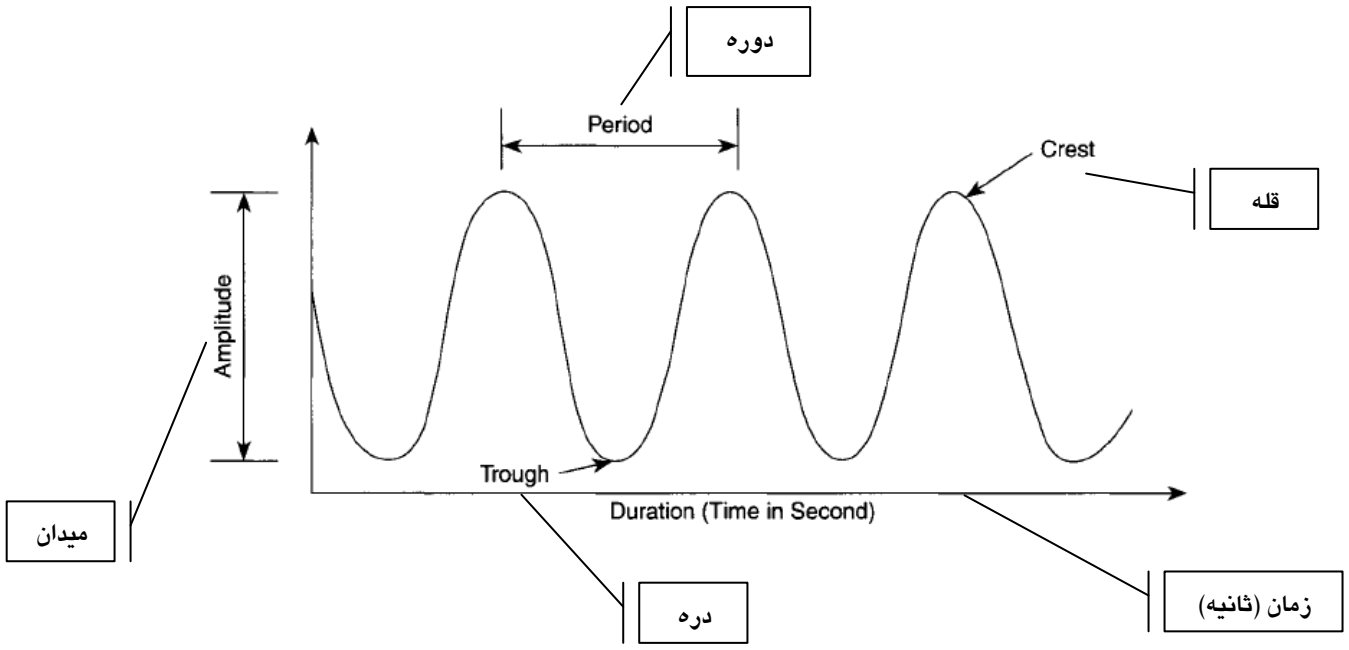
پس، حالا متوجه می‌شوید وقتی گفته می‌شود **صداهای مختلف، فرکانس‌های مختلفی دارند** یعنی چه. «س»ای که شما تلفظ می‌کنید، یک فرکانس خاص دارد و با «س»ای که شخص دیگری تلفظ می‌کند از نظر فرکانسی متفاوت است.

تعریف فرکانس در بحث انتقال آنالوگ:

در بحث الکترونیک و انتقال صدا یا داده از طریق کابل، هر گاه گفته می‌شود فرکانس، یعنی تعداد تغییرات ولتاژ بر روی کابل در یک ثانیه.

از آنجا که مقدار (یا Value) یا شدت صدا در هر لحظه متفاوت است (گاهی کم و گاهی زیاد) و در نتیجه مقدار ولتاژ روی کابل نیز در هر لحظه متغیر می‌شود، برای نمایش نمادین صدا بر روی کابل (در قالب ولتاژ)، از یک موج سینوسی استفاده می‌کنند و آن را «آنالوگ» می‌نامند. (کلمه Analog از کلمه Analogous به معنی نماد گرفته شده است)

بد نیست با برخی از اجزای موج صدا آشنا شویم:



Voice Band و Bandwidth:

به دلیل محدودیت‌های فیزیکی نمی‌توان بر روی رسانه‌های انتقال کمتر از یک حد خاص و یا بیشتر از حد خاصی فرکانس ارسال کرد.

البته گاهی اوقات نیز نمی‌خواهیم یعنی لازم نداریم که کمتر از حد خاصی و یا بیشتر از حد خاصی فرکانس روی یک رسانه قرار دهیم. با توجه به این واقعیت، می‌توان دو مفهوم «باند صدا» و «پهنای باند» را تعریف کرد:

تعریف Voice band:

به بیان پایین‌ترین حجم فرکانس و بالاترین حجم فرکانس که روی یک کابل ارسال می‌شود، Voice band گویند.
آقای گراهامبل Voice band تلفن شهری را بین 300 تا 3300 هرتز تعیین کرد که تا به امروز نیز همین مقدار است.
توجه: اگر یک کاراکتر مثل «س» فرکانس بالایی داشته باشد وکابل نتواند آن را عبور دهد، فرکانس کاراکتر را پایین می‌آورند.

سؤال: با توجه به اینکه فرکانس حروفی مثل «س» بیش از ۳۳۰۰ هرتز است، چرا Voice band تلفن شهری را بیشتر از ۳۳۰۰ هرتز در نظر نمی‌گیرند؟
سؤال: آیا کابل‌ها بیش از ۳۳۰۰ هرتز حجم ندارند؟
خیر. اینکه کابل‌ها حجم ندارند درست نیست. زیرا DSL از یک میلیون بار (1M Bit) تا دو میلیون بار (2M Bit)، لرزش یا Vibration روی کابل‌ها ایجاد می‌کند، پس می‌شود.
سؤال: آیا گوش انسان بیشتراز این نمی‌شنود؟
خیر. زیرا حجم صدایی که انسان می‌شنود از 20 تا 20000 Hz است. یک گوش معمولی تا 7000 یا 8000 Hz را می‌شنود.

پس چرا بیش از ۳۳۰۰ فرکانس روی کابل نمی‌فرستند تا کیفیت بهتر شود؟
جواب: چون اولاً: تولید فرکانس بالا هزینه‌بر است.
ثانیاً نیازی نیست. هم اکنون شما با این فرکانس مشکل خاصی در فهم مکالمات ندارید.

تعریف پهنای باند (Bandwidth) :

پهنای باند نیز در مباحث مختلف معانی درست و غلط زیادی دارد، اما معنی Original یا اصلی آن عبارت است از:
به بالاترین حد فرکانس ارسال شده روی یک رسانه منهای پایین‌ترین حد فرکانس ارسال شده، پهنای باند آن رسانه گفته می‌شود.
پهنای باند معیاری برای‌اندازه گیری **ظرفیت کانال (Channel Capacity)** است.
پس، پهنای باند و ظرفیت کانال تلفن شهری 3300-300=3000 Hz است.
این استاندارد از زمان گراهامبل تا کنون به همین صورت است.

سؤال: به کابل‌های تلفن (و شبکه) در اصطلاح Twisted Pair یا زوج سیم به هم تابیده گفته می‌شود.
سؤال این است که چرا کابل‌های تلفن را به هم می‌تابند؟

اگر به آنتن‌های سنتی تلویزیون‌ها دقت کنید، آنتن دارای دو بخش حلقوی (UHF) و خرگوشی (VHF) است. بخش UHF یک حلقه یا Loop ایجاد می‌کند و امواج هوا را در حلقه گیر می‌اندازد و به کابل منتقل می‌کند. آنتن‌هایی که حلقه یا Loop آن‌ها بزرگ‌تر است دارای UHF قوی‌تر و صاف‌تری هستند. پس یعنی هر چه Loop بزرگ‌تر، سیگنال‌های دریافتی، بیشتر.



در تلفن مشکل این جاست که وقتی گوشی تلفن را برمی‌دارید، در حقیقت یک حلقه بین تلفن شما و مخابرات ایجاد می‌شود که قطر آن به طور مثال، ۵ کیلومتر است!! حالا می‌توانید حدس بزنید در این حلقه چه اتفاقی می‌افتد! بله، این حلقه همه امواج هوا را می‌گیرد

و به گوش ما می‌رساند!! به محض اینکه گوشی را بردارید، فقط صدای خش خش است که می‌شنوید و حتی ممکن است این مشکل، ما را دچار برق گرفتگی کند. به همین دلیل کابل‌ها را به هم می‌تابند تا دو کابل به هم تابیده شده، میدان‌های مغناطیسی یکدیگر را خنثی کنند. در این صورت Loopهای کوچکی در اطراف سیم‌ها ایجاد می‌شوند، اما آنقدر کوچک هستند که نویز خاصی را به خود جذب نمی‌کنند.

نکته: ولتاژ کابل تلفن 48- ولت است و چون خیلی خطرناک است آن را از سوئیچ تا منزل کاربر به 10- ولت می‌رسانند.
سؤال: چرا ولتاژ منفی؟
تجربه نشان داده که ولتاژ مثبت، باعث سریع‌تر اکسید شدن کابل مسی می‌گردد و به مرورآن را از کار می‌اندازد.

ادامه بحث اجزای تلفن:

بخش Protection (محافظت) در گوشی تلفن:

بخش محافظت تلفن است که اگر موج شدیدی به تلفن وارد شود (به طور مثال به دلیل رعد و برق) این بخش روی مدار شما فعال شده و موج را به مخابرات برمی‌گرداند. در مخابرات هم بخش یک محافظت هست که در آن کابلی از سوئیچ متصل به زمین است که موج را به زمین منتقل می‌کند.

بخش Ringer یا همان زنگ تلفن:

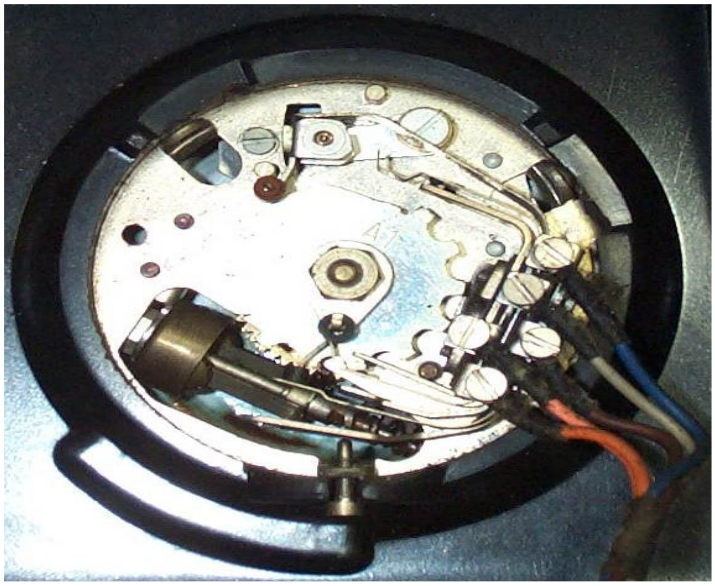
تلفن شما چطور زنگ می‌خورد؟
به طور معمول، ولتاژ روی کابل، ۱۰ ولت است. زمانی که سوئیچ مخابرات تشخیص داد که شخصی شماره تلفن شما را گرفته است، برای ۲ ثانیه ولتاژ کابل شما را بالا می‌برد و سپس ٤ ثانیه صبر می‌کند. مجدداً ۲ ثانیه ولتاژ را بالا می‌برد و ٤ ثانیه صبر می‌کند. این روال آنقدر ادامه پیدا می‌کند تا شما گوشی را بردارید.
زنگی که در گوشی تلفن به کار گرفته می‌شود، با ولتاژ ۱۰ فعال نمی‌شود، اما زمانی که در آن ۲ ثانیه ولتاژ بالا رفت، حالا زنگ با آن ولتاژ کار به کار می‌افتد و صدا تولید می‌کند.

پس یک نکته ایمنی:

اگر با کابل تلفن کار می‌کنید، مواظب باشید کسی شماره شما را نگیرد! چون در آن ۲ ثانیه، ولتاژ بالاتر از حد عادی است و ممکن است کمی شما را بلرزاند!! ☺

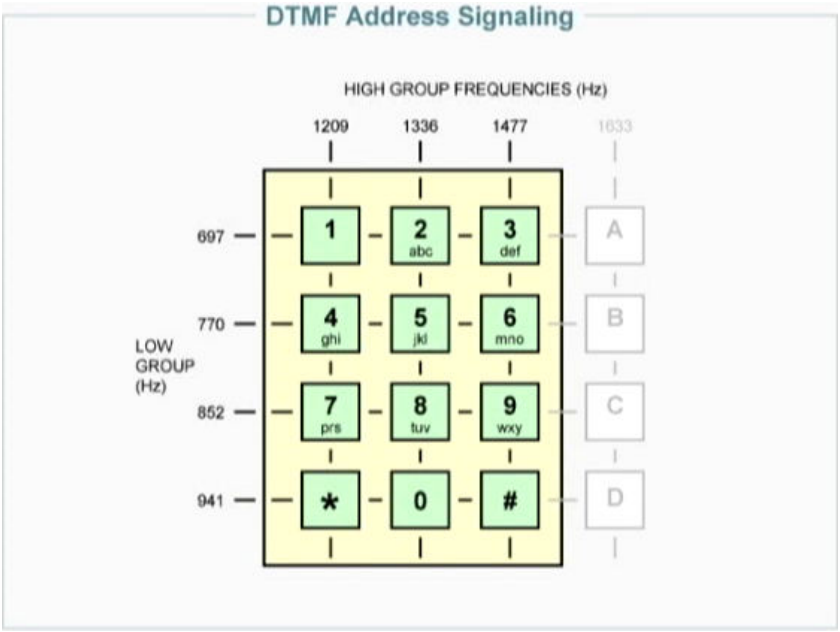
سوئیچ‌های درون تلفن:

در تلفن یک سوئیچ همیشه بسته (Rotary Dial) و یک سوئیچ همیشه باز (Hook Switch) وجود دارد. زمانی قصد شماره گیری دارید، به محض برداشتن گوشی، Hook Switch بسته می‌شود وLoop بین شما و مخابرات برقرار می‌شود.
حالا تا چند ثانیه مدار در اختیار شماست و زمان شماره گیری است. **شماره گیری یعنی قطع و وصل کردن مدار**، همین! (و قطع و وصل کردن مدار یعنی تولید **پالس**) یعنی شما بدون وجود تلفن هم می‌توانید شماره گیری کنید. فقط کافی‌ست چند ثانیه کابل‌ها را به هم متصل کنید تا لوپ برقرار شود، سپس برای گرفتن عدد دلخواه، به همان تعداد کابل‌ها را سریعاً جدا کرده و مجدداً به هم بچسبانید. (بعد از کمی تمرین، خواهید توانست شماره دلخواهتان را بدون تلفن بگیرید)
در تلفن‌های قدیمی اگر یادتان باشد، زمانی که شماره گیر را می‌چرخاندید تا مثلاً شماره ٤ را بگیرید در هنگام برگشت دایره، چهار بار صدای تق تق می‌شنیدید. علت آن این است که برآمدگی‌ای که داخل آن دایره وجود دارد، باعث می‌شود ٤ بار سوئیچ Rotary Dial باز شده و دوباره متصل شود و این به سوئیچ مخابرات می‌فهماند که منظور من شماره ٤ است. سوئیچ چند ثانیه صبر می‌کند تا شما دوباره با قطع و وصل کردن مدار، عدد بعدی را به او بگویید و این روال ادامه می‌یابد تا تمام شماره‌ها را بگیرید. (از آن‌جا که هر دو سوئیچ کار مشابهی انجام می‌دهند، یعنی قطع و وصل کردن مدار، در تلفن‌های جدید به جای دو سوئیچ از یک سوئیچ استفاده شده است)



تصویری از داخل یک شماره‌گیر تلفن

DTMF(Dual Tune Multiple Frequency):



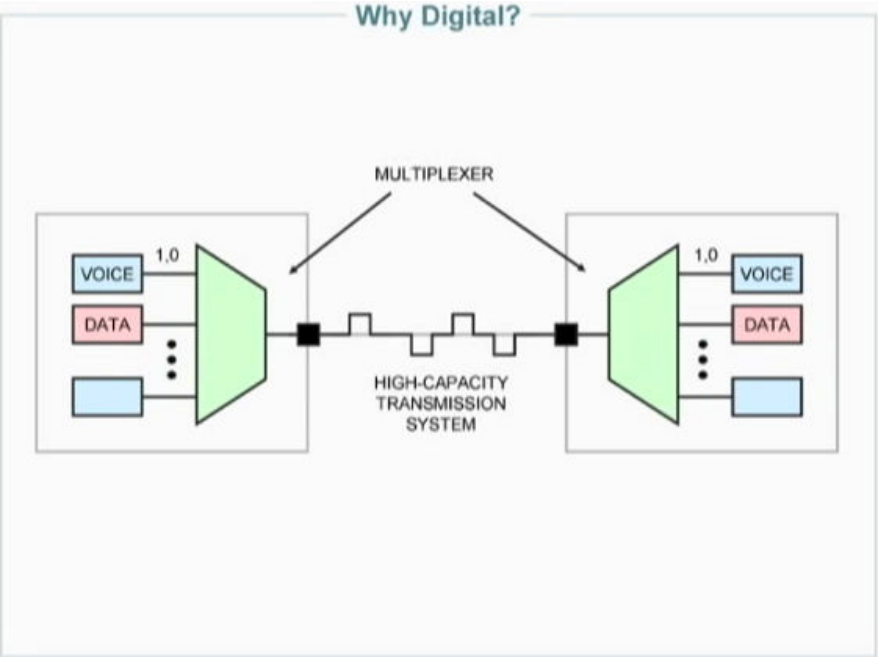
اگر بخواهید با تلفن‌های بدون دایره شماره گیری، کارکنید باید برای هر شماره یک Tuner یا تولید کننده پالس داشته باشید. به طور مثال برای شماره ۳ باید سه Tuner داشته باشید. اما شرکت AT&T ایده‌ای را ارائه داد که به DTMF معروف شد. ایده به این صورت است که به هر شماره یک عدد اختصاص دهیم. مثلاً به جای اینکه ۱۲ تا تولید کننده پالس داشته باشیم ۷ تا در نظر بگیریم یعنی (صرفه جویی در پول) و برای هر شماره همزمان این دو را ارسال کنیم. مثلاً اگرعدد یک را فشار دهیم به طور همزمان فرکانس ۶۹۷ و ۱۲۰۰ ارسال می‌شود. در مخابرات هم به ۷ تا جداکننده (یا Tuner Detector) بیشتر نیاز نداریم. پس طبق این ایده به جای اینکه ۱۲ تا تولید کننده و دریافت کننده پالس داشته باشیم برای هر شماره به طور همزمان دو فرکانس را ارسال می‌کنیم. در نتیجه در مخابرات هم به ۷ جدا کننده بیشتر نیاز نداریم.

مدارهای دیجیتال

(Digital Circuits)

دنیا در حال گذر از آنالوگ به دیجیتال است. اما چرا؟

چرا در خطوط تلفن باید سیگنال Analog را به Digital تبدیل کرد؟



برتری‌های دیجیتال نسبت به آنالوگ:

۱- ظرفیت بالای مدارهای دیجیتال و امن بودن در برابر نویز (Circuit Density):

با دیجیتال شدن خطوط، می‌توان فرکانس‌های بسیار بالاتری بر روی کابل ارسال کرد. (به طور مثال سرعت خط دیجیتال ADSL و خطوط آنالوگ قدیمی را مقایسه کنید!)

۲- کشف و عیب یابی خطا (Error Performance):

سیگنال Analog با سپری کردن مسیر، تضعیف می‌شود. شاید بگویید می‌توان برای تقویت آن از دستگاهی به نام Amplifier (آمپلی فایر) استفاده کرد اما دقت کنید که با این کار، نویز هم تقویت می‌شود. (مثل اینکه یک صدای خش دار را با بلندگو پخش کنیم، صدای خش خش آن نیز تقویت می‌شود)

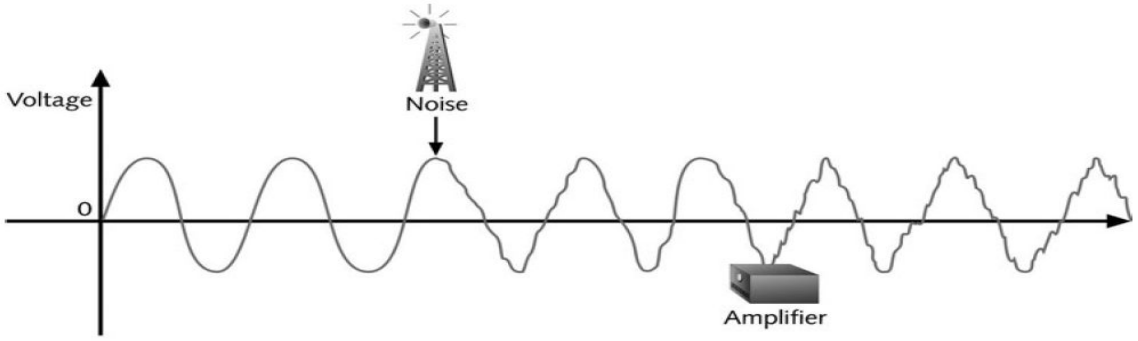


FIGURE 3-12 *An analog signal distorted by noise and then amplified*

یعنی در دیجیتال، تضعیف نداریم؟

چرا، سیگنال Digital نیز تضعیف شده و نویز می‌گیرد، اما برای ما چه اهمیتی دارد؟ یادتان هست که دیجیتال یعنی «بودن یا نبودن» (همان 0 و 1). اگر در کابل ولتاژی بود، یعنی 1 و اگر نبود، یعنی 0.

مهم این است که ما برای فهماندن 1، فقط کمی ولتاژ به تکرارکننده (Repeater) برسانیم حالا چه بدون نویز و قوی و چه با نویز و ضعیف! تقویت‌کننده به محض اینکه آن ولتاژ را دریافت کرد، متوجه می‌شود که این، همان ۵۰ ولت ابتدای مسیر یا همان عدد 1 بوده است و اگر دریافت نکرد، یعنی 0 بوده است. پس، وقتی قصد دارد آن را دوباره تولید کند، خودش به جای ولتاژ ضعیف شده، ولتاژ کامل (یعنی مثلاً همان ۵۰ ولت) تولید می‌کند و به جای ولتاژ 0 هیچ ولتاژی نمی‌فرستد. (متوجه شدید چه ایده ساده و جالبی‌ست؟)

تحقیق:

در مورد تلویزیون دیجیتال تحقیق کنید. چطور است که این نوع تلویزیون‌ها کیفیت بهتری را ارائه می‌کنند؟

می‌توانید متوجه شوید که مهم‌ترین مزیت Digital، کشف آسان خطاها و اصلاح آن‌هاست.

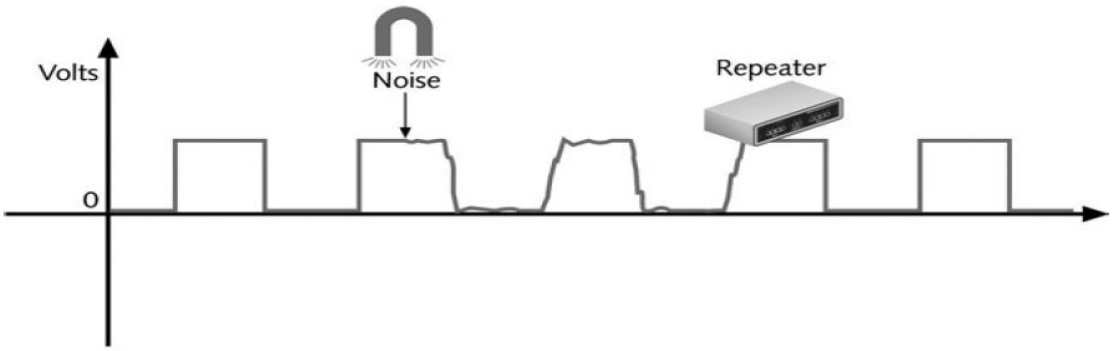


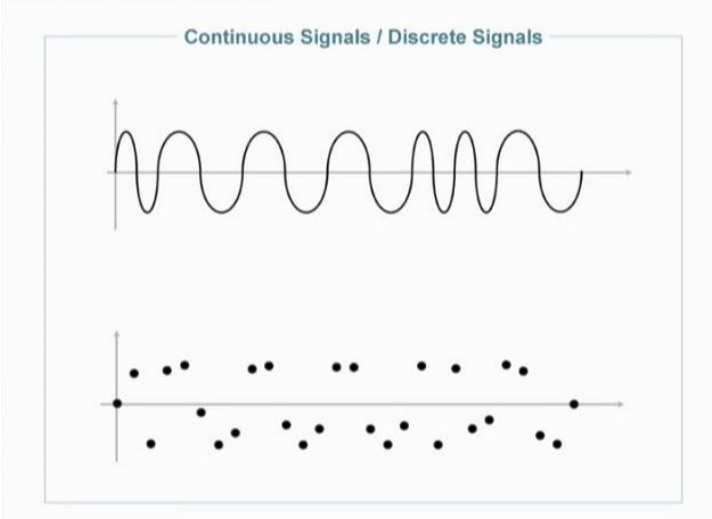
FIGURE 3-13 *A digital signal distorted by noise and then repeated*

۳- یکپارچگی سرویس‌ها (Integration Of Services) :

روی مدارهای Analog فقط می‌توان یک نوع اطلاعات را ارسال کرد مثلاً فقط Voice. اما با استفاده از Digital می‌توان انواع اطلاعات و سرویس‌ها را ارائه کرد. از سرویس‌های قابل ارائه توسط Digital می‌توان Data، Voice، Video را نام برد. (فکس، ویدئو کنفرانس، صدا و ... از طریق خطوط دیجیتال به راحتی ممکن است)

۴- پردازش (Processing) :

زمانی که داده‌ها تبدیل به کدهای 1 و 0 شدند توسط CPU قابل پردازش می‌گردند. از پردازش‌های انجام شده توسط Digital می‌توان Sound Recognition و Speaker Recognition را نام برد.



نکته: سیگنال‌های Analog به هم پیوسته و ادامه دار (Continuous) هستند یعنی در هر لحظه از زمان یک مقدار سیگنال را داریم ولی سیگنال‌های Digital گسسته (Discrete) هستند.

وقتی پی بردیم که دیجیتال بهتر از آنالوگ است، حالا باید دید چطور آنالوگ را تبدیل به دیجیتال می‌کنند.

سه گام تبدیل سیگنال Analog به سیگنال Digital :

۱- تدریج (Quantization) :

در این گام مقدار بالا و پایین یک موج را در محور Value در نظر می‌گیرند، یعنی محدوده مقادیری که یک سیگنال ممکن است داشته باشد در نظرگرفته می‌شود و به Levelها یا سطوح مختلفی (مساوی) تقسیم می‌شوند.

سپس هر مقدار از سیگنال که در یک قسمت قرار دارد، شماره آن قسمت را به خود اختصاص می‌دهد.



۲- نمونه برداری (Sampling) :

در این گام زمان به قطعات مساوی تقسیم می‌شود و هر نقطه از سیگنال که در آن واحد از زمان قرار دارد Value مربوط به خـود را کسب می‌کند. در حقیقت نقاط تقاطع با سیگنال، روی یک Level می‌افتد وآن Level را به آن نقطه اختصاص می‌دهند.



۳- تبدیل اعداد هر نمونه به کدهای 0 و1 (Coding) :

واضح است که بر روی خطوط دیجیتال فقط 0 و 1 می‌توان ارسال کرد (بودن یا نبودن ولتاژ) پس باید اعداد مربوط به هر نمونه به باینری (دو-دویی) تبدیل شوند تا بتوان آن‌ها را از طریق بودن یا نبودن ولتاژ، به آن طرف کابل منتقل کرد.

در این گام مقادیر مربوط به نقاط، به باینری (Binary) تبدیل می‌شوند:



پس از اینکه مشخص شد در هر لحظه از زمان موج چه مقداری داشته و مقادیر نیز به دیجیتال تبدیل شدند، حالا می‌توان آن‌ها را از طریق کابل منتقل کرد.

در آن طرف، برای فهم صدای شما توسط مخاطب، سیگنال دیجیتال باید به سیگنال آنالوگ تبدیل شود.

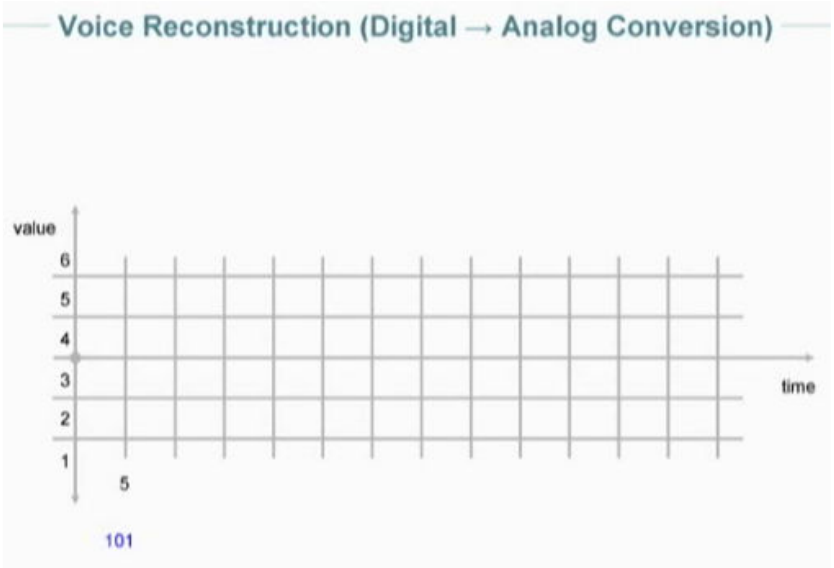
دو گام تبدیل سیگنال Digital به سیگنال Analog:

۱- تبدیل اعداد باینری (Binary) به دسیمال (Decimal) و پیدا کردن نقاط:

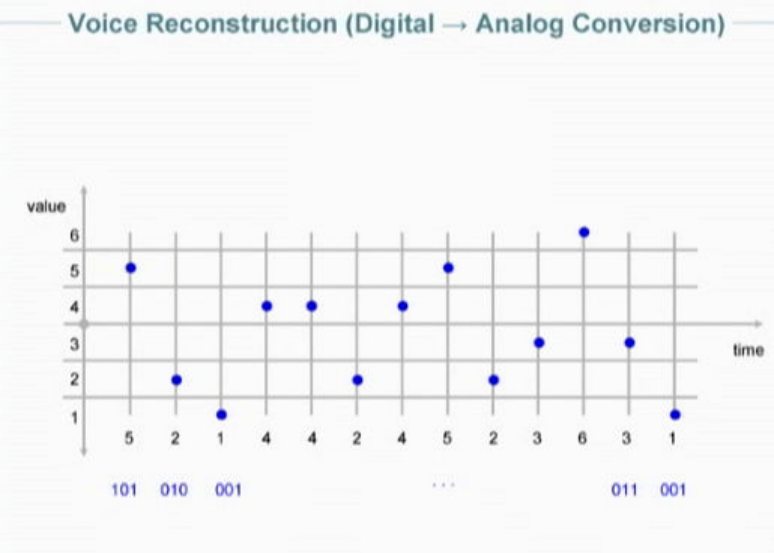
در این مرحله، مودمی که مسؤول تبدیل دیجیتال به آنالوگ است، منتظر دریافت اعداد باینری است.

دقت کنید که در بحث انتقال، همیشه باید مقدار زمان انتظار برای دریافت یک پالس مشخص باشد. به طور مثال باید بین فرستنده و دریافت کننده تعیین شده باشد که هر یک میکروثانیه یک پالس می‌آید.

مودم پس از دریافت دیجیتال‌ها، آن‌ها را به ده‌دهی (Decimal) تبدیل می‌کند و در سطح مربوطه در محور Value یک نقطه را در نظر می‌گیرد.



عدد 101 دریافت شده است



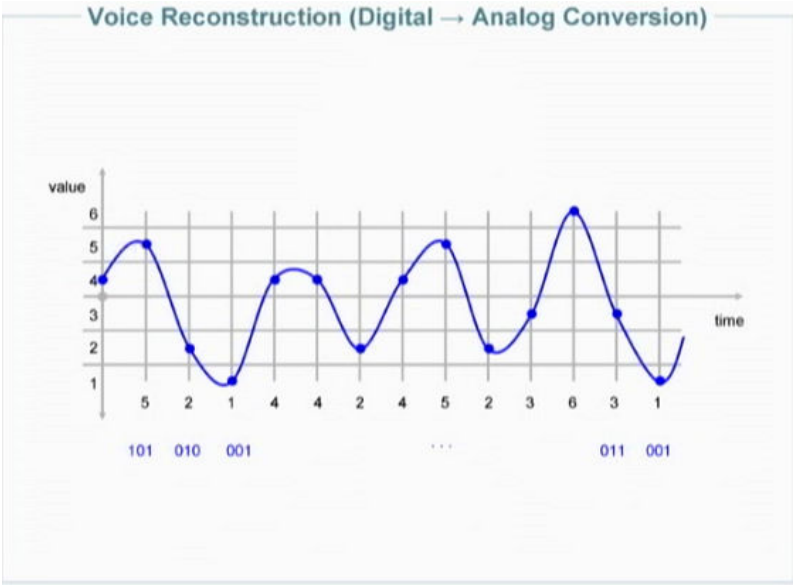
نقطه معادل اعداد باینری روی سطوح مختلف ترسیم شده است

۲- متصل کردن نقاط به یکدیگر:

پس از به دست آمدن نقاط، کافی‌ست آن‌ها را به هم متصل کنیم تا موجی دقیقاً مثل سیگنال اول تولید شود. (دقت کنید که وقتی گفته می‌شود نقاط به هم وصل شوند، در عمل منظور این است که ولتاژهای مختلف بین دو نقطه تولید شود و روی کابل ارسال شود)

دقیقاً مثل سیگنال اول؟

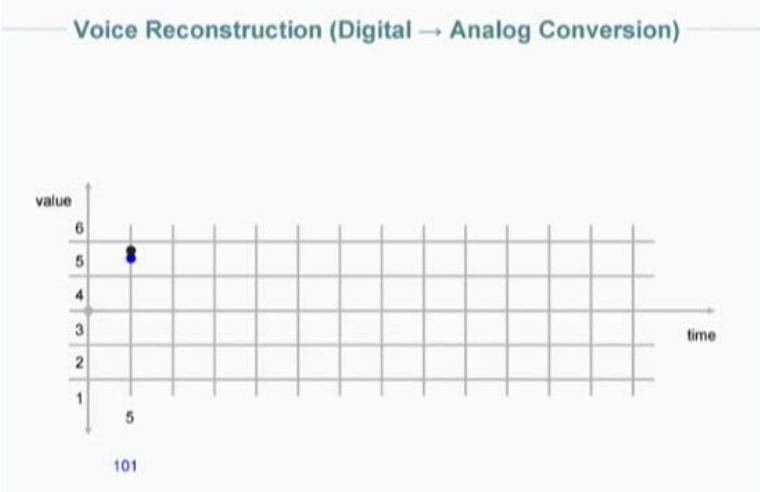
آیا این عبارت درست است؟ یعنی آیا سیگنال نهایی دقیقاً مثل سیگنال اول خواهد بود؟



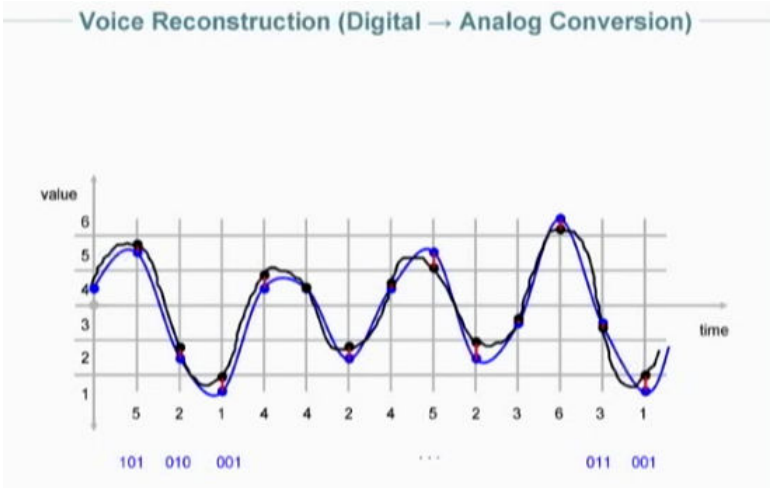
خطای تدریج (Quantization Error) :

همانطور که اکنون میدانید، در تبدیل سیگنال آنالوگ به دیجیتال، در فاز «تدریج» پایین‌ترین و بالاترین سطحِ میدان موج (محور Value) در نظرگرفته می‌شود و این محدوده به سطوح مختلفی تقسیم می‌گردد (به طور مثال ۲۵۶ سطح). سپس در فاز «نمونه برداری» در واحد زمان، به تعداد دفعات مشخصی (به طور مثال ۸۰۰۰ بار در ثانیه) نقاطی برروی موج Analog تصویر می‌شود. طبیعتاً هر نقطه در یک قسمت از تقسیم‌بندی محور Value قرار می‌گیرد (مثلاً بخشی از سیگنال در محدوده ٤ قرار می‌گیرد) که عدد مربوط به آن قسمت به آن نقطه نسبت داده می‌شود و بعد تبدیل به ۰ و ۱ شده و ارسال می‌شود. در مقصد، لازم است که این سیگنال Digital به Analog تبدیل شود. در تبدیل همین سیگنال Digital به Analog، عدد مربوط به این نقاط دریافت می‌شود و در همان محدوده مقادیر یک نقطه در نظر گرفته می‌شود.

مشکل اینجاست که تقسیم‌بندی‌های محور Value به صورت اعداد صحیح هستند (۱ و ۲ و ۳ و ...) ولی مقادیر آنالوگ همیشه به هم پیوسته و در این تقسیم‌بندی به صورت اعشاری‌اند (یعنی به طور مثال می‌توان بین دو عدد۵ و ۶، ده‌ها نقطه با مقدار اعشاری تصور کرد). در نتیجه نقطه دقیق زمان تبدیل آنالوگ به دیجیتال مشخص نیست و ما در تبدیل دیجیتال به آنالوگ، برای تمام قسمت‌های موج که در یک محدوده افتاده‌اند (مثلاً بخش‌هایی از موج که بین اعداد ۵ تا ۶ قرار می‌گیرند، چه ۵.۵ باشد و چه ۵.۸ و چه ۵.۱) یک عدد خاص (مثلاً ۵ یا ۵.۵) را در نظر می‌گیریم (چون نمیدانیم عددی که الان ۵ در نظر گرفته شده، در ابتدا ۵.۱ بوده یا ۵.۵ یا ۵.۸، همه را ۵ تصور کرده‌ایم).



مشخص است که مقداری خطا در تعیین آن نقطه وجود دارد. به این مقدار خطا که مربوط به فاز «تدریج» یا Quantization است، در اصطلاح «خطای تدریج» یا Quantization Error گفته می‌شود.



پس برای اینکه سیگنال تولید شده مشابه سیگنال ابتدایی شود یا کیفیت بهتری داشته باشد، باید Quantization افزایش یابد و Levelها بیشتر شوند تا به هم نزدیک شوند و اعدادی که به دست می‌آیند دقیق‌تر شوند. (خیلی‌ها به اشتباه تصور می‌کنند که Sampling باید افزایش یابد در حالی که مشکل اصلی در مرحله تدریج است)

طبق استاندارد بین المللی، در مخابرات ۲۵۶ سطح Quantization داریم.

سؤال: چرا ۲۵۶؟ چرا ۵۱۲ یا ۱۲۸ و یا هر عدد دیگری نه؟

پاسخ: زیرا اولاً ۲۵۶ توانی از ۲ است و نمایش آن به صورت باینری راحت‌تر است و ثانیاً تجربه و آزمایشات روی انسان‌های مختلف نشان داده که آن‌ها کیفیت سیگنال ۲۵۶ سطحی را از هر سیگنال دیگری بهتر و باکیفیت‌تر تشخیص داده‌اند و حتی جالب است که سیگنال ۵۱۲ هم روی مغز انسان نویز ایجاد می‌کند.

سؤال: چرا کیفیت فونوگراف از CD که Digital است بهتر می‌باشد؟

پاسخ: زیرا فونوگراف موسیقی از نوع Analog و به طور پیوسته است. اما موسیقی روی CD به Digital تبدیل شده است و طبق «خطای تدریج» زمانی که مجدداً به Analog تبدیل می‌شود تا ما بشنویم، با موسیقی اولیه کمی متفاوت خواهد بود.

سؤال: در مخابرات چند بار در ثانیه Sampling داریم؟

پاسخ: شخصی به نام Harry Nyquist آزمایشات زیادی انجام داد و فرضیه‌ای به نام Nyquist Theorem را ارائه داد که طبق این فرضیه برای اینکه تبدیل Digital به Analog با کیفیت خوبی انجام شود و سیگنالی بسیار شبیه به همان سیگنال Analog اولیه داشته باشیم، باید دو برابر پهنای باند فرکانسی، Sampling انجام دهیم. مثلاً برای سیستم‌های مخابراتی که دارای پهنای باند 3000 Hz هستند باید ۶۰۰۰ بار در ثانیه Sampling انجام داد.PSTN برای این که به مشکل برنخورد به جای مقدار ۶۰۰۰ بار در ثانیه، ۸۰۰۰ بار در ثانیه Sampling انجام می‌دهد.

خلاصه دیجیتالی کردن صدا:

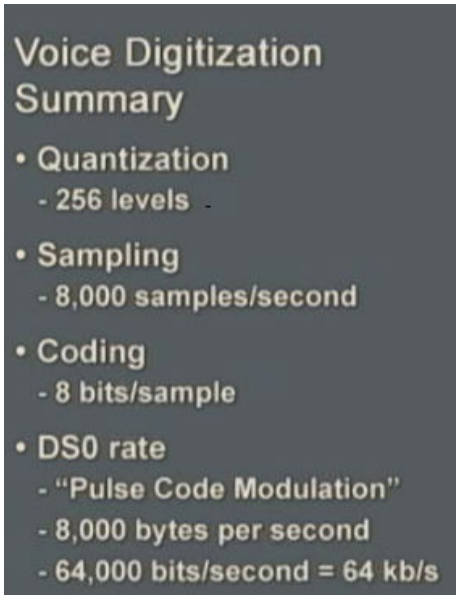
تعداد سطوح تدریج: ۲۵۶ سطح

تعداد نمونه برداری: ۸۰۰۰ بار در ثانیه

تعداد بیت در نظر گرفته شده برای هر نمونه: نهایتاً عدد ۲۵۶ را داریم پس با ۸ بیت می‌توان نمایش داد.

نرخ ارسال در یک ثانیه: ۸۰۰۰ نمونه در ثانیه، برای هر نمونه ۸ بیت، پس: ٦٤٠٠٠ بیت در ثانیه یا 64kbps نرخ ارسال در سیستم مخابرات است که این استاندارد به نام DS0 شناخته می‌شود.

نکته: واحد پهنای باند در Analog، Hz (تغییر ولتاژ) و در Digital، bps (Bits Per Second) است.



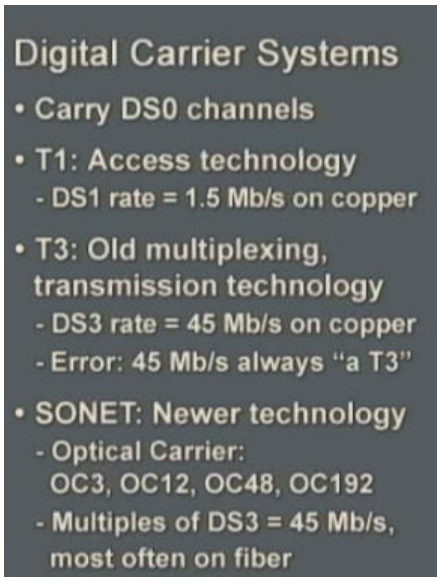
سرعت انتقال خطوط در استانداردهای مختلف:

The Digital Hierarchy: Industry Standard Line Speeds

DS0	**64 kb/s**	**one voice channel**
DS1	**1.5 Mb/s**	**24 DS0**
E1	2.0 Mb/s	32 DS0
~~DS2~~	~~6.3 Mb/s~~	~~4 DS1 = 3 E1~~
DS3	**45 Mb/s**	**28 DS1**
STM	155 Mb/s	3 DS3

دقت کنید خطوط مخابراتی ایران از نوع Analog است که نهایتا 56 Kbps است یعنی سرعت آن حتی به DS0 هم نمی‌رسد.

تکنولوژی‌های انتقال دیجیتال مشهور در دنیا :



سه تکنولوژی برای اتصالات بین سوئیچ‌ها و کاربرها در مخابرات:

1- POTS (Plain Ordinary Telephone Service):

مربوط به سال ۱۸۷٤می شود. نهایت سرعت انتقالی را که پشتیبانی می‌کند 53kbps است و البته در تکنولوژی‌های جدیدتر، تا 56kbps نیز رسیده است.

2- ISDN (Integrated Services Digital Network):

مربوط به سال ۵-۱۹٦٤می شود. سرعت انتقال 128kbps را پشتیبانی می‌کند.

Integrated Services یکی از اهداف Digital است که می‌توان data، voice، video را ارسال کرد.

سؤال: اگر بخواهیم بین دو مرکز از طریق خطوط تلفن Video conference (ویدئو کنفرانس) داشته باشید، آیا می‌توانیم خطوط مستقیم POTS را به هم متصل کنیم؟

پاسخ: خیر. آن‌ها Analog هستند و برای ویدئو کنفرانس و کارهای دیگری مانند فکس باید خطوط را به Digital تغییر داد (ISDN) و یا از مودم برای این کار استفاده کرد.

در حقیقت تلفن‌ها امکان انجام چنین کاری را به طور پیشفرض ندارند، اما با مودم و کامپیوتر می‌توان این ضعف را حذف کرد.

3- DSL (Digital Subscriber Line):

مربوط به سال ۱۹۹۸ بوده و سرعت انتقال 3Mpbs را پشتیبانی می‌کند.

مزایای Digital کردن خطوط انتقال:

1- Voice Application (کاربرد صدایی) :

۱- هرنوع صدایی را می‌توان ارسال کرد.

۲- می‌توان فشرده سازی روی صداها داشت.

2- Data Application (کاربرد داده‌ای) :

۱- اتصال به کامپیوترها به صورت راه دور(Remote).

۲- فکس کردن (Fax).

۳-اتصال WANهای مختلف (اتصال شبکه‌های گسترده مختلف از طریق خطوط).

3- Video Application (کاربرد ویدئویی) :

۱- انتقال انواع Video از طریق خطوط با کیفیت‌های مختلف، که بستگی به پهنای باند دارد.

مشهورترین ابعاد Videoها :



352*258 ابعاد VCDها است. (کیفیت پایین)

720*480 ابعاد DVD است. (کیفیت متوسط)

کیفیت High Definition (وضوح بالا) دو نوع است:

1- 1280*720 که به 720p (progressive) یا 720i (interlace) معروف است.

2- 1920*1080 که آن را 1080p یا 1080i هم می‌نامند.

تفاوت progressive و interlace :

p یعنی نوع ترسیم فریم‌های ویدئو **Progressive** (یعنی پیشرفتی) است. Progressive یعنی فریم‌های ویدئو به سرعت و به صورت پیکسل به پیکسل از بالا سمت چپ تا پایین سمت راست ترسیم می‌شوند البته تعریف دیگر آن این است که خط به خط از بالا به پایین ترسیم می‌شوند.

اما i یعنی نوع ترسیم فریم‌های ویدئو **Interlace** (یعنی در هم بافته) است. Interlace یعنی فریم‌ها خط به خط (Line by Line) به صورت یک در میان (ابتدا خط‌های فرد و سپس زوج) ترسیم می‌شوند و بنابراین کمی پرش در تصویر خواهیم داشت.

Progressive استاندارد جدیدتر برای ترسیم فریم‌هاست.

سوئیچینگ بسته‌ای

Packet Switching یا Data Switching

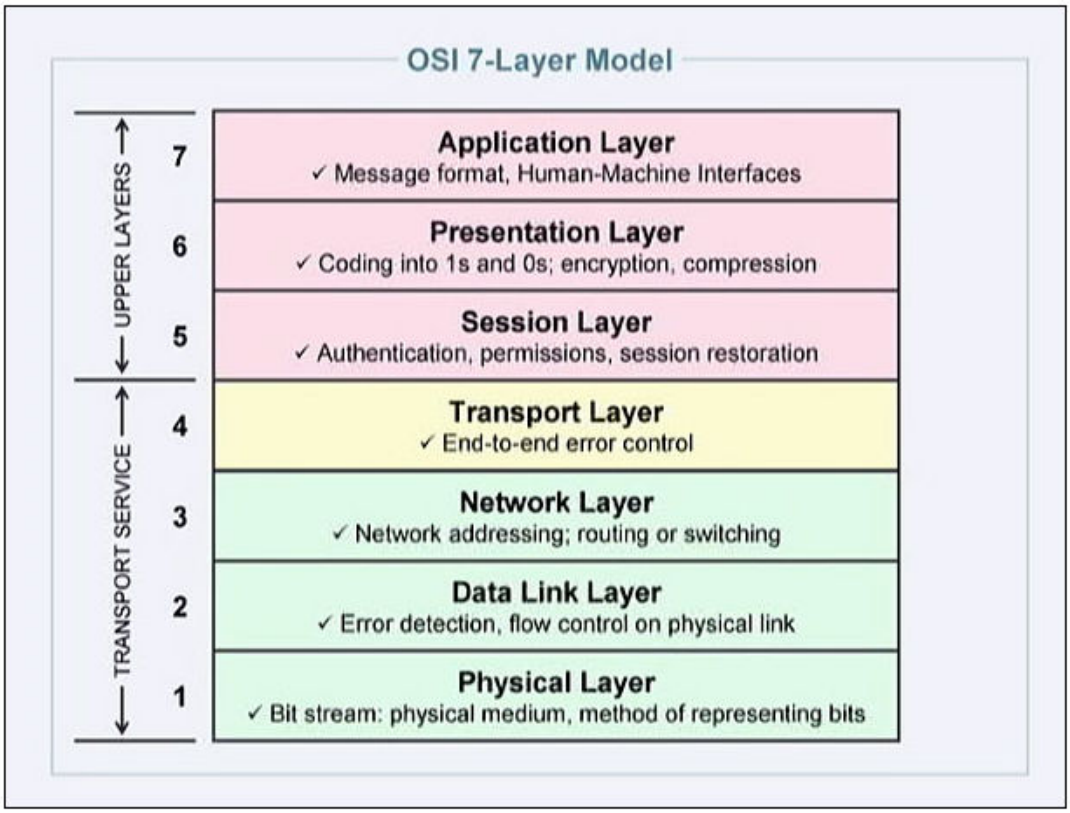
همانطور که قبلاً گفته شد، اتصالات بین تلفن‌ها به صورت سیستم مداری یا Circuit Switching است. یعنی قبل از اینکه کاربر شروع به تبادل داده کند، باید یک مدار اختصاصی (Dedicated Circuit) یا کانال برای او ایجاد شود.

اما نوع دیگری از اتصالات که به ویژه در شبکه‌های کامپیوتری مورد استفاده قرار می‌گیرد، Packet Switching نامیده می‌شود که در این بخش با آن آشنا می‌شویم.



آشنایی عمیق‌تر با لایه‌های مدل OSI:

با تشریح مدل OSI می‌توان کلیه مباحث شبکه را پوشاند.



چگونه نام و ترتیب این لایه‌ها را حفظ کنیم؟

در بین شبکه‌کارها این رسم است که برای حفظ کردن نام لایه‌ها، یک جمله را حفظ می‌کنند که با نام این لایه‌ها هماهنگ است.

به طور مثال جمله به زیر دقت کنید:

All People Seems To Need Data Processing

اگر بتوانید این جمله ساده را حفظ کنید، ترتیب لایه‌ها را به راحتی حفظ کرده‌اید.

معنی جمله این است: به نظر می‌رسد همه مردم به پردازش داده‌ای نیاز داشته باشند.

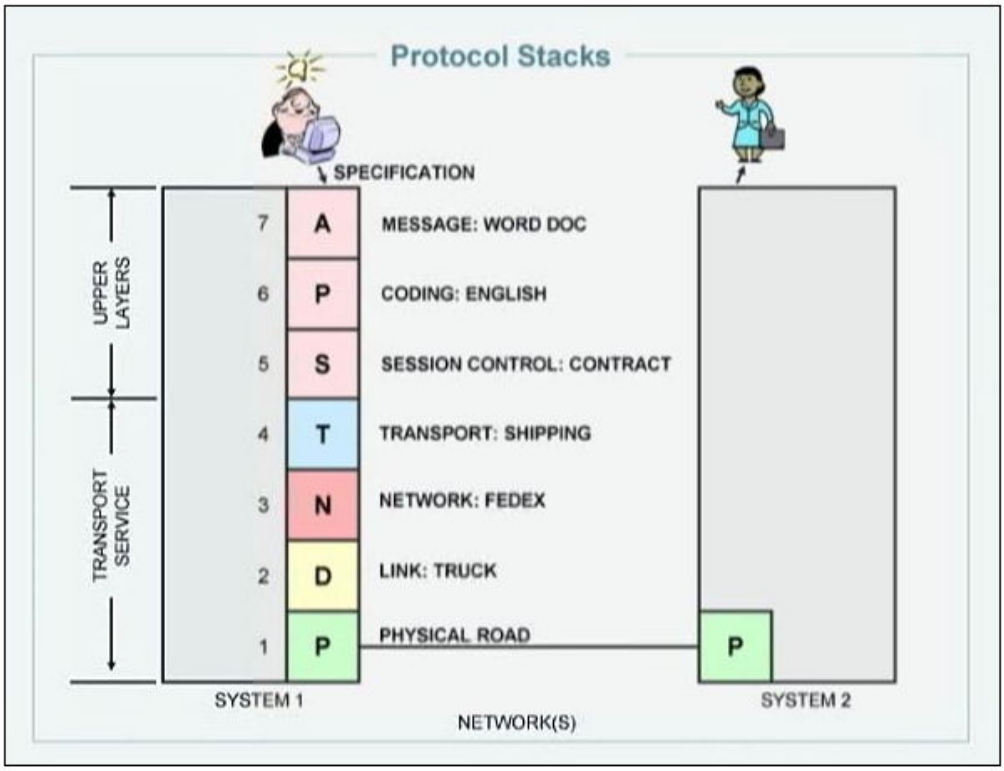
چگونه کاربرد هر لایه را حفظ کنیم؟

مدلی که در زمینه ارتباطات شبکه در OSI ارائه می‌شود شباهت‌های بسیار زیادی به ارتباطات در دنیای واقعی دارد. برای اینکه بدانید هر لایه چه وظیفه‌ای دارد، به این مثال دقت کنید:

قبل از مثال، دقت کنید که بسیاری از قوانین دنیای تکنولوژی از روی رفتار انسان‌ها وضع شده است. پس این مثال می‌تواند منبع افکار طراح مدل OSI را مشخص کند.

فرض کنید می‌خواهیم به عنوان یک کارمند در یک سازمان، با کارمند دیگری در سازمانی در شهر بغداد مکاتبه کنیم (مثلاً مسؤول بازاریابی یک شرکت هستیم و می‌خواهیم با مسؤول بازاریابی یک شرکت عراقی مکاتبه کنیم).

واضح است که نمی‌توانیم این کار را به طور مستقیم انجام دهیم، چون مشکلاتی مثل یکسان نبودن زبان و ندانستن آدرس و رعایت نکردن اصول نامه‌نگاری ممکن است نامه را بی‌اثر کند. پس باید یک روال منظم طی شود:



۱- بسیاری از کارشناسان معتقدند که هدف اصلی در یک شبکه، تبادل افکار می‌باشد. برای این که بتوانیم افکارمان را تبادل کنیم ابتدا باید آن‌ها را در برنامه‌ای مانند Word تایپ کنیم. (لایه Application یا برنامه‌های کاربردی)

۲- در مرحله بعد باید قبل از این که نامه به دست شرکت عراقی برسد ترجمه شود. به چه زبانی ترجمه شود؟ طبیعتاً به زبان مشترک دنیا یعنی انگلیسی. به آنجا که رسید، مترجم به عربی ترجمه می‌کند. پس برای این کار نامه را به مرکز دارالترجمه در سازمان تحویل می دهیم. (لایه Presentation یا ارائه)

۳- سپس نامه ترجمه شده تحویل مرکزی داده می‌شود که مسؤول برقراری ارتباط می‌باشد. این مرکز میداند چطور (طبق قوانینی خاص) با کشورها و سازمان‌های دیگر ارتباط رسمی برقرار کند. اگر به طور مثال یک نامه ضمیمه از رئیس سازمان لازم باشد این مرکز میداند و آن‌را تهیه می‌کند... (لایه Session یا جلسه)

٤- در مرحله بعد نامه از مرکز برقراری ارتباط، به مرکز مسؤول انتقال نامه به مقصد، تحویل داده می‌شود. شیوه‌های مختلفی برای ارسال وجود دارد. نامه به صورت پست پیشتاز فرستاده شود یا مثلاً به خاطر امنیت بالا، یک پیک اختصاصی آن‌را به مقصد برساند و یا اینکه به خاطر امنیت پایین، نامه را در یک صندوق در خیابان بیندازیم!!! (مثل اینترنت در بحث شبکه!!) به هر حال، این شیوه توسط مرکز برقراری ارتباط تعیین می‌شود. (لایه Transport یا انتقال)

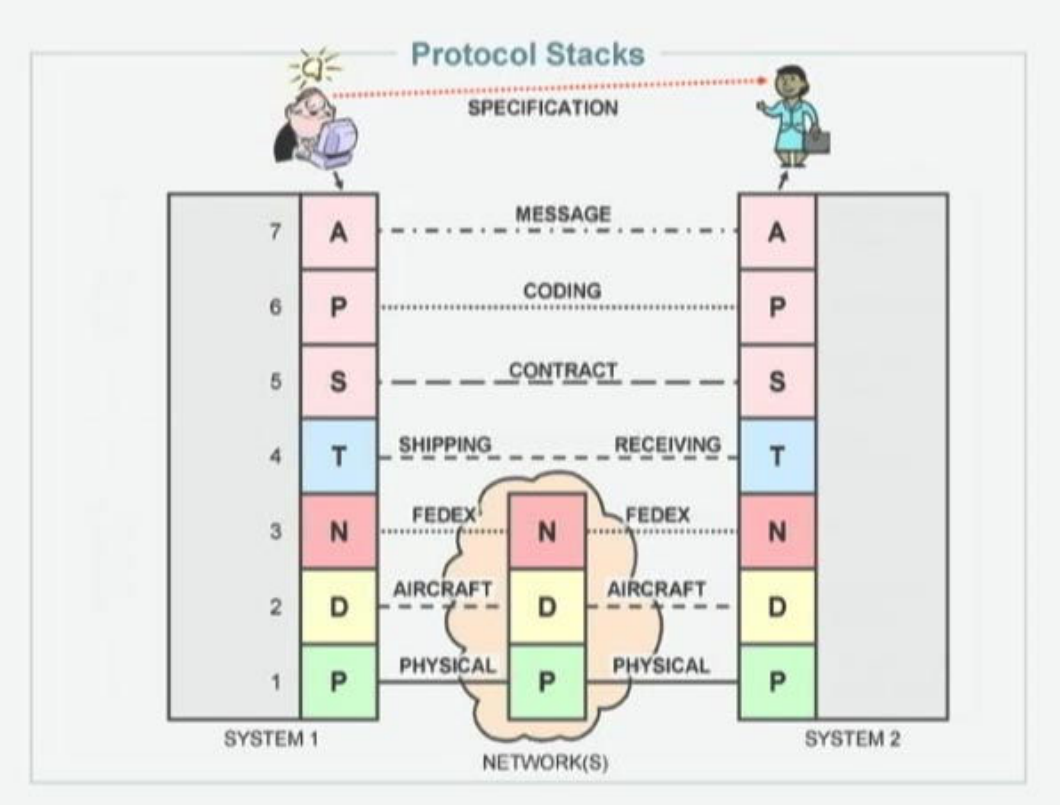
٥- در قسمت دیگری در بخش پست، آدرس دقیق مبداءِ و مقصد مشخص و بر روی نامه درج می‌گردد و تمبر به آن می‌چسپد. (لایه Network یا شبکه)

٦- در بخش دیگری از سازمان ما، این نامه و دیگر نامه‌ها که باید ارسال شوند، در یک جعبه یا قاب نهایی قرار می‌گیرند و آدرس اداره پست بعد که باید این نامه‌ها را دریافت کند، روی این قاب درج می‌گردد. (لایه Data link یا پیوند داده‌ای)

٧- و در نهایت وقتی آن قاب آماده ارسال شد، به وسیله انتقال یعنی یک ماشینِ حملِ نامه یا هر وسیله انتقال دیگر سپرده می‌شود و این رسانه آن را تا مقصد بعدی حمل می‌کند. (لایه Physical یا فیزیکی)

در مرکز پستی، آدرس روی جعبه یا قاب ممکن است تغییر کند. مثلاً نامه‌هایی که قرار است از ساوه به مشهد ارسال شوند ابتدا از سازمان ما به اداره پست ساوه، سپس از پست ساوه به پست تهران و سپس شهر بعد و در نهایت به مشهد که مقصد ماست می‌رسد. پس هر بار مقصد بعدی روی این قاب نوشته می‌شود تا در هر لحظه مشخص باشد که مقصد بعدی کجاست.

در مدل OSI دقیقاً همین روال دنبال می‌شود:



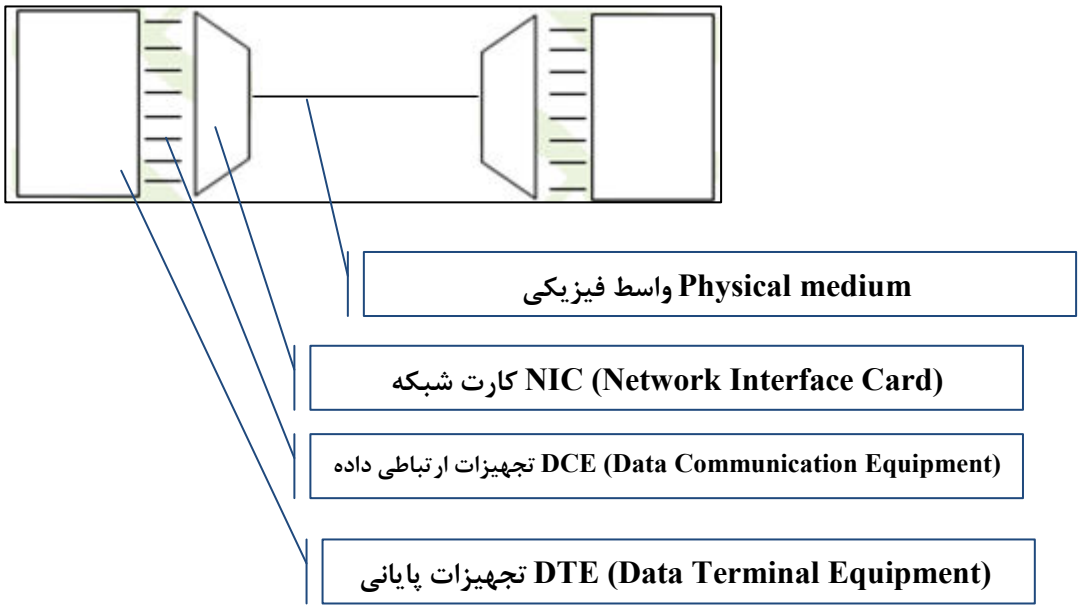
افکار در لایه Application به صورت فایل متنی پیاده‌سازی می‌شوند و در لایه Presentation به زبان 0 و 1 تبدیل می‌شوند. لایه‌ای به نام Session مسؤول برقراری ارتباط با قراردادهایی خاص بین مبدأ و مقصد می‌باشد. این لایه پس از برقراری ارتباط، اطلاعات را تحویل لایه Transport می‌دهد. این لایه تصمیم می‌گیرد با چه پروتکلی (مثلاً TCP/IP یا UDP) اطلاعات، انتقال پیدا کنند. سپس این لایه

اطلاعات را تحویل لایه Network می‌دهد. لایه شبکه آدرس مبدأ و مقصد را به اطلاعات اضافه می‌کند و اطلاعات تحویل لایه Data link داده می‌شود. در این لایه با توجه به آدرس مقصد، آدرس روتر بعدی به اطلاعات اضافه می‌شود و در نهایت اطلاعات به لایه Physical داده می‌شود.

نکته: در OSI، لایه‌ها ضمن ارتباط بالا به پایین و برعکس، با هم یک رابطه مجازی مستقیم هم دارند. مثلاً وقتی نامه تایپ می‌شود باید مطمئن شد که طرف مقابل هم نرم افزار Word دارد و این یعنی یک رابطه بین دو Application وجود دارد و یا لایه Transport با هم ارتباط دارند که ببینند آیا سیگنال دریافت شد یا نه؟

آشنایی با لایه فیزیکی در مدل OSI :

شکل کلی اتصال دو کامپیوتر در یک شبکه و اجزای فیزیکی مورد نیاز در این اتصال:



DTE (تجهیزات پایانه داده) :

مانند کامپیوتر، فکس، پرینتر، موبایل، دستگاه‌های پرداخت الکترونیک و... که در خطوط انتقال داده‌ای، پایان دهنده هستند و در نهایت اطلاعات به آن‌ها می‌رسد و اطلاعات را پردازش می‌کنند.

DCE (تجهیزات ارتباطی داده) :

سریال یا موازی؟

فرض کنید که می‌خواهیم ۸ بیت داده را بین دو نقطه منتقل کنیم.

چه راه‌هایی به نظرتان می‌رسد؟

طبیعتاً به دو صورت ممکن است:

۱- هشت کانال رسم کنیم و از هر یک، یک بیت بفرستیم.



۲- یک کانال رسم کنیم و ۸ بیت را یکی یکی و پشت سر هم ارسال کنیم.



به روش اول، موازی (Parallel) و به روش دوم سری (Serial) گفته می‌شود.

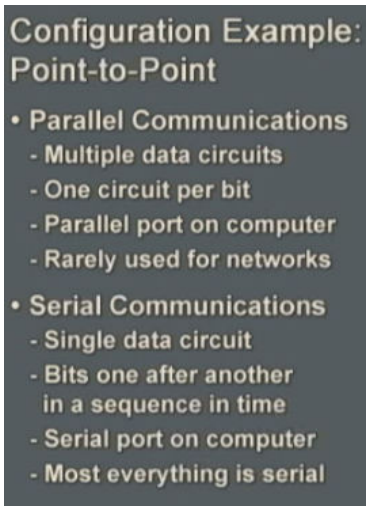
سؤال: فکر می‌کنید کدام روش سریع‌تر است؟ درست است، پارالل.

سؤال: اما چطور شد که با وجود سرعت بالای انتقال پارالل، این روزها همه چیز به سمت سریال شدن می‌رود؟ به طور مثال، کابل‌های پرینتر قبلاً از نوع Parallel Port بود اما اکنون از نوع USB یا Universal **Serial** Bus است. اتصال Hard disk به Mother Board قبلاً IDE یا ATA بود اما الان SATA(Serial ATA) است. چرا؟

پاسخ: طبق معمول، دلیل اول: پول! هزینه خطوط موازی بالا است زیرا برای هر کانال علاوه بر این‌که تجهیزات ارسال داریم باید برای نقطه مقابل نیز تجهیزات دریافت و تبدیل داشته باشیم (در مثال بالا، موازی، هشت برابرِ سریال هزینه دارد). برای همین دنیا به سوی خطوط سریال پیش می‌رود.

در داخل کامپیوتر، خطوط جا به جایی به صورت Parallel است ولی خطوط انتقال، از نوع سریال است پس به تجهیزاتی نیاز داریم که خطوط موازی را به سریال تبدیل کند. در شبکه این دستگاه را کارت شبکه (NIC) می‌نامند. کارت‌های شبکهLAN از تکنولوژی سریال استفاده می‌کنند.

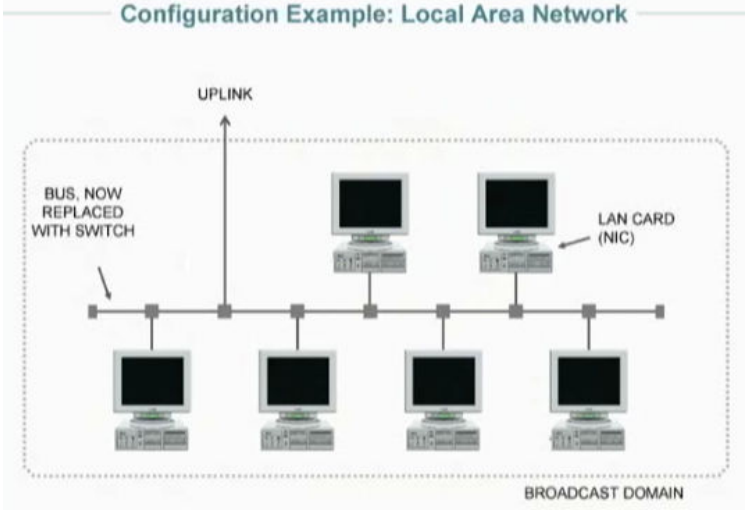
Parallel و Serial :



- در موازی مدار چندگانه و در سریال، یک مدار داریم.
- در موازی هر مدار به یک بیت اختصاص دارد ولی در سریال، داده‌ها بیت به بیت، پشت سر هم ارسال می‌شود.
- موازی به ندرت در شبکه استفاده می‌شود. اکثر چیزهایی که داریم، سریال است.

سؤال: اگر چند کامپیوتر (DTE) را با واسطه فیزیکی مانند کابل وکارت شبکه (DCE) به یکدیگرمتصل کنیم در حالی که یک کامپیوتر اطلاعاتی را روی کابل می‌گذارد. کابل از کجا می‌فهمدکه اطلاعات به کدام کامپیوتر باید برسد؟

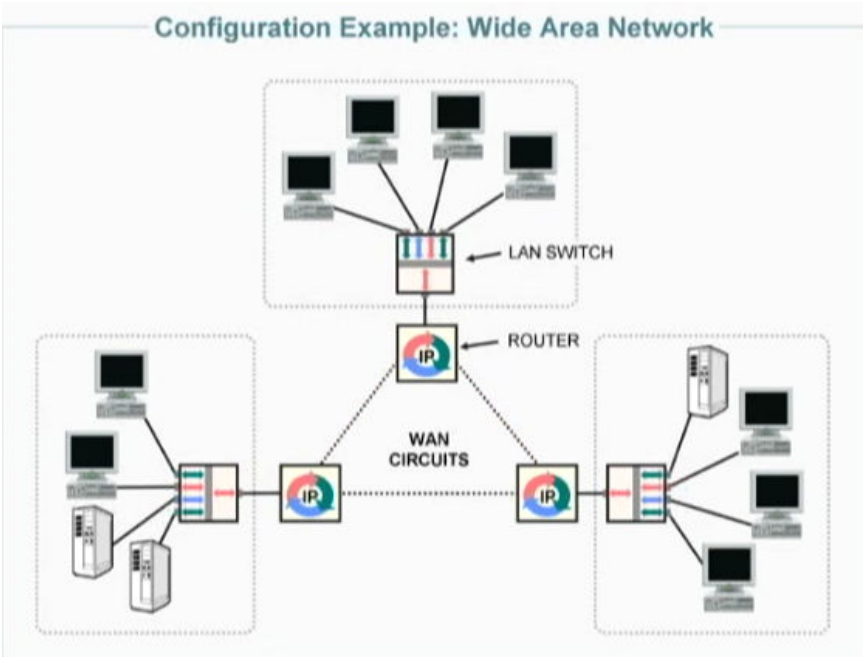
پاسخ: آدرس کامپیوتر مقصد (IP) را به داده یا اطلاعات متصل می‌کنیم و برای اینکه داده در اختیاردیگر کامپیوترها قرار نگیرد روی شبکه کنترل کننده دسترسی (Access Controller) را تعبیه می‌کنیم که در شبکه این دستگاه به Hub معروف است.



وظیفه Hub :

- آدرس مقصد را از بین اطلاعات جدا می‌کند.
- اطلاعات را به مقصد ارسال و راهنمایی می‌کند.

WANS (شبکه‌های گسترده) یا Multidrop Circuit :



در WAN یک مسیر نداریم بلکه چندین مسیر مختلف داریم. زمانی که اطلاعات از جایی به جای دیگر ارسال می‌شوند نیاز به مسیریابی یا Route دارند. بهترین دستگاهی که این کار را انجام می‌دهد Router نامیده می‌شود. کامپیوتر مقصد اطلاعاتی به Router ارسال می‌کند و Router از روی آدرس مقصد مسیر را پیدا می‌کند.

پس هرکامپیوتر در شبکه باید دارای آدرس واحد (IP) باشد.

مشهورترین استاندارد آدرس دهی به کامپیوترهای یک شبکه، استاندارد IP Version 4 (IP V4) می‌باشد.

آشنایی با لایه پیونده داده‌ای (Data Link) در مدل OSI :

جدول ASCII (American Standard Code For Information Interchange):

جدول ASCII کد استاندارد آمریکایی برای انتقال وتبادل اطلاعات است. در شبکه منظور از داده همان کدهای صفر و یک است که برای تبدیل کاراکترها (مثلاً y) به صفر و یک و برای ارسال اطلاعات به مقصد تقریباً در همه جای دنیا از جدول ASCII استفاده می‌کنند.

ASCII Code Set

BITS 4,3,2,1 \ BITS 7,6,5		000	001	010	011	100	101	110	111
		0	1	2	3	4	5	6	7
0000	0	NUL	DLE	SP	0	@	P	`	p
0001	1	SOH	DC1	!	1	A	Q	a	q
0010	2	STX	DC2	"	2	B	R	b	r
0011	3	ETX	DC3	#	3	C	S	c	s
0100	4	EOT	DC4	$	4	D	T	d	t
0101	5	ENQ	NAK	%	5	E	U	e	u
0110	6	ACK	SYN	&	6	F	V	f	v
0111	7	BEL	ETB	'	7	G	W	g	w
1000	8	BS	CAN	(	8	H	X	h	x
1001	9	HT	EM	)	9	I	Y	i	y
1010	A_H	LF	SUB	*	:	J	Z	j	z
1011	B_H	VT	ESC	+	;	K	[	k	{
1100	C_H	FF	FS	,	<	L	\	l	|
1101	D_H	CR	GS	-	=	M	]	m	}
1110	E_H	SO	RS	.	>	N	^	n	~
1111	F_H	SI	US	/	?	O	-	o	DEL

همانطور که قبلاً گفته شد، وظیفه اصلی لایه پیوند داده‌ای، فرمت بندی داده‌هاست.

اما چگونه داده‌ها فرمت بندی می‌شوند؟

- در اولین گام داده‌ها به صفر و یک تبدیل می‌شوند. (برای این کار از جدول ASCII استفاده می‌شود).

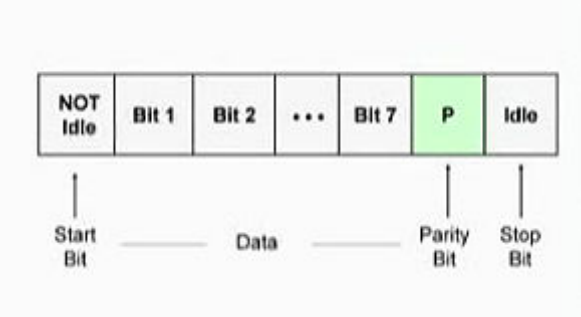
بعد از تبدیل اطلاعات به صفر و یک، ممکن است خطاهایی در ارسال رخ دهد.

به همین دلیل، دو وظیفه مهم این لایه عبارتند از:

۱- تشخیص خطا (Error Detection)

۲- تصحیح خطا (Error Correction) [البته اگر خطایی رخ داده بود]

- برای تشخیص و تصحیح خطا، در ابتدا و انتهای هر هشت بیت، یک بیت معین می‌گذارند (Stop Bit و Start Bit) و ارسال می‌کنند. به مجموعه داده‌ها و این دو بیت در اصطلاح یک قاب (Frame) گفته می‌شود. در مقصد این دو بیت چک می‌شوند. اگر چندین فریم پشت سر هم، بیت‌های Start و Stop صحیحی داشتند، یعنی داده‌ها درست ارسال شده‌اند.



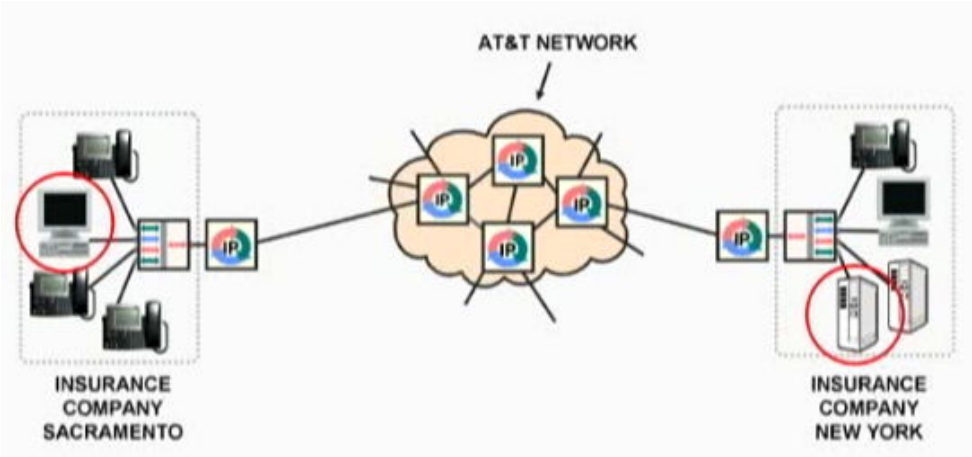
توجه: هر کاراکتر طبق جدول ASCII با ۷ بیت قابل نمایش است. در اینجا معمولاً یک بیت که به نام Parity Bit شناخته می‌شود در نظر گرفته می‌شود. Parity Bit یک روش ساده برای تشخیص خطاست. اگر در یک مجموعه مورد نظر از بیت‌ها، تعداد بیت‌ها فرد باشد بیت توازن 1 و اگر زوج باشد، 0 در نظر گرفته می‌شود.

اینکه داده‌ها یک بایت یک بایت ارسال می‌شود و در ابتدای هر بایت یک Start Bit و در انتهای آن، یک Stop Bit است، یک ایده ابتدایی از ارسال و کشف خطا به حساب می‌آید. در این ایده برای هر ۱۰ بیت ارسالی ۳ بیت برای کشف خطا است یعنی ۳۰ درصد از اطلاعات ارسالی داده‌های ما نیست، بیت‌هایی برای کشف خطاست.مشخص است که کار بیهوده‌ای انجام می‌شود. پس ایده مناسب و بهینه‌ای نیست.

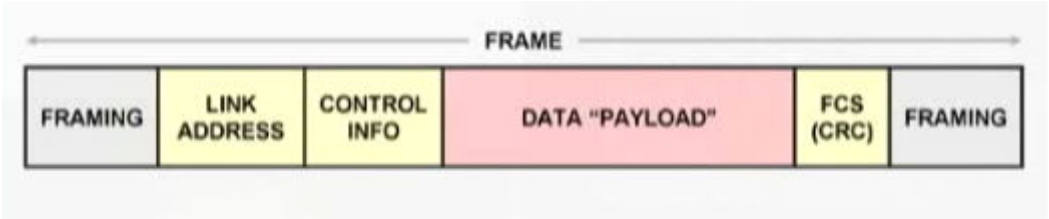
در ایده جدیدتر یک بلاک (Block) از اطلاعات شامل چند بایت را در کنار هم قرار می‌دهند (مثلاً ۸ بایت یعنی ۶۴ بیت را) و سپس Framing را انجام داده و برای کشف خطا در ابتدا و انتهای آن بلاک یک بیت ابتدایی و انتهایی قرار می‌دهند.

Router یا مسیریاب چه کاری انجام می‌دهد؟

اگر قرار باشد اطلاعات به کامپیوتری خارج از شبکه جاری ارسال شود (به طور مثال، در حال استفاده از اینترنت هستید و سایتی را فراخوانی می‌کنید که در شبکه دیگری قرار دارد. دقت کنید که اینترنت شبکه‌ای از شبکه‌هاست)، مشخص است که بین کامپیوتر شما و کامپیوتر مقصد (مثلاً کامپیوتری که در شرکت یاهو و اطلاعات سایت yahoo.com بر روی آن است)، یک کابل مستقیم وصل نیست بلکه ده‌ها مسیریاب (Router – روتر) به هم متصل شده‌اند تا اتصال شما با کامپیوتر مقصد برقرار شود. در نتیجه هر روتر به چندین روتر دیگر متصل است. حالا سؤال این است که وقتی یک روتر یک فریم را دریافت کرد، از کجا باید بداند که این فریم را باید به کدام روترِ متصل به خود تحویل دهد؟



برای رفع این مشکل، به محض ارسال اطلاعات از کامپیوتر شما، آدرس نزدیک‌ترین روتر به فریم می‌چسبد (یادتان هست در اداره پست شهر شما، آدرس مرکز پستی بعدی به باکس حاوی نامه‌ها می‌چسبید؟). به این آدرس در اصطلاح Link Address گفته می‌شود.



هر روتر به محض دریافت یک فریم، فریم را باز کرده و آدرس مقصد نهایی را (که بعداً خواهیم گفت که در لایه شبکه به پکت‌ها چسبیده است) نگاه می‌کند.

هر روتر شامل یک جدول نرم افزاری است (Router Table). در این جدول مشخص شده است که هر کابل روتر به چه مقصدهایی منتهی می‌شود.

با توجه به مقصد نهایی، روتر تصمیم می‌گیرد که باید فریم شما را به کدام روتر متصل به خود تحویل دهد. در نتیجه Link Address را پاک کرده و آدرس روتر بعدی را به جای آن می‌نویسد و فریم را تحویل کابل می‌دهد.

در حقیقت در هر روتر، آدرس فریم به آدرس روتر بعدی تغییر می‌کند.
مثلاً فرض کنید فریمی را به کربلا فرستاده‌اید. فریم شما از شهرستان، به تهران رسیده است. در روتر تهران اولین اتفاقی که می‌افتد، این است که مقصد نهایی بررسی می‌شود. سپس به جدول روتر مراجعه می‌شود. در آنجا نوشته شده است که به طور مثال، اگر مقصد نهایی فریم، کربلا بود، آدرس روتر بعدی عبارت است از بغداد. پس روتر تهران، Link Address را به «بغداد» تغییر می‌دهد و تحویل کابل می‌دهد. وقتی فریم به بغداد رسید، در بغداد باز هم آدرس مقصد نهایی بررسی می‌شود: کربلاست. روتر بغداد به جدول خود مراجعه می‌کند: اگر مقصد نهایی کربلا بود، روتر بعدی، فلان آی.اس.پی (ISP) در شهر بغداد است و آنجا هم همینطور و این روال ادامه پیدا می‌کند تا در نهایت فریم به مقصد برسد.
می‌توانید حدس بزنید که **کاربرد اصلی Router** اتصال دو شبکه با رِنج IPهای مختلف است. مثلاً برای اتصال کامپیوتر خود به شبکه جهانی نیاز به یک Router داریم که رنج IP کامپیوتر ما را با آن هماهنگ کند. (مودم ADSL شما یک نوع روتر است)

نکته مهم: با توجه به آنچه گفته شد، می‌توانید متوجه شوید که روتر (مسیریاب)، سخت افزاری است که در لایه Network کار می‌کند.
(این نکته معمولاً در کنکورها سؤال است)
چرا لایه سه؟
چون روتر باید به پکت‌ها (که در لایه شبکه) دسترسی داشته باشد تا بتواند آدرس مقصد نهایی پکت را بفهمد و طبق آن و با نگاه به جدول خود، تصمیم بگیرد که روتر بعدی کجا خواهد بود که به فریم بچسباند.

نکته: کلمه Router را در اکثر نقاط دنیا، «راوتر» تلفظ می‌کنند و برخی کشورها مثل ایران نیز «روتر».

Asynchronous (غیرمتقارن) :
به ایده کد کردن یک کاراکتر (یک کلید صفحه کلید) به یک بایت (با استفاده از جدول ASCII) و انجام عمل کشف خطا و Framing (قاب بندی) و ارسال آن، در مجموع Asynchronous گفته می‌شود.

تعریف Frame:
به مجموعه بیت‌های مربوط به قاب بندی، آدرس مقصد، اصل داده و چند بیت مربوط به کشف خطا و کنترل اطلاعات، Frame گفته می‌شود.

تحقیق: نوعی از الگوریتم‌های کشف خطا، به نام CRC (Cyclic Redundancy Check) شناخته می‌شود. در مورد آن تحقیق کنید.

آشنایی با لایه شبکه (Network) در مدل OSI :

فرض کنید شما درخواست خود برای نمایش سایت یاهو را به کامپیوتر شرکت یاهو ارسال می‌کنید. با درخواست شما موافقت می‌شود و قرار است اطلاعات سایت برای شما ارسال شود. یاهو باید از کجا آدرس کامپیوتر شما را بداند تا اطلاعاتش را برای شما بفرستد؟

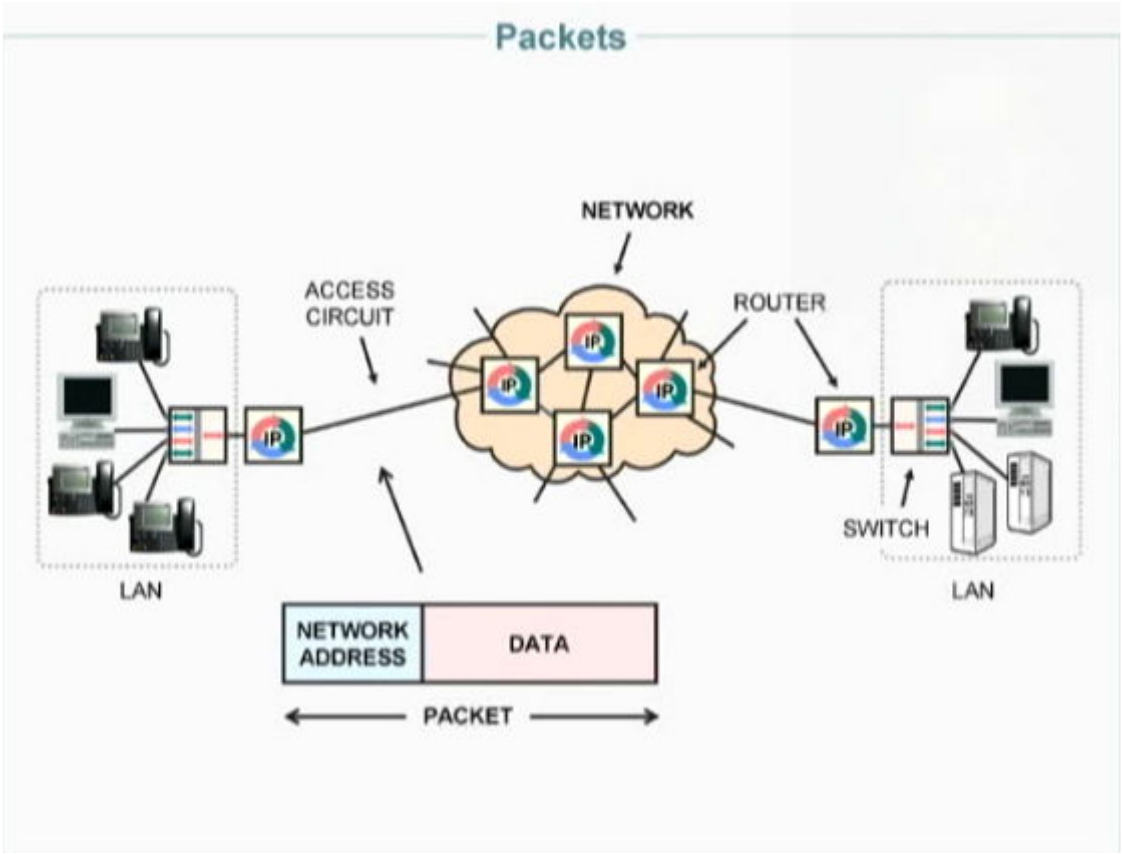
برای اینکه اطلاعات ارسالی گم نشوند و مشخص باشد که از کجا آمده‌اند و به کجا می‌روند، آن‌ها را در لایه شبکه در بسته‌هایی قرار می‌دهیم و آدرس مبدأ و مقصد را به این بسته‌ها می‌چسبانیم. این بسته‌ها را از این پس Packet (پَکِت) یا «بسته» می‌نامیم.

وقتی اطلاعات به مقصد رسید، جوابیه آن‌ها باید ارسال شود. آدرس مبدأ و مقصد بسته‌های اولیه برداشته می‌شوند و جا به جا می‌شوند. سپس به بسته‌های جوابیه ارسال می‌شوند. (آدرسی که زمان ارسال، آدرس مبدأ بود، حالا جای آدرس مقصد می‌نشیند و آدرس مقصد می‌شود آدرس مبدأ)

شما حالا قادر هستید به این سؤال پاسخ دهید:

چرا به شبکه‌های کامپیوتری، Packet Switching گفته می‌شود؟

ساده است: زیرا اطلاعات قبل از ارسال به Packet یا بسته‌هایی تقسیم بندی می‌شوند.

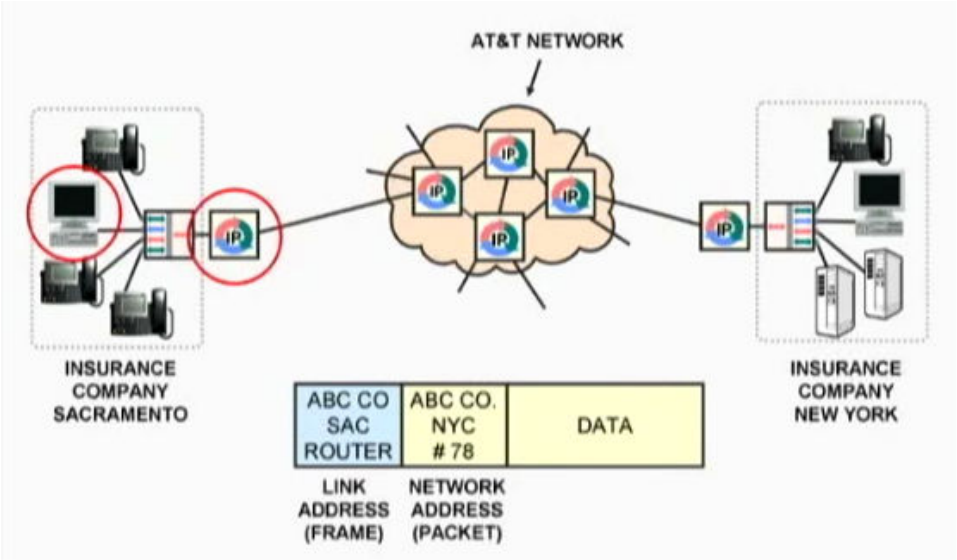


خلاصه مطلب:

وقتی اطلاعات از کامپیوتر مبدأ ارسال می‌شود آدرس مقصد و مبدأ در کنار Packet قرار می‌گیرد (کارلایه Network). آدرس Routerای که به کامپیوترجاری متصل است در بخشی از Frame قرار دارد (کار لایه Data Link).

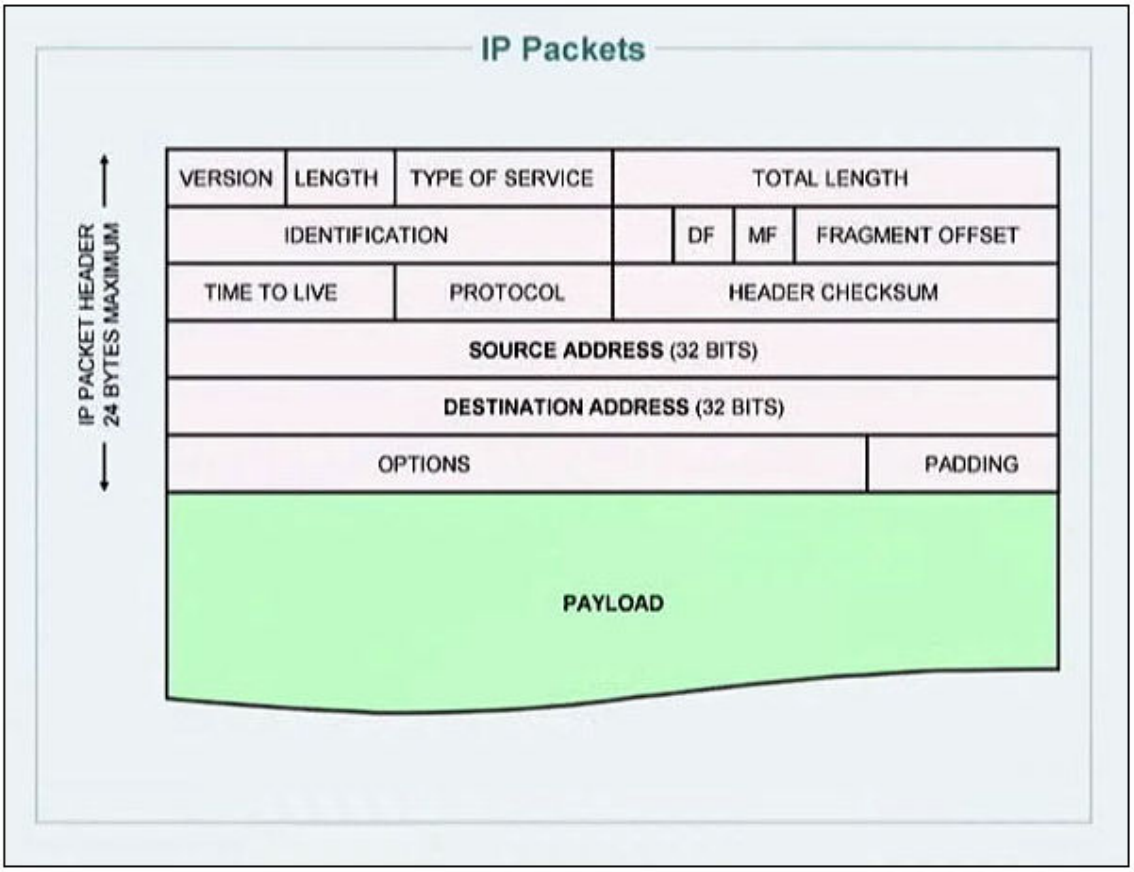
وقتی بسته به روتر رسید، روتر، آدرس مقصد را چک می‌کند و به جدول خود نگاه می‌کند سپس آدرس Router بعدی را به جای Link Address (جای آدرس Router قبلی) قرار می‌دهد و همینطور در Router بعدی... تا اطلاعات به مقصد برسد.

پس آدرس Frame در هر Router عوض می‌شود اما آدرس Packet همیشه ثابت است.



نکته: به Packet، گاهی اوقات IP Packet هم گفته می‌شود.

اجزای IP Packet :



- VERSION :

ورژن آی.پی. دو نوع مهم آن IP_{V4} و IP_{V6} می‌باشد.

- LENGTH :

طول Header را مشخص می‌کند.

- TYPE OF SERVISE:

نوع سرویس Packet را مشخص می‌کند. مثلاً Video یا Voice یا Data و....

- TOTAL LENGTH:

طول کل Packet را مشخص می‌نماید.

- IDENTIFICATION:

هر پکت یک ID یا شناسه به خود می‌گیرد که در این بخش نگهداری می‌شود.

- FRAGMENT OFFSET:

گاهی اوقات یک بسته به چندین تکه تقسیم و ارسال می‌شود. در اینصورت هر قسمت یک آفست به خود می‌گیرد.

اگر به چند تکه تقسیم شود آنگاه MF =1 می‌گردد و اگر به چند تکه تقسیم نشود آنگاه DF =1 می‌شود.

- TIME TO LIVE :

مدت زمان عمر یک Packet را مشخص می‌کند. (هر پکت تا مدتی سرگردان می‌ماند اگر به مقصد نرسد، شما پیغام «مقصد غیرقابل دسترسی است» را مشاهده می‌کنید)

- PROTOCOL :

پروتکل لایه انتقال را در این بخش از Header نگه می‌دارد. معروف‌ترین پروتکل‌ها TCP/IP و UDP است.

- HEADER CHECKSUM :

اطلاعات مربوط به نگهداری Header را داراست.

- SOURCE ADDRESS :

آدرس مبدأ را داراست.

- DESTINATION ADDRESS :

آدرس مقصد را داراست.

- OPTION :

اطلاعات اضافه مربوط به Header را نگهداری می‌نماید.

- PADDING :

ممکن است فاصله خالی option را پر کند.

- PAYLOAD :

اصل داده است.

نکته: کل اطلاعات یک Header در نهایت می‌تواند ۲٤ بیت باشد.

IPها:

در هر شبکه، هر DTE (یعنی هر قطعه پایانی مثل کامپیوتر، پرینتر، موبایل و ...) باید یک آدرس یکتا داشته باشند. مثل اینکه هر خانه در یک کشور، یک آدرس و کد پستی یکتا دارد. به این آدرس یکتا در شبکه در اصطلاح IP Address یا به طور خلاصه، IP گفته می‌شود.

IPهای ورژن ٤، ٣٢ بیتی هستند و از ٤ قسمت ٨ بیتی تشکیل شده‌اند که به هر کدام یک Octet گفته می‌شود. پس هر IP v4 از چهار اکتت تشکیل شده است.

نمونه یک آدرس آی.پی در یک شبکه:

192.168.0.10

اینکه گفته می‌شود یک اکتت، ٨ بیتی است به چه معنی است؟

بد نیست کمی در مورد بیت و بایت و این اصطلاحات صحبت کنیم:

بحث آزاد:

bit یعنی چه؟

همانطور که می‌دانید، در کامپیوتر برای نمایش داده‌ها از دو مفهوم استفاده می‌کنیم: بودن یا نبودن! منظور همان صفر و یک است.

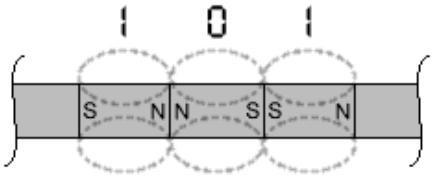
توجه کنید که صفر و یک، **نماد** است. صفر، نماد یک وضعیت و یک، نماد وضعیتی دیگر. همه اطلاعات کامپیوتر در نهایت تبدیل به همین 0ها و 1ها می‌شوند. چندین 0 و 1 کنار هم قرار می‌گیرند و داده‌های مختلف را پدید می‌آورند. به طور مثال اگر ٧ تا 0 و 1 به صورت 1000001 کنار هم قرار بگیرند، طبق جدولی به نام جدول اسکی، کامپیوتر آن‌ها را کاراکتر a به حساب خواهد آورد.

اما از نظر سخت افزاری بحث چگونه است؟

یعنی به نظر شما یک فلاپی چگونه 0 و 1ها یا همان اطلاعات را بر روی خود نگاه می‌دارد؟

بر روی فلاپی قطعات بسیار ریز مغناطیسی (Magnetic Particles) وجود دارند که توانایی حفظ خاصیت مغناطیسی خود را برای مدت طولانی دارند.

هر قطعه قطب شمال (N) و جنوب (S) مربوط به خود را دارد.



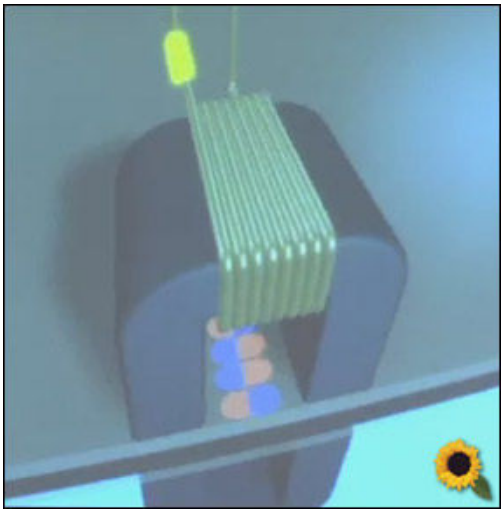
حالا باید تصور کنید که چطور می‌توان با این قطعات ریز، 0 و 1 را نمایش داد؟

خیلی ساده است، به طور مثال اگر قطب S در سمت راست بود، این قطعه را می‌گیریم نماد 0 و اگر قطب S در سمت چپ بود، می‌گیریم نماد 1.

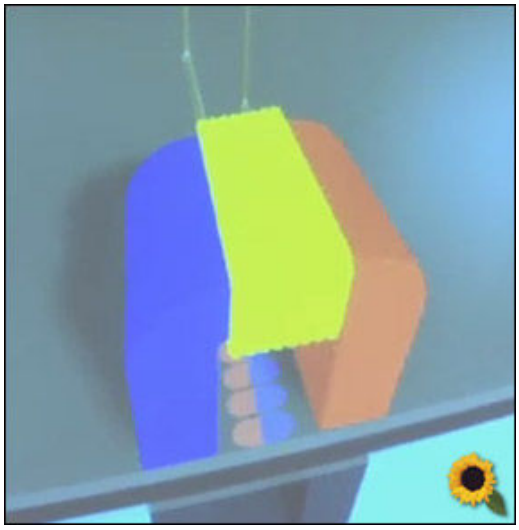
سؤال این است که چطور قطب این قطعات را جا به جا کنیم که نماد صفر یا یک شوند؟ یعنی در حقیقت **چطور بر روی فلاپی بنویسیم؟**

در فلاپی درایو (Floppy Drive) یک هد (head) برای خواندن و نوشتن داریم.

این هد با سطح فلاپی در تماس است. این هد در حقیقت یک سیم‌لوله است. وقتی قرار است یک قطعه نماد صفر شود، به طور مثال پالس مثبت را به سیم سمت چپ هد می‌فرستیم.



میدانی که در سیم‌پیچ ایجاد می‌شود، آن را تبدیل به یک آهن‌ربا می‌کند و باعث می‌شود سمت راست میله قطب N شود و در نتیجه قطب N مربوط به هر قطعه‌ای که بین این آهن‌ربا قرار گیرد دفع شده و از آن دور می‌شود (قطب‌های مشابه همدیگر را دفع می‌کنند). یعنی در حقیقت چنین اتفاقی در مورد قطعات روی دیسک می‌افتد:



قطعات با توجه به پالسی که به هد دادیم، سر و ته می‌شوند. (قرمز از قرمز دور می‌شود و آبی از آبی)

به هر حال، هر یک از این قطعات، نماد یک بیت است. این بیت‌ها کنار یکدیگر چیده می‌شوند و داده‌ها را تشکیل می‌دهند.

تبدیل اعداد دودویی (Binary) به دەدهی (Decimal):

در بحث IP و بحث Subnetting، نیاز دارید که بتوانید بیت‌های در مبنای دو را به عدد دەدهی معادل آن تبدیل کنید.

مطمئناً به خاطر دارید که چطور اعداد دودویی را به دەدهی تبدیل می‌کردیم:

$$(110)_2 = (1 \times 2^2 + 1 \times 2^1 + 0 \times 2^0) = 4 + 2 + 0 = 6$$

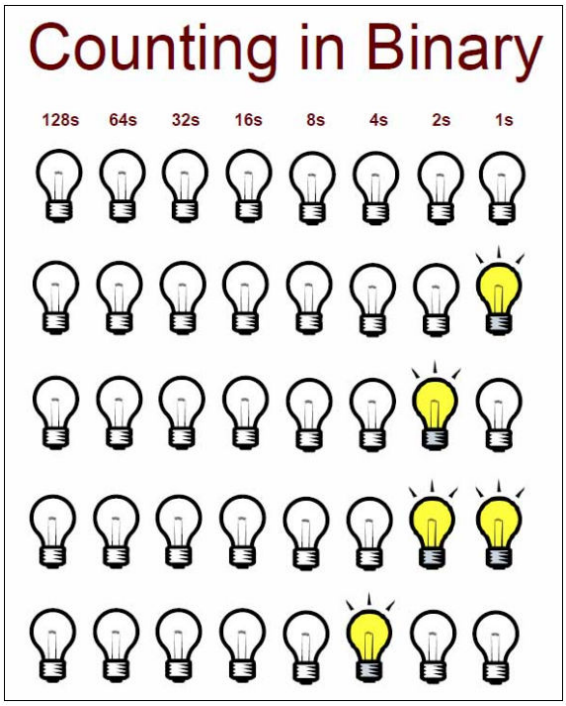
$$2^2\ 2^1\ 2^0$$
$$(1\ 1\ 0)_2 = (6)_{10}$$

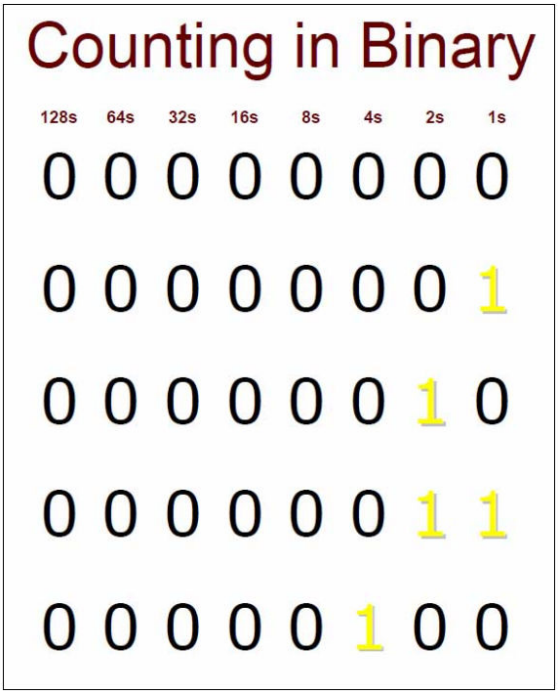
سعی کنید اعداد دودویی را به صورت لامپ‌هایی ببینید که در ستون‌هایی که هر کدام ارزش مشخصی دارند، قرار گرفته‌اند.

هر لامپی که روشن بود، عدد مربوط به ارزش ستونش را با لامپ‌های روشن دیگر جمع بزنید.

به طور مثال، شمارش ۰ و ۱ و ۲ و ۳ و ٤ به صورت زیر خواهد بود.

به ارزش ستون‌ها دقت کنید:



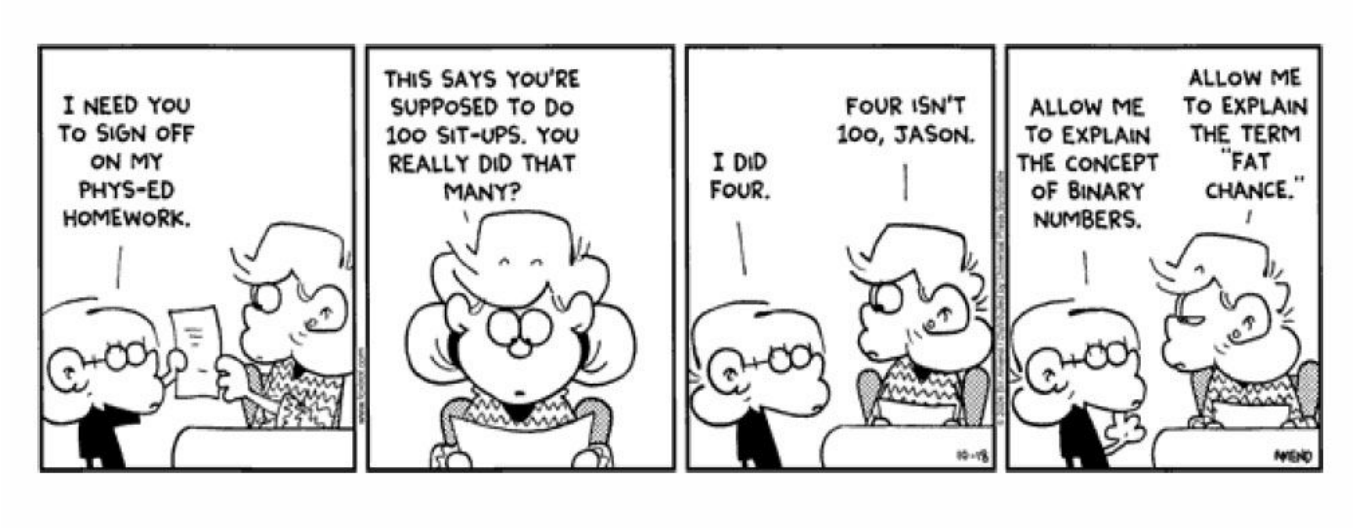


تبدیل اعداد دهدهی (Decimal) به دودویی (Binary):

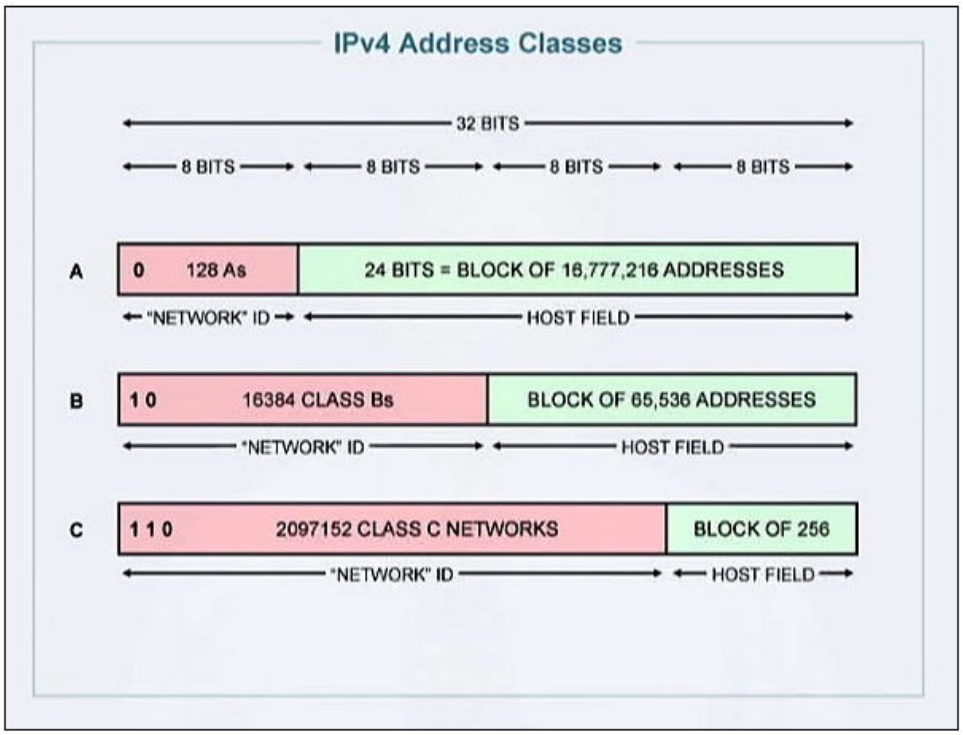
برای تبدیل اعداد دهدهی به دودویی، خیلی سریع ستون‌ها و ارزش‌های آن‌ها را بچینید و از سمت چپ شروع به تقسیم کردن عدد دهدهی به ارزش ستون‌ها کنید. (مثلاً اول ۷۵ را به ۱۲۸ تقسیم کنید) اگر عدد دهدهی بزرگ‌تر از آن ارزش بود، در آن ستون، 1 بگذارید در غیراینصورت 0 . سپس 1 یا 0 را در ارزش ضرب کنید و از عدد دهدهی کم کنید و باقیمانده را با ستون بعد مقایسه کنید... این روال را ادامه دهید تا به ستون آخر برسید.

	128	64	32	16	8	4	2	1
75	0	1	0	0	1	0	1	1
201	1	1	0	0	1	0	0	1
255	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0

تفریح: اگر توانایی‌تان در تبدیل مبناها قوی باشد، باید این جوک را درک کنید و به آن بخندید ☺ :



کلاس‌های IP :



در $IP\ v_4$ پنج کلاس مختلف قابل تصور است: کلاس‌های A، B، C، D، E.

نکته: کلاس D برای Multi casting و کلاس E برای Broad casting می‌باشد و در شبکه کاربرد خاصی ندارد.

در کامپیوتر با کلاس‌های A، B، C سر و کار داریم و کلاس‌های D و E روی هیچ کامپیوتری قابل set کردن نیست.

نکته: هر کلاس با اولین Octet از سمت چپ شناخته می‌شود.

√	.	.	.

کلاس A :

مشخصه این کلاس این است که: سمت چپ‌ترین بیت این کلاس با 0 شروع می‌شود.

کمترین IP در این کلاس (یعنی کمترین مقدارOctet چپ) 00000000 و بیشترین IP در این کلاس 01111111 است.

A	128	64	32	16	8	4	2	1	
کمترین	0	0	0	0	0	0	0	0	0
بیشترین	0	1	1	1	1	1	1	1	127

پس کلاس A در Octet سمت چپ مقداری بین 127-0 دارد.

کلاس B :

دو بیت سمت چپ این کلاس با 10 شروع می‌شود.

کمترینIP در این کلاس (کمترین مقدارOctet چپ) 10000000 و بیشترین مقدار 10111111 است.

B	128	64	32	16	8	4	2	1	
کمترین	1	0	0	0	0	0	0	0	128
بیشترین	1	0	1	1	1	1	1	1	191

پس کلاس B در Octet سمت چپ مقداری بین 191-128 دارد.

کلاس C :

سه بیت سمت چپ این کلاس با 110 شروع می‌شود.

کمترین IP در این کلاس (یعنی کمترین مقدارOctet چپ) 11000000 و بیشترین IP در این کلاس 11011111 است.

C	128	64	32	16	8	4	2	1	
کمترین	1	1	0	0	0	0	0	0	192
بیشترین	1	1	0	1	1	1	1	1	223

پس کلاس C در Octet سمت چپ مقداری بین 223 -192 دارد.

Default Subnet Mask (سابنت مَسکِ پیشفرض) :

نکته: هر کلاس یک Default Subnet Mask دارد که در زیر مشخص است:

	Default Subnet Mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

Subnet Mask به سوئیچ و روتر کمک می‌کند تا شبکه‌ای که یک کامپیوتر به آن متعلق است را شناسایی کند.

در ادامه به کاربردهای Subnet Mask آشنا خواهید شد.

Private IPs (IPهای خصوصی) :

در هر کلاس یک رِنج IP با عنوان Private IP در نظر گرفته شده است. این IPها در اینترنت تعریف نشده و غیر قابل استفاده هستند. اگر این آی.پی‌ها نباشند، در یک شبکه محلی که در یک اتاق دارید، باید تمام کامپیوترهایی که قصد اتصال به اینترنت را دارند، هر کدام جداگانه اشتراک اینترنت بگیرند. (یعنی اینطور بخواهد بود که یکی به اینترنت وصل شود و بقیه نیز از اینترنت آن استفاده کنند)

در اصطلاح گفته می‌شود IPهای خصوصی در اینترنت non-Routable هستند. (غیرقابل مسیردهی)

	Private IP Range
Class A	10.0.0.0 - 10.255.255.255
Class B	172.16.0.0 - 172.31.255.255
Class C	192.168.0.0 - 192.168.255.255

Loop Back IP Address:

رنج IP از 127.0.0.0 تا 127.255.255.255 نیز رنج Private IP به حساب می‌آیند. و آی.پی 127.0.0.1 با نام Loop Back Address شناخته می‌شود. 127.0.0.1 یعنی همین کامپیوتر جاری. هر چه به این آی.پی بفرستید در حقیقت به کامپیوتر خودتان فرستاده‌اید.

نکته: Loop Back Addressها non-Routable و non-usable هستند. (نه قابل مسیردهی و نه قابل استفاده)

Host Address و Network Address :

اگر IP یکی از کامپیوترها در یک شبکه را با Default Subnet Mask آن AND کنیم Network Address یا (IP شبکه) به دست می‌آید.

مثال:

192 . 168 . 1 . 1

AND { 11000000 . 10101000 . 00000001 . 00000001
11111111 . 11111111 . 11111111 . 00000000

پاسخ AND کردن : 11000000 . 10101000 . 00000001 . 00000000

و این یعنی : 192 . 168 . 1 . 0

به بخشی که بعد از AND کردن، تغییر نکرده است، Network Address و به بخشی که با AND کردن تغییر می‌کند، Host Address گفته می‌شود.

Host Address در حقیقت شناسه این کامپیوتر در شبکه 192.168.1 است.

پس داریم:

Class C	192	.	168	.	1	.	1
	11000000	.	10101000	.	00000001	.	00000001
Subnet Mask	255	.	255	.	255	.	0
	11111111	.	11111111	.	11111111	.	00000000
And result	192	.	168	.	1	.	0
	11000000	.	10101000	.	00000001	.	00000000
	Network Address						Host Address

نکته: دقت کنید که در هر شبکه Network Address باید برای تمام کامپیوترهای آن شبکه یکسان باشد در غیر اینصورت آن کامپیوتر در شبکه مورد نظر شما به حساب نمی‌آید و شناخته نمی‌شود.

نکته: اگر Network Address مربوط به دو کامپیوتر متفاوت باشد، چون در دو شبکه با رنج آی.پی‌های متفاوت قرار می‌گیرند، بین آن‌ها باید یک **Router** قرار گیرد تا بتوانند به یکدیگر دسترسی داشته باشند.

در هر کلاس چند هاست و چند شبکه مختلف می‌توان متصور شد؟

با توجه به اینکه در کلاس A، یک بیت سمت چپ، ثابت است و هفت بیت متغیر در اکتت سمت چپ داریم، بنابراین در این کلاس 2^7=128 شبکه مختلف می‌توان داشت و ۲٤ بیت نیز مربوط به Host Address می‌شود، پس:

در کلاس A می‌توان 2^{24}-2 (یعنی ۱۶۷۷۷۲۱٤) هاست مختلف داشت.

با توجه به اینکه در کلاس B، دو بیت سمت چپ، ثابت است و ۱٤ بیت متغیر در دو اکتت سمت چپ داریم، بنابراین در این کلاس 2^{14}=16384 شبکه مختلف می‌توان داشت و ۱۶ بیت نیز مربوط به Host Address می‌شود، پس:

در کلاس B می‌توان 2^{16}-2 (یعنی ٦٥٥۳٤) هاست مختلف داشت.

با توجه به اینکه در کلاس C، سه بیت سمت چپ، ثابت است و ۲۱ بیت متغیر در سه اکتت سمت چپ داریم، بنابراین در این کلاس 2^{21}=2**097**152 شبکه مختلف می‌توان داشت و ۸ بیت نیز مربوط به Host Address می‌شود، پس:

در کلاس C می‌توان 2^8-2 (یعنی ۲٥٤) هاست مختلف داشت.

نکته: در هر رنج IP ، کمترین وبیشترین مقدارها نمی‌توانند به عنوان Host Address استفاده شوند یعنی بیت‌های بخش Host نمی‌توانند همه 0 یا همه 1 باشند.

به طور مثال در رنج آی.پی *.192.168 به آی.پی 192.168.1.0 آی.پی شبکه یا همان Network Address گفته می‌شود و قابل استفاده نیست و به آی.پی 192.168.1.255 آی.پی انتشار یا BroadCast IP گفته می‌شود و باز هم قابل استفاده نیست. (اگر اطلاعاتی را به 192.168.1.255 بفرستید، به تمام کامپیوترهای شبکه فرستاده می‌شود)

Class	Leading Bits	Size of *Network Number* Bit field	Size of *Rest* Bit field	Number of Networks	Addresses per Network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

چند مثال:

مثال ۱: Network IP مربوط به آی.پی زیر را به دست آورید:

192.149.24.191

پاسخ: با توجه به اینکه در کلاس C قرار دارد، ساب‌نت مسک پیشفرض (Default Subnet Mask) برابر است با: 255.255.255.0

به جای AND کردن می‌توانیم هر جا که 255 بود خود آن عدد و هر جا که 0 بود 0 می‌نویسیم. پس آی.پی شبکه برابر است با: 192.149.24.0

مثال ۲: Network IP مربوط به آی.پی زیر را به دست آورید:

10.10.10.10
255.0.0.0
10.0.0.0

روش دیگر: با استفاده از AND کردن بیت‌ها:

```
AND { 11111111 . 00000000 . 00000000 . 00000000
    { 00001010 . 00001010 . 00001010 . 00001010
      00001010 . 00000000 . 00000000 . 00000000
```

این یعنی 10.0.0.0 (Network Address).

بحث Subnetting:

همیشه رنج آی.پی‌های زیادی در اختیار نداریم که بخواهید با تغییر رنج، یک شبکه جدید ایجاد کنیم!

فرض کنید برای کشور ایران، یک رنج آی.پی به صورت 117.*.*.* از طرف مؤسسه مرکز تخصیص آی.پی به کشورها در نظر گرفته شده است.

طبیعتاً باید برای ۳۲ استان کشور شبکه ایجاد کرد به طوری که دقیقاً مشخص باشد یک آی.پی از کدام استان به اینترنت متصل شده است.

می‌دانید که آی.پی بالا در کلاس A قرار دارد یعنی می‌توان $2^{24}-2$ کامپیوتر مختلف را همزمان به اینترنت وصل کرد.

اما مشکل این است که ما چگونه باید این رنج را به شبکه‌های مختلف تقسیم کنیم؟

بله،اگر دستمان باز بود، کلاس B را انتخاب می‌کردیم و می‌گفتیم مثلاً: 128.1.*.* تهران باشد. 128.2.*.* مثلاً اصفهان باشد و ...

اما الان ما فقط یک آی.پی شبکه در اختیار داریم.

اینجاست که بحث Subnetting مطرح می‌شود.

Subnetting یعنی تبدیل یک شبکه (Net) به چندین زیرشبکه (Subnet).

در این عملیات، ما با تغییر Subnet Mask تعدادی از بیت‌های مربوط به Host را قرض گرفته و به بیت‌های Network اختصاص می‌دهیم.

اگر فقط یک بیت از بخش Host را قرض بگیریم، دو شبکه مختلف می‌توانیم ایجاد کنیم.

در مثال بالا داریم:

IP: 117.0.0.0 = 01110101.00000000.00000000.00000000
Default Subnet Mask: 255.0.0.0 = 11111111. 00000000.00000000.00000000

یک بیت را برای Network Address قرض می‌گیریم. پس Subnet Mask دیگر همان ساب‌نت مسک پیشفرض (Default) نخواهد بود. بلکه سفارشی است. یعنی:

Custom Subnet Mask: 11111111.10000000.00000000.00000000 = 255.128.0.0

در این صورت یکی از شبکه‌ها رنج آی.پی‌هایشان می‌شود:

117.0.0.0 تا 117.127.255.255

و دیگری می‌شود:

117.128.0.0 تا 117.255.255.255

یعنی دو شبکه مختلف با رنج آی.پی‌های مختلف از همان آی.پی اول ایجاد کردیم! به این کار Subnetting گفته می‌شود.

حالا محاسبه کنید که برای اینکه آن رنج را به ۳۲ شبکه مختلف تقسیم کنیم، باید چند بیت را قرض بگیریم؟

واضح است که باید دید با چند بیت می‌توان ۳۲ را نمایش داد؟

با ۵ بیت.

پس باید ۵ بیت از بخش Host Address را برای شبکه قرض گرفت:

Custom Subnet Mask: 11111111.11111000.00000000.00000000 = 255.248.0.0

در شبکه بالا، تعداد زیرشبکه‌ها می‌شود: « ۲ به توان تعداد بیت‌های قرض گرفته شده »

و تعداد هاست‌ها در هر زیر شبکه می‌شود: « ۲ به توان تعداد بیت‌های باقیمانده برای بخش Host منهای ۲ » (یعنی منهای پایین‌ترین و بالاترین مقدار هاست که قبلاً گفته شد که قابل استفاده نیست)

پس:

تعداد زیرشبکه‌ها = 2^5 = ۳۲ (یعنی همان چیزی که انتظار داشتیم)

تعداد آدرس‌های هاست قابل استفاده در هر زیرشبکه: 2^{19}-2 = 524288-2 = ۵۲٤۲۸۶

فرمول‌های کلی:

تعداد زیرشبکه‌ها: 2^s

s = تعداد بیت‌های قرض گرفته شده.

تعداد هاست‌های قابل استفاده: 2^h-2

h = تعداد بیت‌های بخش Host

مثال: با توجه به ساب‌نت مسک 255.255.255.192 تعیین کنید که این شبکه چند زیرشبکه و در هر زیرشبکه چند هاست می‌تواند داشته باشد؟

	128	64	32	16	8	4	2	1
192	1	1	0	0	0	0	0	0

s = تعداد بیت های قرض گرفته شده = 2

تعداد زیر شبکه = $2^s = 2^2 = 4$

	128	64	32	16	8	4	2	1
192	1	1	0	0	0	0	0	0

h= تعداد بیت های در نظر گرفته شده برای هاست = 6

تعداد Host $= 2^h = 2^6 - 2 = 62$

مثال دیگر:

Number of needed subnets **14**
Number of needed usable hosts **14**
Network Address **192.10.10.0**

Address class C

Default subnet mask 255 . 255 . 255 . 0

Custom subnet mask 255 . 255 . 255 . 240

Total number of subnets 16

Total number of host addresses 16

Number of usable addresses 14

Number of bits borrowed 4

مثال دیگر:

Number of needed subnets **1000**
Number of needed usable hosts **60**
Network Address **165.100.0.0**

Address class B
Default subnet mask 255 . 255 . 0 . 0
Custom subnet mask 255 . 255 . 255 . 192
Total number of subnets 1,024
Total number of host addresses 64
Number of usable addresses 62
Number of bits borrowed 10

تمرین بیشتر:

سعی کنید تمامی تمرینات کتاب IP addressing and subnetting (workbook) را حل کنید.

IPv6:

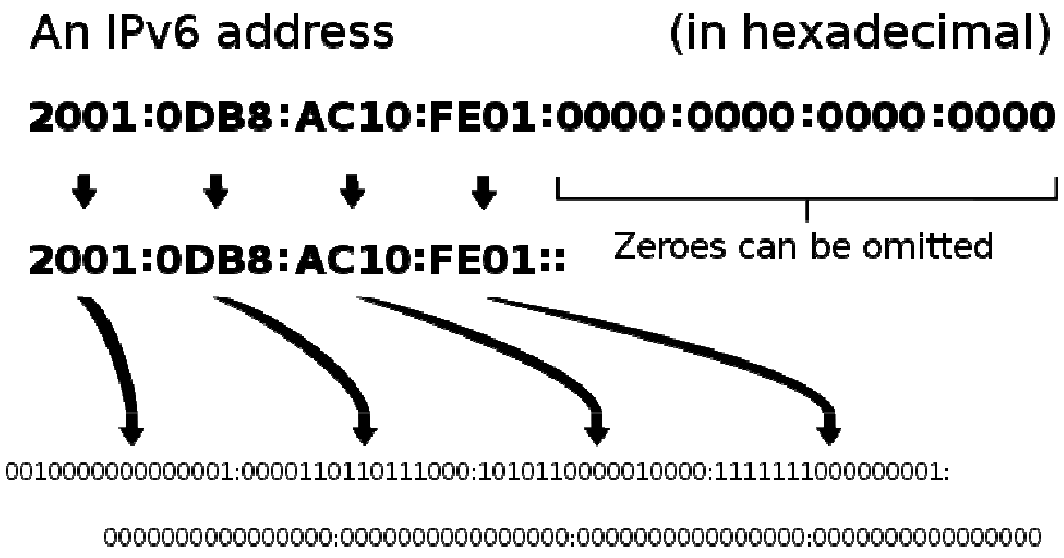
با توجه به رزرو بودن بسیاری از رنج‌های IP در ورژن ٤ (مثل آی.پی‌های Private) و با توجه به اینکه دائماً شاهد افـزایش پایانـه‌هـای متصل به اینترنت هستیم، پیش‌بینی می‌شود به زودی با کمبود IP معتبر مواجه شویم.

به همین دلیل در سال ۱۹۹۸ مؤسسه IETF ورژن ۶ از IP را معرفی کرد.

این نسخه، ۱۲۸ بیتی است در حالی که IP نسخه ٤، ۳۲ بیتی بود. در نتیجه در IPv6 تعداد 2^{128} یعنی تقریباً ۳.٤ ضـرب در 10^{38} آی.پـی مختلف می‌توان متصور شد! و این انعطاف‌پذیری و قدرت تصمیم‌گیری بهتری نسبت به ٤ میلیارد آی.پی در IPv4 به انسان می‌دهد.

برای نمایش IPv6 از مبنای ۱۶ (Hexadecimal) استفاده می‌شود.

پس ۸ بخش خواهد داشت که با : از هم جدا می‌شوند. در هر بخش ٤ عدد می‌بینید بین 0 تا F:



بخش‌هایی که 0 هستند، می‌توانند نمایش داده نشوند.

هر عدد در مبنای ۱۶ را می‌توان با ٤ بیت نشان داد ($2^4=16$) پس ۳۲ عدد داریم که هر کدام ٤ بیتـی هسـتند، یعنـی IPv6، ۱۲۸ بیتـی است.

مشهورترین پروتکل‌های شبکه:

پروتکل: قوانینی هستند که ارتباط بین شبکه‌ها را مدیریت می‌کنند.

Protocol: is a rule that governs how networks communicate.

TCP/IP Protocol: Transmission Control Protocol / Internet Protocol

TCP/IP فقط یک پروتکل نیست بلکه شامل چندین SubProtocol (زیرپروتکل) است مانند ARP ، UDP، TCP، IP و... اما اکثر مدیران شبکه به این گروه از پروتکل‌ها TCP/IP و یا حتی IP می‌گویند.

ریشه‌های TCP/IP را باید در سازمان دفاع آمریکا (Defense Of The U.S.) جست که این پروتکل را برای Advanced Research Projects Agency NETwork (شبکه آژانس پروژه‌های تحقیقاتی پیشرفته) (که مخفف آن ARPANET است) توسعه داد.

ARPANET نمونه اولیه اینترنت امروزی است.

این پروتکل به خاطر Open source بودن (استفاده از کدها به صورت آزاد و رایگان) خیلی سریع (1960-70) گسترش یافت .

برای اطمینان از انتقال صحیح یک Packet از یک نقطه به نقطه دیگر، از پروتکل TCP استفاده می‌شود. این پروتکل در لایه Transport از مدل OSI عمل می‌کند.

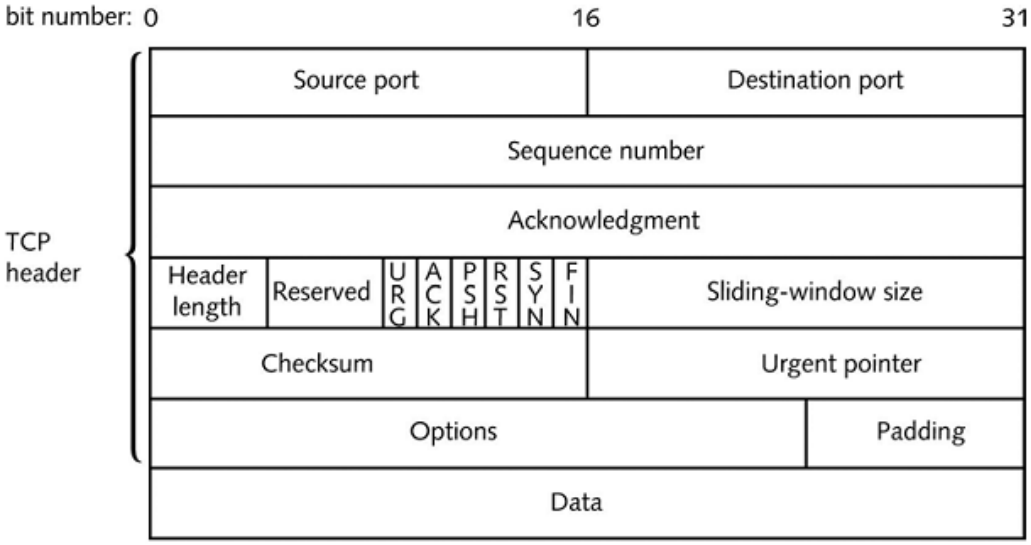
وظیفه این پروتکل در یک جمله:

Provides reliable data delivery services

یعنی سرویس‌های مربوط به تحویل موفقیت آمیز داده‌ها را فراهم می‌کند.

اجزای TCP:

در حقیقت TCP با استفاده از اجزایی به اصل داده اضافه می‌کند؛ مثل checksum و acknowledgment و شماره port مبدأ و مقصد، کار اطمینان از صحت ارسال داده‌ها را انجام می‌دهد.



Port چیست؟

همانطور که می‌دانید برنامه‌ها و سرویس‌های مختلفی مثل مرورگر، ایمیل، برنامه چت و نرم افزارهای مختلف دیگر، از طریق یک اتصال شبکه کار می‌کنند. سؤال این است که وقتی یک Packet وارد کامپیوتر شما می‌شود کامپیوتر چگونه می‌فهمد که این Packet برای برنامه ایمیل است یا مرورگر یا دیگر برنامه‌ها؟

پاسخ: هر برنامه یا سرویس در دنیا یک شماره مختص و ثبت شده دارد که به آن شماره port گفته می‌شود. این شماره توسط مؤسسه IANA (مخفف Internet Assigned Number Authority به معنی مسؤول عدد نسبت داده شده اینترنتی) تعیین می‌شود.

لیستی از پورت‌ها در آدرس مقابل قابل مشاهده است: http://www.iana.org/assignments/port-numbers

به طور مثال شماره پورت برنامه Telnet عدد ۲۳ است، شماره پورت Ftp عدد ۲۰، شماره پورت Http عدد ۸۰ و شماره پورت Smtp عدد ۲۵ است.

برخی از مهم‌ترین سرویس یا برنامه‌ها و شماره پورت آن‌ها:

Table 4-3 Commonly used TCP/IP port numbers

Port Number	Process Name	Protocol Used	Description
7	ECHO	TCP and UDP	Echo
20	FTP-DATA	TCP	File Transfer - Data
21	FTP	TCP	File Transfer–Control
22	SSH	TCP	Secure Shell
23	TELNET	TCP	Telnet
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP and UDP	Domain Name System
69	TFTP	UDP	Trivial File Transfer Protocol
80	HTTP	TCP and UDP	World Wide Web HTTP
110	POP3	TCP	Post Office Protocol 3
119	NNTP	TCP	Network News Transport Protocol
143	IMAP	TCP	Internet Message Access Protocol
443	HTTPS	TCP	Secure implementation of HTTP

وقتی یک Packet به پروتکل TCP تحویل داده می‌شود در همان ابتدا با زدن برچسب شماره Port مشخص می‌کند که این Packet از چه برنامه‌ای آمده و به چه برنامه‌ای خواهد رفت.

Acknowledgment :

پروتکل TCP بر روی هر Packet یک عدد به عنوان Acknowledgment (ACK) (به معنی تأییدیه) قرار می‌دهد و اگر Packet با موفقیت به مقصد رسید این عدد به عنوان تأییدیه ارسال صحیح، به فرستنده ارسال می‌شود.

Checksum :

مانند روش CRC روشی برای چک کردن رخ دادن یا ندادن خطا ارائه می‌کند. در حقیقت از Header و داده‌ها محافظت می‌کند.
در مواردی که نیاز به اطمینان از رسیدن موفقیت آمیزداده‌ها است از checksum استفاده می‌شود.

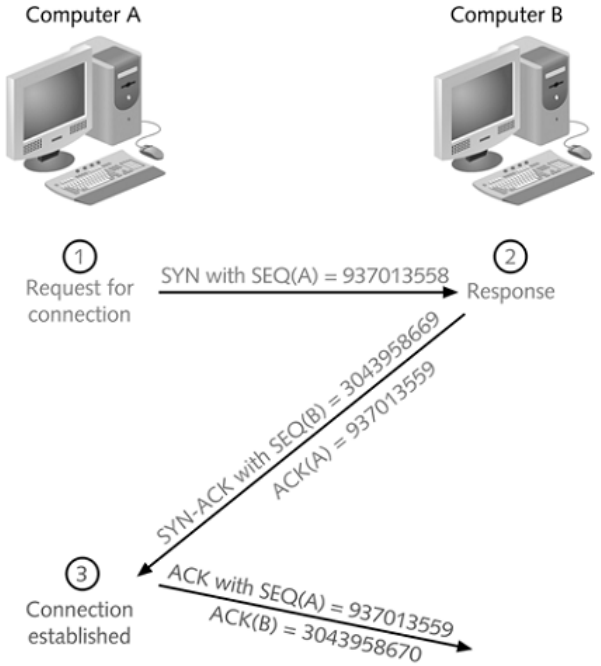


FIGURE 4-3 *Establishing a TCP connection*

تصویری از اجزای یک قطعه داده که با پروتکل TCP ارسال شده است:

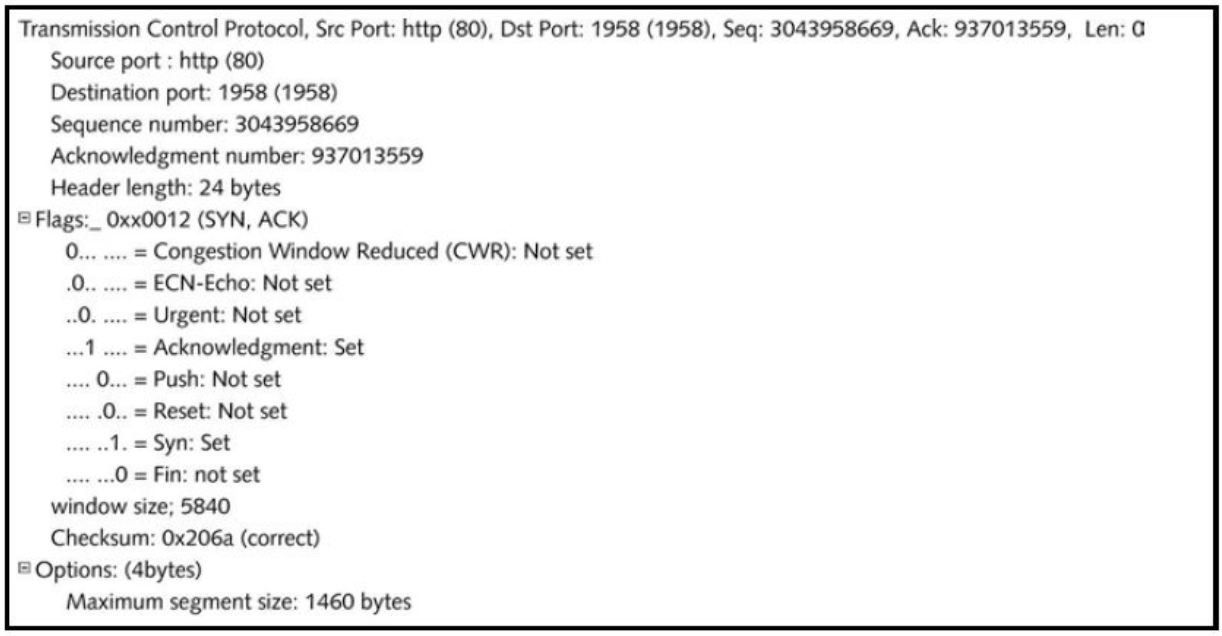


FIGURE 4-2 *TCP segment data*

UDP (User Datagram Protocol):

در پروتکل TCP رسیدن صحیح Packetها مهم است اگر یک Packet به درستی نرسد عمل ارسال دوباره و دوباره اتفاق می‌افتد. در حقیقت در این روش به محض ارسال یک Packet، یک ساعت فرضی شروع به کار می‌کند، اگر در زمان مشخصی ACK رسید همه چیز درست است اما اگر در آن زمان بسته نرسید دوباره و دوباره ارسال می‌شود. این کار آنقدر اتفاق می‌افتد تا این که بسته برسد و یا اینکه نهایتاً پیغام Destination unreachable مشاهده شود. به عبارتی پروتکل TCPرسیدن بسته را ضمانت می‌کند:

TCP Guarantees Delivery

این در مورد ارسال فایل و یا ایمیل خوب است اما تصور کنید بخواهیم صدا یا ویدئو را به صورت زنده و Real-time از طریق TCP ارسال کنیم (مثل بحث جدید Voice Over IP = VOIP که در آن شما از طریق اینترنت با افراد مختلف گفتگوی صوتی یا ویدئویی انجام می‌دهید) آیا در این نوع ارسال‌ها، زمان کافی (Time) برای این هست که هر Packet که ارسال شد منتظر جواب بمانیم و اگر اشتباه شد دوباره ارسال کنیم؟

واضح است که خیر، نمی‌توان کاربر را آنطرف خط معطل نگاه داشت تا یک پکت به مقصد برسد!

گفته می‌شود: There is no time to retransmit data

در این حالت به جای TCP از UDP استفاده می‌شود.

پس TCP برای ارسال داده و UDP برای ارسال صدا و ویدئو است. (دقت کنید که ویدئو و صدا به صورت زنده و نه یک کلیپ ویدئویی که قبلاً ضبط شده و حالا می‌خواهید بفرستیم)

با توجه به توضیحات بالا مدل UDP بسیار ساده‌تر است:

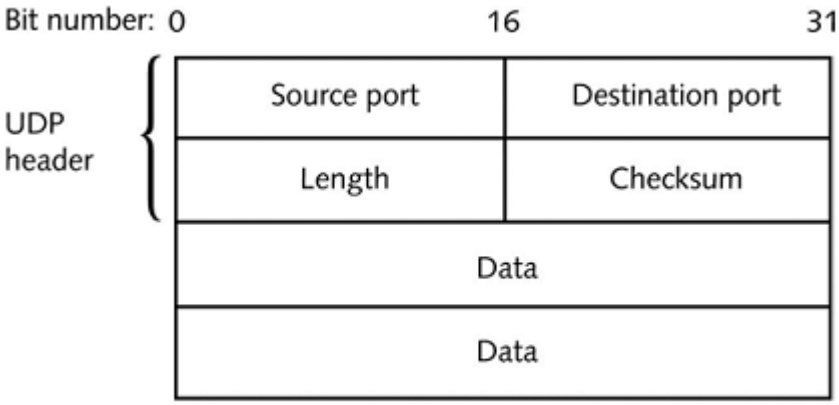


FIGURE 4-4 *A UDP Segment*

نکته ۱: checksum در پروتکل UDP اختیاری است اما برای امنیت بیشتر در ارسال، بهتر است که باشد.

نکته ۲: در اصطلاح گفته می‌شود TCP، وابسته به اتصال (Connection-Oriented) و UDP، غیروابسته به اتصال (Connection-Less) می‌باشد.

وقتی گفته می‌شود TCP یک مدل اتصال محور است یعنی یک کانکشن باید بین مبدأ و مقصد برقرار (Establish) باشد تا پروتکل شروع به انتقال داده کند.

تمرین: برای فهم بهتر TCP و UDP، متن زیر را به فارسی ترجمه کنید:

TCP is a connection-oriented subprotocol, which means that a connection must be established between communicating nodes before this protocol will transmit data. TCP further ensures reliable data delivery through sequencing and checksums. Without such measures, data would be transmitted indiscriminately, without checking whether the destination node was offline, for example, or whether the data became corrupt during transmission. Finally, TCP provides flow control to ensure that a node is not flooded with data.

UDP is a connectionless transport service. In other words, UDP offers no assurance that packets will be received in the correct sequence. In fact, this protocol does not guarantee that the packets will be received at all. Furthermore, it provides no error checking or sequencing. Nevertheless, UDP's lack of sophistication makes it more efficient than TCP. It can be useful in situations where a great volume of data must be transferred quickly, such as live audio or video transmissions over the Internet. In these cases, TCP— with its acknowledgments, checksums, and flow control mechanisms—would only add more overhead to the transmission. UDP is also more efficient for carrying messages that fit within one data packet.

IP (Internet Protocol):

Internet Protocol در لایه Network عمل می‌کند. این پروتکل اطلاعاتی در مورد این که چگونه (How) و در کجا (Where) باید برسند ارائه می‌نماید. این پروتکل شامل آدرس مبدأ و مقصد داده‌هاست. این مدل همان مدل مربوط به Packet است که قبلاً بحث شد. به Packet، (IP Datagram) نیز گفته می‌شود.

لیست برخی دیگر از پروتکل‌ها :

پروتکل‌های لایه Application :

SMTP (Simple Mail Transfer Protocol).
POP3 (Post Office Protocol 3).
FTP (File Transfer Protocol).
HTML (Hyper Text Markup Language).
HTTP (Hyper Text Transfer Protocol).

پروتکل‌های لایه Transport :

TCP
UDP

پروتکل‌های لایه Network :

PPP (Point to Point Protocol).
IPv4
IPv6
PPPOE (Point to Point Protocol Over Ethernet).
OSPF (Open Shortest Path First)

دنیای بی‌سیم
Wireless

منظور از Wireless همان امواج رادیویی است .

ویکی‌پدیا در مورد امواج رادیویی می‌گوید:

موج‌های رادیویی گونه‌ای موج الکترومغناطیسی است که طول موج آن در طیف الکترومغناطیسی بلندتر از InfraRed است. همانند دیگر موج‌های الکترومغناطیسی، موج‌های رادیویی نیز با سرعت نور حرکت می‌کنند. موج‌های رادیویی به صورت طبیعی توسط آذرخش و اجرام فلکی تولید می‌شوند. موج‌های رادیویی تولید شده بصورت مصنوعی، در سیستم‌های ارتباطاتی ثابت و متحرک، broadcasting، رادار و دیگر سیستم‌های ناوبری، ارتباطات ماهواره‌ای، شبکه‌های رایانه‌ای و بسیاری دیگر کاربرد دارند.

کمی بحث تخصصی در مورد امواج رادیویی:

موج الکترومغناطیسی (یا Electromagnetic Radiation = EMR) نوعی موج است که در فضا انتشار می‌یابد و از میدان‌های الکتریکی و مغناطیسی ساخته شده‌است. این میدان‌ها در حال انتشار بر یکدیگر و بر جهت پیشروی موج عمود هستند.نسبت به طول موج و فرکانسی که دارند به انواع مختلفی تقسیم می‌شوند:

از فرکانس ۳۰ اگزا هرتز تا ۳۰۰ اگزا هرتز را اشعه گاما (gamma rays) می‌نامند.

از فرکانس ۳ اگزا هرتز تا ۳۰ اگزا هرتز را اشعه ایکس سخت (HX = Hard X-rays) می‌نامند.

از فرکانس ۳۰ پتا هرتز تا ۳ اگزا هرتز را اشعه ایکس نرم (SX = Soft X-rays) می‌نامند.

از فرکانس ۳ پتا هرتز تا ۳۳ پتا هرتز را اشعه فرا بنفش دور (EUV) می‌نامند.

از فرکانس ۷۵۰ ترا هرتز تا ۳ پتا هرتز را اشعه فرا بنفش نزدیک (NUV) می‌نامند.

از فرکانس ٤۰۰ ترا هرتز تا ۷۵۰ ترا هرتز را نور مرئی (visible light) می‌نامند.

از فرکانس ۲۱٤ ترا هرتز تا ٤۰۰ ترا هرتز را فروسرخ نزدیک (NIR = Near ultraviolet) می‌نامند.

از فرکانس ۱۰۰ ترا هرتز تا ۲۱٤ ترا هرتز را موج کوتاه فروسرخ (SIR) می‌نامند.

از فرکانس ۳۷,۵ ترا هرتز تا ۱۰۰ ترا هرتز را موج متوسط فروسرخ (MIR) می‌نامند.

از فرکانس ۲۰ ترا هرتز تا ۳۷,۵ ترا هرتز را موج بلند فروسرخ (HIR) می‌نامند.

از فرکانس ۳۰۰ گیگا هرتز تا ۲۰ ترا هرتز را فروسرخ بسیار دور (FIR = Far Infrared) می‌نامند.

موج‌های با فرکانس پایین‌تر را در دسته امواج رادیویی (radio waves) **می‌دانند:**

از فرکانس ۳۰ گیگا هرتز تا ۳۰۰ گیگا هرتز را بسامد مافوق بالا (EHF) می‌نامند. (ریزموج = microwaves)

از فرکانس ۳ گیگا هرتز تا ۳۰ گیگا هرتز را بسامد بسیار بالا (SHF) می‌نامند. (ریزموج = microwaves)

از فرکانس ۳۰۰ مگا هرتز تا ۳ گیگا هرتز را بسامد فرابالا (UHF) می‌نامند.

از فرکانس ۳۰ مگا هرتز تا ۳۰۰ مگا هرتز را بسامد خیلی بالا (VHF) می‌نامند.

از فرکانس ۳ مگا هرتز تا ۳۰ مگا هرتز را بسامد بالا (HF) می‌نامند.

از فرکانس ۳۰۰ کیلو هرتز تا ۳ مگا هرتز را بسامد متوسط (MF) می‌نامند.

از فرکانس ۳۰ کیلو هرتز تا ۳۰۰ کیلو هرتز را بسامد پایین (LF) می‌نامند.

از فرکانس ۳ کیلو هرتز تا ۳۰ کیلو هرتز را بسامد خیلی پایین (VLF) می‌نامند.

از فرکانس ۳۰۰ هرتز تا ۳ کیلو هرتز را بسامد در حد صوت (VF) می‌نامند.

از فرکانس ۳۰ هرتز تا ۳۰۰ هرتز را بسامد بسیار پایین (ELF) می‌نامند.

γ = Gamma rays
HX = Hard X-rays
SX = Soft X-Rays
EUV = Extreme ultraviolet
NUV = Near ultraviolet
Visible light
NIR = Near infrared

MIR = Moderate infrared
FIR = Far infrared

Radio waves:
EHF = Extremely high frequency (Microwaves)
SHF = Super high frequency (Microwaves)
UHF = Ultrahigh frequency
VHF = Very high frequency
HF = High frequency
MF = Medium frequency
LF = Low frequency
VLF = Very low frequency
VF = Voice frequency
ULF = Ultra low frequency
SLF = Super low frequency
ELF = Extremely low frequency

تحقیق: در مورد سلاح HAARP و ربط آن به امواج رادیویی تحقیق کنید!

دو نوع انتقال از طریق Wireless :

۱- Analog Radio :

اگر بخواهیم صدای انسان را از طریق Wireless ارسال کنیم یک مشکل پیش می‌آید و آن این است که فرکانس صدایی که انسان می‌شنود از 20 - 20000 Hz می‌باشد در حالی که فرکانس امواج رادیویی اکثراً در حد مگا یعنی چندین میلیون هرتز (لرزش در ثانیه) است!

طبیعتاً ارسال فرکانس صدای انسان از طریق Wireless در حالت عادی بعید به نظر می‌رسد. چگونه موجی با چند هزار بار لرزش را روی موجی با میلیون‌ها بار لرزش ارسال کنیم؟

در نتیجه باید از روش‌هایی برای ترکیب صدای انسان با امواج رادیویی استفاده کرد.

یکی از این روش‌ها در نظر گرفتن موجی به نام Carrier Signal (سیگنال حامل) است.

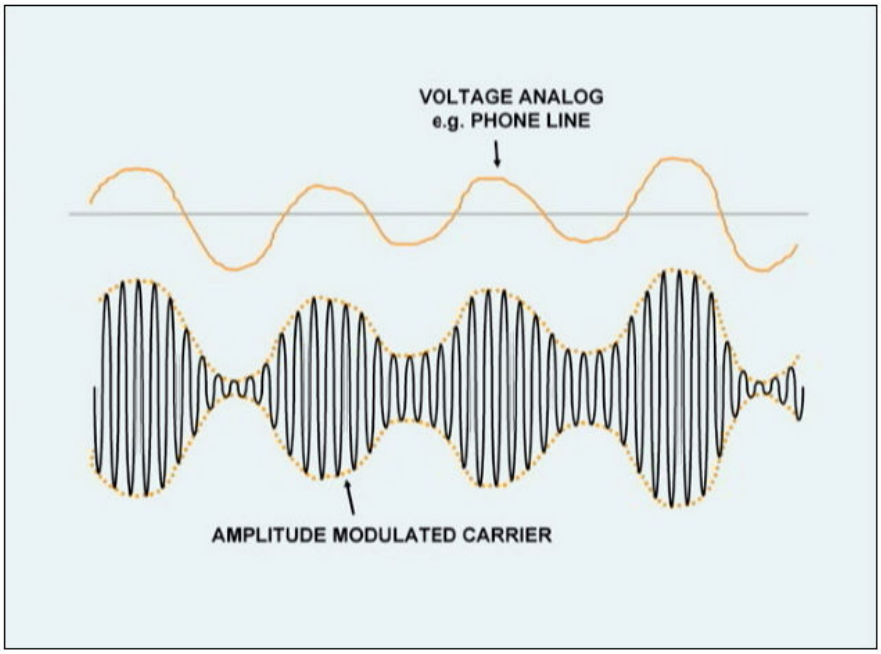
روش‌های Analog Radio در انتقال اطلاعات:

1- Amplitude Modulation (AM) :

در این روش میدان را در ثانیه طوری کم و زیاد می‌کنند یا (خواص سیگنال را طوری تغییر می‌دهند)، که در نهایت موجی شبیه به موج صدای انسان، ایجاد شود و سیگنال نهایی شبیه به سیگنال اولیه شود. یعنی پس از اینکه به مقصد رسید و Demodulation شد (با استفاده از مودم) سیگنال مورد نظر ایجاد گردد.

در کل در این روش روی تغییر میدان سیگنال کار می‌کنند. (سطح میدان را بالا و پایین می‌آورند).

به تصویر زیر دقت کنید:



نکته: بزرگ‌ترین عیب AM این است که بسیار به نویز (Noise) حساس است. AM به آب یا باران نیز حساس است.

حالا که کلمه Noise را به کار بردیم، بد نیست کمی در مورد عوامل مخرب سیگنال‌ها صحبت کنیم:

عوامل مخرب و محدودیت‌ها در امواج رادیویی:

۱- Spreading – Propagation : امواج هر چه دورتر می‌شوند ضعیف‌تر می‌شوند.

۲- موانع؛ از جمله:

- Water (آب): از بزرگ‌ترین موانع عبور امواج است.

تحقیق: با توجه به مانع بودن آب در انتشار امواج رادیویی، تحقیق کنید که چطور می‌توان به صورت بی‌سیم با یک زیردریایی ارتباط برقرار کرد؟ یا زیردریایی‌ها چطور با یکدیگر تماس برقرار می‌کنند؟

- Wood (چوب)
- Concrete (بتون)

۳- Fading (محو شدن): سیگنال‌ها در یکدیگر محو می‌شوند.

آیا تا به حال متوجه شده‌اید که صدای بلندگوی مساجد شهر در هنگام اذان صبح به راحتی به گوش می‌رسد اما در ظهر و شب نمی‌توان چیزی از آن را شنید؟ چون امواج بلندگو در امواجی که از انسان‌ها و ماشین‌ها تولید می‌شود، محو می‌شوند.

٤- یکی دیگر از موانع این است که برای کار کردن در سطح گسترده باید از دولت اجازه گرفت (و از فرکانسی استفاده کرد در محدوده کاری شما توسط سازمان دیگری استفاده نشده باشد و موجب تداخل شود)

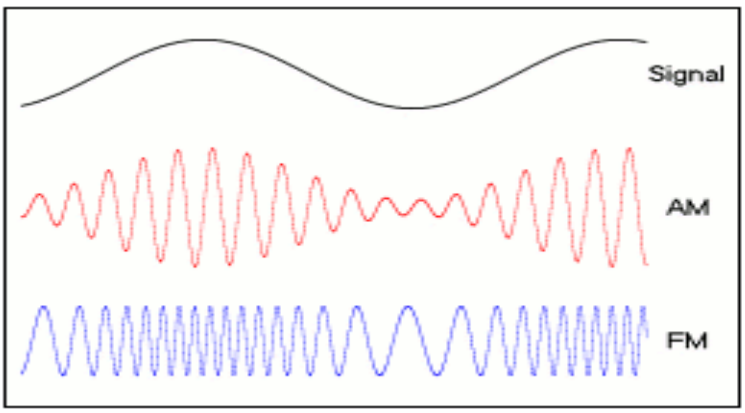
نکته : سیگنال‌های با فرکانس بالاتر در عبور از موانع دچار مشکلات بیشتری هستند و سخت‌تر عبور می‌نمایند.

روش بهبود یافته AM، روش FM است.

2- Frequency Modulation (FM) :

در این روش، تعداد فرکانس را در یک ثانیه تغییر می‌دهند. (فرکانس را کم و زیاد می‌کنند).

برای درک بهتر آنچه که اتفاق می‌افتد، به تصویر زیر دقت کنید:



توجه: در یک ثانیه، تعداد لرزش (فرکانس) ثابت است و فقط میزان آن در یک ثانیه کم و زیاد می‌شود و از روی میزان فشردگی فرکانس متوجه می‌شوند که منظور چه مقدار ولتاژ است .

3- Phase Modulation (PM) :

این روش با جابجایی موج‌ها کار می‌کند و هنوز، خیلی معمول نشده است.

۲- Digital Radio :

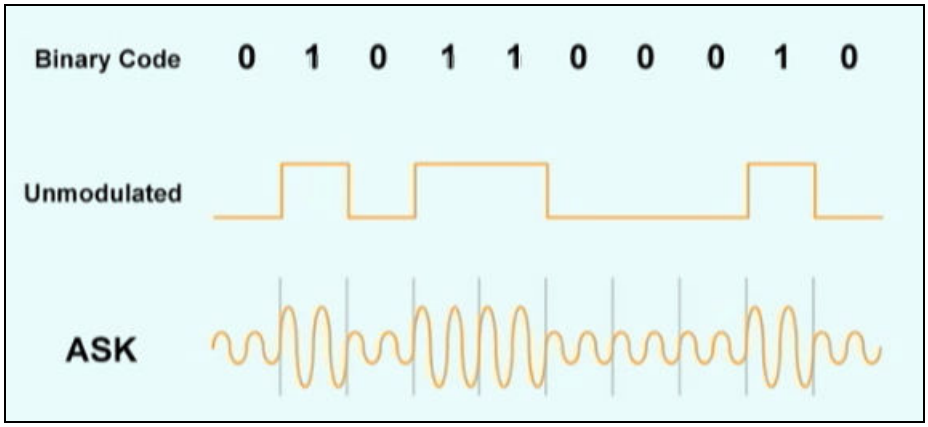
منظور از Digital پالس‌هایی است که نماد صفر و یک شوند .

سؤال این است که چطور می‌توان روی یک موج رادیویی پالس‌هاس صفر و یک را ارسال کرد و در نهایت چطور متوجه شد که این موج ارسال شده، صفر است یا یک؟

روش‌های Digital Radio (رادیویی دیجیتال) در انتقال اطلاعات:

1- Amplitude Shift – Keying (ASK) :

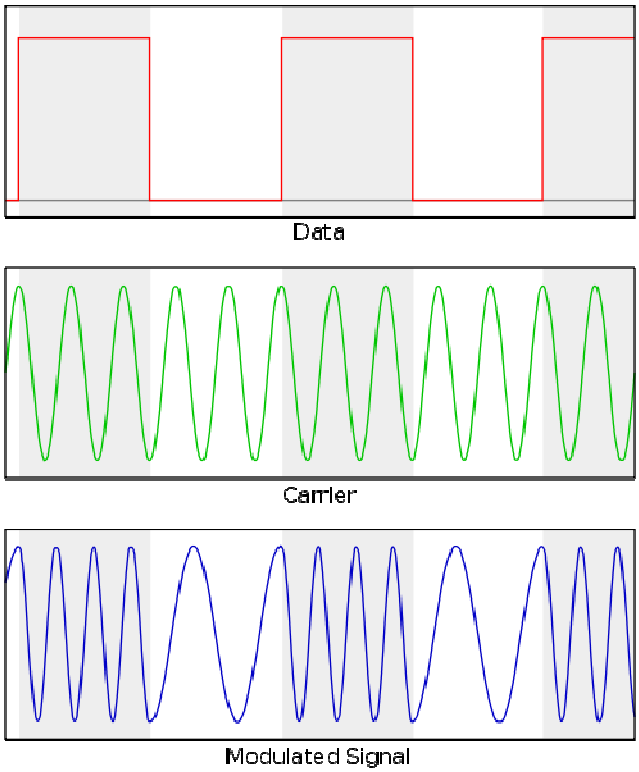
این روش دو سیگنال با میدان‌های مختلف (یکی با میدان پایین و دیگری با میدان بالا) در نظر می‌گیرند و بین این دو سیگنال مدام Shift می‌کند. اگر موج با میدان بالایی ارسال شد یعنی یک و اگر موج با میدان پایینی ارسال شد یعنی صفر.



2- Frequency Shift – Keying (FSK) :

در این روش دو سیگنال با فرکانس‌های مختلف یکی به عنوان صفر و یکی به عنوان یک در نظر می‌گیرند و داده‌ها را ارسال می‌کنند.

به تصویر زیر دقت کنید:



روش‌های دیگر:

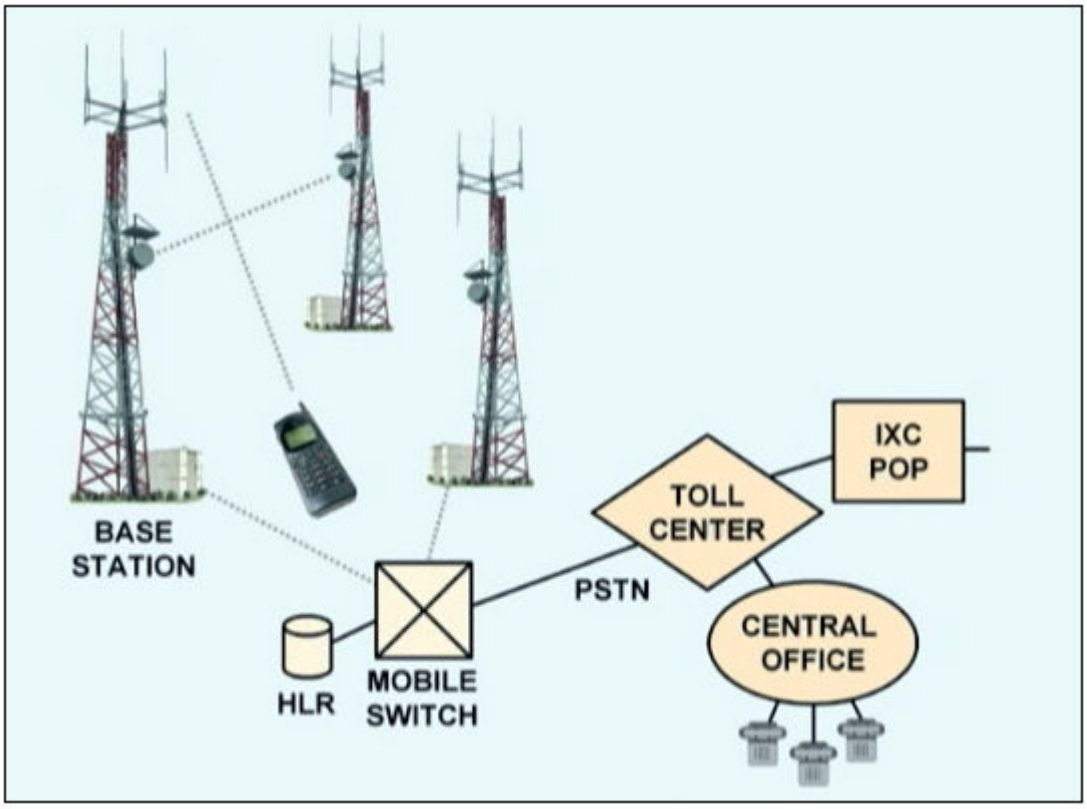
3- Phase Shift – Keying (PSK) .

4- QAM Shift – Keying (QSK) : این روش ترکیبی از PSK و ASK می‌باشد.

ارتباطات سیار

Mobile Communication

مطمئناً در نقاط مختلف شهر، دکل‌ها یا برج‌هایی را که مربوط به ارتباطات موبایلی است، دیده‌اید.



به آن‌ها در اصطلاح Base Station یا BS گفته می‌شود هرکدام از سه جزءِ تشکیل شده‌اند:

۱- آنتن (Antenna)

۲- دکل یا برج (Tower)

۳- مخزن تولید الکتریسیته (برق) یا BTS .

به این مخزن، BS Transceiver (ایستگاه پایه ارسال و دیافت کننده) می‌گویند.

این مخازن معمولاً با کابل فیبر نوری به سوئیچ‌های مخابراتی که به نام Mobile Switch شناخته می‌شوند، متصل هستند.

دکل‌هایی که در نقاط دورتری نسبت به سوئیچ قرار گرفته‌اند و امکان کابل‌کشی نیست، با استفاده از دیش به دکل‌های نزدیک‌تر متصل‌اند. (به تصویر بالا دقت کنید)

در مخابرات، سوئیچ موبایل به کامپیوتری متصل است که بر روی این کامپیوتر یک بانک اطلاعاتی (Database) قرار دارد که در اصطلاح به آن HLR می‌گویند (مخفف Home Location Register)

مفهوم Registration یا ثبت نام و روال یافتن شما و گوشی موبایلتان جهت ارسال سیگنال به آن:

وقتی گوشی موبایل شما روشن می شود به نزدیک‌ترین دکل متصل شده و یک پیغام به آن می‌فرستند که در اصطلاح گفته می‌شود گوشی به دکل «سلام می‌کند».

گوشی موبایل شما یک شماره سریال یکتا دارد. این شماره سریال و شماره خط شما به همراه شماره دکل به سوئیچ ارسال می‌شود و سوئیچ این شماره‌ها را در دیتابیس HLR ذخیره می‌کند. هر گوشی معمولاً هر ۱۰ الی ۳۰ ثانیه (بسته به نوع گوشی) وظیفه دارد موقعیت خود را در دیتابیس ثبت کند. به این پروسه Registration می‌گویند.

به سیگنالی که از گوشی ما به دکل ارسال می‌شود یا بالعکس به سیگنالی که از دکل به گوشی ما ارسال می شود اصطلاحاً Page گفته می‌شود.

وقتی کسی با شما تماس می‌گیرد ، سوئیچ HLR را چک می‌کند. با توجه به اطلاعات HLR می‌تواند بفهمد چه شماره تلفنی آخرین بار در اطراف کدام دکل و با چه گوشی‌ای مشاهده شده است. پس سیگنال را دقیقاً به محل گوشی ارسال می‌کند.

این روال کلی یافتن شما و گوشی‌تان در دنیا است.

فرض کنید بعد از آخرین ثبت نام، گوشی شما خاموش شود و شما از محدوده آخرین دکلی که در آن ثبت نام کرده بود خارج شوید (و یا به محدوده‌ای بروید که آنتن‌دهی صفر است) و سیگنال ارسالی به گوشی شما نرسد، در اینصورت سوئیچ این سیگنال را به دکل‌های همسایه می‌فرستد. اگر آنجا هم جواب نگرفت به دکل‌های سطح شهر و بعد از آن دکل‌های سطح کشور و اگر از دکل‌های کشور هم جواب نگرفت به دکل‌های کشورهایی ارسال می‌کند که خط ما در آنجا Roaming شده باشد. در واقع این کار را آنقدر ادامه می‌دهد تا گوشی موبایل را پیدا کند و یا اینکه شما را نیابد و پیغام «مشترک مورد نظر در دسترس نمی‌باشد» را اعلام کند. (تعجب نکنید! این پروسه به ظاهر طولانی، در یک چشم بر هم زدن اتفاق می‌افتد)

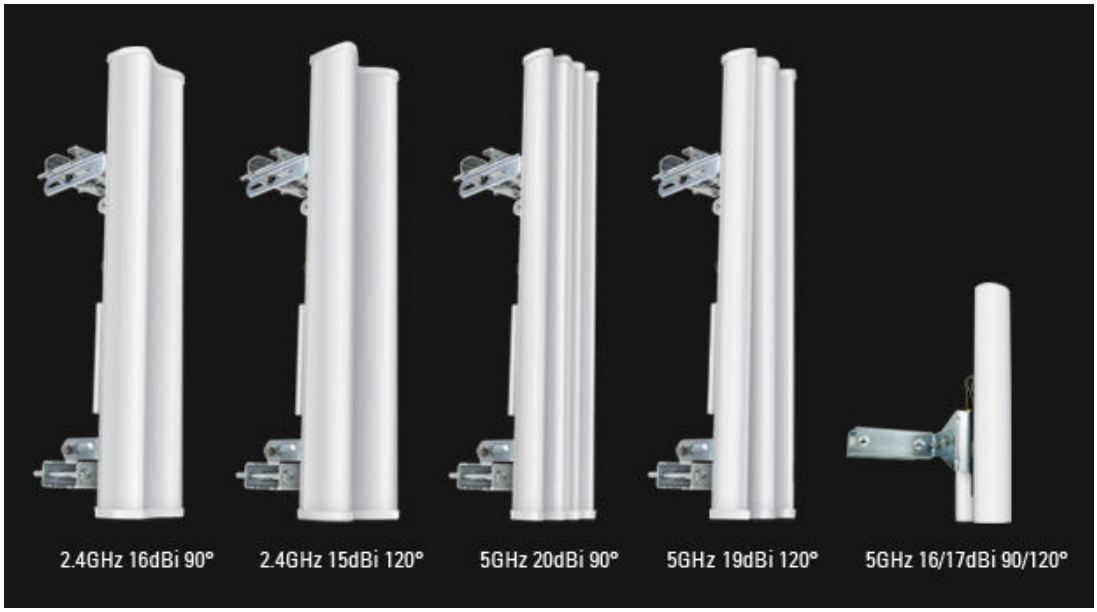
تحقیق: با توجه به آنچه گفته شد، تحقیق کنید که اگر گوشی موبایل شما دزدیده و یا گم شده باشد، پلیس چگونه آن را خواهد یافت؟

Antenna :

آنتن‌هایی که در اکثر نقاط دنیا داریم به آنتن‌های Sectorized مشهورند.

معمولاً هر آنتن ۱۲۰ درجه را پوشش می‌دهد که در مجموع با سه آنتن می‌توان همه ۳۶۰ درجه را پوشش داد. شعاع پوشش آنتن‌ها ٤ تا ٥ کیلومتر است.





تعریف سکتور (Sector) :

ناحیه‌ای که هر آنتن (نه هر BTS) پوشش می‌دهد، سکتور گفته می‌شود.

BTS (Base Transceiver Station):

به محفظه یا Boxی که کنار هر برج قرار دارد و وظیفه آن دریافت از و ارسال الکتریسته به آنتن‌ها است در اصطلاح BTS یا «ایستگاه گیرنده-فرستنده پایه» گفته می‌شود.

تعریف Cell یا سلول:

به منطقه‌ای که یک BTS پوشش می‌دهد، Cell گفته می‌شود.

ظرفیت BTSها:

ظرفیت هر BTS به صورت x+x+x نشان داده می‌شود که عدد مربوط به هر x ضرب در ۷ می‌شود و تعداد اتصالاتی که می‌توانند به طور همزمان به آن BTS متصل شوند به دست می‌آید.

مثلاً:

۱+۱+۱ یعنی:

۷+۷+۷ = ۲۱ اتصال همزمان

۲+۲+۲ یعنی:

۱٤+۱٤+۱٤ = ٤۲ اتصال همزمان

۳+۳+۳ یعنی:

۲۱+۲۱+۲۱ = ۶۳ اتصال همزمان

٤+٤+٤ یعنی:

۲۸+۲۸+۲۸ = ۸٤ اتصال همزمان

یعنی ۸٤ نفر به طور همزمان می‌توانند از طریق این بی‌تی‌اس به شبکه موبایل متصل شوند و صحبت کنند. ممکن است ظرفیت یک BTS به طور مثال ۸۰ بیان شود. این یعنی ٤ کانال برای عابران در نظر گرفته شده است. یعنی کسانی که در حین عبور از کنار این ایستگاه می‌گذرند و طبیعتاً باید سرویس‌دهی شوند . (تصور کنید شما در ماشین در حال حرکت هستید، اگر در ماشین از محدوده یک آنتن خارج شوید و به محدوده آنتن بعد وارد شوید شما برای آنتن دوم یک عابر به حساب می‌آیید.)

تمام BTSها در مخابرات جمع می‌شوند و به دستگاه‌هایی به نام BSC متصل می‌شوند.

BSC (Base Station Controller):

BSC، وظیفه کنترل کردن BTSها را بر عهده دارد. از یک طرف به BTSها و از طرف دیگر به سوئیچ مخابرات (MSC) متصل است.

MSC (Mobile Switching Center):

همه BTSها در نهایت به یک سوئیچ متصل می‌شوند که وظیفه اصلی آن ایجاد هماهنگی در برقراری ارتباط بین کاربران موبایل (GSM) و کاربران تلفن شهری (PSTN) می‌باشد. به این سوئیچ MSC گفته می‌شود.

تصویر یک MSC :



برای درک بهتر نام دستگاه‌ها و عملکرد هر یک، به دقت به تصویر زیر نگاه کنید (از پایین تصویر، مسیر را دنبال کنید به سمت بالا):



شبکه‌های سلولی

Cellular Networks

از آنجا که فرکانس‌های مختلف توسط شبکه‌های مختلف رادیویی و تلویزیونی رزرو شده است بزرگ‌ترین مشکل بانیان شبکه‌های سلولی این است که نمی‌توانند از هر فرکانسی که خواستند استفاده کنند بلکه یک رِنج فرکانسی خاص به آن‌ها داده می‌شود و فقط باید از آن رنج استفاده کنند.

پس هر بانی (مثلاً ایرانسل در ایران) باید طوری این محدوده فرکانسی را در ایستگاه‌های مختلف تقسیم کند که:

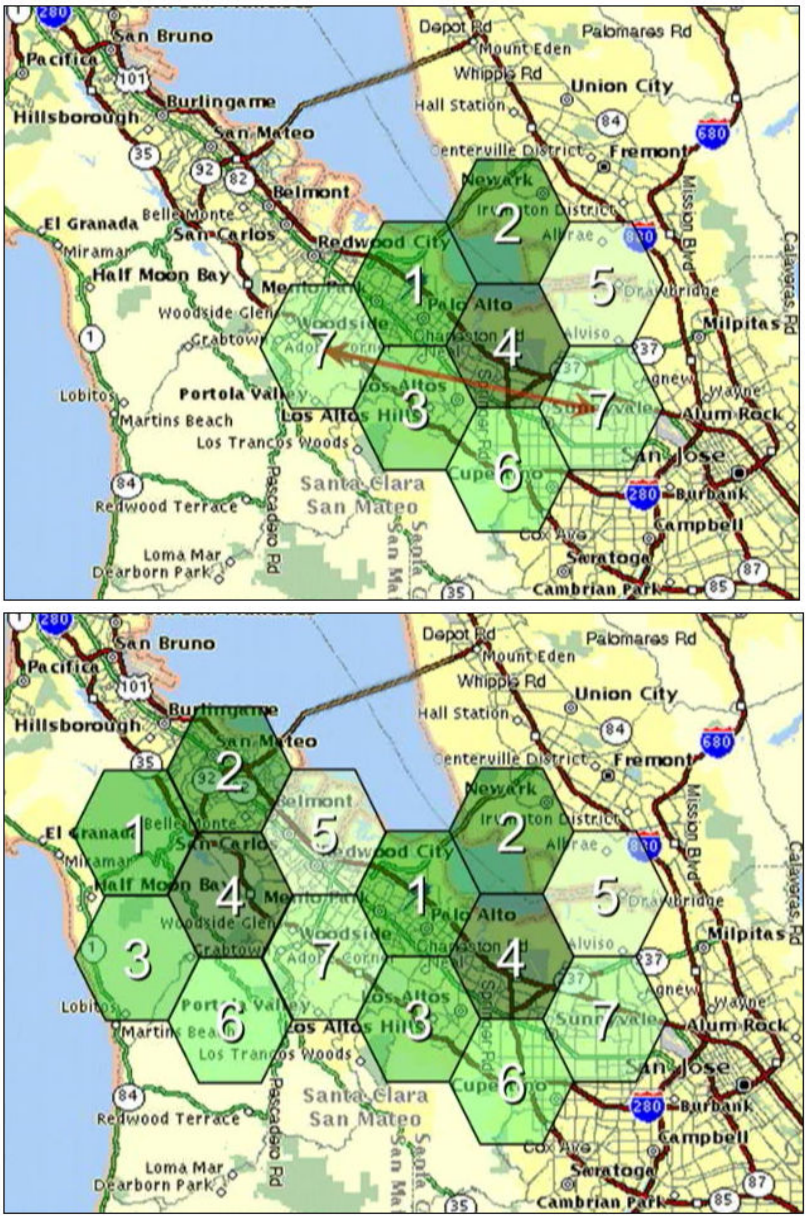
اولاً: بتواند چندین فرکانس روی یک ایستگاه داشته باشد (برای هر مشترک یک فرکانس خاص). یعنی مثلاً روی هر ایستگاه باید ۸٤ فرکانس مختلف داشته باشیم.

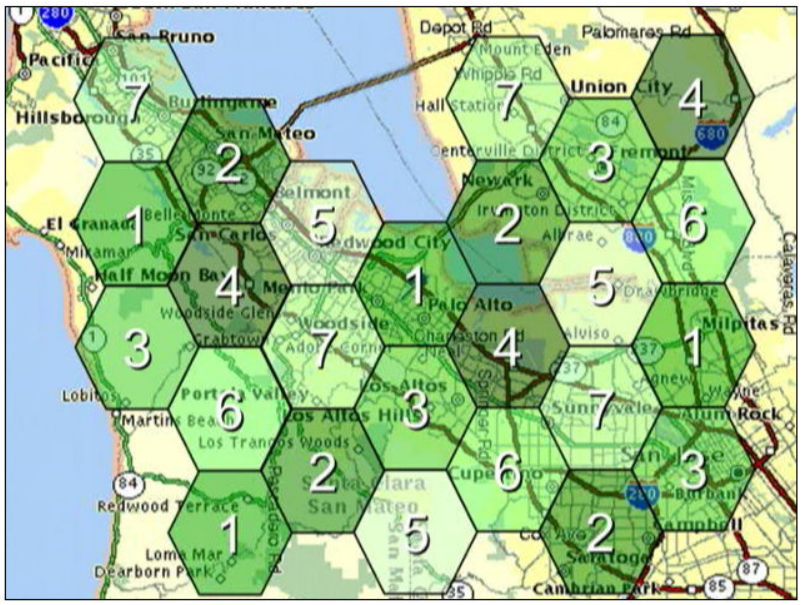
ثانیاً: این فرکانس‌ها نباید در ایستگاه‌های مجاور استفاده شده باشند.

هر ایستگاه تا شعاع ٤ تا ٥ کیلومتررا پوشش می‌دهد که معمولاً این محدوده را به صورت شش ضلعی منظم (سلول) نشان می‌دهند پس دو سلول مجاور نباید فرکانس‌های مشابه داشته باشند.

محاسبات نشان می‌دهد که اگر محدوده فرکانسی که بانی در اختیار دارد را به عدد ۷ تقسیم کنیم، می‌توان با این ۷ محدوده به دست آمده، سلول‌ها را طوری کنار هم چید که هیچ سلولی با کنار خود هم‌فرکانس نشود.

به تصاویر زیر دقت کنید:





همانطور که می‌بینید، کل یک منطقه را با ۷ فرکانس مختلف طوری سلول‌بندی کرده‌اند که هیچ دو فرکانسی کنار هم نیستند.

پس، بانی شبکه محدوده فرکانسی خود را به هفت تقسیم می‌کند و عدد به دست آمده را بر تعداد مشترکین هر ایستگاه تقسیم می‌کند در این صورت هر مشترک در بین سلول‌های مجاور خود فقط یک فرکانس خاص خواهد داشت و تداخل هم رخ نخواهد داد.

مثال: فرض کنید یک بانی محدوده فرکانسی 800-870 MHz را در اختیار دارد و BTSهای این بانی به صورت 2+2+2 هستند.

با توجه به این اطلاعات سلول‌بندی را انجام دهید.

محدوده فرکانسی‌ای که این بانی در اختیار دارد را به هفت قسمت تقسیم می‌کنیم. پس در این هفت سلول چنین محدوده‌های فرکانسی‌ای خواهیم داشت:

سلول ۱: 800 تا 810

سلول ۲: 810 تا 820

سلول ۳: 820 تا 830

سلول ٤: 830 تا 840

سلول ۵: 840 تا 850

سلول ۶: 850 تا 860

سلول ۷: 860 تا 870

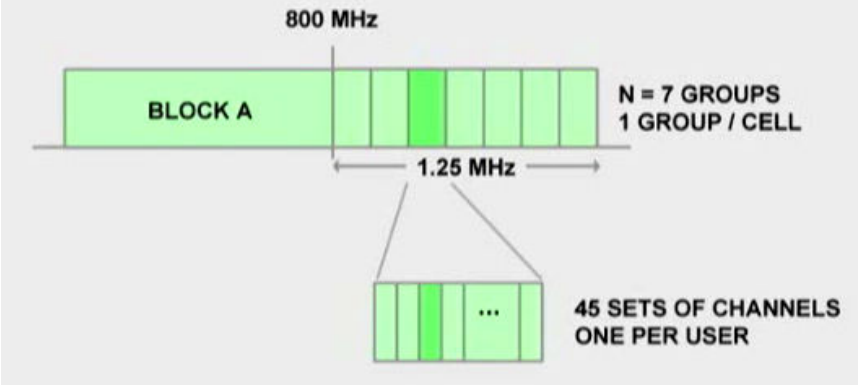
محدوده فرکانسی هر سلول ۱۰ مگاهرتز است و در هر سلول ١٤+١٤+١٤ نفر باید بتوانند به طور همزمان مکالمه کنند. پس ۱۰ را تقسیم بر ٤۲ می‌کنیم، می‌شود 0.23 هرتز.

از ۸۰۰ هرتز شروع می‌کنیم و 0.23 هرتز دائماً به ۸۰۰ اضافه می‌کنیم تا فرکانس هر مشترک مشخص شود.

مثلاً نفر اول در سلول اول فرکانس 800.23 MHz خواهد داشت.

نفر دوم، 800.46 ... الی آخر.

مثالی دیگر:



توجه: سلول بندی شبکه‌های سلولی از مشکل‌ترین کارهاست. اینکه گاهی می‌بینید فرکانس شما با فرکانس یک نفر دیگر یکی می‌شود و در اصطلاح عامیانه «خط رو خط» می‌شود، به خاطر ناشی بودن طراح سلول‌ها است.

نسل‌ها و استانداردهای شبکه‌های سلولی (Cellular) :

1G (نسل اول):

* توجه: G مخفف Generation است به معنای نسل.

در این نسل از تکنیک‌های Analog برای ارسال صوت استفاده می‌شد. در واقع همان گوشی‌های بی‌سیم.

از ایرادات بزرگ این نسل، یکی نویزپذیری بسیار زیاد آن است و دیگری اینکه سیگنال‌ها محدوده کمی را پوشش می‌دهند.

مشهورترین استانداردهای این نسل عبارتند از: AMPS, NMT, TACS

2G (نسل دوم):

در این نسل از تکنیک‌های Digital استفاده می‌شود. در ایران و اروپا از استاندارد GSM و در آمریکا از استانداردهای TDM وCDMA استفاده می‌گردد. در این نسل می‌توان تا 115Kbps داده ارسال کرد. (البته در عمل کمتر از این مقدار است)

2.5G (نسل ۲.۵) یا General Packet Radio Service (G.P.R.S) :

در این نسل اطلاعات در قالب Packet (بسته) ارسال می‌شوند و از روش آماری (Statistical) برای این کار استفاده می‌شود. در روش Statistical که بهبودیافته روش TDM بود، ظرفیت کانال رزرو نمی‌شد هر وقت هر کس سیگنال داشت ارسال می‌کرد در نتیجه در نسل G.P.R.S که بیشتر برای اتصال گوشی به اینترنت استفاده می‌شود شما همیشه به شبکه متصل هستید و فقط هزینه ارسال و دریافت پکت را می‌دهید چون ظرفیت کانال را اشغال نمی‌کنید و هر وقت Packet داشتید، ارسال و دریافت می‌کنید.

در حقیقت مثل اتصال به اینترنت از نوع ADSL، مدت زمانِ اتصال محاسبه نمی‌شود. در حالی که در اتصال Dial-up شما بر اساس مدت زمان اتصال هزینه می‌دهید. به همین دلیل در ADSL شما همیشه به شبکه وصل هستید و فقط هزینه ارسال و دریافت را می‌دهید چون ظرفیت کانال‌ها را اشغال نمی‌کنید.

- برای اینکه یک اپراتور بتواند G.P.R.S را پشتیبانی کند، باید تجهیزاتی بخرد و روی برج‌ها نصب کند.
- نهایت سرعت این نسل در محیط آزمایشگاهی (علمی) ۱۱۵ کیلوبیت در ثانیه است اما در عمل بین ۲۸ تا ٤٠ کیلوبیت در ثانیه است.

3G (نسل سوم):

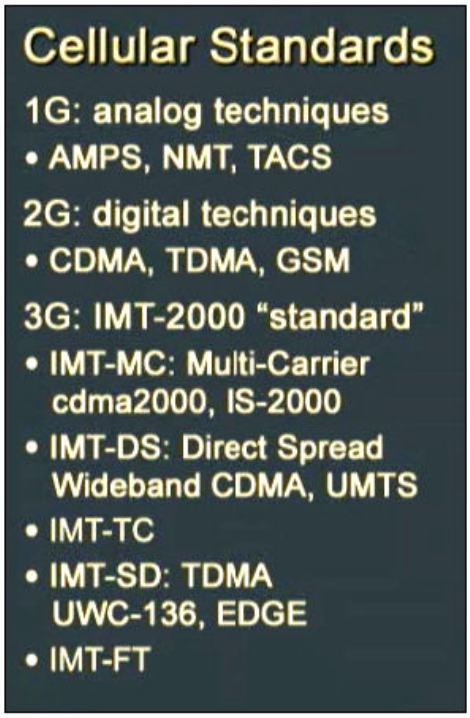
یک مشکل اساسی در نسل‌ها و تکنولوژی‌های مختلف این است که اگر شما فرضاً در شبکه G.S.M باشید، نمی‌توانید با همان سیم کارت در استانداردهای دیگر متصل شوید یعنی هر سیم کارت فقط در شبکه‌ای با استاندارد و شرکت خودش قابل استفاده است.

این مشکل مثل این است که برای اتصال به اینترنت، هر ISP یک مودم خاص خودش را داشته باشد!!

این مشکل باعث شد که مؤسسه ITU یک استاندارد جدید به نام 3G (تری.جی) معرفی کند. با این استاندارد شما با یک سیم کارت می‌توانید به تمام اپراتورهایی که از این استاندارد پشتیبانی می‌کنند متصل شوید.

فعلاً شرکت‌های محدودی مثل AT&T آن را پشتیبانی می‌نمایند. در این نسل می‌توان تا 2Mbps داده ارسال کرد. این نسل برای دنیای Broadband (پهن‌باند) است. از طریق خطوط این نسل خیلی راحت می‌توان از طریق خط موبایل انواع فیلم را دانلود کرده و دید و پیام‌های صوتی و تصویری را در عرض چند ثانیه ارسال نمود.

نسل‌های مختلف و استانداردهای هر نسل در تصویر زیر مشخص است:



4G (نسل چهارم):

نسل چهارم ارتباطات تلفن همراه از نظر سرعت ۱۰ برابر سریع تر از نسل سوم عمل می‌کند. سرعت بالای این شبکه سبب می‌شود که تلفن‌های هوشمند خیلی بیشتر به کامپیوترها شبیه شوند و امکان برقراری ارتباط‌های چند رسانه‌ای سریع را داشته باشند.

نسل چهارم شبیه به نسل سوم از دو تکنولوژی اصلی LTE و WiMax استفاده می‌کند. هر کدام از اپراتورها یکی از این دو فناوری را برای ارایه خدمات انتخاب می‌کنند.

در نسل سوم، سرعت انتقال اطلاعات به صورت تئوری ۲ مگابیت در ثانیه است. اما در عمل حداکثر سرعت دریافتی بین ۵۰۰ کیلوبیت در ثانیه تا ۱.۵ مگابیت در ثانیه متغییر است. نسل چهارم افق‌های جدیدی را در پهنای باند موبایل باز کرده است. سرعت دانلود ۶ مگابیت در ثانیه و آپلود ۱ مگابیت در ثانیه هدیه 4G به کاربران تلفن همراه است. جالب اینجا است که این شبکه ظرفیت افزایش سرعت را تا ۱۰۰ مگابیت هم دارد. البته این اعداد آزمایشگاهی هستند و وقتی در شبکه با میلیون‌ها تلفن همراه تست شوند، سرعت مقداری کمتر خواهد بود.

پاسخ به یک سؤال جانبی: چرا تعداد دکل‌های ایرانسل بیشتر از اپراتور اول است؟

در تکنولوژی‌های جدیدتر، برخی اپراتورها سلول‌های خود را کوچک‌تر می‌کنند. این کار چند مزیت دارد:

۱- عمر باطری گوشی‌ها بیشتر می‌شود: هر چه سلول کوچک‌تر شود، دکل‌ها به شما نزدیک‌تر می‌شوند. پس سیگنالی که گوشی شما ارسال می‌کند به مسیر کوتاه‌تری ارسال می‌شود و در نتیجه باطری کمتری برای ارسال سیگنال لازم است.

۲- آنتن‌ها کوتاه‌تر می‌شوند.

۳- هزینه‌های تعمیر و ارتقا و تولید آنتن‌ها به دلیل کوتاه‌تر شدن، کمتر می‌شود.

٤- از همه مهم تر: کیفیت صدا بیشتر می‌شود.

پس این که ایرانسل، تعداد بیشتری دکل دارد، به خاطر کوچک‌تر کردن سلول‌هاست و در نتیجه بیشتر کردن سلول‌ها و دکل‌ها.