

## فصل اول - آشنایی با مفاهیم شبکه و اجزای آن

### هدف های رفتاری

هنرجو پس از آموزش این فصل می تواند :

هدف از ایجاد شبکه های کامپیوتری را بیان کند.

اجزای شبکه های کامپیوتری را شرح دهد.

تقسیم بندی شبکه های کامپیوتری از نظر ابعاد و گستردگی فیزیکی را شرح دهد.

تقسیم بندی شبکه های کامپیوتری از نظر مدل سرویس دهی را بیان کند

در دهه اخیر شبکه های کامپیوتری به عنوان یکی از بسترهای سریع و کم هزینه ارتباطی مطرح شده اند . این سیر تدریجی منجر به ایجاد روشی شده است که با سازماندهی مناسب آن می توان سریعتر از هر روش دیگری به اطلاعات مختلف دسترسی پیدا کرد . اطلاعاتی که راه گشای پیوندهای گوناگون فرهنگی ، هنری ، خانوادگی و اجتماعی ، سیاسی ، نظامی و همچنین مبادلات اقتصادی و تجاری اعم از خرد و کلان است و می دانیم که امروزه در عصر اطلاعات بسر می بریم، هر که با هزینه کمتر و سرعت بیشتر بتواند به آن دسترسی پیدا کند موفق تر است

تجارت جهانی روی اینترنت و شبکه های کامپیوتری به سرعت به عنوان مفاهیمی کارآمد مطرح می شود . فرقی نمی کند شما در کدام نقطه از کره زمین قرار دارید . در هر لحظه که اراده کنید می توانید اطلاعات مورد نیاز خود را ، حتی بصورت صوت و تصویر زنده از شبکه بدست آورید . اگر نیاز به تبادل مالی داشته باشید باز هم فرقی نمی کند ، پول الکترونیکی در دسترس شماست و به سرعت می توانید با کارت اعتباری خود اقدام به تبادل حفاظت شده ارزی نمایید .

موارد فوق را می توان به صورت زیر خلاصه کرد :

دسترسی افراد به منابع متنوع در شبکه با در نظر گرفتن سطوح امنیتی قابل تعریف . (اشتراک منابع)  
برقراری سرویس های زنده صوتی تصویری بین افراد یا تیمهای فعال در شبکه .  
تبادل نامه بین افراد مختلف .

ایجاد بستری مناسب جهت ارتباط با اینترنت بمنظور دسترسی به شبکه جهانی اطلاعات .  
انجام کارهای شخصی و اداری از هر نقطه در شبکه .  
مدیریت و نظارت از راه دور .

- هدفهای برقراری شبکه کامپیوتری

هدف از ایجاد یک شبکه ی کامپیوتری عبارت است از :

اشتراک منابع

تبادل پیغام

مدیریت از راه دور

فعالیت عملی :

اشتراک منابع : از طریق شبکه به کامپیوتر سرویس دهنده متصل شده ، پوشه و چاپگر به اشتراک گذاشته شده را ببینید . راهنمایی : ابتدا هنر آموز درس یک پوشه و یک چاپگر را در یکی از سیستم عاملهای ، 2003 , XP به اشتراک می گذارد .

تبادل پیغام : حداقل یکی از برنامه های زیر را با تایپ نام برنامه در کادر گزینه Run برای انتقال پیغام آزمایش کنید :

WinChat.exe

Net Meeting (conf.exe)

Command Prompt -> net send <computer\_name> <message\_text>

مدیریت از راه دور : به کمک هنر آموز درس ، یکی از برنامه های ، RA dmin , Ideal Administrator , DameWare یا Net Op School را اجرا کرده و با نظارت و کنترل از راه دور تحت شبکه را بررسی کنید .

1-2 - اجزای یک شبکه کامپیوتری :

شبکه های کامپیوتری از 4 جزء اصلی تشکیل می شوند :

Server-1 : سرویس دهنده .

Client-2 : سرویس گیرنده .  
با نصب یک سخت افزار ارتباطی مانند کارت شبکه یا مودم به شبکه متصل می شوند .

Communication Media-3 : محیط انتقال (مثلاً کابل یا بی سیم)

Protocol-4 : مجموعه قوانینی که با رعایت آنها سرویس دهی در شبکه برقرار می شود .

بدیهی است که سرویس دهنده ها و سرویس گیرنده ها باید طبق یک طرح و نقشه مشخص (بوسیله محیط انتقال) به یکدیگر متصل شوند که به این طرح و نقشه اصطلاحاً پیکربندی (Topology) شبکه گفته می شود . جزئیات هریک از موارد فوق بصورت خلاصه عبارتند از :

**Servers (Services)& Clients**

File , Print , Application , Database , Fax , Email ,  
Web , Communication , Time , Remote Access ,  
Multimedia , ...

**Communication Media :**

**Protocols :**

TCP/IP , IPX/SPX , NetBEUI , ...

Wired :

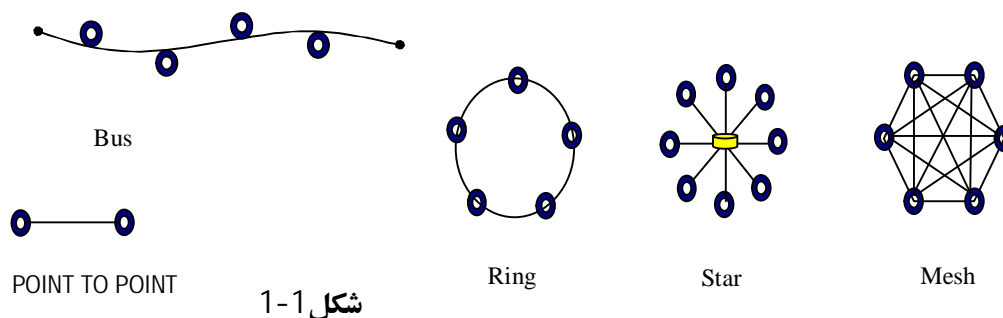
- § Metal : Coaxial , Twisted Pair
- § Non Metal : Fiber Optic

Wireless :

- § Infra Red
- § Laser
- § Radio Waves

**Topologies :**

Bus , Ring , Star , Mesh , Point-to-Point



1-3- تقسیم بندی شبکه‌های کامپیوتری از نظر ابعاد و گستردگی فیزیکی : LAN , MAN, WAN  
 شبکه‌ها را از لحاظ اینکه فاصله مابین اجزای آنها چقدر بوده و اصطلاحاً چگونگی پراکندگی کامپیوترها به 3 دسته کلی تقسیم می‌کنند :

1-3-1- شبکه‌های محلی ، Local Area Networks = LAN :

همانطور که از اسم شبکه‌های محلی پیداست فاصله اجزا در این شبکه‌ها کم بوده و همه نزدیک به یکدیگر قرار دارند در زیر چند مثال از این شبکه‌ها ارایه شده است  
 شبکه‌ای متشکل از 2 کامپیوتر که با یک قطعه کابل به فاصله 100 متر آنها را به یکدیگر وصل کرده‌ایم .  
 شبکه کامپیوتری یک اداره کوچک واقع در یک ساختمان متشکل از 20 کامپیوتر فعال (Active Node) .  
 شبکه کامپیوتری یک سازمان واقع در 5 ساختمان نزدیک بهم با 500 گره فعال (Active Node) .  
 شبکه کامپیوتری یک برج 110 طبقه با 5000 سیستم فعال (Active Node) .

1-3-2- شبکه‌های گسترده ، Wide Area Networks = WAN :

فاصله اجزا در این شبکه‌ها نسبت به LAN طولانی‌تر است به طوری که از نظر حسی دیگر نمی‌توان آنها را نزدیک به یکدیگر تصور کرد :

مثال 1 : شبکه‌ای متشکل از 2 کامپیوتر که بوسیله مودم از طریق خطوط مخابرات به یکدیگر متصلند .  
 مثال 2 : مجموع 2 شبکه محلی که هر کدام واقع در ساختمان مختص به خود به فاصله 10 کیلومتر از یکدیگر قرار دارند. یکی از ساختمانها واقع در مرکز شهر و دیگری در حاشیه غربی آن بوده و ارتباط آنها از طریق خطوط مخابرات یا روشهای دیگری مانند بی سیم برقرار شده .  
 مثال 3 : شبکه کامپیوتری شعبه‌های مختلف یک بانک در شهر .  
 مثال 4 : شبکه کامپیوتری آموزش و پرورش واقع در تهران و شهرستانها .  
 مثال 5 : شبکه اینترنت .

1-3-3- شبکه‌های فرا منطقه‌ای ، Metropolitan Area Networks = MAN :

این شبکه که در ترجمه‌های فارسی به شبکه‌های شهری نیز معروفند از نظر وسعت مابین LAN و WAN قرار دارند .

مثال 1 : برخی ترجیح می‌دهند که مثال 3 از شبکه‌های WAN را MAN اطلاق کنند .  
 مثال 2 : یک مجموعه بزرگ صنعتی یا نظامی واقع در محدوده 30 کیلومتر مربعی که از سوله‌های متفاوت تشکیل شده و در هر سوله یک LAN موجود است . به مجموع شبکه‌های این کمپ نیز می‌توان واژه MAN را اطلاق کرد . البته در این مثال چندین شبکه LAN داریم که در یک کمپ واقع شده‌اند لذا

برخی (از جمله کمپانی معروف Cisco) ترجیح می دهند از واژه Campus LAN یا Campus Area Networks = CAN استفاده کنند .

به هر حال به نظر می رسد تقسیم بندی LAN و WAN کافیست .  
شما و همسایه دیوار به دیوارتان و هر کدام یک دستگاه کامپیوتر دارید . از طریق یک کابل ، هر دو سیستم را به هم متصل می کنید ، در این حالت شبکه حاصل LAN است .  
مثال دیگر - حال فرض کنید که امکان کابل کشی مستقیم ندارید . لذا پس از خرید و نصب مودم دو کامپیوتر مثال بالا را از طریق شبکه مخابرات به یکدیگر وصل می کنید شبکه حاصل WAN خواهد بود . در این مثال ها نشان داده شد که نوع شبکه را طول کابلها (محیط انتقال) تعیین می کند نه فاصله ظاهری بین کامپیوترها .

مقایسه شبکه های LAN و WAN

از نظر سرعت در شبکه های LAN و WAN می توان گفت: سرعت به ابعاد و گستردگی شبکه بستگی ندارد اما معمولاً پیاده سازی تکنولوژی با سرعت بالا در ابعاد LAN کم هزینه تر و ساده تر از WAN انجام می شود لذا معمولاً سرعت در شبکه های LAN از WAN بیشتر است اما این یک قاعده کلی نیست . به عنوان مثال می توان شرایط زیر را در نظر گرفت:

سرعت LAN بیشتر از WAN : وقتی با مودم به اینترنت متصل می شوید بعنوان یکی از اعضای شبکه WAN محسوب شده و سرعت با مودم های خوب حدوداً 40 Kbps است . از طرفی کمترین سرعت در شبکه های LAN که البته در اواخر عمر خود قرار دارند 10 Mbps است . اگر سرعت LAN را بر WAN تقسیم کنیم می بینیم که حدوداً 250 برابر بیشتر است !

سرعت LAN کمتر از WAN : در شاهرگهای اصلی اینترنت یا در ارتباطات میان قاره ای سرعت عموماً بیشتر از 155 Mbps است و اگر آنرا با سرعت معمول در شبکه های LAN یعنی 100 Mbps مقایسه کنیم می بینیم که در همان حد یا بیشتر است .

انواع شبکه های بی سیم از نظر وسعت

WLANs شبکه WLANS ، امکان دستیابی کاربران ساکن در یک منطقه محدود نظیر محوطه یک

دانشگاه و یا کتابخانه را به شبکه و یا اینترنت ، فراهم می نماید .

WPANS : با استفاده از شبکه WPANS ، امکان ارتباط بین دستگاههای شخصی در یک ناحیه محدود

فراهم می شود . در این نوع شبکه ها از دو تکنولوژی متداول IR (Infra Red) و Bluetooth

(IEEE 802,15) استفاده می شود .

WMANS<sup>1</sup> : در این شبکه ها ، امکان ارتباط بین چندین شبکه موجود در یک شهر بزرگ فراهم خواهد

شد . و این اغلب به عنوان شبکه های پشتیبان شبکه کابلی استفاده می شود .

WWANS<sup>2</sup> : در شبکه های فوق ، ارتباط بین شهرها و یا حتی کشورها از طریق سیستم های ماهواره ای

متفاوت فراهم می شود . این شبکه به سیستم های G2 (نسل دوم) معروف هستند .

#### 1-4-1 - تقسیم بندی شبکه‌های کامپیوتری از نظر مدل سرویس دهی (Peer-to-Peer , Server-Based)

مفهوم Server و Client : سرویس دهی در یک شبکه به وسیله ی سیستمهایی صورت می گیرد که در اصطلاح سرویس دهنده (Server) نامیده می شوند . سیستمهایی که از این سرویسها استفاده کنند در اصطلاح سرویس گیرنده (Client) نامیده می شوند برای سرویس گیرنده ها اصطلاح workstation نیز به کار می رود.

##### 1-4-1- شبکه Server-Based:

اگر در یک شبکه تعدادی از سیستمها فقط در نقش سرویس دهنده و تعدادی فقط در نقش سرویس گیرنده ظاهر شوند در آن صورت می گوییم مدل سرویس دهی آن شبکه Server-Based (به اختصار SB) است.

##### 1-4-2- شبکه Peer-to-Peer:

اگر در شبکه ای ، سیستمها همزمان علاوه بر ارائه سرویس ، از سرویسهای بقیه هم استفاده کنند یا بعبارتی بطور همزمان هم سرویس دهنده باشند هم سرویس گیرنده در آن صورت می گوییم مدل سرویس دهی در آن شبکه Peer-to-Peer است (به اختصار PtP)

در مدل SB تجمع سرویسها روی سرویس دهنده s بوده و سرویس گیرنده ها هیچگونه سرویسی ارائه نمی دهند اما در مدل PtP هر سیستم می تواند علاوه بر دریافت سرویس خود سرویس دهنده نیز باشد یعنی هر کامپیوتر هم سرویس گیرنده و هم سرویس دهنده است.

در یک سایت تعدادی از سیستمها فقط سرویس دهنده و بقیه فقط سرویس گیرنده هستند . مدل سرویس دهی SB است اما در یک سایت دیگر هر کدام از کاربران منابعی مانند پوشه ها یا چاپگرها را برای بقیه به اشتراک گذاشته اند . مدل سرویس دهی PtP است .

فرض کنید در ایرانشهر تعدادی مغازه و مراکز خدماتی وجود دارد و تعدادی مشتری و استفاده کننده این خدمات هستند . مدل سرویس دهی آنها SB خواهد بود.

##### 1-4-3- مزایا و معایب هریک از مدل های PtP , SB

در مدل SB چون تمرکز سرویسها فقط در نقاط مشخصی است یعنی سرویس دهنده ها بنابراین مدیریت سرویس ساده تر است . این مدیریت شامل کنترل دسترسی و امنیت ، نحوه ارائه ی سرویس به کاربران ، مونیتورینگ سرویس و چگونگی بهره برداری از آن و پارامترهای دیگریست که براحتی می توان آنها را در سرویس دهنده ها کنترل کرد در صورتیکه انجام این عملیات در مدل PtP پیچیده است ، چرا ؟ به عنوان مثال تصور کنید در یک شبکه حدود 700 سیستم داشته باشیم که مدل سرویس دهی آنها PtP باشد ، یعنی باید روی 700 سیستم عملیات های فوق را انجام دهیم ! که عملی هزینه بر و کسل کننده است .

##### مدل Server Based :

مزیت : مدیریت جامع و متمرکز . مناسب برای استفاده در شبکه های متوسط و بزرگ .

عیب : چنانچه سرویس دهنده دچار مشکل شوند چه اتفاقی می افتد ؟ سرویس دهی در کل شبکه دچار اختلال می شود . راه حل این عیب را بعداً در مبحث Fault-Tolerance اشاره خواهیم کرد .

## مدل Peer-to-Peer :

مزیت : چون مجموعه سرویسها در نقطه خاصی متمرکز نشده‌اند بلکه احتمالاً در نقاط مختلفی از شبکه پراکنده هستند بنابراین در صورت بروز مشکل ، سرویس دهی به صورت ناگهانی دچار اختلال کلی نمی‌شود .

عیب : مدیریت آن پیچیده بوده و هنگامی عملی است که تعداد سیستمها زیاد نبوده (شبکه‌های کوچک) یا اینکه کاربران در مورد نحوه اشتراک گذاری منابع و مدیریت سرویسها آموزشهای لازم را دیده باشند .

1-5- انواع سرویسها یی که سرویس دهنده ارایه می دهد

همانطور که اشاره شد ، هر شبکه کامپیوتری از 4 جزء تشکیل شده که به ترتیب از سمت چپ عبارتند از :

Client , Server , Communication Media & Protocol . مجدداً یادآوری می کنیم که سرویس

دهی در یک شبکه به وسیله ی سیستمهایی صورت می گیرد که در اصطلاح " سرویس دهنده " نامیده می شوند سیستمهایی که از این سرویسها استفاده کنند اصطلاحاً سرویس گیرنده نامیده می شوند . معمولاً در یک شبکه هر کامپیوتری که از نظر سخت افزاری نسبت به سایر کامپیوتر ها قوی تر باشد به عنوان سرویس دهنده در نظر گرفته می شود، البته نوع انتخاب بستگی کامل به نوع سرویس خواهد داشت .

در این قسمت می خواهیم با انواع سرویسها آشنایی بیشتری پیدا کنیم . بدیهی است با شناخت سرویسها مشتری آنها یعنی سرویس گیرنده ها نیز شناخته خواهد شد .

سرویسهایی که در شبکه‌ها ارایه می شوند ممکن است بسیار متنوع باشند هر چه تنوع مشتری و نیازهای او بیشتر باشد تنوع سرویس نیز به همان نسبت افزایش می یابد . آشنایی با همه سرویسها نیاز به بحث طولانی خواهد داشت با این حال معروفترین آنها را نام برده و چهار مورد را که کاربرد بیشتری دارند معرفی می کنیم :

File , Print , Application , Database , Web , Mail , Fax , Modem (Communication) , Remote Access , Internet Sharing , Multimedia , CDROM (DVDROM) , ...

### File Service -1-5-1

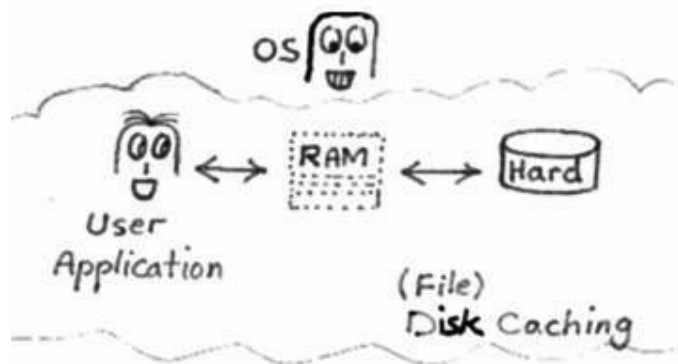
بطور مختصر و ساده File Server یعنی " سریس دهنده فایل " . سخت افزاری است با وسایل ذخیره سازی حجیم ، سریع و پایدار (مانند دیسک سخت) که روی آن انواع پرونده‌ها با در نظر گرفتن سطوح امنیتی ، به وسیله ی کاربران از نقاط مختلف شبکه ذخیره و مورد استفاده قرار می گیرد . البته سخت افزار به تنهایی کافی نبوده و باید نرم افزار خاص File Service نحوه ذخیره سازی ، بازیابی و مدیریت اینگونه کارها را به نحو احسن در شبکه انجام دهد .

برای ذخیره و بازیابی اطلاعات هر چند دیسک سخت<sup>1</sup> وسیله ای نسبتاً سریع برای ذخیره سازی و بازیابی اطلاعات است اما یک وسیله الکترو مکانیکی بوده و سرعت این وسایل هر چه قدر هم زیاد باشد ، نسبت به وسایل ذخیره سازی الکترونیکی محض مانند RAM بسیار ناچیز است لذا در اینگونه سرویس دهنده ها از حافظه RAM برای ذخیره سازی و بازیابی موقت اطلاعات کاربران تا هنگامی که سرویس دهنده روشن است استفاده می شود . عبارتی کاربر یا برنامه ای که با فایل ذخیره شده روی دیسک سخت کار دارد بجای در گیر شدن با یک وسیله مکانیکی ، عملیات خود را بطور نامحسوس روی RAM انجام می دهد و لذا

<sup>1</sup> - معمولاً در سرور ها برای نگهداری اطلاعات زیاد در حد ترا بایت از دستگاهی به نام NAS Server (network Attached

Storage Server) استفاده می شود

سرعت به نحو چشمگیری افزایش می‌یابد. بدیهی است سیستم عامل (یا نرم‌افزار فایل سرور) در زمانهای مناسب بطور خودکار تغییرات انجام شده در RAM را، روی دیسک سخت منتقل می‌کند چرا که محل اصلی و پایدار برای ذخیره سازی اطلاعات است. استفاده از RAM را برای ذخیره سازی موقت اطلاعات دیسک سخت که بمنظور افزایش سرعت انجام می‌شود اصطلاحاً File Caching یا Disk Caching می‌گویند.



شکل 2-1

برخی از فایل-سرورها عملیات تکمیلی دیگری را نیز انجام می‌دهند مانند: فشردن سازی خودکار اطلاعات هنگام ذخیره سازی پرونده‌ها روی دیسک بمنظور کاهش حجم فضای اشغالی.

رمزنگاری اطلاعات برای هر کاربر با کلید رمز جداگانه بمنظور حفظ اطلاعات شخصی و محرمانه. این عملیات تکمیلی هرچه که باشند باری اضافه بر دوش پردازنده سرویس دهنده محسوب می‌شوند و اگر CPU قوی نباشد عملیات به کندی صورت گرفته، شبکه را با پاسخهای توأم با تاخیر مواجه می‌کند.

ویژگی های یک File Server از نظر سخت‌افزاری: وسایل ذخیره‌سازی حجیم، سریع و پایدار که در حال حاضر معمولاً از دیسک سخت استفاده می‌شود. حافظه RAM به میزان کافی برای انجام عملیات File Caching. پردازنده سریع (CPU) برای آن دسته از سرویس دهنده هایی که عملیات تکمیلی مانند فشردن سازی یا رمزنگاری را انجام می‌دهند. البته بطور کلی وجود یک پردازنده سریع در سرویس دهنده مخصوصاً آنهایی که سیستم عامل گرافیکی دارند مانند Windows لازم است اما نقش آن به اندازه موارد اول و دوم در اولویت قرار ندارد.

نکته:

در مجموع برای تمامی سرویس دهنده ها باید دقت داشته باشیم که قدرت سخت‌افزاری سرویس دهنده، نقطه ارتباط سرویس دهنده با شبکه (مانند کارت شبکه)، بستر سخت‌افزاری شبکه و سرعت آن برای ارایه

ی یک سرویس سریع و مطمئن بسیار تعیین کننده است و این موضوع بعداً مورد بحث بیشتری قرار می گیرد

اگر در یک File Server حین انجام کار برق بطور ناگهانی قطع شده یا سرویس دهنده بطور غیرعادی خاموش یا Reset شود برخی از تغییرات که در حافظه RAM انجام شده و هنوز به وسیله ی OS به دیسک سخت منتقل نشده اند از بین می رود بعبارت فنی عملیات File Caching ناقص می ماند لذا بسیار مهم است که سرویس دهنده ها اولاً به UPS متصل بوده ، ثانیاً هیچ گاه آنها را بطور غیرعادی خاموش یا Reset نکنیم بلکه باید طور معمولی خاموش شوند .

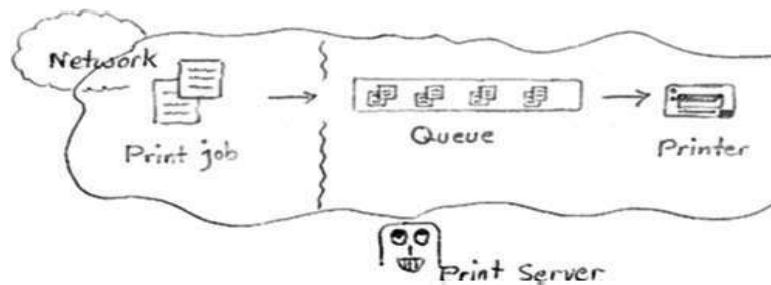
فرایند خاموش شدن معمولی (Shutdown) عبارت است از بسته شدن کلیه پرونده های مورد استفاده ، انتقال اطلاعات تغییر یافته از RAM به دیسک سخت. همانطور که شما پس از پایان ساعات کار ، محل کار خود را مرتب می کنید ، سیستم عامل هم باید اطلاعات را جمع و جور و مرتب کند . هرگونه راه اندازی غیرعادی (مانند فشردن کلید روی Case) به منزله رها کردن محل کار با یک میز نامرتب و به هم ریخته است.

فعالیت عملی : آشنایی با File Server در Microsoft :

یک پوشه حاوی چندین فایل متنوع را به کمک هنر آموز درس در سیستم عامل 2000 , XP یا 2003 به اشتراک گذاشته و از طریق شبکه به آن دسترسی پیدا کنید . در این بخش نیازی به درگیر شدن در جزئیات Security و غیره نیست و هدف تثبیت مفهوم در ذهن هنرجوست . در این صورت هر کامپیوتری که پوشه خود را برای استفاده دیگران به اشتراک می گذارد در عمل تبدیل به یک File Server شده حتی اگر سیستم عامل آن به ظاهر سرویس دهنده نباشد (مثلاً XP\_Professional یا 2000\_Professional باشد)

## 2-5-1- Print Service

این سرویس که معمولاً به وسیله ی Print Server ارائه می شود سخت افزاری است (همراه با نرم افزار) که تعدادی چاپگر متناسب با نیازهای کاربران تحت کنترل آن قرار دارد . کارهای چاپی (Print Jobs) که در نقاط مختلف شبکه به به وسیله ی کاربران ارسال می شود به وسیله ی این سرویس دهنده دریافت شده و ابتدا در یک صف (Queue) قرار می گیرد سپس کار چاپی از صف تحویل چاپگر مربوطه می شود . چاپگرها ممکن است از نظر فیزیکی مستقیماً به سرویس دهنده متصل بوده یا غیرمستقیم از طریق سیستمهای دیگر تحت مدیریت سرویس دهنده باشند ، مهم آنست که چاپگرها تحت کنترل Print\_Server اداره می شوند



شکل 3-1



در سرویس دهنده های چاپ حرفه ای که کارهای چاپی ممکن است حجیم و از نظر تعداد زیاد باشند ، محل فیزیکی ذخیره سازی اطلاعات صف (Queue) روی دیسک سخت است لذا برای یک سرویس دهنده چاپ حرفه ای آنچه که در درجه اول ویژگی سخت افزاری قرار دارد وجود فضای کافی روی یک دیسک سخت خوب و مطمئن است . RAM و CPU در درجه دوم و سوم اهمیت قرار می گیرند .

در مورد سرعت یک Print Server باید توجه داشت که سرعت چاپ بستگی شدید به سرعت فیزیکی چاپ روی کاغذ دارد عبارتی سرویس دهنده های چاپ حتی ضعیفترین آنها دارای توانایی نسبتاً سریع دریافت تمامی کار چاپی و قراردادن آنها را در صف دارا هستند و آنچه که تعیین کننده اصلی سرعت است خصوصیت چاپگر است ، بنابراین :

ویژگی های یک Print Server از نظر سخت افزاری

دیسک سخت با ظرفیت مناسب و مطمئن برای ذخیره سازی اطلاعات صف (Queue) .

حافظه RAM کافی برای انجام عملیات احتمالی Caching (به اندازه File\_Server اهمیت ندارد مگر آنکه Print\_Server صف را مستقیماً در RAM ذخیره کند)

پردازنده سریع (CPU) برای انجام عملیات تبدیل فرمتهای چاپی خاص (Rendering) قبل از ارسال به چاپگرهای خاص . (در خیلی از موارد نیازی نیست چرا که عملیات Rendering معمولاً در ایستگاه ها توسط ارسال کننده Print\_Job صورت می گیرد)

فعالیت عملی : آشنایی با Print Server در Microsoft :

ابتدا یک چاپگر را به کمک هنر آموز درس در سیستم عامل XP , 2000 یا 2003 تعریف کرده سپس به اشتراک گذاشته و از طریق شبکه به آن دسترسی پیدا کنید . در این بخش نیازی به درگیر شدن در جزئیات تنظیمات چاپگر ، Security و غیره نیست و هدف تثبیت مفهوم در ذهن هنرجوست . در این حالت هر کامپیوتری که چاپگر خود را برای استفاده دیگران به اشتراک می گذارد در عمل تبدیل به یک Print Server شده حتی اگر سیستم عامل آن به ظاهر سرویس دهنده نباشد (مثلاً XP\_Professional یا 2000\_Professional باشد)

### 3-5-1 - Application Service

این سرویس معمولاً به وسیله ی Application Server ارائه می شود. فرض کنید که در شبکه سایت هنرستان متشکل از کامپیوترهای Windows قرار دارید . آیکن مربوط به Network\_Neighborhood یا My\_Network\_Places را باز کرده ، لیستی از کامپیوترهای موجود در شبکه را می بینید . یکی از این کامپیوترها بنام « کامپیوتر هنر آموز » است . کنجکاو شده و روی آیکن مربوط به آن Double-Click می کنید . کامپیوتر باز شده و مثلاً یک پوشه را روی آن می بینید که به اشتراک گذاشته شده ، عبارتی کامپیوتر هنر آموز یک File-Server است . پوشه Share شده را باز کرده و داخل آن چندین فایل متنوع با پسوندهای bmp و txt . یکی از فایل ها را انتخاب کرده و روی آیکن مربوطه Double-Click کنید ، می بینیم که فایل باز می شود .

سوال اینست که فایل مذکور کجا اجرا می شود ؟ روی کامپیوتر هنر آموز یا روی کامپیوتر شما (که مثلاً نام آن PC1 است) ؟

با کمی دقت پاسخ خواهید داد که روی PC1 . درست است چرا که کامپیوتر هنر آموز فقط یک File Server است و نه یک Application Server . قرار نیست که کامپیوتر هنر آموز برای ما فایل ها را باز کند یا برنامه ها را اجرا کند ( مگر زمانی که کسی مستقیماً و نه از طریق شبکه روی خود کامپیوتر هنر آموز اقدام به اجرای برنامه کند) . کامپیوتر هنر آموز تنها محل نگهداری فایل مذکور است . وقتی کسی از طریق کامپیوتر خود (مثلاً PC1) و بواسطه شبکه روی آیکن فایلی که روی کامپیوتر هنر آموز قرار داشته و به اشتراک گذاشته شده Double-Click می کند ، این فایل یا برنامه و عبارتی Application از کامپیوتر هنر آموز به PC1 منتقل شده و روی پردازنده ، حافظه و خلاصه کامپیوتر ایستگاه PC1 اجرا می شود . حال اگر بخواهیم فایل روی کامپیوتر هنر آموز اجرا شده و PC1 که به هر دلیلی امکان اجرای آن برنامه را ندارد از آن استفاده ببرد چه باید کرد ؟ پاسخ در استفاده از Application Server است .

تعریف : Application Server کامپیوتریست که نرم افزارهای کاربردی (Applications) را به درخواست کاربران برای آنها اجرا کرده و نتایج حاصل از اجرا را روی کامپیوتر خودشان نمایش می دهد . هسته مرکزی اجرای Application روی سرویس دهنده است و نه سرویس گیرنده . در اینجا سرویس گیرنده تنها بعنوان یک درخواست کننده برای اجرا عمل کرده و بقیه بعهده سرویس دهنده است . اینکه چند درصد کار به وسیله ی سرویس دهنده انجام می شود و چند درصد به وسیله ی ایستگاه ، متغیر بوده و بستگی به ماهیت Application و عملکرد سرویس دهنده دارد . گاهی اوقات ممکن است همه Application روی سرویس دهنده اجرا شده و ایستگاه فقط نتایج را استفاده کند و گاهی ممکن است بخش کوچکی از اجرای Application بعهده سرویس گیرنده بوده و بقیه به عهده سرویس دهنده باشد . به عنوان مثال در برخی از Game Net ها باز ی ها در سرویس دهنده نصب می شود و بقیه کامپیوتر ها که به عنوان سرویس گیرنده هستند از برنامه استفاده می کنند .

برخی از دلایل استفاده از App Server :

امکانات سخت افزاری سرویس گیرنده ممکن است برای اجرای مستقیم برنامه کافی نباشد . مانند : ATM ( عابر بانک )

چون برنامه عمدتاً بطور متمرکز روی یک نقطه یعنی سرویس دهنده اجرا می شود بنابراین مدیریت قویتری را می توان روی آن اعمال کرد .

در نرم افزارهای تحت شبکه ای که برنامه تک تک روی ایستگاه ها ی مختلف بطور کامل اجرا شده اما اطلاعات آنها در یک نقطه متمرکز (مانند File Server) قرار دارد و از طرفی حجم تبادل اطلاعات مابین برنامه اجرایی روی ایستگاه ها و File Server زیاد باشد باعث می شود تا ترافیک شبکه سرعت افزایش پیدا کرده و ضمن اشباع ترافیکی ، مشکلات امنیتی را نیز در پی داشته باشد لذا در اینگونه موارد بهتر است که برنامه بجای اجرای تک تک روی همه ایستگاه ها فقط روی App Server اجرا شده تا از پراکندگی تبادل اطلاعات مابین ایستگاه ها ی مختلف و File Server جلوگیری بعمل آمده و ترافیک تنها مابین Application Server و File Server باشد . درضمن کنترل اطلاعات نیز قویتر صورت می گیرد . در اینگونه موارد معمولاً App Server و File Server از نظر فیزیکی روی یک کامپیوتر قرار می گیرند . مثالی عملی از کاربرد اخیر سرویس دهنده هایی هستند تحت عنوان Database Server که موضوع بحث بعدیست .

ویژگیهای یک Application Server از نظر سخت افزاری  
پردازنده قدرتمند ، چرا که ممکن است تعداد زیاد و متنوعی از نرم افزارها را بخواهد برای کاربران اجرا  
کند . حتی ممکن است نیاز به کامپیوترهای چند پردازنده (Multi Processor) باشد .  
حافظه RAM زیاد چرا که برنامه ها هنگام اجرا همگی در RAM قرار می گیرند .  
دیسک سخت و سایر منابع دیگر بسته به نیاز و تنوع برنامه ها .

فعالیت عملی : آشنایی با Application Server در Microsoft :  
ابتدا (روی کامپیوتری که بعنوان سرویس دهنده در نظر گرفته اید) سرویس Remote Desktop Server  
را به کمک هنر آموز درس در سیستم عامل Server 2003 فعال کرده (در Server 2000 بنام Terminal  
Server) سپس روی ایستگاه برنامه Remote Desktop Client را واقع در Programs->Accessories->Communications  
> اجرا کنید سپس به سرویس دهنده متصل شده ، با نام Administrator وارد شده  
و Desktop مربوط به سرویس دهنده را در اختیار بگیرید . چون این Desktop مربوط به سرویس دهنده  
است و نه ایستگاه لذا هر برنامه ای که اجرا می کنید (مانند ماشین حساب) در واقع روی سرویس دهنده  
اجرا می شود . به کمک Task Manager نشان دهید که ماشین حساب در سرویس دهنده اجرا شده نه در  
ایستگاه . در این حالت هر کامپیوتری که Desktop خود را برای استفاده دیگران در اختیار آنها می گذارد  
در عمل تبدیل به یک Application Server شده حتی اگر سیستم عامل آن به ظاهر سرویس دهنده  
نباشد (مثلاً XP Professional) . با توجه به محدودیت سرویس Remote Desktop Server که در حالت  
خاص خود فقط اجازه اتصال همزمان 2 ایستگاه را می دهد لذا بهتر است این تمرین در گروههایی مرکب  
از 3 کامپیوتر انجام شود که یکی از آنها دارای سیستم عامل 2003 بوده ، سرویس Remote Desktop را  
روی آن فعال شده و بعنوان سرویس دهنده عمل می کند . 2 کامپیوتر دیگر نیز بعنوان سرویس گیرنده با  
هر سیستم عامل دلخواهی از مجموعه Microsoft می توانند باشند حتی 98 . فقط باید نرم افزار Remote  
Desktop Client روی آنها نصب باشد .

4-5-1- آشنایی با Database Service که معمولاً به وسیله ی Database Server ارایه می شود :  
فرض کنید که هنگام ثبت نام است و طی 3 روز 1000 هنرجوی جدید می خواهند نام خود را در  
دوره های آموزشی مورد پذیرش ثبت کنند . برای جلوگیری از ازدحام ، 3 نفر از پرسنل موسسه را همزمان  
بعنوان مسوول در نظر گرفته و به هر کدام یک کامپیوتر مجهز به نرم افزار ثبت نام را تحویل می دهیم . با  
توجه به اینکه هر 3 نفر باید روی یک بانک اطلاعاتی مشترک کار کنند لذا یک شبکه ساده متشکل از 3  
کامپیوتر مذکور برپا کرده و ضمناً یک FileServer برای ذخیره سازی بانک اطلاعاتی در نظر می گیریم  
یعنی در مجموع 4 کامپیوتر . هر کدام از افراد ، نرم افزار ثبت نام را جداگانه روی ماشین خود اجرا کرده ،  
از طریق شبکه به بانک مربوطه که مشترک بوده و روی FileServer ذخیره شده دسترسی پیدا کرده و  
عملیات ثبت ، گزارش گیری و ... را انجام می دهند . در پایان کار ثبت نام ، مدیر موسسه گزارشی را مبنی  
بر تنوع رشته های نام نویسی شده ، سن و سال هنرجویان ، میزان شهریه پرداختی و ... را درخواست  
می کند . هریک از پرسنل مسوولیت تهیه بخشی از گزارش را تقبل کرده ، نرم افزار خود را اجرا می کنند و  
مشغول تهیه گزارش می شوند . در این قسمت برای ادامه کار می توان دو حالت متفاوت را در نحوه کار  
نرم افزار متصور شد :

حالت اول : هریک از برنامه‌های اجرا شده روی کامپیوترها ، بانک اطلاعاتی موجود بر FileServer را باز کرده ، کلیه اقلام اطلاعاتی آنرا از طریق شبکه به کامپیوتر خود انتقال داده (دفعته یا تدریجی) سپس اطلاعات را در کامپیوتر خود بررسی کرده و در صورت صدق در شرایط آنرا چاپ کند . در این حالت اگر بعنوان مثال 1000 رکورد در بانک موجود است ، هر کامپیوتر باید همه آنها را از طریق شبکه به کامپیوتر خود انتقال داده و عملیات پردازش را روی ماشین خودش انجام دهد (البته می‌توان از تکنیکهایی استفاده کرد که نیاز به انتقال همه رکوردها نباشد) . چون 3 کامپیوتر مشغول به گزارش‌گیری هستند لذا تقریباً 3000 رکورد اطلاعاتی در ترافیک شبکه سهم می‌شوند . ممکن است با خود بگوییم که 3000 رکورد را کامپیوترها سریع می‌خوانند ، و زمانی طول نخواهد کشید. این طرز فکر درست است اما تصور کنید که با یک بانک اطلاعاتی حجم درگیر شویم مثلاً بانک اداره ثبت احوال با فرض شصت میلیون رکورد ! در اینجا دیگر نمی‌توان مابین ترافیک شصت میلیون رکورد در شبکه و 3 برابر آن یعنی یکصد و هشتاد میلیون تفاوت قائل نشد .

حالت دوم : مشکلی که در حالت قبلی وجود دارد آنست که حجم ترافیک شبکه با افزایش اطلاعات بانک و تعداد کاربران سرعت زیاد شده و باعث اشباع شبکه می‌شود بنابراین بهتر است هر کامپیوتر بجای آنکه خودش رأساً مبادرت به خواندن اطلاعات بانک از File Server و پردازش آن در ایستگاه کند از سرویس دهنده بخواهد که عملیات را انجام دهد . بدین ترتیب که یک Application Server روی همان File Server نصب کرده سپس از ایستگاه به سرویس دهنده فرمان می‌دهیم که سرویس دهنده اطلاعات را جستجو کند و فقط نتایج را برای ما ارسال نماید نتیجه‌ای که از این کار به دست می‌آید آنست که دیگر هیچ نیازی به انتقال حجم اطلاعات در شبکه و پردازش آن در ایستگاه نبوده لذا هم ترافیک شبکه به حداقل می‌رسد و هم پردازش ایستگاه سبک می‌شود چرا که ایستگاه فقط نتایج را از سرویس دهنده دریافت کرده و برای کاربر نمایش می‌دهد ، بنابراین :

تعریف : به یک Application Server که روی بانکهای اطلاعاتی کار می‌کند اصطلاحاً Database Server (به اختصار DB Server) می‌گوییم . پس می‌بینیم که DB Server یک سرویس دهنده جدید نیست بلکه همان AppServer است که برای کار روی بانکهای اطلاعاتی طراحی شده و عبارتی همان کاربرد سوم App Server است که در بخش مربوطه اشاره شد . از سرویس دهنده های معروف بانکهای اطلاعاتی می‌توان به Oracle و Microsoft SQL Server اشاره کرد که با آنها در درس بانک اطلاعاتی آشنا می‌شوید .

#### ویژگیهای سخت‌افزاری یک Database Server

ویژگی های این سرویس دهنده نیز همانند App Server است علاوه بر این دیسک سخت هم مثل CPU و RAM در درجه اول اهمیت قرار می‌گیرد . پس توجه همزمان به هر 3 پارامتر مهم است .

سرویس دهنده ها به چه سیستم عاملی نیاز دارند؟

اما پاسخ به این سوال مستلزم آشنایی و طبقه‌بندی محصولات سیستم عامل و ویژگیهای مربوطه است که خود بحث مفصلی است لذا به تیترا آنها اکتفا کرده و بحث پیرامون آنها را به توضیحات هنر آموز درس و تحقیقات خواننده واگذار می‌کنیم، البته در این مرحله نیاز به دانستن و پرداختن به جزئیات فنی سیستم عاملها نبوده، آشنایی کلی، کاربرد و عمومیت حوزه مصرفی آنها کفایت می‌کند.

6-1- طبقه‌بندی محصولات Microsoft در زمینه سیستم عامل ها  
شرکت مایکروسافت بطور کلی در مورد سیستمهای عامل، 2 دسته محصول ارائه کرده است:  
سیستم عاملهایی که برای نصب و کاربرد در سرویس گیرنده.  
سیستم عاملهایی که برای نصب و کاربرد در سرویس دهنده .

در متن زیر طبقه بندی این سیستم عامل ها نشان داده شده است:

#### **Client Operating Systems :**

- DOS Family : DOS (v1, ... , v6,2 , v6,22 , v7,0 )
- Windows 3.x Family : Windows 3,1 , 3,11 (Windows for Workgroups)
- Windows 9x Family : Windows 95 , 97 (95 OSR2) , 98 , 98 SE , ME
- Windows NT Family :
  - NT 3,51 Workstation
  - NT 4,0 Workstation

NT 5,0 : 2000 Professional

NT 5,1 : XP (Home , Professional , Media center , Tablet PC)

#### **Server Operating Systems :**

- NT 3,51 Server
- NT 4,0 Server
- NT 5,0 : 2000 Server Family : (Server, Advanced Server, Data center)
- NT 5,2 : 2003 Server Family : (Standard, Enterprise, Data center, Web edition)

همانطور که دیده می شود ویندوز 2000 بنام NT 5,0 ، XP بنام NT 5,1 و 2003 بنام NT 5,2 نیز خوانده می شوند . در کل به هر 3 سیستم عامل ، خانواده NT 5.x گفته می شود.

XP فقط در گروه سرویس گیرنده و 2003 فقط در گروه Server قرار گرفته . عبارت دیگر XP نسخه سرویس دهنده نداشته و 2003 نیز نسخه سرویس گیرنده ندارد.

هرچند خانواده 9x و XP جایی در گروه سرویس دهنده ها ندارند اما خیلی از کاربران تجربه اشتراک گذاری پوشهها و چاپگرهای خود را در آنها داشته اند، یعنی کامپیوتری که سیستم آن مثلاً 98 است تبدیل به File Server یا Print Server می شود. این موضوع ناقض طبقه بندی فوق نیست ، عبارتی هرچند 98 هم می تواند در مواردی تبدیل به سرویس دهنده شود اما قرار نگرفتن آن در گروه سرویس دهنده ها به معنی آنست که 98 یا XP عمدتاً برای کاربرد در ایستگاه ها طراحی شده اند.

مایکروسافت فقط خانواده NT را برای کاربرد در سرویس دهنده ها پیشنهاد داده است.

نام برخی از محصولات شرکت های دیگر در زمینه سیستم عامل ها (که عمدتاً برای کار در سرویس دهنده ها استفاده می شوند)

-UNIX (SCO , Solaris , BSD , Free BSD , AIX , HP , Linux , ...)

- Novell Netware
- IBM OS/2 , IBM LAN Server
- Apple Macintosh (Used in Graphic Stations)
- ...

خانوادهٔ UNIX تقریباً در همهٔ زمینه‌ها کاربرد دارد. امروزه در ایران شبکه‌های بانکی، شرکت نفت، شهرداری، بیمه و... همگی از این خانواده بعنوان سیستم عامل اصلی در سرویس دهنده‌ها بهره می‌برند.

Novell در ایران عمدتاً بعنوان File Server و تا حدی Print Server بکار می‌رود هرچند که در خیلی از مکانها Database Server نیز روی Novell اجرا می‌شود.

#### 1-7- آشنایی با ویژگیهای سیستم عامل های شبکه‌ای

سیستمهای عامل که در شبکه استفاده می‌شوند باید ویژگیهایی را افزون بر سیستمهای عامل که در کاربردهای خانگی مورد استفاده قرار می‌گیرند داشته باشند. هرچند امروزه اکثر کاربران خانگی به محض اتصال به اینترنت عملاً بعنوان کاربر شبکه محسوب می‌شوند بنابراین خصوصیات سیستمهای عامل شبکه برای سیستمهای خانگی نیز (در حدی کمتر) معنی پیدا می‌کند. برخی از این ویژگیها به ترتیب اهمیت عبارتند از:

- Security
- Multitasking
- Multi Processor Support
- Reliable & Stable
- Fault Tolerance
- Backup Utilities
- Simple & Unified Administrative Tools
- Support

با برخی از این ویژگیها قبلاً در درس سیستم عامل آشنا شده اید.

#### 1-7-1 Security:

امنیت، مهمترین ویژگی است. متأسفانه دنیا ایده‌آل نیست لذا در نظر گرفتن مسایل امنیتی هرچند که باعث کندی سیستم می‌شود اما بعنوان رکن کار هر سیستم عامل شبکه محسوب می‌شود. امنیت برای سیستم عامل را می‌توان در حوزه‌های مختلفی بررسی کرد بعنوان مثال:

(الف) امنیت در حوزهٔ دسترسی به دیسک و فایل -سیستم (Disk & File-System Security)

(ب) امنیت در حوزهٔ عملیاتی که کاربرد عام دارند مانند:

تغییر ساعت سیستم (Changing System time)

نصب نرم‌افزار، سخت‌افزار و انجام تنظیمات (Hardware & Software Installation)

اجرای برنامه‌ها و تغییر در پارامترهای مربوطه (Running Applications & Services)

(ج) امنیت در حوزهٔ شبکه و اطلاعات تبادلی (Network Security)

#### (د) امنیت در ورود به سیستم (System Login)

مثال : Win 3,1 ، Dos و خانواده 9x جزو آندسته از سیستمهایی هستند که امنیت چندانی مخصوصاً در حوزه‌های "الف"، "ب" و "ت" ندارند. همه می‌دانیم که پس از روشن کردن یک کامپیوتر با سیستم 98 براحتی می‌توان بدون هیچگونه گذر واژه ای وارد آن شده، به هر جا روی دیسک دسترسی پیدا کرده (که با FAT آماده شده)، هر برنامه‌ای را نصب، حذف یا اجرا کرده و هرگونه تغییر سخت‌افزاری را اعمال کرد! در صورتیکه این امر در خانواده NT براحتی امکان‌پذیر نیست، فقط کاربرانی که عضو گروه Administrators باشند توانایی تام در انجام عملیات فوق را دارا هستند.

نکته : کاربرانی که هنگام نصب XP تعریف می‌شوند همگی عضو گروه Administrators بوده و برای کاهش قدرت آنها باید بعد از نصب از طریق برنامه‌ی مربوطه وارد عمل شد و گروه آن‌ها را به Limited (users) تبدیل کرد. چنانچه در XP فقط یک کاربر تعریف کنیم، در آنصورت کامپیوتر پس از Boot شدن خودبخود وارد سیستم می‌شود بدون آنکه گذر واژه‌ی از ما خواسته شود، در این حالت سیستم عامل XP بطور خودکار همان یک کاربر را Auto Login می‌کند و این بمعنای نقض امنیت در ورود به سیستم نیست، می‌توان این ویژگی را غیرفعال کرد. ضمناً این خصوصیت یعنی Auto Login در بقیه اعضای خانواده NT نیز وجود دارد.

فعالیت عملی مربوط به ویژگی Security :

الف) نشان دهید که در XP کاربران تعریف شده هنگام نصب، عضو گروه Administrators هستند.

ب) نشان دهید که در XP، یک کاربر عادی (عضو گروه Users) قادر به ایجاد فایل جدید در ریشه دیسک که با فایل -سیستم NTFS فرمت شده نیست (پوشه جدید را می‌توان درست کند اما فایل را خیر)

ج) نشان دهید که در XP، یک کاربر عادی (عضو گروه Users) نمی‌تواند ساعت سیستم را تغییر دهد.

د) نشان دهید که در XP، یک کاربر عادی (عضو گروه Users) نمی‌تواند از طریق Device Manager یک سخت‌افزار را (مثلاً Mouse) غیر فعال (Disable) کند.

#### Multi Tasking - 1-7-2 :

چند وظیفه‌ای، توانایی اجرای همزمان چندین برنامه با هم. این ویژگی نیازی به شرح بیشتر نداشته و امروزه در تمامی سیستمها وجود دارد و یک ویژگی عادی بشمار می‌رود. DOS بعنوان یک سیستم قدیمی Multi task نیست اما بقیه تقریباً همگی Multi Task هستند منجمله Windows 3.x.

تقسیم زمانی بین کارهای مختلف و گردش سریع بین آنها. این تکنیک در اصطلاحات فنی Time\_Sharing یا "اشتراک زمانی" خوانده می‌شود. تکنیک اشتراک زمان نه تنها در اجرای برنامه‌ها به وسیله CPU بلکه در مخابرات و شبکه نیز کاربردهای فراوانی در انتقال اطلاعات دارد و یکی از روشهایی است که می‌توان اطلاعات چندین فرستنده را روی یک محیط انتقال بطور همزمان ارسال کرد. البته این تکنیک در اصطلاحات مخابراتی TDM = Time Division Multiplexing خوانده می‌شود.

#### Multi Processor Support - 1-7-3 :

پشتیبانی از چندین پردازنده، می‌دانیم که هرچه تعداد پردازنده‌های موجود بر روی یک برد اصلی بیشتر باشد کارها سریعتر انجام می‌شود. امروزه بردهای چند پردازنده در 2 زمینه عمده کاربرد دارند :

سرویس دهنده ها ، مخصوصاً App Server و DB Server که قبلاً اشاره شد .  
کامپیوترهایی که عملیات سنگین گرافیکی و پویا را انجام می دهند . (Graphic Workstations)  
بنابراین در مواردی که نیاز به استفاده از بردهایی با بیش از یک CPU باشد لازم است تا سیستم عامل نیز  
بتواند آنها را شناسایی کرده و استفاده کند . در خانواده Microsoft فقط سیستمهای NT قادر به شناسایی و  
بهره برداری از چندین CPU هستند .

تحقیق : پشتیبانی از چندین پردازنده در سیستم عامل ها با 2 سیاست کلی متقارن و نامتقارن انجام می شود ،  
(SMP=Symmetric Multi Processing , AMP=Asymmetric Multi Processing) ، هر یک را به  
اختصار بررسی کرده و بگویید که میکروسافت در سیستمهای خود از کدام روش استفاده می کند ؟  
4-7-1- تحمل خطا Fault Tolerance :

تحمل خطا ، عدم تأخیر در ارائه سرویس و قدرت تحمل در هنگام بروز مشکل و خطاهای عمدتاً  
سخت افزاری است بعبارت دیگر Fault Tolerance (باختصار FT) قابلیت است در سیستم عامل که  
می تواند هنگام بروز مشکلات از تجهیزات جایگزین استفاده کرده و بدون تأخیر (یا با تأخیر بسیار کوتاه)  
بطور خودکار به سرویس دهی ادامه دهد . نکته اصلی در FT اینست که هنگام بروز خطا اولاً زمان قطعی  
سرویس صفر یا بسیار کوتاه بوده و ثانیاً عملیات جایگزینی بدون عوامل انسانی و بطور خودکار صورت  
می گیرد . مسوول سیستم در فرصت مناسب می تواند عیوب را بررسی و رفع کند .  
مثال 1 : فرض کنید که یک File Server داریم که تمامی اطلاعات خود را روی یک دیسک سخت ذخیره  
کرده است . اگر برای دیسک مشکلی بروز کند مثلاً بر اثر یک شوک الکتریکی در برق بخشی از قطعات آن  
بسوزد چه اتفاقی می افتد ؟ بدیهی است که سرویس قطع می شود ، چکار کنیم که سرویس قطع نشود ؟  
الف) شرایط سخت افزاری لازم را مهیا کنید یعنی از ابتدا 2 دیسک سخت روی سیستم نصب کنید .  
ب) سیستم عاملی را انتخاب کنید که دارای قابلیت FT در زمینه دیسک باشد . سیستم عامل در شرایط عادی  
هر اطلاعاتی را که روی دیسک اول می نویسد عیناً روی دیسک دوم نیز کپی می کند بعبارتی دیسک دوم  
همانند آینه ایست از دیسک اول (Disk Mirroring , Disk Duplexing) حال اگر به هر دلیل یکی از  
دیسکها از کار بیافتد سیستم عامل می تواند بدون لحظه ای تأخیر اطلاعات را با دیسک دوم تبادل کند . مثال  
فوق در اصطلاحات کامپیوتری Disk\_Fault\_Tolerance با تکنیک Mirror یا Duplex یا RAID 1 خوانده می شود .  
از میان محصولات میکروسافت ، سیستمهای NT که در گروه سرویس دهنده قرار دارند  
همگی قابلیت Disk Fault Tolerance را دارا هستند .

مثال 2 : یک سرویس دهنده داریم (از هر نوع دلخواه) که با یک کارت شبکه (NIC) به شبکه متصل شده  
و کامپیوترها از آن سرویس می گیرند . اگر برای کارت شبکه یا خط متصل به آن اتفاقی بیافتد چه می شود ؟  
بدیهی است که سرویس قطع می شود اگر بخواهیم که سرویس قطع نشود باید :  
الف) شرایط سخت افزاری لازم را مهیا کنید یعنی از ابتدا 2 عدد NIC روی سیستم نصب کنید .  
ب) سیستم عاملی را انتخاب کنید که دارای قابلیت FT در این زمینه باشد . سیستم عامل در شرایط عادی  
اطلاعات را تقسیم کرده و از هر 2 کارت برای ارسال و دریافت استفاده می کند (که البته باعث افزایش  
سرعت نیز می شود) حال اگر به هر دلیل یکی از کارتها از کار بیافتد ، سیستم از کارت دیگری برای ادامه  
کار استفاده می کند . مثال فوق در اصطلاحات کامپیوتری NIC Fault Tolerance خوانده می شود و در



برخی از متون به آن Port Trunk یا Port Aggregation یا Link Aggregation می‌گویند که بعداً نیز مورد بحث قرار خواهد گرفت. از میان محصولات مایکروسافت، سیستمهای NT اعم از سرویس گیرنده یا Server در صورتیکه کمپانی سازنده کارت شبکه درایور مناسب را برای محصول خود ارائه داده باشد می‌توان از این خاصیت بهره برد.

مثال 3: فرض کنید که یک سرویس دهنده داریم (از هر نوع دلخواه) و این سرویس دهنده ممکن است هریک از موارد قبلی Fault tolerance را اعم از Disk یا NIC داشته باشد یا خیر. اگر به هر دلیل سرویس دهنده بطور کامل از کار بیافتد چه می‌شود؟ بدیهی است که سرویس قطع می‌شود، چکار کنیم اختلالی در سرویس دهی بروز نکند؟

الف) شرایط سخت‌افزاری لازم را مهیا کنید یعنی از ابتدا 2 یا چند سرویس دهنده را با تجهیزات ویژه به یکدیگر متصل کنید. به این مجموعه از سرویس دهنده ها اصطلاحاً یک "خوشه سرویس دهنده" یا Server Cluster گفته می‌شود.

ب) سیستم عاملی را انتخاب کنید که دارای قابلیت FT در زمینه Clustering باشد. کلیه سیستمها در شرایط عادی اطلاعات مورد نیاز را با یکدیگر تبادل کرده (Synchronize) و چنانچه یکی از اعضای Cluster (یعنی یکی از سرویس دهنده ها) از کار افتد بقیه می‌توانند سرعت و بدون تأخیر کار او را جبران کنند. از میان محصولات مایکروسافت فقط چند سیستم از مجموعه NT در خانواده سرویس دهنده دارای قابلیت Cluster هستند بعنوان مثال 2000 Server فاقد آن بوده اما 2000 Advanced Server و 2000 Data center Server دارای توانایی آن هستند.

#### 5-7-1- نرم افزار تهیه نسخه پشتیبان Backup Utilities:

امروزه اهمیت تهیه Backup برای یک کاربر باتجربه پوشیده نیست، بالاخره هر کس که با کامپیوتر سروکار دارد با لحظه‌ای مواجه شود که به هر دلیل اطلاعات اصلیش مخدوش یا غیرقابل دسترس شده است در این حالت با نسخه پشتیبان می‌توان اطلاعات را دوباره بازگرداند. اطلاعات را در حالت کلی می‌توان به دو دسته تقسیم کرد:

الف) اطلاعاتی که کاربر مستقیماً و کم و بیش از آن آگاه بوده و اهمیتش بر او پوشیده نیست مانند انواع پرونده‌ها یا حتی برنامه‌های کاربردی که تهیه و نصب کرده‌است: (User Data)

ب) اطلاعاتی که کاربر مستقیماً با آن سروکار ندارد بلکه برای سیستم عامل مهم است: (System Data) اغلب کاربران پس از مدت کوتاهی با نحوه تهیه Backup از اطلاعات خودشان یعنی User Data آشنایی شود اما کمتر کاربر عادی پیدا می‌شود که طی مدت کوتاهی بتواند بطور کامل از System Data نیز Backup گرفته یا Restore کند چرا که با توجه به پیچیدگی سیستم عاملها، کسب آگاهی نسبت به ظرفتهای سیستم عامل در زمان کوتاه امر ساده‌ای نبوده و نیاز به تجربه و تخصص دارد.

چگونه می‌توان از System Data بدون مهارت لازم Backup گرفت؟  
یک راه حل مناسب آنست که سیستم عامل ابزارهای قوی و عین حال User Friendly در اختیار کاربر بگذارد تا او بتواند اولاً براحتی اطلاعات را دسته‌بندی کند ثانیاً بدون داشتن تخصص زیاد قادر به تهیه

Backup از System Data باشد. خوشبختانه ابزارهای تهیه Backup در سیستمهای NT 5.x دارای چنین تواناییایی بوده و کاربر می تواند در صورت داشتن مجوز، تنها با علامتگذاری در قسمت "System State" اقدام به تهیه پشتیبان از System\_Data کند.

ممکن است بخواهید بدانید تفاوت بین ابزارهای خاص تهیه Backup (مانند NTBackup در NT 5.x) با ابزارهای عمومی مدیریت فایلها که عملیاتی مانند Copy-Paste را انجام می دهند (مانند My Computer Explorer) چیست؟ در جواب باید گفت: قابلیتایی که در ابزارهای خاص وجود دارد در برنامه های عمومی (مانند My Computer) نیست. اهم این قابلیتها عبارتند از:

(الف) به کمک ابزارهایی مانند NTBackup ب راحتی از System Data نسخه پشتیبان تهیه می شود.  
(ب) با این ابزارها، از فایلهایی که در حال استفاده هستند (Open Files) می توان به راحتی نسخه پشتیبان تهیه کرد.

(ج) سیاستهای تهیه Backup یا بعبارت فنی Backup Policy در ابزارهای خاص تنوع بیشتری دارد، بدان معنی که انتخاب فایلها برای Backup می توان با معیارهایی همچون "فقط فایلهای تغییر یافته" و... صورت گیرد. که در ابزارهای معمولی تنوع این معیارها کمتر است.

(د) با ابزارهای خاص می توان انجام عملیات را بطور خودکار در موعد دلخواه زمانبندی کرد (Scheduling).

(ه) ابزارهای خاص می توانند از مجوزهای امنیتی (لیست دسترسی افراد به فایلها = Access Control List) که باختصار ACL خوانده می شود نیز Backup گرفته و Restore کنند. منظور از ACL لیستی است در فایل-سیستمهایی مانند NTFS که تعیین می کند چه افرادی چه عملیاتی را با یک فایل یا پوشه می توانند انجام دهند. بدیهی است که ACL در FAT یا FAT 32 وجود ندارد چرا که FAT امنیت ندارد. فرایند Backup برای خود جزو مباحث مهم بوده و معمولاً در درس سیستم عامل پیشرفته یا سرویس دهنده مورد بحث قرار می گیرد با اینحال برای تثبیت نکات یاد شده فوق، انجام این کار را اکیداً توصیه می کنیم که باید به کمک هنر آموز درس انجام شود.

(الف) نشان دهید که با NTBackup می توان ب راحتی از اطلاعات سیستم Backup تهیه کرد.

(ب) دقیقاً با کدام کاربر وارد سیستم شده اید؟ پس از پاسخ به این سوال، برنامه My Computer را اجرا کرده سپس پارتیشنی را که سیستم عامل روی آن نصب شده باز کرده (مثلاً دیسک C:) وارد پوشه Documents\_and\_Settings شوید. قاعدتاً باید یک پوشه همنام با کاربری را که با آن وارد سیستم شده اید ببینید. حال سعی کنید که (با استفاده از برنامه My Computer) از این پوشه Copy-Paste بگیرید. آیا امکان پذیر است؟ قطعاً خیر! چرا که یکی از فایلهای موجود در این پوشه (که البته مخفی نیز هست) بنام NTUser.dat در حال استفاده بوده اصطلاحاً Open است و برنامه My Computer نمی تواند از آن کپی تهیه کند. حال با استفاده از برنامه NTBackup از همین پوشه کپی بگیرید. نتیجه چیست؟ بلی، امکان پذیر است. بنابراین نشان دادید که NTBackup قدرت بیشتری نسبت به My Computer در تهیه پشتیبان از فایلها و پوشه ها دارد.

#### 6-7-1- ابزار های مدیریتی Simple and Unified Administrative Tools :

ابزارهای مدیریتی ساده ، قدرتمند و یکپارچه . هر سیستم عاملی هرچقدر هم که قوی باشد اما اگر پیکربندی ، تنظیمات و بطور کلی مدیریت آن پیچیده باشد با عدم استقبال عامه مواجه می شود و این دقیقاً یکی از دلایلی است که UNIX بویژه نسخه های قدیمی تر فقط در بین متخصصین محبوبیت پیدا کرد (البته امروزه نسخه های جدیدتر از این حیث کامل هستند اما اندکی دیر شده چرا که مایکروسافت از این طریق در بین کاربران عادی کاملاً جای خود را تثبیت نموده است.

فعالیت عملی : آشنایی با یکی از ابزارهای مدیریتی قوی در NT 5.x :

یکی از برنامه های قدرتمند برای مدیریت بخشهای مختلف ، برنامه ایست بنام Computer Management . برای اجرای این برنامه راههای متفاوتی وجود دارد اما 2 راه را بیان می کنیم :

(الف) روی آیکن My Computer واقع بر دسکتاپ کلیک راست کرده ، گزینه Manage را انتخاب کنید

(ب) از طریق Run تایپ کنید : compmgmt.msc

پس از اجرای برنامه ، بررسی کنید که بوسیله آن چه کارهایی را می توان انجام داد .

#### 7-7-1- قابلیت اطمینان و پایداری Reliable and Stable :

قابل اطمینان و پایدار ، با یک مثال مفهوم این ویژگی برای ما تثبیت می شود ، تجربه شده است که سیستم عامل ویندوز 98 برخلاف سیستم عامل UNIX و LINUX پس از نصب چندین برنامه مختلف بهم می ریزد حال بنظر شما چنین سیستمی مناسب شبکه و مخصوصاً سرویس دهنده است؟! خوشبختانه سیستمهای NT 5.x و مخصوصاً NT 5.x در وضعیت بسیار بهتری نسبت به خانواده 9x قرار دارند و بدین لحاظ برای کاربرد در شبکه ها اعم از سرویس گیرنده یا سرویس دهنده مناسب ترند .

#### 8-7-1- پشتیبانی Support :

پشتیبانی ، هر سیستم عاملی اعم از قوی یا ضعیف نیاز به رشد و رفع مشکلات و نواقص دارد و این میسر نیست مگر با پشتیبانی از طرف تهیه کننده گان یا تیمهای جنبی . خوشبختانه در زمینه محصولات مایکروسافت با وجود نواقص بسیار مخصوصاً در زمینه امنیتی ، پشتیبانی آن قوی بوده و اکثراً تجربه بروز رسانی سیستم عاملهای NT 5.x را از طریق برنامه Automatic Update داشته ایم .

خود آزمایی و تحقیق

1- شبکه اینترنت از نظر سرویس دهی به کدام دسته شبکه های کامپیوتری تعلق دارد؟

2- از لحاظ تقسیم بندی شبکه های کامپیوتری از نظر گستردگی فیزیکی سیستم بانکی شتاب به کدام دسته تعلق دارد؟

3- سرویس های رایج در شبکه های کامپیوتری را نام ببرید؟

4- نقش حافظه RAM را در هر یک از انواع File Server ، Print Server ، Applicatin Server بررسی کنید؟

5- داشتن چندین پردازنده در کدام یک از انواع سرویس دهنده می تواند مفید باشد؟

6- System Data و User Data را تعریف کنید؟

7- ویژگی های مهم سیستم عامل های سرویس دهنده را نام ببرید؟

8- تفاوت Multi Tasking و Multi Programing را بنویسید.

9- تحقیق کنید که یک سرویس دهنده NAS به لحاظ سخت افزاری باید چه قابلیت هایی داشته باشد؟

10- تحقیق کنید که حداقل سخت افزار لازم برای نصب هر یک از سیستم عاملهای محصول میکروسافت چیست و آنها را با هم مقایسه کنید.

## فصل دوم- سیستم های انتقال دیجیتال

هدف های رفتاری

روش ارسال اطلاعات به صورت موازی را بیان کند.

روش های ارسال اطلاعات به صورت سری را شرح دهد.

انواع روش های انتقال اطلاعات بر اساس جهت آنها را تعریف کند.

سیگنال های اطلاعات و انواع آن را شرح دهد.

پهنای باند را تعریف کند

نویز و انواع آن را شرح دهد.

یکی از مسایل مهم در شبکه های کامپیوتری نحوه برقراری ارتباط بین کامپیوترهاست . منظور از برقراری ارتباط این است که اطلاعات به چه ترتیبی ارسال شوند.می توان این پرسش ها را مطرح کرد که آیا روش ارسال به صورت بیت به بیت و جداگانه باشد یا گروهی از اطلاعات با هم و به صورت گروهی ارسال شوند یا این که آیا فرستنده آن ها را همانند یک ایستگاه فرستنده رادیویی ارسال نماید یا از روشی که در مخابرات برای انتقال صورت به کار می رود ، استفاده شود .جواب این پرسش ها این است که اطلاعات در شبکه به صورت کدهای دودویی ارسال می شوند . در سیستم دودویی فقط از دو کد صفر و یک استفاده می شود که در کامپیوتر مقصد از ترکیب این کدها ، اعداد ، حروف و کاراکترهای ویژه به دست می آید .

ارسال اطلاعات به صورت دودویی می تواند به دو صورت انجام شود:

1-Parallel (یا موازی )

2-سریال ( پشت سرهم )

در روش موازی تعدادی از بیت ها با هم و به صورت گروهی ارسال می شوند ولی در روش سریال ، بیت ها تک به تک و پشت سرهم ارسال می شوند . نحوه ارسال به صورت موازی فقط یک شیوه دارد ، در صورتی که ارسال سریال از دو روش ارسال هم زمان (Synchronous) و غیر هم زمان (Asynchronous) استفاده می شود.

1-2- ارسال موازی (Parallel)

در این روش اطلاعات قبل از ارسال تبدیل به کدهای باینری شده و یک به یک ارسال می شوند . برای مثال می توان گفت که این عمل مانند این است که یک نامه را تبدیل به حروف تشکیل دهنده آن کرده و حروف را یک به یک ارسال کنیم.

حال تعدادی کد باینری داریم که می خواهیم ارسال کنیم؛ اگر تعدادی از آن ها را تبدیل به یک گروه کرده و باهم بفرستیم ارسال سریعتر انجام می شود و این چیزی است که در ارسال موازی اتفاق می افتد در این روش تعدادی کاراکتر از طریق چند خط ارتباطی و به صورت هم زمان با هم ارسال می شوند؛ این خطوط می توانند در درون یک کابل شبکه یا یک شبکه بی سیم بنا شده باشند به صورت پیش فرض 8 خط برای ارسال موازی در نظر گرفته شده است یعنی می توانیم حداکثر 8 کد را هم زمان ارسال کنیم .

## 2-2- ارسال سریال

در ارسال سریال ، بیت ها به دنبال هم و به صورت سری انتقال می یابند ؛ به این ترتیب که بیت ها پشت سرهم قرار گرفته و یک رشته را می سازند و این رشته به کامپیوتر مقصد ارسال می شود . در حین ارسال ممکن است عوامل مختلفی مثل نویز و هم شنوایی که در همین واحد کار در مورد آن ها توضیح داده شده است ، روی اطلاعات اثر گذاشته و آن را خراب کنند . برای کنترل بیت ها و کمک به ارسال عاری از اشکال ، ابتدا و انتهای بیت ها با یک سری علامت به نام های بیت شروع<sup>2</sup> بیت پایان<sup>3</sup> مشخص می شود که در روش های مختلف ارسال سریال محل قرار گیری این علامت ها و محتوای آن ها متفاوت است . ارسال سریال به دو روش امکان پذیر است .

### 1-2-2- ارسال سریال غیر هم زمان

دلیل نام گذاری این روش به غیر هم زمان این است که زمان بندی در هنگام ارسال اطلاعات مهم نیست و زمان بندی بین دو واحد فرستنده و گیرنده انجام می شود . در این روش انتقال اطلاعات براساس الگوهای ارسال و دریافت که از قبل مشخص شده است ، انجام می شود و تا وقتی این الگوها رعایت شوند ارسال بدون وقفه انجام می پذیرد. در این روش هر 8 بیت اطلاعات تبدیل به یک رشته شده و قبل از هر رشته یک Start Bit و پس از هر رشته یک Stop Bit قرار می گیرد . در صورتی که هر کدام از بیت ها هنگام ارسال آسیب ببینند ، آن بیت مشخص شده و دوباره ارسال می شود . در ارسال غیر هم زمان 25% از کل ظرفیت خط ارتباطی صرف کنترل ترافیک شده و تنها 75% ظرفیت برای انتقال اطلاعات استفاده می شود .

<sup>۲</sup>-Start Bit

<sup>۳</sup>-stop Bit

توانایی کامپیوترها در ارسال و دریافت اطلاعات از نظر سرعت متفاوت است؛ بنابراین ممکن است یک کامپیوتر بتواند در واحد زمان، مقدار بیشتری اطلاعات به سمت کامپیوتر مقصد ارسال کند.

بدیهی است در چنین حالتی، کامپیوتر گیرنده که با سرعت کمتری کار می کند نمی تواند تمامی اطلاعات ارسال شده را دریافت نماید، در نتیجه مقداری از این اطلاعات در شبکه از بین می رود، بنابراین در کامپیوترهایی که در حال تبادل اطلاعات هستند، همواره سرعت ارسال و دریافت را باهم چک کرده و در صورت لزوم سرعت ارسال را کم یا زیاد می کنند. در روش انتقال غیر هم زمان هیچ زمان بندی برای ارسال یا دریافت صورت نمی گیرد و کنترل ترافیک به صورت لحظه ای انجام می شود. به همین دلیل در روش انتقال غیر هم زمان، 75% ظرفیت خط انتقال صرف کنترل ترافیک می شود. منظور از ظرفیت خط انتقال تهمان پهنای باند است که در همین واحد کار توضیح داده شده است.

#### 2-2-2- ارسال سریال هم زمان

در روش ارسال هم زمان همانند روش ارسال غیر هم زمان اطلاعات ابتدا به کدهای دودویی تبدیل می شوند، سپس تعدادی بیت که حاوی اطلاعات ارسالی هستند در امتداد یکدیگر قرار گرفته و یک رشته را تشکیل می دهند، این رشته همانند رشته هایی که در روش ارسال غیر هم زمان ساخته می شوند، به وجود می آیند؛ سپس تعدادی از آن ها به هم متصل شده و رشته طولانی تری را پدید می آورند، پس از آن ابتدا و انتهای این رشته به وسیله ی بیت شروع و بیت پایان مشخص می شود؛ در این لحظه قبل از شروع ارسال، دو کامپیوتر به وسیله ی سیستم زمان بندی داخلی، خود را با هم هماهنگ می کنند سپس کامپیوتر ارسال کننده، ارسال را شروع کرده و کامپیوتر گیرنده اطلاعات را دریافت می کند.

زمان ارسال یا دریافت اطلاعات به وسیله ی سیستم زمان بندی برای هر دو کامپیوتر مشخص می شود، در نتیجه هیچ گاه کامپیوترها ارسال اطلاعات را هم زمان با یکدیگر انجام نمی دهند و عمل انتقال اطلاعات به صورت نوبتی انجام می شود.

در روش ارسال هم زمان علاوه بر استفاده از سیستم انتقال سریع تر، عمل کنترل ترافیک نیز انجام نمی شود و از تمام ظرفیت خط انتقال برای ارسال و دریافت استفاده می شود؛ به همین دلیل سرعت انتقال به مراتب بالاتر از روش غیر هم زمان است.

#### 2-3- جهت انتقال اطلاعات

بین دو واحد فرستنده و گیرنده همیشه اطلاعاتی در حال جا به جا شدن است که در محیط های مختلف جهت آن متفاوت است. ارتباط بر اساس جهت های انتقال به سه گروه تقسیم می شوند؛

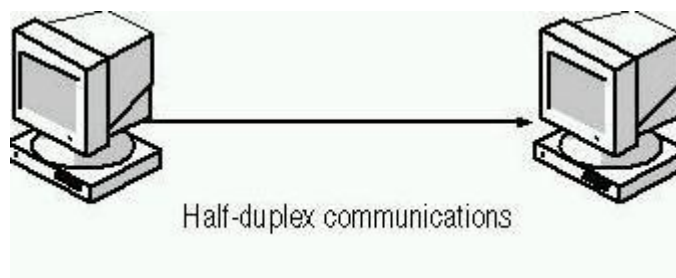
1- یک طرفه<sup>4</sup>

2- دوطرفه غیر هم زمان<sup>5</sup>

3- دوطرفه هم زمان<sup>6</sup>

1-3-2- ارتباط یک طرفه

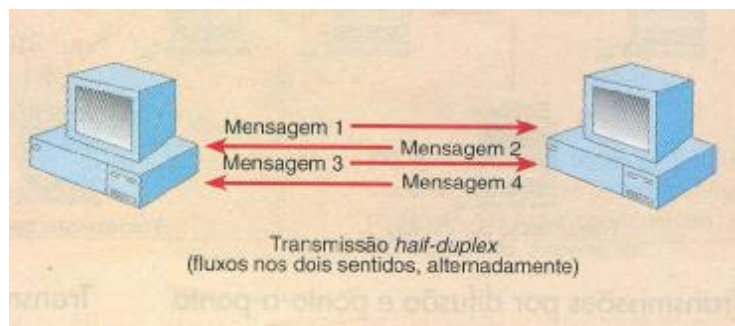
در این روش یک فرستنده و یک گیرنده ثابت وجود دارد و هیچ گاه جای این دو عوض نمی شود. در روش یک طرفه، اطلاعات به وسیله ی فرستنده ارسال و به وسیله ی گیرنده دریافت می شود. برای مثال می توان به رادیو یا تلویزیون اشاره کرد. در هر کدام از این سیستم ها، اطلاعات به وسیله ی یک فرستنده رادیویی یا تلویزیونی ارسال و به وسیله ی گیرنده که همان دستگاه رادیو یا تلویزیون است دریافت می شود و هیچگاه ارسال تغییر نمی کند. به این روش ارسال، یک طرفه می گویند.



شکل 2-1

2-3-2- ارتباط دو طرفه غیر هم زمان

در روش دوطرفه غیر هم زمان ارسال دوطرفه ولی غیر هم زمان است یعنی دو واحد A و B نمی توانند هم زمان برای یکدیگر اطلاعات ارسال کنند و این کار باید متناوب انجام شود. در واقع هنگامی که واحد A ارسال اطلاعات است، واحد B فقط باید دریافت کننده باشد و برعکس. برای مثال می توان به واکی - تاکی یا فرستنده - گیرنده های بی سیم اشاره کرد.



شکل 2-2

<sup>4</sup> - Simplex

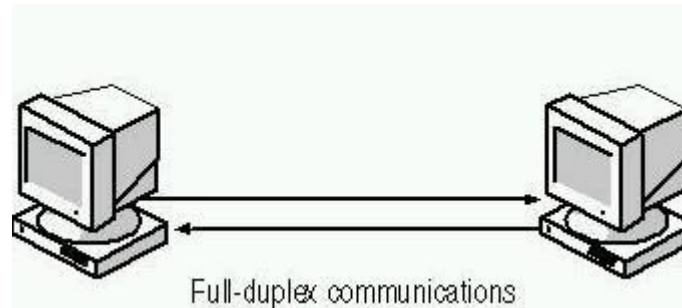
<sup>5</sup> - Half-Duplex

<sup>6</sup> - Full-Duplex



### 3-2-3- ارتباط دو طرفه هم زمان

در روش دوطرفه هم زمان هر دو واحد A و B می توانند به صورت هم زمان فرستنده و گیرنده اطلاعات باشند. به طور مثال می توان از طریق دو دستگاه تلفن بدون هیچ مشکلی به صورت هم زمان و دو طرفه ارتباط برقرار کرد. انتقال اطلاعات در تلفن، نمونه ای از انتقال اطلاعات به صورت دو طرفه هم زمان است.

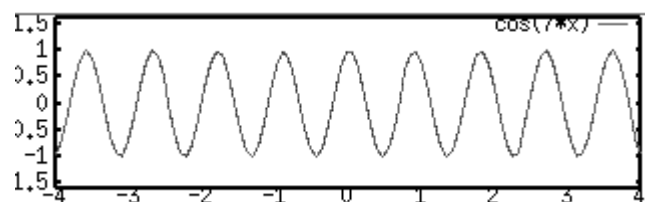


شکل 3-2

### 4-2-2- سیگنال های اطلاعات

مفهومی را که به انتقال اطلاعات از نقطه ای به نقطه دیگر و هم چنین یک سری از پالس ها در کامپیوتر اشاره می کند، سیگنال می نامند. امواج رادیویی و ویدیویی نمونه ای از این سیگنال ها هستند.

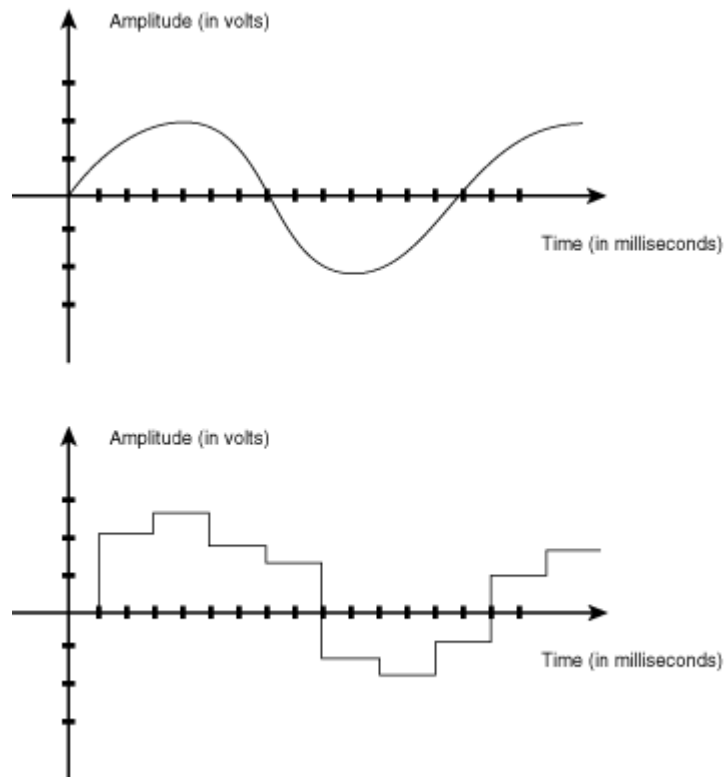
سیگنال های اطلاعات می توانند به دو صورت دیجیتال یا آنالوگ باشند. سیگنال های آنالوگ شبیه یک موج هستند که در زمان های مختلف مقادیر مختلفی دارند یعنی از زمان شروع موج به جلو، در هر لحظه این موج مقدار متفاوتی با لحظه قبلی دارد. این موج را معمولا روی بردار نمایش می دهند. محور عمودی نمایانگر مقدار عددی موج و محور افقی نمایانگر زمان است.



شکل 4-2

صدای شخصی که در حال صحبت کردن است، نمونه ای از یک سیگنال آنالوگ می باشد؛ به این صورت که صدا به صورت ممتد تولید شده و بلندی صدا دائما در حال تغییر است.

در مقابل ، سیگنال دیجیتال فقط دو حالت دارد بدین مفهوم که ارزش عددی سیگنال دیجیتال صفر یا یک است ؛ یعنی در واحدهای زمانی مختلف فقط دو ارزش عددی متفاوت داریم . اگر بخواهیم مثالی برای یک سیگنال دیجیتال بیاوریم ، می توانیم به یک لامپ اشاره کنیم که فقط دو وضعیت خاموش یا روشن دارد . این موج را روی بردار به صورتی که در شکل 2-5 نمایش داده شده است ، می بینید .



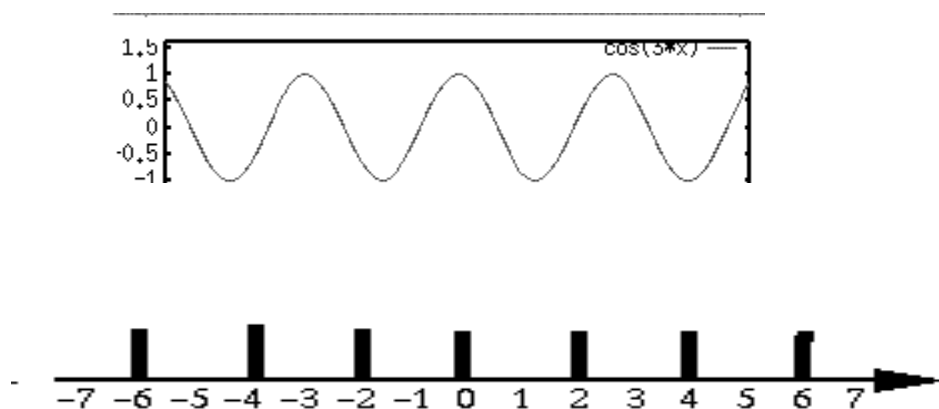
شکل 2-5

#### - سیگنال های Periodic و Aperiodic

هر دو نوع سیگنال های آنالوگ و دیجیتال به دو فرم Periodic و Aperiodic به کار می روند .

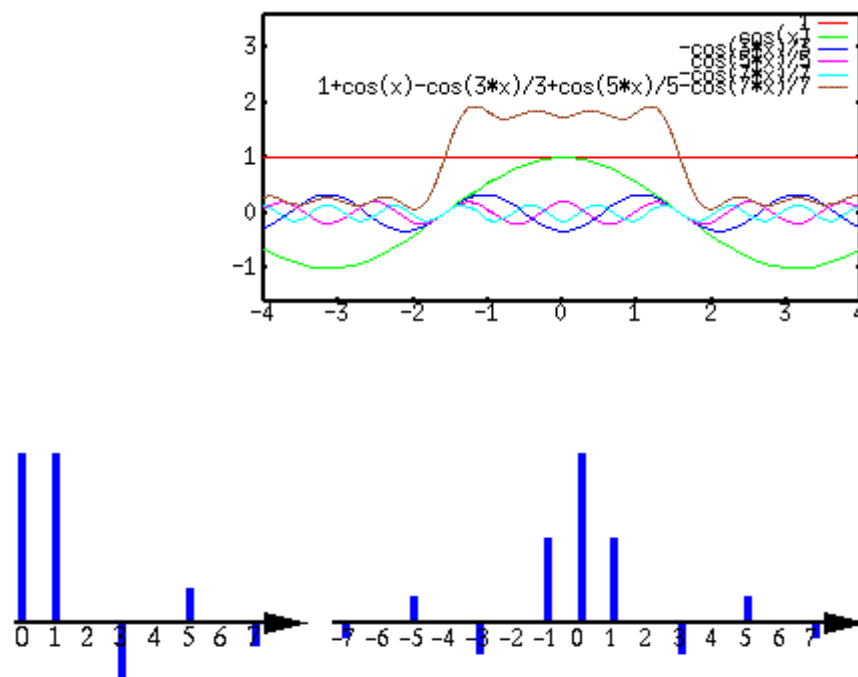
##### الف - سیگنال های Periodic

اگر الگو یا همان شکل سیگنال ها در فاصله های زمانی مشخص تکرار شود ، به آن سیگنال Periodic می گویند . در سیگنال های اگر الگو کامل شود و در آستانه تکرار قرار گیرد ، به آن یک Cycle یا چرخه می گویند یک Period یا دوره ، به مقدار زمانی می گویند که یک چرخه یا Cycle در آن اتفاق می افتد .



شکل 2-6

ب- سیگنال های Aperiodic  
سیگنال های Aperiodic الگو و شکل مشخصی ندارند و الگوهای آن در فاصله های زمانی غیر قابل پیش بینی تکرار می شوند .



شکل 2-7

## 5-2- پهنای باند<sup>7</sup>

یکی از مسائلی که به هنگام طراحی و راه اندازی شبکه همواره مورد توجه قرار می گیرد و از درجه اهمیت بالایی برخوردار است ، پهنای باند می باشد . پهنای باند به طور کلی تعریفی است که برای سیستم های انتقال آنالوگ استفاده می شود . هر سیستم انتقال آنالوگ توانایی محدودی در انتقال امواج دارد ؛ بدین صورت که پایین ترین و بالاترین فرکانسی که یک رسانه برای انتقال اطلاعات استفاده می کند ، مشخص است ؛ به طور مثال پایین ترین فرکانس 300HZ و بالاترین فرکانس 3300 HZ است .

واحد سنجش فرکانس هرتز<sup>8</sup> می باشد . حداقل این دو فرکانس یعنی فاصله بین پایین ترین و بالاترین عدد ، پهنای باند رسانه نامیده می شود . رسانه ای با مشخصات ذکر شده فقط قادر به ارسال سیگنال هایی است که در محدوده بین 300 و 3300 هرتز قرار گرفته باشند . در واقع پهنای باند ، ظرفیت انتقال اطلاعات به وسیله ی رسانه است . در سیستم های انتقال دیجیتال ، ظرفیت انتقال اطلاعات با واحد بیت در ثانیه<sup>9</sup> سنجیده می شود . برای مثال می توان به پهنای باند یک مودم اشاره نمود . منظور از مودم 56Kbps این است که پهنای آن 56000 بیت در ثانیه می باشد .

از عوامل موثر در پهنای باند طول ، قطر و جنس کابل است . طول کابل با پهنای باند نسبت معکوس و قطر کابل با پهنای باند نسبت مستقیم دارد یعنی هرچه طول کابل بیشتر شود ، پهنای باند کمتر شده و هرچه قطر کابل بیشتر شود ، پهنای باند نیز بیشتر می شود . برای انتقال اطلاعات به دوروش از پهنای باند استفاده می شود . این دو روش عبارتند از :

تک باند<sup>10</sup>

باند پهن<sup>11</sup>

در روش تک باند از تمام پهنای باند برای ارسال یا دریافت اطلاعات استفاده می شود ؛ به این معنی که تک باند در هر لحظه فقط می تواند یک سیگنال را از خود عبور دهد ، در نتیجه ارسال نوبتی می شود و اطلاعات پشت سرهم و به صورت سری ارسال می شوند . به این نوع شبکه تک باند گفته می شود . روش انتقال تک باند دلیل به وجود آمدن مفهوم packet است . از این روش در شبکه های محلی استفاده می شود .

در روش تک باند برای ارسال و دریافت اطلاعات به دورشته کابل نیاز است که یکی از کابل ها وظیفه ارسال اطلاعات را به عهده دارد و کابل دیگر دریافت اطلاعات را انجام می دهد . سیستم انتقال دیجیتال نیز از روش تک باند استفاده می کند .

<sup>7</sup>-Band Width

<sup>8</sup> - Hz

<sup>9</sup> - Bps

<sup>10</sup> - Base band

<sup>11</sup> - Broad band

روش دیگر انتقال ، انتقال باند پهن است. در سیستم انتقال باند پهن ، اطلاعات به صورت آنالوگ ارسال می شوند. به این ترتیب باند پهن می تواند از یک کابل ، یک یا چند سیگنال را به طور هم زمان عبور دهد. هر سیگنال به صورت جداگانه ارسال می شود و تداخلی بین سیگنال های متفاوت به وجود نمی آید. از این روش در شبکه تلویزیون کابلی استفاده می شود. در شبکه های محلی این روش کاربردی ندارد ولی در شبکه های WAN همواره مورد توجه است.



شکل 8-2

## 2-6- نویز:

ازجمله مشکلاتی که در شبکه به وجود می آید ، نویز است. نویز عامل مخربی است که شکل سیگنال ها را تغییر می دهد و باعث بروز اختلال می شود. عوامل مختلفی باعث به وجود آمدن نویز می شوند. تعدادی از این عوامل عبارتند از: حرارت ، القا و هم شنوایی. حرارت: نویزهایی که در اثر حرارت ایجاد می شوند ، بدین گونه عمل می کنند که حرارت باعث می شود الکترون ها در جهات نامشخص شروع به حرکت نمایند؛ این حرکت گاهی با سیگنال ها هم جهت شده و اندازه و شکل آن ها را که همان الگوی سیگنال هاست ، تغییر می دهد.

القا: نویزهای القایی نویزهایی هستند که موتورهای مکانیکی مثل موتور ماشین یا وسایل الکتریکی مانند موتورهای الکتریکی وسایل خانگی تولید می کنند ، این وسایل شبیه یک آنتن

فرستنده عمل می کنند و می توانند نویز را ارسال کنند و کابل شبکه ، شبیه یک آنتن گیرنده نویزهای ارسال شده را دریافت می کند.

هم شنوایی<sup>12</sup> : هم شنوایی اثر میدان های مغناطیسی یک کابل مجاور خود است . نویزهایی که کابل های برق فشار قوی یا رعد و برق ایجاد می کنند نیز از انواع نویزهای القایی محسوب می شوند.

سرعت انتقال اطلاعات : به مقدار اطلاعاتی که در واحد زمان به وسیله ی تجهیزات شبکه ارسال می شود ، سرعت انتقال اطلاعات می گویند و واحد اندازه گیری آن bps است . سرعت انتقال اطلاعات در وسایل مختلف متفاوت است .

به طور مثال کارت های شبکه با سرعت 10Mbps توانایی انتقال 10 مگابیت در ثانیه را دارند و کارت های 100Mbps می توانند در ثانیه 100 مگابیت اطلاعات به مقصد ارسال کنند . سرعت انتقال اطلاعات با پهنای باند ارتباط مستقیم دارد ، هر چه پهنای باند بیشتر شود سرعت انتقال اطلاعات نیز بیشتر می شود .

نکته : پهنای باند ، ظرفیت انتقال یک رسانه یا کابل است . در صورتی که سرعت انتقال ، سرعت ارسال اطلاعات در واحد زمان است .

### خود آزمایی و تحقیق

سرعت ارسال اطلاعات در کدام یک از روش های سری و موازی بیشتر است؟

در کدام یک روش های ارسال سریال هم زمان و غیر هم زمان کنترل ترافیک امکان پذیر است؟

سیگنال چیست؟

تفاوت سیگنال دیجیتال و آنالوگ را بنویسید و با ذکر دلیل مشخص کنید کیفیت و سرعت کدام یک برای ارسال اطلاعات بهتر است؟

نویز چیست؟ اثر نویز بر روی کدام یک از سیگنال های آنالوگ یا دیجیتال بیشتر است؟

تحقیق کنید که گذرگاه های COM، LPT و USB از چه سیستمی برای انتقال اطلاعات استفاده می کنند؟

تحقیق کنید که واحدهای Bps و bps چه تفاوتی با هم دارند؟

<sup>۱۲</sup> - crosstalk

## فصل سوم- پیکر بندی شبکه و محیط انتقال

هدف های رفتاری - هنر جو پس از پایان این فصل باید بتواند :

انواع توپولوژی شبکه را شرح دهد.

انواع محیط های انتقال را شناسایی کند.

انواع کابل های مورد استفاده در شبکه را نام ببرد.

اتصالات مورد نیاز برای کابل کشی شبکه را نام ببرد

کابل کشی یک شبکه را انجام دهد.

کارت شبکه و وظایف آن را تعریف کند.

کابل رابط بین شبکه و سویچ را ایجاد کند .

روش های دسترسی به خط انتقال را شناسایی کند.

### 1-3- توپولوژی انواع آن

اجزای سخت افزاری در شبکه طبق یک طرح و نقشه بهم متصل می شوند که به آن اصطلاحاً توپولوژی شبکه می گویند . در ابتدا ممکن است تصور کنیم که توپولوژی فقط به معنی نقشه فیزیکی و ظاهری شبکه است و چگونگی گردش اطلاعات و همچنین نحوه دسترسی کامپیوترها به محیط انتقال در آن اهمیتی ندارد اما این حالت کافی نبوده و در توصیف و بررسی یک توپولوژی باید علاوه بر چگونگی اتصال ظاهری ، نحوه تبادل اطلاعات را هم جزو توپولوژی به حساب آورد بنابراین توپولوژی را به شکل زیر تعریف می کنیم

تعریف توپولوژی :

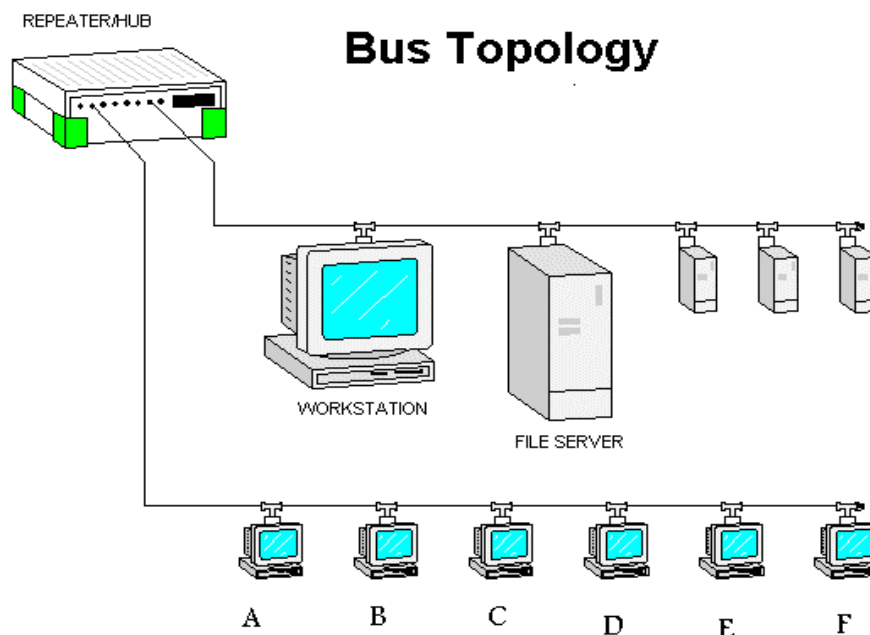
چگونگی اتصال ظاهری اجزا از طریق محیط انتقال به یکدیگر .

نحوه دسترسی اجزا به محیط انتقال و گردش اطلاعات مابین آنها .

با این حال در ادامه بحث و شرح بیشتر ، گاهی اوقات به یکی از جنبه ها توجه بیشتری می کنیم . (ضمناً برای ساده تر شدن بحث ، فرض کنید که محیط انتقال از نوع "سیم" است (کابل) و فعلاً محیطهای انتقال بی سیم را منظور نمی کنیم).

### 1-1-3- توپولوژی خطی (Bus) :

جنبه ظاهری : کلیه سیستمها از طریق یک قطعه کابل به یکدیگر متصل شده و اطلاعات خود را از طریق آن تبادل می کنند . نکته اصلی در توپولوژی خطی آنست که یک قطعه کابل بین کلیه کامپیوترها مشترک بوده و همه از طریق همان یک قطعه با هم ارتباط دارند .



شکل 3-1

چگونگی دسترسی کامپیوترها به خط و نحوه گردش اطلاعات : هر سیستمی که بخواهد اطلاعاتی را روی خط ارسال کند (مثلاً کامپیوتر A) ابتدا باید ببیند خط آزاد است یا خیر و اگر پاسخ مثبت بود اقدام به ارسال اطلاعات برای کامپیوتر(های) مقصد می کند. (این موضوع بعداً مورد بحث بیشتری قرار می گیرد)

اگر کامپیوتر A بخواهد اطلاعاتی را برای B ارسال کند بقیه کامپیوترها (C,D) هم از این اطلاعات باخبر می شوند چون محیط انتقال مشترک بوده و کنترلی روی آن وجود ندارد. به محض آنکه سیگنال ارسال شده از A روی خط قرار بگیرد، سرعت در تمامی محیط انتقال منتشر شده و همه آنرا دریافت می کنند اما بدیهی است که فقط گیرنده (گیرندگان) تعیین شده از طرف فرستنده آنرا مورد استفاده قرار می دهد و بقیه گیرندگان به آن دسترسی ندارند. فرض کنید در یک جمع نشسته اید، چه با یک نفر صحبت کنید چه با همه، نتیجه آنست که همه صحبت های شما را می شنوند اما بدیهی است فقط فرد یا افرادی که مخاطب شما هستند از آن استفاده برده و بقیه به امور شخصی خود می پردازند. در اینجا هم علت مشابه است یعنی محیط انتقال یا عبارتی "هوا" برای همه افراد جمع مشترک بوده و سیگنال فرستنده یعنی صحبت های گوینده به محض خروج از دهان او در تمام فضای اطراف جمع (تا فاصله ای محدود و بسته به



قدرت فرستنده) منتشر شده و همه آنرا می‌شنوند. ولی فقط کسی که مورد پرسش قرار دارد باید پاسخ بگوید .

برخورد یا Collision :

فرض کنیم A در حال ارسال اطلاعات برای B باشد ، همزمان C هم میخواهد اطلاعاتی را برای D بفرستد در این حالت، چون فقط یک محیط انتقال وجود دارد که آنهم بین همه مشترک است . به محض آنکه A اطلاعات خود را روی خط بفرستد ، خط اشغال شده و بقیه باید صبر کنند تا ارسال A به اتمام رسیده و خط مجدداً آزاد شود. البته اگر کامپیوتر A کارش طولانی باشد باید کار خود را به صورت مقطعی انجام دهد بدین معنی که پس از ارسال قسمتی از اطلاعات، خط را آزاد می‌کند تا بقیه هم امکان دسترسی و استفاده از خط را داشته باشند. در صورتی که به طور همزمان C نیز بخواهد برای D اطلاعاتی را ارسال نماید باعث "تصادم اطلاعاتی" یا Collision شده و سیگنالها بهم می‌ریزد . بنابر این در یک لحظه مشخص فقط یک فرستنده می‌تواند وجود داشته باشد .

البته خیلی از کاربران در شبکه‌هایی با توپولوژی خطی تجربه انتقال همزمان اطلاعات را مابین سیستمهای مختلف داشته‌اند مثلاً در حالی که یک فایل بزرگ 1 GByte از کامپیوتر A به B انتقال می‌یابد ، همزمان C و D هم با یکدیگر مشغول تبادل هستند . موضوع چیست ؟ آیا تناقضی با مثال فوق ندارد ؟ باید گفت : که در این حالت کار بصورت مقطعی انجام می‌شود . قبلاً در مبحث "ویژگی سیستم عامل ها" نیز اشاره شد به "اشتراک زمان" یا "تقسیم زمان" . با استفاده از این تکنیک ، هر فرستنده کسری از زمان را (یا حجم محدودی از اطلاعات را) برای ارسال در نظر گرفته که پس از به پایان رسیدن مجبور است خط را آزاد کرده تا دیگران نیز شانس ارسال را داشته باشند . در این تکنیک هرچند که بطور واقعی و در یک لحظه مشخص چندین فرستنده با هم وجود ندارند اما در مجموع همه می‌توانند ارسال اطلاعات خود را با هم به پیش ببرند .

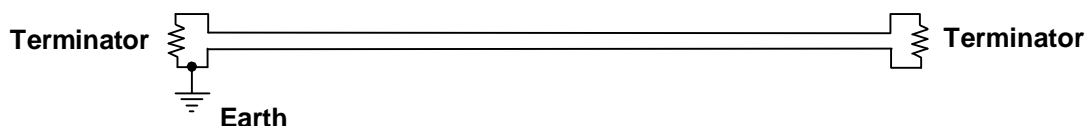
در تکنیک TDM در یک لحظه مشخص ، باز هم بطور واقعی فقط یک فرستنده محیط انتقال را در اختیار می‌گیرد ، در عمل با مثالهایی روبرو می‌شویم که در آن واحد بطور همزمان و بطور کاملاً واقعی همه فرستنده‌ها با هم روی یک محیط انتقال مشترک کار می‌کنند . فضای مادی را بعنوان یک محیط انتقال مشترک در نظر بگیرید . می‌دانیم که در یک لحظه صداها فرستنده تلوزیونی ، رادیویی ، مخابراتی و ... امواج خود را در همین فضا پخش می‌کنند و بعبارتی اطراف ما پر از امواج فرستنده‌های گوناگون است و با یکدیگر تداخلی هم ندارند ، موضوع چیست ؟ توجیه این واقعه استفاده از فرکانسهای مختلف برای ارسال داده ها می‌باشد بعبارتی هیچ 2 فرستنده‌ای (در یک محدوده معین) نباید دارای فرکانس یکسان باشند . به این تکنیک اصطلاحاً "تقسیم فرکانسی" یا Frequency Division Multiplexing = FDM گفته می‌شود .

نتیجه گیری : در محیطهای انتقال مشترک ، هیچ 2 فرستنده ای نمی توانند همزمان با هم اقدام به ارسال اطلاعات کنند مگر آنکه از تکنیکهای TDM یا FDM استفاده شود .

اثر قطع شدن کابل اصلی در توپولوژی خطی :

اگر در توپولوژی خطی، قسمتی از کابل اصلی قطع شود تمامی شبکه از کار می افتد بعنوان مثال حد فاصل بین B و C قطع می شود اما ارتباط دو به دو مابین (A,B) و همچنین (C,D) برقرار است ، چرا می گوئیم کل شبکه از کار می افتد ؟ علت آن است که در شبکه های کامپیوتری از جریانهای متناوب (Alternative Current = AC) برای ارسال اطلاعات استفاده می شود، همچون امواج دریا . می دانیم که اگر امواج دریا پس از رسیدن به ساحل با یک مانع همچون تخته سنگ برخورد کنند شدت برگشه و موج رفت و برگشت با یکدیگر تصادم می کنند (Collision) و این تداخل باعث بهم ریختن شکل موج می شود، اما اگر مانعی که در ساحل وجود دارد یک ساحل شنی نرم (یا در ذهن خود تصور کنید یک ابر اسفنجی بزرگ) باشد ، موج به آرامی جذب ساحل شده و "موج برگشت" آنچنان شدتی برای بهم ریختن "موج رفت" ندارد . در شبکه های کامپیوتری نیز اوضاع به همین مفهوم است ، چنانچه یک قطعی در کابل رخ دهد ، این قطعی مصادف با روبرو شدن موج با "هوا" است و می دانیم که "هوا" عایق الکتریسیته بوده و برای آن حکم تخته سنگ را دارد بنابراین موج در "نقطه قطع شده" برگشت کرده و با "موج رفت" تصادم می کند (Collision) و این برخورد باعث بهم ریختن شکل موج شده و در نتیجه تمامی قسمت را تحت تأثیر قرار می دهد .

نتیجه گیری که از این مبحث می شود آن است که در توپولوژی خطی باید به گونه ای عمل کرد که در هیچ قسمتی از کابل Collision اتفاق نیافتد و این شامل ابتدا و انتهای خط نیز می شود . در طرفین خط باید ترتیبی اتخاذ کرد تا امواج پس از رسیدن به آنجا اصطلاحاً جذب شده و تداخل درست نکنند و این امر با قرار دادن مقاومتی (Resistor) در ابتدا و انتهای خط که اصطلاحاً به آنها Terminator گفته می شود میسر می شود . مقدار این مقاومتها بستگی به مشخصات الکتریکی کابل و پارامترهای دیگر داشته و مثلاً در نوع خاصی از شبکه ها 50 W است.



شکل 2-3

مزایا و معایب توپولوژی خطی :

مزایا :

افزایش و کاهش سیستمها براحتی (تا حد مجاز) صورت می گیرد .

در کل ساده و کم هزینه است .

معایب :

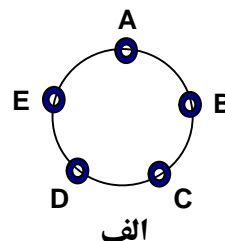
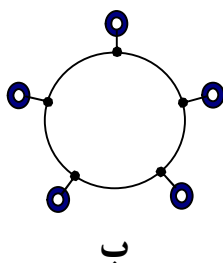
در صورت قطعی در یک قسمت از کابل اصلی ، تمامی شبکه از کار می افتد ،

عیب یابی آن وقت گیر است

نیاز به نگهداری و مراقبت بیشتری نسبت به سایر توپولوژیهای دیگر دارد .

3-1-2- توپولوژی حلقوی (Ring) :

جنبه ظاهری : کلیه کامپیوترها در یک حلقه به یکدیگر متصل می شوند . بدیهی است وقتی می گوئیم حلقه ، منظور آنست که آخرین کامپیوتر هم باید به اولین متصل شود .



شکل 3-3

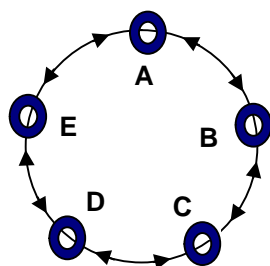
در شکل 3-3-قسمت ب را نمی توان حلقوی به حساب آورد زیرا اگر به شکل دقت کنید این شبکه هیچ فرقی با شبکه خطی ندارد بجز آنکه سر و ته خط به یکدیگر وصل شده است و در واقع هیچ مزیتی نسبت به خطی ندارد .

تفاوت توپولوژی خطی با توپولوژی حلقوی : در توپولوژی حلقوی هر سیستم ، دو گذرگاه (Port) اما در توپولوژی خطی فقط یک گذرگاه برای عبور اطلاعات دارد .

چگونگی دسترسی کامپیوترها به خط و نحوه گردش اطلاعات : از نظر نحوه گردش اطلاعات ، دو نوع توپولوژی حلقوی را می توان متصور شد :

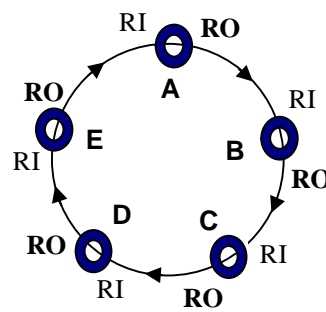
الف) توپولوژی حلقوی یکطرفه : اطلاعات فقط در یک جهت گردش می کند .

ب) توپولوژی حلقوی دوطرفه : اطلاعات در هر دو جهت می تواند گردش کند .



توپولوژی حلقوی  
دوطرفه

RI = Ring In  
RO = Ring Out



توپولوژی حلقوی  
یکطرفه

شکل 3-4

بزودی خواهیم دید که حلقوی دوطرفه در واقع حالت خاصی از توپولوژی Mesh است، لذا در سایر متون وقتی صحبت از حلقوی می‌شود عموماً منظور حلقوی یکطرفه است مگر صراحتاً خلاف آن ذکر شود.

مزایا و معایب حلقوی (یکطرفه) نسبت به خطی :

مزیت : در بخش "روشهای دسترسی به محیط انتقال" خواهیم دید که نحوه گردش اطلاعات در حلقوی نسبت به خطی دارای مزایایی از قبیل اولویت‌بندی و زمان‌بندی است که خطی از آن محروم است.

معایب :

مصرف کابل در آن نسبت به توپولوژی خطی بیشتر است !

همچون توپولوژی خطی اگر یک قسمت از حلقه قطع شود، کل حلقوی از کار می‌افتد البته نه بدلیل Collision، بلکه بدین سبب که اطلاعات قادر به گردش کامل نخواهد بود.

در واقع قانون گردش اطلاعات در حلقه‌های یکطرفه بگونه‌ای طراحی شده که اولاً هر اطلاعاتی که از یک سیستم خارج می‌شود باید دور زده و سر جای اول خود برگردد، ثانیاً همه سیستمها باید قادر به تبادل اطلاعات باشند. بعنوان مثال در شکل حلقوی یکطرفه دقت کنید، اگر حد فاصل بین A و B قطع شود در آن صورت هر چند ممکن است تصور شود که B می‌تواند برای C، D، E و A اطلاعات بفرستد، اما عکس آن امکان‌پذیر نیست و این بمعنای آنست که همه سیستمها نمی‌توانند به تبادل اطلاعات بپردازند، در نتیجه هر دو قانون فوق نقض شده و حلقه بطور کامل غیر قابل استفاده می‌شود.

نکته : مشکل فوق در حلقه‌های دوطرفه (که حالت خاصی از Mesh محسوب می‌شوند) وجود ندارد .

پرسش : چرا در توپولوژی حلقوی (اعم از یکطرفه یا دوطرفه) ، از Collision بعنوان عاملی بازدارنده یاد نمی‌شود ؟

### 3-1-3- توپولوژی ستاره‌ای (Star) :

جنبه ظاهری : کلیه کامپیوترها به یک نقطه مرکزی بنام Hub متصل می‌شوند.  
نکته : واژه Hub بطور کلی یعنی "نقطه مرکزی" و نحوه عملکرد این "نقطه مرکزی" و همچنین نام دقیق آن بستگی به نوع شبکه‌ای دارد که در آن استفاده می‌شود. در این بخش هرگاه صحبت از Hub می‌شود منظور استفاده از آن در نوع خاص و رایجی از شبکه‌ها بنام شبکه عول بعدی است.



شکل 3-4

چگونگی دسترسی کامپیوترها به محیط انتقال و گردش اطلاعات بسته به نوع Hub ، نحوه گردش اطلاعات به دو حالت متفاوت انجام می‌شود :  
به محض آنکه یک سیستم اطلاعاتی را ارسال کند ، Hub اشغال شده و سیستمهای دیگر نمی‌توانند بطور همزمان فرستنده اطلاعات باشند (همانند گردش اطلاعات در توپولوژی خطی) .  
دقت کنید که Hub ، خود بعنوان بخشی از محیط انتقال و توپولوژی بشمار می‌رود .  
چنانچه یک سیستم اطلاعاتی را برای یک مقصد مشخص بفرستد ، بقیه مسیرها برای عبور همزمان دیگر سیستمها باز هستند و اگر اطلاعاتی را برای همه بفرستد بدیهی است که همه خروجیها اشغال می‌شوند. به این نوع هاب مخصوص اصطلاحاً Switch Hub ، Hub Switch یا به اختصار Switch گفته می‌شود. امروزه عمدتاً در شبکه‌های کامپیوتری با توپولوژی ستاره‌ای بجای هاب

معمولی از سویچ استفاده می‌شود که از ویژگی های آن عملکرد هوشمندانه در پیدا کردن مقصد نسبت به Hub می باشد.

در یک شبکه ، اگر ارسال اطلاعات فقط به سمت یک مقصد مشخص باشد اصطلاحاً واژه Unicast و اگر ارسال اطلاعات برای چند سیستم مشخص باشد واژه Multicast و اگر همگان مورد خطاب قرار گیرند واژه Broadcast بکار می‌رود.

اگر مسیر ارتباطی بین هاب و یک کامپیوتر قطع شود ، Collision حاصله در این قسمت باعث تأثیر گذاری در کل شبکه نمی‌شود معمولاً طراحی اکثر هابهایی که امروزه ساخته می‌شود بگونه ایست که اصطلاحاً "اجازه عبور Collision" را به خطوط دیگر نمی‌دهد.

در توپولوژی ستاره‌ای که از یک هاب معمولی در آن استفاده می‌شود ، اگر A اطلاعاتی را به مقصد B بفرستد ، دیگر سیستمها نیز از آن آگاهی می‌یابند زیرا همانطور که گفته شد، چگونگی گردش اطلاعات اگر هاب معمولی باشد مانند توپولوژی خطی است. در حالی که در سویچ ، فقط گیرنده مربوطه اطلاعات را دریافت می‌کند ، مگر آنکه گیرنده اصطلاحاً "همگان" باشند یا در واژه‌های کامپیوتری مقصد "Broadcast" باشد.

مزایا و معایب توپولوژی ستاره ای نسبت به توپولوژی خطی :

قطع شدن یک خط بطور معمول بقیه شبکه را تحت تأثیر قرار نمی‌دهد.

اگر از Switch استفاده شود امکان تبادل اطلاعات دودو بصورت همزمان وجود دارد ، در نتیجه حجم ترافیک بیشتری در واحد زمان می‌تواند انجام شود.

اگر از Switch استفاده شود چون ترافیک مقصد به یک ایستگاه روی گذرگاههای (Ports) دیگر ارسال نمی‌شود لذا ترافیک ناخواسته کاهش یافته و ضریب ایمنی در تبادل اطلاعات افزایش می‌یابد.

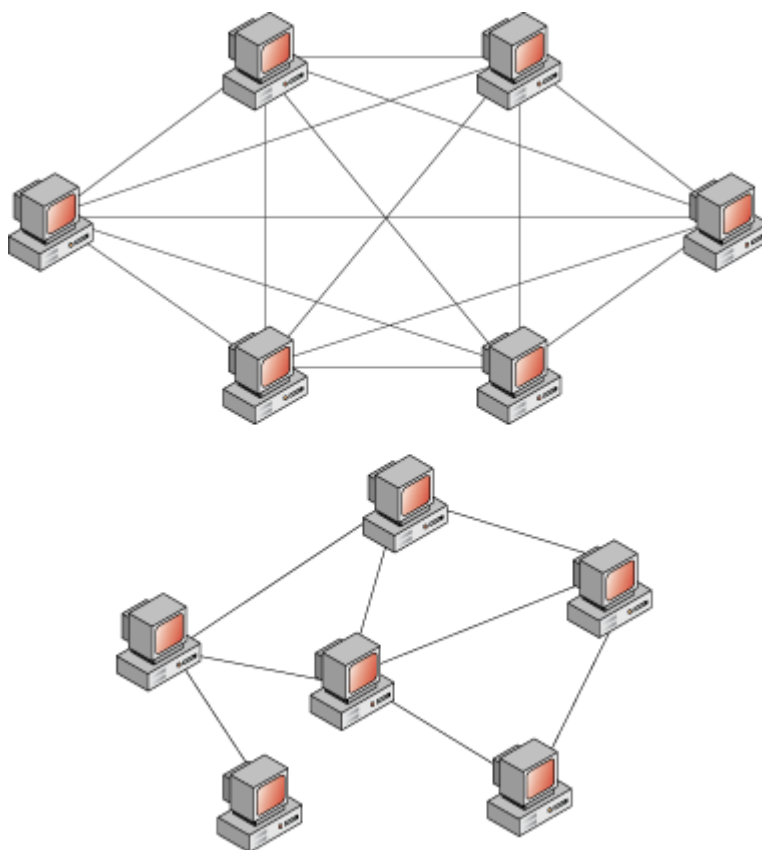
معایب :

اگر به هر دلیلی "نقطه مرکزی" از کار بیافتد ، کل شبکه از کار باز می‌ایستد ، به همین 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. در شبکه‌هایی که ضریب حساسیت آنها بیشتر است ، ترکیبی از دو یا چند سویچ را در توپولوژی Mesh قرار داده و بدین ترتیب اگر یکی از سویچها از کار بیافتد ، سویچهای دیگر بلافاصله وارد عمل شده و ترافیک از طریق آنها به عبور خود ادامه می‌دهد. (Fault Tolerance)

مصرف کابل و بطور کلی هزینه پیاده‌سازی آن نسبت به خطی بیشتر است . البته در عوض هزینه نگهداری و رفع عیب (Maintenance & Trouble Shooting) پایین تر است زیرا کمتر دچار مشکل شده و عیب یابی در آن ساده تر و سریعتر انجام می‌شود.

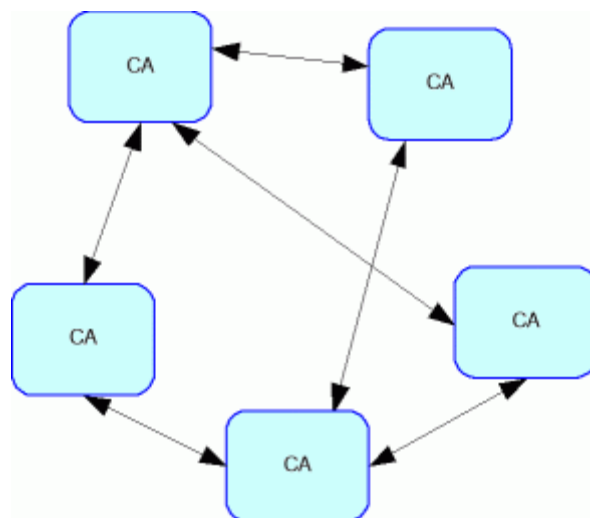
#### 3-1-4- توپولوژی مش (Mesh) :

جنبه ظاهری : در هر سیستم به تعداد لازم ، سخت افزار شبکه (Network Interface) نصب شده و همگی مستقیماً بصورت 2 به 2 به یکدیگر متصل می شوند. البته این حالت ایده آل بوده که اصطلاحاً گراف کامل (Complete Mesh) خوانده می شود.



شکل 3-5

در عمل ممکن است ارتباط 2 به 2 برای همه امکان پذیر نباشد لذا توپولوژی به حالت یک گراف ناقص درمی آید (Partial Mesh)



شکل 3-6

2. چگونگی دسترسی کامپیوترها به محیط انتقال و گردش اطلاعات : چون هر سیستم ارتباط دوطرفه‌ای با بقیه داشته و از طرفی بیش از یک مسیر برای رسیدن به مقصد وجود دارد لذا پس از انتخاب مسیر بهینه ، اطلاعات به مقصد می‌رسد. در توپولوژی مش بحث جدیدی بنام مسیریابی Routing مطرح می‌شود و به هر سیستمی که کار مسیریابی را انجام دهد اصطلاحاً مسیریاب "Router" گفته می‌شود.

مسیریاب (Router): مسیریاب یا روتر به سخت‌افزاری گفته می‌شود مجهز به حداقل 2 کارت شبکه (Network Interface) که نرم‌افزار مسیریابی (Routing) روی آن فعال شده و کار انتخاب مسیر بهینه و هدایت ترافیک را روی اطلاعات انجام می‌دهد. چون روتر محل عبور و تلاقی مسیرهای مختلف برای تبادل ترافیک است لذا علاوه بر "پلیس راهنمایی و رانندگی"، در برخی از روترها "پلیس ایست-بازرسی" نیز وجود داشته ، نوع و محتوای ترافیک را کنترل می‌کند. بعبارت فنی عملیات Filtering و Firewall را هم انجام می‌دهند.

مثال 1 : یک کامپیوتر شخصی شامل یک کارت شبکه و مودم به همراه نرم‌افزار مسیریابی را می‌توان یک روتر نامید.

مثال 2 : یک کامپیوتر شخصی مجهز به چندین کارت شبکه یا مودم به همراه نرم‌افزار مسیریابی را می‌توان یک روتر نامید.

مثال 3 : سخت‌افزارهای خاصی وجود دارند به‌مراه نرم‌افزار مربوطه که فقط بعنوان روتر استفاده می‌شوند مانند روترهای ساخت کمپانی Cisco .



مزایا و معایب توپولوژی Mesh نسبت به سایر توپولوژیها :

مزیت: چون بیش از یک مسیر برای هدایت ترافیک وجود دارد بنابراین به احتمال زیاد ، قطعی در یک مسیر باعث اختلال کلی در ارتباط نمی‌شود و بالاخره شانس برای رسیدن به مقصد وجود دارد ضمن آنکه بعضی از روترها در حالت عادی ترافیک را روی چندین مسیر تقسیم می‌کنند و بنابراین حجم تبادلات نیز افزایش می‌یابد. خلاصه آنکه توپولوژی مش دارای ویژگی Redundancy یا Fault Tolerance و همچنین Load Balancing است

معایب Mesh نسبت به سایر توپولوژیها : بدیهی است که پیچیده‌تر و پرهزینه‌تر از بقیه است. اصولاً انتخاب توپولوژی ربطی به ابعاد و گستردگی فیزیکی شبکه (LAN-WAN) ندارد اما بدیهی است که هر نوع توپولوژی را می‌توان چه در LAN و چه در WAN استفاده کرد اما با توجه به اینکه احتمال تأثیرگذاری عوامل بازدارنده در شبکه‌های WAN نسبت به LAN بیشتر است لذا معمولاً در شبکه‌های WAN از توپولوژی Mesh استفاده شده و خطی ، ستاره ای ، حلقوی را در LAN بکار می‌برند. البته ستاره ای در WAN هم کاربرد دارد.

شبکه حلقوی دوطرفه (Bi-Directional) را می‌توان حالت خاصی از Mesh به حساب آورد زیرا چنانچه اقطار یک مش کامل را حذف کنیم شکل حاصله یک مش ناقص خواهد شد که همان شبکه حلقوی دوطرفه است. رینگهای دوطرفه در شبکه‌های صنعتی که معمولاً Campus LAN هستند بکار می‌رود. در اینگونه شبکه‌ها توپولوژی ستاره‌ای به تنهایی پاسخگوی سرعت و پایداری نبوده لذا مش وارد عمل می‌شود. از طرفی چون "مش کامل" بسیار پیچیده و پرهزینه است بنابراین از مش‌های ناقص برای پیاده‌سازی توپولوژی استفاده می‌شود و شبکه حلقوی دوطرفه یکی از بهترین انتخابها در این زمینه بشمار می‌رود.

## 3-2 محیط های انتقال

برای آنکه ایستگاه‌های مختلف در یک شبکه بتوانند با یکدیگر ارتباط برقرار کنند نیاز به یک "محیط انتقال" مانند یک قطعه سیم دارند..

تعریف: به هر رسانه‌ای که بتواند اطلاعات را به گردش درآورده و هدایت کند اصطلاحاً "محیط انتقال" می‌گوییم.

با ذکر چند مثال می‌خواهیم محیط انتقال را توضیح دهیم

- مثال 1: وقتی صحبت می‌کنیم، امواج صوتی از طریق هوا بین گوینده و شنونده انتقال می‌یابد در این مثال "هوا" به عنوان محیط انتقال محسوب می‌شود.
- مثال 2: یک فرستنده تلویزیونی، امواج الکترومغناطیسی را از طریق آنتن در فضای اطراف خود پخش می‌کند و این امواج با سرعتی تقریباً معادل با سرعت نور به اطراف انتقال پیدا می‌کنند لذا "فضای مادی" بعنوان محیط انتقال محسوب می‌شود.

مثال 3: اطلاعاتی را با روشن و خاموش کردن یک منبع تولید نور از طریق یک رشته کابل نوری که از ترکیبات فشرده مخصوص ساخته شده است و نور را از خود هدایت می کند ارسال می کنیم کابل نوری در اینجا به عنوان محیط انتقال محسوب می شود

مثال 4: وقتی بوسیله گوشی FF با فردی که کنار در ورودی ایستاده صحبت کنید صدای ما تبدیل به انرژی الکتریکی شده و به وسیله ی الکترونها از طریق سیم مسی جریان می یابد در اینصورت "سیم مسی" بعنوان محیط انتقال محسوب می شود.

### 1-2-3- گروه بندی محیطهای انتقال

محیط های انتقال را می توان به دو دسته کلی سیمی و بی سیم تقسیم کرد.

محیط انتقال سیمی (Wired)

یک یا چند رشته سیم از جنس فلزات هادی یا آلیاژهای آنها مانند مس، آلومینیوم، ... برای انتقال الکتریسته.

یک یا چند رشته سیم از جنس ترکیبات مخصوص مانند پلاستیک فشرده و سیلیس برای انتقال نور.

بی سیم (Wireless) (انتشار از طریق فضای مادی)

استفاده از نور مادون قرمز (Infra Red) مانند کنترل تلویزیون.

استفاده از نور لیزر (Laser) که در واقع تک فرکانس است.

استفاده از امواج رادیویی (Radio Waves) در فرکانسهای مختلف مانند رادیو، تلویزیون،

ماهواره، مخابرات میکروویو، بی سیمهای شخصی و نظامی و ....

نکته: هر چند بوسیله انتقال صوت (مثال 1) از طریق هوا هم می توان اطلاعات را رد و بدل کرد

اما این شیوه در شبکه های کامپیوتری بدلیل محدودیتهایی که دارد استفاده نمی شود

### 2-2-3- بررسی محیطهای انتقال "سیمی" یا "کابلی" (Wired)

در شبکه های کامپیوتری 3 نوع سیم (کابل) متداول بوده است:

الف) کابل "هم محور" یا Coaxial مانند کابل آنتن تلویزیون.

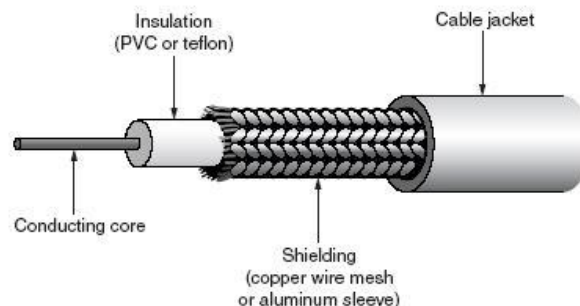
ب) کابل "زوج بهم تابیده" یا Twisted Pair مانند سیم تلفن.

ج) کابل "فیبر نوری" یا Fiber Optic که معمولاً در سرعت های زیاد یا مسافت های طولانی

کاربرد داشته و نویز روی آن اثر ندارد.

### 3-2-3- کابل هم محور: در واقع کلمه Coaxial ترکیبی است از Co + axial یعنی

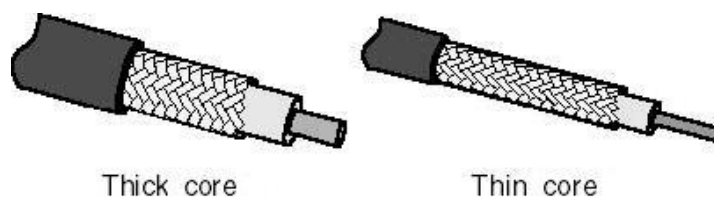
"هم محور". علت این نامگذاری از شکل پیداست:



شکل 3-7

جریان الکتریکی از طریق هسته از سمت فرستنده به گیرنده گسیل شده و مسیر برگشت خود را از طریق حفاظ (Shield) طی می‌کند. حفاظ علاوه بر تأمین مسیر برگشت برای الکترونها، وظیفه دیگری را نیز به عهده دارد و آن جذب نویزهای حاصل از "القای امواج الکترومغناطیسی در فضا" و هدایت آنها به زمین (Earth) است تا بدینوسیله از ایجاد نویز در هسته جلوگیری کند. البته یادمان باشد که جلوگیری از القای نویز روی هسته به وسیله ی حفاظ بصورت 100% نبوده و نسبی است چنانچه شدت میدان الکترو مغناطیسی اطراف کابل هم محور قوی باشد در آنصورت حفاظ هم مقاومت چندانی نمی تواند بکند و اطلاعات هسته نویزی و مخدوش می‌شود. در کابل‌های هم محور هر چه قطر هسته و متناسب با آن غلظت بافت الیاف فلزی حفاظ بیشتر باشد، مقاومت کابل در برابر عبور الکتریسته کمتر شده و لذا شدت جریان برای عبور با مانع کمتری مواجه می‌شود و این امر سبب می‌شود در مسافتهای طولانی‌تری بتوان از آن استفاده کرد از این رو در شبکه‌های کامپیوتری دو نوع کابل هم محور از نظر ضخامت وجود دارد:

نازک، با قطر حدوداً 6,5mm معروف به Thin .  
 ضخیم، با قطر حدوداً 13mm معروف به Thick.



شکل 3-7

کابل Thin از Thick سبک تر و انعطاف پذیرتر بوده و ارزانتر است اما در فواصل کوتاهتری بکار می‌رود از طرفی وزن کابل Thick بعلت قطر بیشتر آن زیاد شده قیمت آن افزایش یافته،

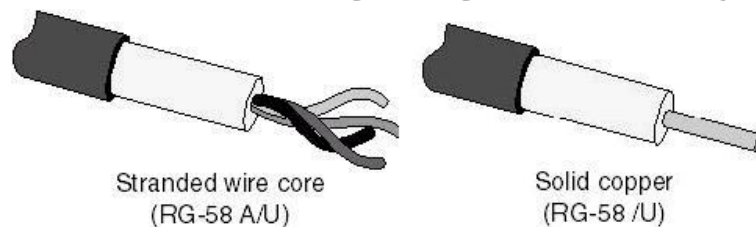
انعطاف پذیری آن کمتر شده و کار با آن سخت تر می شود اما در عوض نسبت به Thin در فواصل طولانی تری استفاده می شود.

سابقاً نوع خاصی از کابل کواکس Thin معروف به RG58 در شبکه های کامپیوتری استفاده بیشتری داشت که آنرا دقیق تر بررسی می کنیم. RG58 در سه مدل موجود است:

(1) RG58 U : که در آن، هسته تک رشته (مفتولی) است. در اصطلاح معروف است به Solid Core

(2) RG58 A/U : که در آن، هسته چند رشته (افشان) است. در اصطلاح به آن Stranded Core می گویند که انعطاف پذیری بیشتری نسبت به RG58 U دارد.

(3) RG58 C/U : نسخه نظامی A/U، در اصطلاح Military Version of A/U که مناسب برای کاربرد در محیطهای نظامی و صنعتی است.

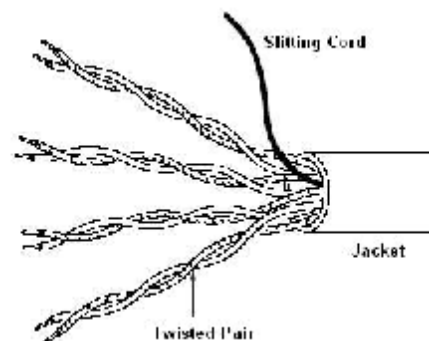


شکل 3-7

نکته: بطور کلی سیمهای مفتولی و افشان علاوه بر تفاوت در انعطاف پذیری، در مشخصه الکتریکی (تحت فرکانسهای زیاد) نیز با هم فرق دارند (اثر پوسته ای یا Skin Effect) اما این تفاوت در شبکه های کامپیوتری با توجه به فرکانس مورد استفاده و شدت جریان پایین چندان مد نظر نبوده و فقط مشخصه مکانیکی یعنی انعطاف پذیری مهم است.

3-2-4 - کابل Twisted Pair = TP :

این کابل که در مخابرات کاربرد فراوانی دارد تشکیل شده از یک زوج سیم که به هم تابیده شده اند :



شکل 3-8

علت تاییدن سیمها بهم انست که اولاً میدانی را در اطراف خود القا نکنند ثانیاً اثرات نویز القا شده روی خود را خنثی کنند. در عمل کابلهای TP از چندین زوج بهم تاییده تشکیل می شوند و هر زوج برای یک کانال مخابراتی مورد استفاده قرار می گیرد. البته می توان از تکنیکهای TDM یا FDM استفاده کرده و چندین کانال مخابراتی را نیز بطور همزمان از یک زوج عبور داد.

مزایا و معایب این کابل نسبت به هم محور به اختصار عبارتند از:

مزیت: ارزانتر بوده و در شبکه مخابرات به وفور از آن استفاده می شود.

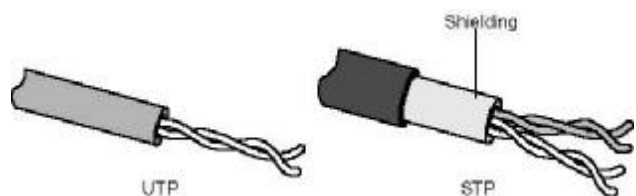
معایب: 1 - نسبت به هم محور، نویز روی TP اثر بیشتری دارد.

2 - بروز یک مشکل جدید بنام هم شنوایی یا Cross Talk.

مزیت یاد شده باعث شد تا طراحان شبکه، ایده استفاده از این کابل را در شبکه های کامپیوتری در ذهن خود پرورش دهند و این امر باعث پیدایش مودمها شد. مودم وسیله ای است که اجازه می دهد تا از طریق بستر مخابراتی موجود که مملو از کابلهای TP است یک شبکه کامپیوتری در ابعاد WAN (و البته سرعت نسبی پایین) برقرار کنیم.

سپس متخصصان شبکه به فکر استفاده از کابلهای TP با کیفیت بهتر و بطور مستقل از مخابرات در ابعاد شبکه های LAN افتادند و این امر با پیدایش کارتهای شبکه مناسب که کابل TP به آنها متصل می شد محقق شد. امروزه اکثر شبکه های LAN از این کابل بهره برده و توپولوژی آنها نیز ستاره ای است.

از طرفی عیب یاد شده در این کابلها باعث شد تا نوعی خاص از TP که دارای حفاظ نیز باشد ساخته شود که به کابل STP معروف شد. بنابراین کابلهای TP در حالت کلی به دو نوع تقسیم می شوند:



UTP = Unshielded Twisted Pair  
STP = Shielded Twisted Pair

شکل 9-3

مورد مصرف کابلهای STP نسبت به نوع معمولی آن یعنی UTP در محیطهایی است که اثرات میدانهای الکترومغناطیسی در آنها قویتر است. البته بدیهی است که یک کابل STP نسبت به کابل هم محور Thin گرانتر است و لذا مزیت آن یعنی "ارزانتر بودن" زیر سوال می رود اما با توجه به اینکه در شبکه های LAN ابعاد محدود بوده و فواصل کوتاه است این "گرانی" چندان خود را نشان نمی دهد.

در هر صورت تکنولوژی، سرمایه گذاری خود را در شبکه‌های کامپیوتری بر روی کابل‌های TP اعم از UTP یا STP گسترش داده و کار چندانی با هم محور ندارد.

اکثر کابل‌های TP متداول در شبکه از 4 زوج که در کنار یکدیگر تحت یک پوشش کلی قرار گرفته‌اند. از طرفی گفتیم که به هم تابیدن سیم‌ها باعث می‌شود تا میدانی در اطراف سیم‌ها القا نشود اما این موضوع قطعی نبوده و به هر حال یک زوج سیم به هم تابیده که از آن جریانی عبور می‌کند باعث القای میدانی هر چند ضعیف در اطراف خود می‌شود و همین می‌تواند سبب ایجاد اختلال در زوج‌های مجاور شود. زوج‌های مجاور نیز هر کدام به نوبه خود چنین مشکلی را برای بقیه بوجود می‌آورند. به این پدیده اصطلاحاً هم‌شنوایی یا Cross Talk گفته می‌شود و اکثر ما تجربه آنرا بصورت "خط روی خط افتادن" در مخابرات داشته‌ایم. بعنوان مثال دیگری از این پدیده، یک جمع کوچک را تصور کنید مثلاً شامل 8 نفر که افراد دو به دو گروه‌بندی شده و همزمان اعضای هر گروه با یکدیگر صحبت می‌کنند. هر چقدر هم افراد آهسته صحبت کنند با اینحال روی بقیه تأثیر گذاشته و برای دیگران حکم نویز و پارازیت و اختلال را دارد. برای کاهش این اثر چه پیشنهادی دارید؟

پاسخ را در تبصره 5 همین بخش خواهیم دید.

کابل‌های TP صرف نظر از UTP یا STP، بر اساس حداکثر سرعت و نوع کاربردی که در شبکه‌ها دارند به چند دسته یا Category تقسیم می‌شوند که عبارت است از :

کاربرد	سرعت	نام گروه
مورد مصرف در شبکه‌های مخابراتی	-	Category 1 = Cat 1
مورد مصرف در شبکه‌های با سرعت حداکثر	4 Mbps	Category 2 = Cat 2
مورد مصرف در شبکه‌های با سرعت حداکثر	10 Mbps	Category 3 = Cat 3
مورد مصرف در شبکه‌های با سرعت حداکثر	16 Mbps *	Category 4 = Cat 4
مورد مصرف در شبکه‌های با سرعت حداکثر	100 Mbps **	Category 5 = Cat 5
مورد مصرف در شبکه‌های با سرعت از	1000 Mbps تا سقف 100 Mbps -	Category 5e = Cat 5e
مورد مصرف در شبکه‌های با سرعت	و بالاتر 1 Gbps -	Category 6 = Cat 6

جدول 3-1

\*: کابل CAT 4 توانایی انتقال تا نرخ 20 Mbps را نیز دارد اما در عمل شبکه‌هایی که از این کابل بهره می‌برند تا حداکثر 16 Mbps از آنرا استفاده می‌کنند.

\*\* : در برخی از متون به 1000 Mbps نیز اشاره شده اما بهتر است اطمینان نکرده و برای سرعت‌های 1000 از کابل‌های با نمره بالاتر مثلاً Cat5e یا Cat 6 استفاده کنیم.

بطور کلی در مورد همه کابل‌های فوق دقت داشته باشید که سرعت‌های نوشته شده الزاماً بیانگر حداکثر ظرفیت کابل نیست بلکه بیانگر سرعت تجهیزاتی است که از آنها برای انتقال اطلاعات استفاده می‌کنند. بعنوان مثال یک زوج از Cat 3 تا حدود 30 Mbps نیز می‌تواند اطلاعات را از خود عبور دهد و در نوع خاصی از شبکه‌ها که بعداً به آن اشاره خواهیم کرد، 3 زوج از یک کابل Cat3 با هم می‌توانند تا 100 Mbps اطلاعات را عبور دهند. کابل Cat3 در مجموع دارای 4 زوج یا 8 رشته سیم است.

در مورد Cat 1 سرعت را عنوان نکردیم؟ علت آنست که برای انتقال اطلاعات از طریق شبکه مخابرات معمولاً از مودم استفاده می‌کنیم و مودم‌ها نیز انواع گوناگون با تکنولوژی‌ها و استانداردهای متفاوت داشته و سرعت در آنها متنوع است. همچنین سرعت در شبکه‌های مخابراتی که در واقع از دیدگاه کامپیوتری یک شبکه WAN محسوب می‌شود بستگی به فاصله، شرایط محیطی، کیفیت خطوط و اتصالات و همچنین تقویت‌کننده‌های بین راه دارد. لذا ترجیح دادیم حرفی از سرعت به میان نیاوریم با این حال از تجارب شخصی هر کس می‌داند که مثلاً با استفاده از مودم‌های Dial up از نوع آنالوگ و در صورت مطلوب بودن شرایط می‌توان تا سرعت‌های حدوداً 33 Kbps دست پیدا کرد و یا با استفاده از مودم‌های DSL که در واقع دیجیتالی هستند می‌توانیم در فواصل کوتاه (تا حداکثر 3 الی 5 کیلومتر) و شرایط مطلوب به سرعت‌های حدوداً 2 Mbps هم دسترسی داشته باشیم.

رایج ترین شبکه‌های LAN به لحاظ سابقه تاریخی آنها تا به امروز عبارتند از:

کابل Thin Coax RG58 با سرعت 10 Mbps در توپولوژی خطی : تقریباً منسوخ شده‌اند.

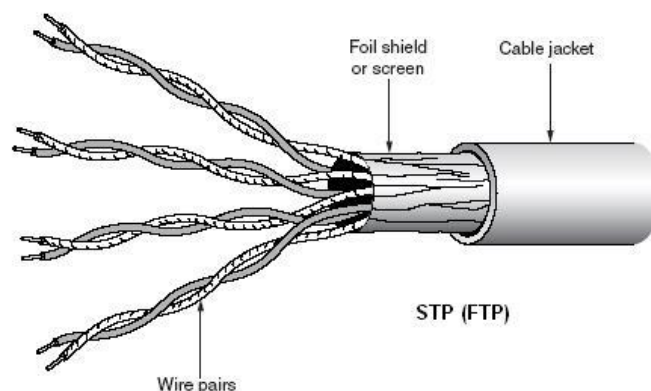
کابل Twisted Pair Cat3 با سرعت 10 Mbps در توپولوژی ستاره ای : تقریباً منسوخ شده‌اند.

کابل TP Cat5 یا Cat5e با سرعت 100 Mbps در توپولوژی ستاره ای : امروزه بسیار رایج است.

کابل TP Cat5e یا Cat6 با سرعت 1000 Mbps در توپولوژی ستاره ای : رفته‌رفته جای خود را باز می‌کنند.

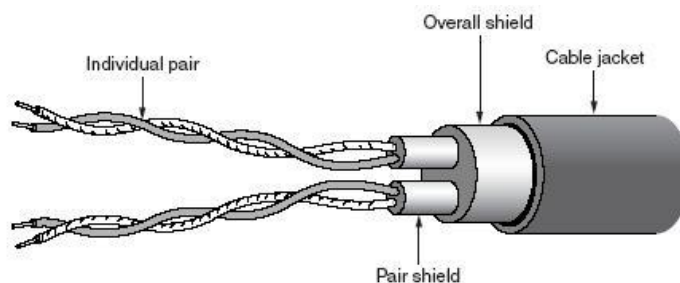
مطالعه آزاد :

ممکن است به کابل‌های TP که از فویل آلومینیوم بعنوان حفاظ استفاده می‌کنند اصطلاحاً FTP گفته شود.



شکل 10-3

برخی از کابل‌های TP برای هر زوج نیز یک حفاظ در نظر می‌گیرند اعم از کلاف سیمی بافته شده (زره) یا فویل آلومینیوم و مزیت آن‌هم در آنست که Cross Talk را کم می‌کند. در برخی علاوه بر آنکه هر زوج دارای حفاظ خاص خود است، یک حفاظ کلی نیز روی همه آنها کشیده می‌شود و در نتیجه واژه‌های SSTP، SFTP، FSTP، FFTP برای توصیف آنها بکار می‌روند. در هر صورت هر چه که باشند دارای حفاظ بوده و در محیط‌های نویزی تا حد مجاز تعریف شده می‌توانند بکار روند.

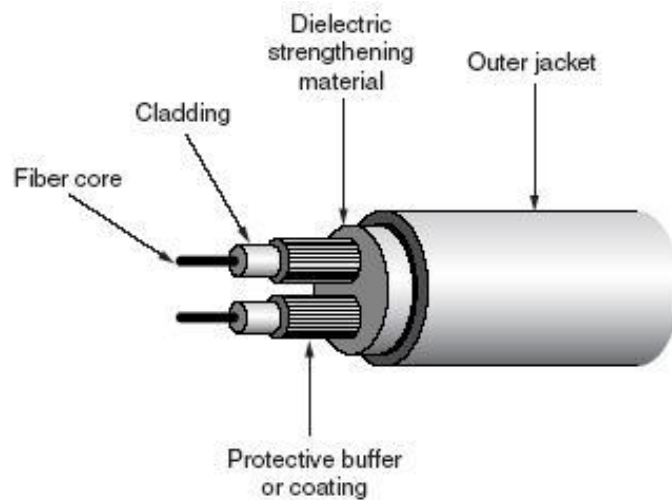


شکل 11-3

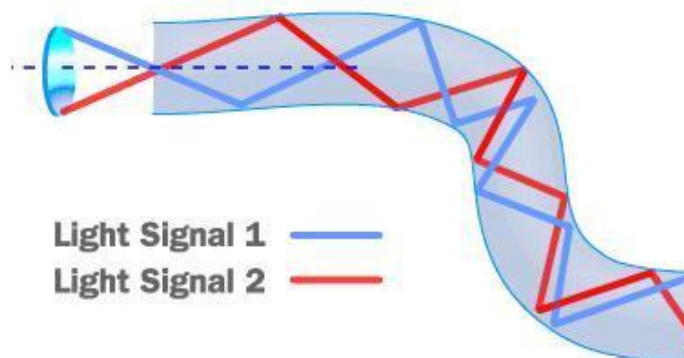
### 3-2-5- کابل نوری (Fiber Optic = FO):

فیبر نوری از ترکیبات خاص پلاستیک فشرده یا سیلیس ساخته می‌شوند و می‌تواند پالس‌های نور را از یک سمت به سمت دیگر هدایت کند (شکل 12-3).

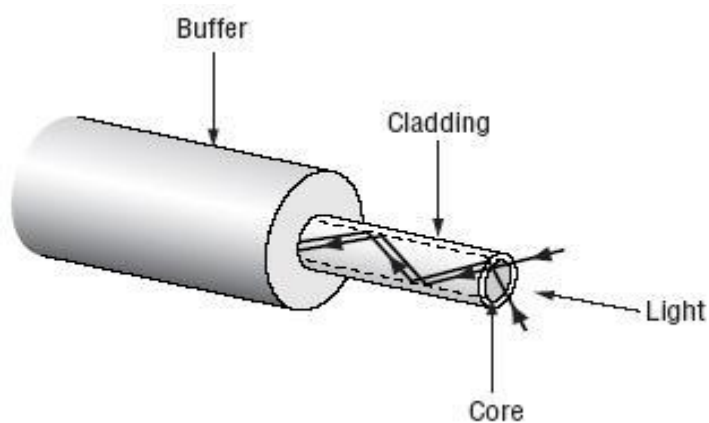




شکل 3-12 ساختمان فیبر نوری

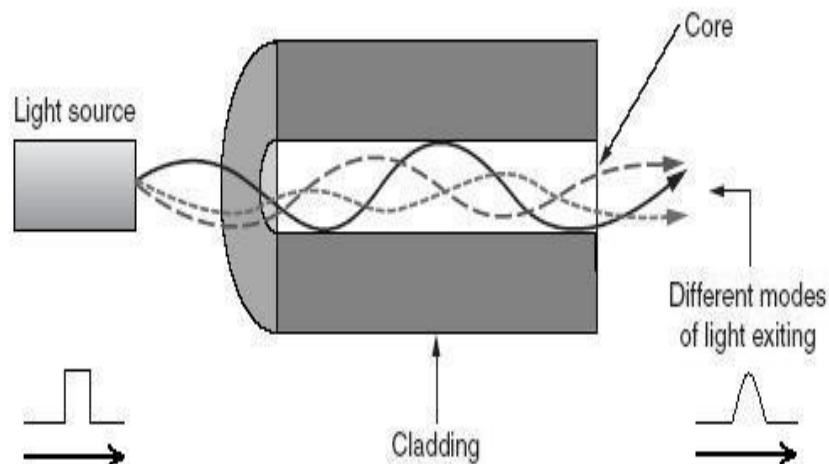


شکل 3-13 هدایت نور در فیبر نوری



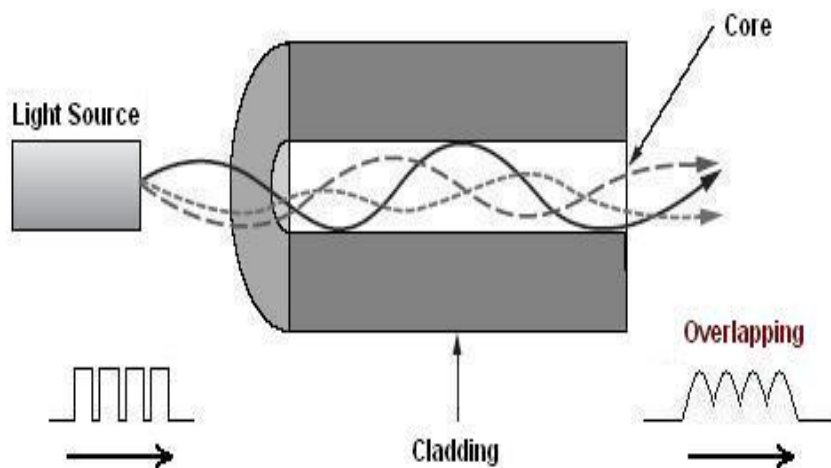
شکل 3-14

قسمت مرکزی کابل که نور از آن عبور می کند معروف به هسته (Core) بوده و لایه انعکاس دهنده نیز به Clad مشهور است. جنس Core/Cladding هر دو یکی است و تفاوت در ضریب شکست شان است. همانطور که از شکل 3-15 نشان داده شده است وقتی یک پالس نوری از ابتدای خط ارسال می شود بدلیل اختلاف مسیر در شعاعهای مختلف نور، پالس خروجی به همان شکل نبوده و کمی تغییر شکل می دهد:



شکل 3-15

حال چنانچه فرکانس فرستنده از حد معینی بیشتر شود پالسهای خروجی با یکدیگر همپوشانی پیدا می کنند (Overlapping) و این باعث بروز خطا می شود. چنانچه ضخامت هسته طوری باشد که اجازه عبور چندین شعاع نوری را در زوایای مختلف بدهد به آن کابل نوری MM = Multi Mode گفته می شود.



شکل 3-16

مزایای کابل نوری با توجه به خصوصیات آن عبارتست از:

امکان استفاده در فواصل طولانی تر.

نرخ انتقال بیشتر.

عدم نویز پذیری نسبت به میدانهای الکترومغناطیسی.

امنیت بیشتر. سرقت اطلاعات از سیمهای فلزی بوسیله اتصال مستقیم یک سیم بصورت انشعاب و یا

بطور غیر مستقیم از طریق القای امواج، امری است امکان پذیر، اما در مورد فیبرهای نوری به

دلیل ظریف بودن هسته نمی توان براحتی و بدون صرف وقت و امکانات از کابل انشعاب گرفت

ضمن آنکه القای امواج نیز در مورد فیبر نوری بی معنی است. بنابراین سرقت اطلاعات از

فیبر نوری بسیار دشوارتر از سیمهای فلزی است و در نتیجه امنیت انتقال اطلاعات از طریق

فیبر نوری بیشتر است.

ارتباط راحت مابین ساختمانهای مختلف که دارای چاههای ارت مستقل از یکدیگرند. (عدم بروز

پدیده Ground Loop)

فرض کنید که ارتباط شبکه ای مابین 2 ساختمان از طریق کابل هم محور باشد. برای دفع نویز به

سمت زمین و جلوگیری از تأثیر گذاری آن روی اطلاعات، قسمت حفاظ کابل هم محور به

Earth متصل می شود. حتی اگر حفاظ مستقیماً به ارت (Earth) وصل نباشد، از طریق کانتکتور

متصل به آن و بدنه یکی از کامپیوترها که با ارت ارتباط داشته باشد به زمین وصل می شود.

چنانچه چاه ارت هر دو ساختمان یکی باشد مشکلی بروز نمی کند اما اگر ساختمانها دارای

چاههای ارت جداگانه ای باشند در آنصورت بعلت مغایرت بین مشخصات فیزیکی چاهها از نظر

رطوبت نسبی و ...، جریانی ضعیف از یک سو به سوی دیگر برقرار می شود که اصطلاحاً به آن

Ground Loop گفته می شود. این جریان در واقع خود بعنوان یک عامل مزاحم محسوب

می شود. حال اگر ارتباط مابین ساختمانها را از طریق فیبر نوری برقرار کنیم Ground Loop در

کار نخواهد بود چون از فیبر نوری اساساً الکتریسیته عبور نمی کند.

تحقیق، در مورد ترکیبات روکش انواع کابلها ی نوری و خصوصیات آن تحقیق کنید

ضد جوندگی: Anti Rodent

ضد رطوبت و آب: Anti Humidity, Water Blocking

روکش مسلح: Armored

ضد تولید گاز سمی: Halogen Free (Plenum Grade)

### 3-3- کابل کشی UTP

مراحل مهم پیاده سازی سخت افزاری یک شبکه کامپیوتری را می توان به ترتیب زیر بیان کرد.

- تصمیم گیری در مورد نوع شبکه
- تهیه نقشه اجرایی
- انتخاب و تهیه سخت افزار مورد نیاز
- نصب تجهیزات
- کابل کشی و نصب کابل
- برقراری اتصالات

#### 3-3-1- طراحی و اجرای عملیات کابل کشی:

نکات مهم هنگام طراحی و اجرای عملیات کابل کشی: کابل های "فلزی" مانند کابل هم محور یا Twisted Pair تحت تأثیر میدانهای الکترومغناطیسی فضای اطراف خود قرار گرفته و روی آنها Noise ایجاد می شود. اینگونه میدانها در مجاورت کابل های برق و مخصوصاً وسایل الکتریکی دارای "سیم پیچ" مانند انواع الکتروموتورها اعم از کاربردهای خانگی یا صنعتی و انواع ترانسفورماتورها و ترانسفورمرها بیشتر بوده و بطور کلی باید از عبور کابل در مجاورت نزدیک با کابل برق یا وسایل فوق پرهیز کرد:



شکل 3-17

چنانچه کابل های برق و شبکه به موازات هم باشند در آن صورت حداقل فاصله ای که باید بین آنها باید رعایت شود بستگی به شدت میدان الکترومغناطیسی کابل برق دارد که آنهم تابعی است از جریان الکتریکی عبوری از کابل. در عمل بسته به این شدت جریان، حداقل از 5 Cm تا 30 Cm یا بیشتر فاصله بین کانالهای برق و شبکه قرار می دهند.

### 2-3-3- Duct :

به کانالهایی که روی دیوار برای عبور کابل نصب می شود اصطلاحاً Duct یا Trunk گفته می شود و از نظر جنس بر دو نوعند:  
پلاستیکی و فلزی.



شکل 18-3

نکته برخی از کانالها دارای 2 یا 3 قسمت مجزا هستند و از آنها می توان برای عبور کابل های برق و شبکه در کنار هم استفاده کرد اما بدیهی است که در اینگونه موارد باید:  
اولاً دیواره حایل بین قسمتها باید ترجیحاً فلزی بوده ثانیاً شدت جریان عبوری از کابل برق زیاد نباشد ثالثاً کابل شبکه در صورت امکان دارای حفاظ باشد رابعاً بدنه کانال اگر فلزی است به Earth متصل شود.

### 3-3-3- عوامل موثر در تعیین نوع کابل کشی:

سنگینی ترافیک شبکه ،

طول کابل کشی

بودجه تعیین شده برای کابل کشی

نیازهای ایمنی شبکه

نوع کابل کدام های موجود

مشخصات	کواکسیال نازک	کواکسیال ضخیم	زوج به هم تابیده	فیبر نوری
هزینه کابل طول کابل segment سرعت انتقال	ارزان 185 متر 10Mbps	گران 500 متر 10Mbps	ارزان 100 متر 4 تا 100 Mbps	متوسط 2 کیلومتر (90 کیلومتر) 100Mbps یا بیشتر (بیشتر از 1Gbps)
نصب	نصب آسان	نصب آسان	خیلی آسان با امکان نصب قبلی	نصب دشوار (نیاز به متخصص و تجهیزات مخصوص دارد)
تداخل	مقاومت خوب در مقابل تداخل	مقاومت خوب در مقابل تداخل	مستعد برای تداخل	مستعد تداخل نمی باشد.
سایر خصوصیات	نیاز به اجزای پشتیبانی کمتری نسبت به ضخیم T.P. دارد.	نیاز به اجزای پشتیبانی کمتری نسبت به ضخیم T.P. دارد	همانند سیم تلفن، اغلب در ساختمانها، از قبل نصب می شود.	از داده ها، صوت و تصویر، با ایمنی بالایی پشتیبانی می کند.

جدول 2-3 خلاصه مقایسه کابلها

#### 3-3-4- اهمیت Earth:

ارت بعنوان یک عامل مهم در تخلیه نویز در کابلهای دارای حفاظ بشمار می رود (مانند کابل هم محور یا STP). چنانچه در شبکه ای از این کابلها استفاده شود و حفاظ به ارت متصل نشود کارکرد شبکه توأم با اختلال خواهد بود که این اختلال بشکل خطا در انتقال اطلاعات، کندی سرعت و حتی قطعی موقتی خود را نشان می دهد. بنابراین توصیه می شود حتماً چاه ارت مناسب برای کامپیوترها، شبکه و تجهیزات مربوطه تهیه شده و هرگز از ارت مربوط به برق گیر (که روی بام برجها نصب می شود) برای شبکه استفاده نشود.

3-3-5- تجهیزات مورد نیاز برای اتصال کابل به کانکتور :

تجهیزات مورد نیاز برای ایجاد کابل های UTP عبارتند از :

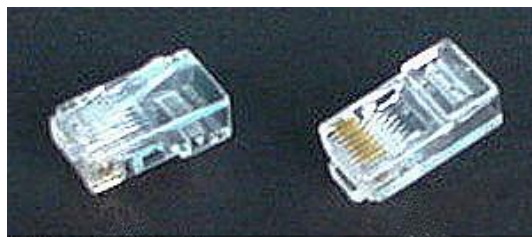
کانکتورهای RJ-45

کابل UTP

آچار پرس RJ-45

سیم لخت کن

که در شکل 3-19 نشان داده شده است.

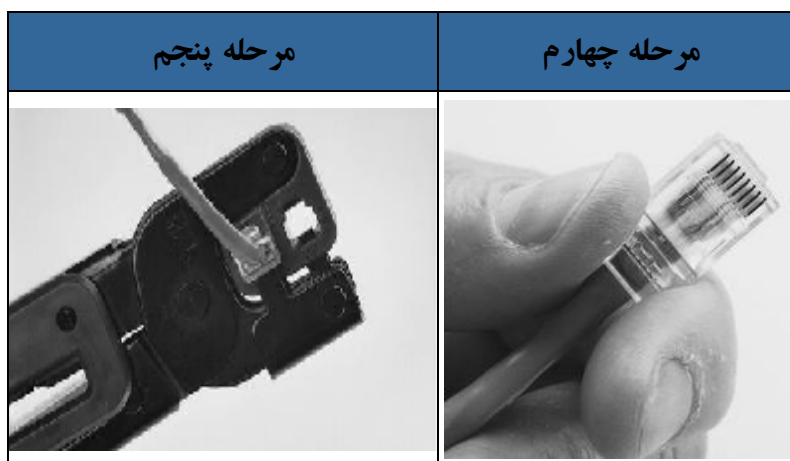


شکل 3-19

3-3-6- ایجاد کابل Straight :

مراحل ایجاد یک کابل : شکل 3-18 مراحل لخت کردن سیم و اتصال کانکتور را نشان می دهد.

مرحله سوم	مرحله دوم	مرحله اول
		



شکل 3-20

مدل های متفاوت کابل کشی کابل ها :

به منظور کابل کشی کابل های UTP از دو استاندارد متفاوت T-568A و T-568B استفاده می شود . تفاوت دو مدل فوق مربوط به رنگ زوج هائی است که به یکدیگر متصل می شوند. در کابل های UTP از کانکتورهای استاندارد و چهار زوج سیم بهم تاییده استفاده می گردد :

زوج اول : آبی و سفید/ آبی

زوج دوم : نارنجی و سفید / نارنجی

زوج سوم : سبز و سفید/ سبز

زوج چهارم : قهوه ای و سفید / قهوه ای

در شبکه های Mbit 10/100 از زوج های دو و سه استفاده شده و زوج های یک و چهار به عنوان رزو باقی می ماند . در شبکه های گیگاترنت از تمامی چهار زوج استفاده می گردد. کابل های CAT5 متداولترین نوع کابل UTP بوده که دارای انعطاف مناسب بوده و نصب آن ها به راحتی انجام می شود .

ایجاد یک کابل UTP به منظور اتصال کامپیوتر به هاب (معروف به کابل های Straight) اترنت عموماً با استفاده از هشت کابل به همراه هشت پین ماژولار plugs/jacks ، داده را حمل می کند . کانکتور استاندارد، RJ-45 نامیده شده و مشابه کانکتور استاندارد RJ-11 است که در تلفن استفاده می گردد. یک رشته کابل CAT5 شامل چهار زوج سیم بهم تاییده است که هر زوج دارای دو رشته سیم با رنگ هائی خاص است . (یک رشته رنگی و یک رشته سفید با نواری به رنگ رشته زوج مربوط ) . به منظور تسهیل در امر نگهداری ، می بایست به اندازه ضروری سیم های بهم تاییده را از حالت پیچش خارج نمود ( مثلاً "حدود یک سانتیمتر) . زوج های در نظر گرفته شده برای اترنت ده و یکصد مگابیت به رنگ نارنجی و سبز می باشند . از دو زوج دیگر (رنگ قهوه ای و آبی) می توان به منظور یک خط اترنت دوم و یا اتصالات تلفن استفاده نمود .

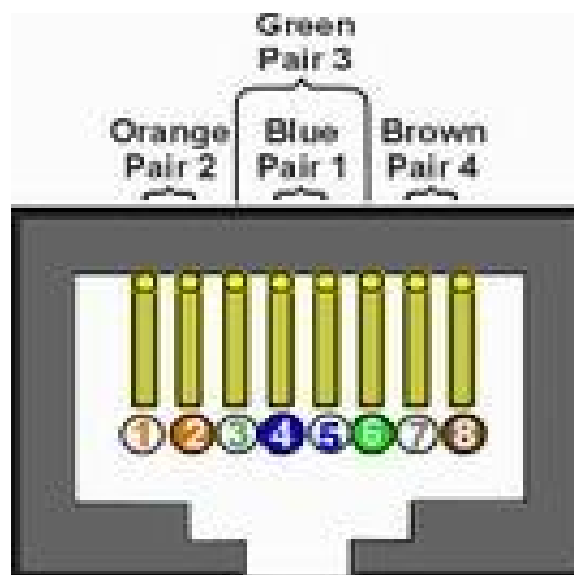


به منظور کابل کشی کابل های UTP از دو استاندارد متفاوت با نام T-568B (یا EIA) و T-568A (یا T&A ، A258) ، استفاده می گردد . تنها تفاوت موجود بین آنان ترتیب اتصالات است .

شماره پین های استاندارد T568B همانگونه که در جدول زیر مشاهده می گردد ، شماره پین های فرد همواره سفید بوده که با یک نوار رنگی پوشش داده می شوند .

کد رنگ ها در استاندارد B568T			
شماره پین	رنگ	زوج	کاربرد
یک	سفید / نارنجی	دوم	TxData+
دو	نارنجی	دوم	TxData-
سه	سفید / سبز	سوم	RecvData+
چهار	آبی	یک	
پنج	سفید / آبی	یک	
شش	سبز	سوم	RecvData-
هفت	سفید / قهوه ای	چهارم	
هشت	قهوه ای	چهارم	

جدول 3-3



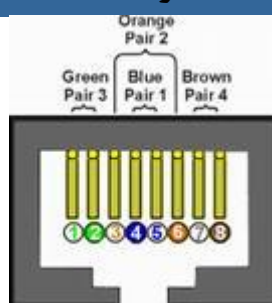
شکل 21-3 استاندارد B568T

## شماره پین های استاندارد T568A

در استاندارد 568A ، اتصالات سبز و نارنجی برعکس شده است ، بنابراین زوج های یک و دو بر روی چهار پین وسط قرار می گیرند (سازگاری با telco voice). (جدول 3-4)

کد رنگ ها در استاندارد A568T			
شماره پین	رنگ	زوج	کاربرد
یک	سفید / سبز	سوم	RecvData+
دو	سبز	سوم	RecvData-
سه	سفید / نارنجی	دوم	TxData+
چهار	آبی	یک	
پنج	سفید / آبی	یک	
شش	نارنجی	دوم	TxData-
هفت	سفید / قهوه ای	چهارم	
هشت	قهوه ای	چهارم	

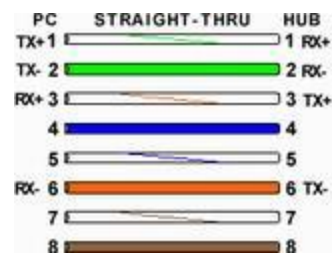
## استاندارد A568T



شکل 22- 3

موارد استفاده کاربرد کابل straight :

یک کابل straight ، به طور معمول برای برقراری اتصال بین کامپیوتر و هاب / سوئیچ به کار می رود .



شکل 3-23

شکل 3-23 یک اتصال استاندارد straight در کابل های CAT5 را نشان می دهد که از آن به منظور اتصال یک کامپیوتر به هاب استفاده می گردد. با اینکه در ظاهر TX+ یک طرف به TX+ طرف دیگر متصل نشده است ولی زمانی که کامپیوتر شخصی به هاب متصل می گردد، هاب به صورت اتوماتیک و با استفاده از مدارات داخلی خود کابل را X-over نموده و بدین ترتیب، پین شماره یک از کامپیوتر (TX+) به پین شماره یک هاب (RX+) متصل می شود. در صورتی که هاب عملیات x-over را انجام ندهد (در زمان استفاده از درگاه Uplink)، پین شماره یک کامپیوتر (TX+) به پین شماره یک هاب (TX+) متصل می گردد. بنابراین مهم نیست که چه نوع عملیاتی را با درگاه HUB انجام می دهیم (Uplink یا نرمال)، سیگنال های نسبت داده شده به هشت پین سمت کامپیوتر شخصی، همواره یکسان باقی مانده و هاب با توجه به نوع استفاده از درگاه (نرمال و یا Uplink) عملیات لازم را انجام خواهد داد.

### 3-3-7- ایجاد کابل X-Over

کابل های کراس CAT5 UTP که از آنان با نام X-over نیز نام برده می شود، یکی از متداولترین کابل های استفاده شده پس از کابل های Straight می باشند. با استفاده از کابل های فوق، می توان دو کامپیوتر را بدون داشتن هاب یا سوئیچ به یکدیگر متصل نمود. با توجه به این که هاب عملیات X-over را به صورت داخلی انجام می دهد، در زمانی که یک کامپیوتر را به یک هاب متصل می کنید، فقط به کابل Straight نیاز است. و در صورتی که قصد اتصال دو کامپیوتر به هم را بدون استفاده از هاب دارید، می بایست عملیات X-over را به صورت دستی انجام دهید و کابل X-over را ایجاد نمایید.

### عملکرد کابل های X-over

در زمان مبادله داده بین دو کامپیوتر، یکی از آنان به عنوان دریافت کننده و دیگری به عنوان فرستنده ایفای وظیفه می نماید. تمامی عملیات ارسال داده از طریق کابل های شبکه انجام می شود. یک کابل شبکه از چندین رشته سیم دیگر تشکیل می گردد. از برخی رشته سیم ها به منظور ارسال داده و از برخی دیگر به منظور دریافت داده استفاده می شود. در ساخت کابل X-

over از اصول فوق استفاده شده و TX (ارسال) یک سمت به RX (دریافت) سمت دیگر، متصل می گردد.

اتصال دو کامپیوتر به یکدیگر با استفاده از یک کابل X-over



شکل 3-24

### کابل CAT5 X-over

به منظور ایجاد کابل های کراس CAT5 صرفاً از یک روش استفاده می گردد. همانگونه که قبلاً اشاره گردید، یک کابل X-over پین TX یک سمت را به پین RX سمت دیگر متصل می نماید (و برعکس). شکل زیر شماره پین های یک کابل CAT5 معمولی X-over را نشان می دهد.

شماره پین های یک کابل CAT5 X-over



شکل 3-25

همانگونه که در شکل 3-25 مشاهده می کنید در کابل X-over از پین های شماره یک، دو، سه و شش استفاده می گردد. پین های یک و دو بمنزله یک زوج بوده و پین های سه و شش زوج دیگر را تشکیل می دهند. از پین های چهار، پنج، هفت و هشت استفاده نمی گردد. (فقط چهار پین از هشت پین کانکتور، استفاده می شود).

### کاربرد کابل های X-over

از کابل های X-over تنها برای اتصال دو کامپیوتر استفاده نمی شود بلکه از آن می توان در دستگاه های متفاوتی نظیر سوئیچ یا هاب نیز استفاده کرد. در صورتی که قصد داشته باشیم دو هاب را به یکدیگر متصل نمائیم، معمولاً از درگاه uplink استفاده می گردد. درگاه فوق،

بخش های tx و rx را کراس نمی نماید. شکل زیر نحوه اتصال دو هاب به یکدیگر با استفاده از یک کابل Straight و از طریق درگاه Uplink را نشان می دهد :

### اتصال دو هاب با استفاده از درگاه Uplink و یک کابل Straight



شکل 3-26

با توجه به وجود درگاه uplink، نیازی به استفاده از یک کابل x-over نخواهد بود. در صورتی که امکان استفاده از درگاه uplink وجود نداشته باشد و بخواهیم دو هاب را با استفاده از درگاه های معمولی به یکدیگر متصل نماییم، می توان از یک کابل X-over استفاده نمود. شکل زیر نحوه اتصال دو هاب به یکدیگر با استفاده از یک کابل X-over را و بدون استفاده از درگاه Uplink نشان می دهد :

### اتصال دو هاب با استفاده از درگاه معمولی و یک کابل X-over



شکل 3-27

### 3-4- کارت شبکه و وظایف آن

کارت های شبکه، به عنوان میانجی (Interface) فیزیکی یا رابط بین کامپیوتر و کابل شبکه، عمل می کنند. کارت ها در شکاف (Slot) توسعه هر کامپیوتر و سرویس دهنده شبکه نصب می شوند. پس از آنکه که کارت شبکه متعصب گردید، کابل شبکه به درگاه کارت متصل می شود تا ارتباط واقعی فیزیکی بین کامپیوتر و باقیمانده شبکه را برقرار می سازد.



شکل 3-28

#### 1-4-3- وظایف کارت شبکه

وظایف کارت شبکه عبارت است از:

آماده سازی داده های کامپیوتر برای انتقال به کابل شبکه

ارسال داده ها به کامپیوتر دیگر

کنترل جریان داده ها بین کامپیوتر و سیستم کابل کشی

کارت شبکه همچنین داده های وارده شونده را از کابل دریافت می کند و آن را به داده های قابل پردازش در CPU تبدیل می کند

آماده سازی داده ها: قبل از آنکه داده ها بتوانند از طریق شبکه ارسال شوند، کارت شبکه باید آن را از شکل قابل پردازش در کامپیوتر به شکل قابل انتقال از طریق کابل شبکه تغییر دهد. داده ها در داخل کامپیوتر از طرق مسیرهایی به نام گذرگاهها (BUS) حرکت می نمایند. آنها چندین مسیر داده ای هستند که به طور موازی و پهلوی هم قرار گرفته اند، چون چندین مسیر پهلو به پهلو هستند، داده ها می توانند به جای عبور تکی در هر لحظه به صورت گروهی با یکدیگر عبور کنند.

در کابل شبکه، داده ها باید در جریان تک بیتی حرکت نمایند. وقتی داده ها از کابل شبکه عبور می کنند گفته می شود به صورت انتقال سریال (serial) حرکت می نمایند زیرا هر بیت به دنبال بیت دیگر جریان دارد. به عبارت دیگر، کابل بزرگراه یک باند می باشد. داده ها در این بزرگراه ها همیشه در هر لحظه فقط یک باند حرکت دارند. کامپیوتر ها یا داده ها را می فرستند و یا دریافت می دارند.

کارت شبکه، عبور داده ها را به صورت موازی و به شکل گروهی می گیرد و آنها را طوری مجدداً می سازد که از طریق مسیر سریال به پهنای 1 بیت در کابل شبکه جریان یابند. این کار با تبدیل سیگنالهای دیجیتال کامپیوتر به سیگنالهای الکتریکی ونوری که می توانند از طریق کابلهای شبکه حرکت نمایند انجام می گیرد. قطعه مسئول این کار، فرستنده گیرنده (Transceiver) است.

#### 2-4-3- آدرس شبکه

علاوه بر تبدیل داده، کارت شبکه محل کارت یا آدرس را به باقیمانده شبکه نشان می دهد تا از تمام کارتهای دیگر شبکه تمیز داده شود.

آدرسهای شبکه از کمیته IEEE ( تلفظ می شود آی تریپل ای ، مخفف انستیتوی مهندسان برق والکترونیک ) تعیین می گردد. این کمیته ، محدوده ای از آدرسها را به هریک از سازندگان کارتهای شبکه اختصاص می دهد . سازندگان به طور سخت افزاری ، این آدرسها را در تراشه (Chip) های روی کارت قرار می دهند . با این روش ، هر کارت ، و در نتیجه هر کامپیوتر ، آدرس منحصر به فردی در شبکه دارد .

داده ها اغلب می توانند سریعتر از کارت شبکههای که آنها را اداره می کنند حرکت نمایند. به این دلیل داده به بافر (RAM) کارت فرستاده می شوند و در آنجا به طور موقت هم در ارسال و هم در دریافت ، نگهداری می شوند.

#### 3-4-3- ارسال و کنترل داده ها:

قبل از آن که کارت شبکه ، عملاً داده ها را به شبکه ارسال نماید ، محاوره ای الکترونیکی با کارت گیرنده انجام می دهد به طوری که هر دو کارت با موارد زیر موافق باشند:

میزان داده های ارسالی قبل از تایید

هر کارت قبل از سرریز شدن داده چه مقدار داده را می تواند نگهداری نماید.

سرعت انتقال داده ها

اگر کارت با سرعت بالاتر ، برای ارتباط آهسته تر مورد نیاز باشد ، هر دو کارت نیازمند یافتن سرعت انتقال مشترکی هستند که هر دو بتوانند انجام دهند . هر کارت به کارت دیگر علامت می دهد و با این عمل ، عوامل ( پارامترهای ) خود را به دیگری اطلاع و یا خودش را با عوامل دیگری تنظیم می نماید .

وقتی تمام جزییات ارتباط تعیین گردید ، دو کارت ، شروع به ارسال و دریافت داده ها می نمایند.

#### 4-4-3- پیکر بندی (configuration) کارت شبکه

کارتهای شبکه ، اغلب دارای گزینه های قابل پیکر بندی هستند که باید برای کارکرد صحیح کارت شبکه تنظیم گردند . مثلاً :

وقفه (IRQ (Interrupt

آدرس پایه درگاه ورودی - خروجی (Base I/O port)

آدرس پایه حافظه (Base Memory)

نحوه تنظیم گزینه ها در کارتهای شبکه متفاوت است . گاهی امکان دارد به کمک جامپر (jamper) روی کارت تنظیم نمود.

بعضی کارتها به کمک کلیدهای ریزی (DIP Switch) بر روی کارت شبکه پیکر بندی می شوند . در اغلب کارتهای شبکه که بدون جامپر

(Jampe less) و DIP Switch هستند ، تنظیم پیکر بندی در آنها با نرم افزاری که همراه کارت شبکه فر وخته می شود ، انجام می گیرد . نحوه تنظیم پیکر بندی ، در دفترچه های راهنما یا فایل های راهنما ، همراه کارت شبکه ، مشخص می گردد.

وقفه (IRQ): خطوط تقاضای وقفه ، خطوط سخت افزاری هستند که از طریق آنها دستگاههایی مانند پورتهای ورودی / خروجی ، صفحه کلید ، درایوهای دیسک و کارتهای شبکه می توانند و قفه ها یا تقاضاها را برای گرفتن خدمات ، به CPU کامپیوتر برسانند . خطوط درخواست وقفه در سخت افزار داخلی کامپیوتر تعبیه شده و سطوح مختلفی از تقدم را به گونه ای اختصاص می دهد که CPU بتواند اهمیت نسبی تقاضاهای خدمات وارد شده را تعیین نماید.

وقتی کارت شبکه تقاضایی برای کامپیوتر می فرستد ، از وقفه ، یعنی سیگنال الکترونیکی ارسالی به CPU کامپیوتر استفاده می کند .

هر قسمت سخت افزاری در کامپیوتر باید از خط تقاضای وقفه یا IRQ متفاوتی بهره بگیرد . خط وقفه ، زمانی که قسمت سخت افزاری کامپیوتر پیکر بندی می شود ، مشخص می گردد . آدرس پایه I/Q: درگاه ورودی / خروجی (I/Q) پایه مسیری را مشخص می کند که از طریق آن داده ها بین سخت افزار کامپیوتر (از قبیل کارت شبکه ) و CPU آن جریان می یابد . CPU، هر پورتی را با آن آدرس می شناسد.

هر قسمت سخت افزاری در سیستم ، باید شماره درگاه I/O پایه متفاوتی داشته باشد . آدرسهای پایه پورتها ( اعداد مبنای شانزده ) که برای کارت شبکه به کار می روند ، نباید قبلا از سوی قسمت دیگری استفاده شده باشد.

آدرس پایه حافظه : آدرس پایه حافظه ، محلی را در حافظه کامپیوتر (RAM) مشخص می کند . این محل ، به صورت ناحیه بافر برای ذخیره کرده داده های دریافتی و ارسالی از کارت شبکه به کار می رود . البته بعضی کارتهای شبکه تعریفی برای آدرس پایه حافظه ندارند زیرا آنها از هیچ یک از آدرسهای RAM سیستم استفاده نمی کنند .

معماری گذرگاه داده ها : در محیط کامپیوتر های شخصی ، معماریهای مختلفی برای گذرگاه داده ها در کامپیوتر وجود دارد . از جمله معروف ترین این گذرگاهها می توان به استاندارد ISA (آیزا) و PCI (پی سی آی) اشاره نمود . هر نوع گذرگاه به طوری فیزیکی از سایر گذرگاه ها جداست . ضروری است که کارت شبکه و گذرگاه هماهنگ باشند.



نکته: امروزه بیشتر بردهای اصلی دارای کارت شبکه به صورت On Board هستند و از گذرگاه های داخلی برد اصلی استفاده می کنند.

#### 5-4-3- اتصال کارت شبکه

کارت شبکه ، سه عمل مهم زیر را در هماهنگی فعالیتهای بین کامپیوتر و کابل انجام می دهد :

انجام اتصال فیزیکی با کابل

تولید سیگنالهای الکتریکی که از کابل می گذرند .

پیروی از قوانین مشخص نحوه دسترسی به کابل به منظور انتخاب کارت مناسب شبکه ، لازم است ابتدا نوع کابل و اتصالات آن تعیین شده باشند . هر نوع کابل خصوصیات فیزیکی متفاوتی دارد که کارت شبکه باید با آن مطابقت نماید . هر کارت برای پذیرش نوع خاصی از کابل مانند هم محور ، زوج به هم تابیده شده یا فیبر نوری ، ساخته شده است . برخی از کارتهای شبکه بیش از یک اتصال میانجی دارند . مثلاً بعضی از کارت شبکه ها ، دو درگاه اتصال هم محور نازک (BNC) و زوج به هم تابیده شده (RJ-45) را دارند

#### 5-3- روشهای دسترسی به خط انتقال

مجموع قوانینی که تعریف می کنند کامپیوتر چگونه داده ها را در کابل شبکه قرار می دهد و آنها را از کابل می گیرد «روش دسترسی» نامیده می شود از آنجا که در اکثر سیستمهای شبکه ، کانال ارتباطی در یک زمان معین تنها می تواند در اختیار یک ایستگاه باشد و از طرف دیگر ، هر یک از ایستگاههای شبکه در هر لحظه ممکن است احتیاج به استفاده از کانال ارتباطی داشته باشند ، رعایت یک روش و قانون مشخص برای دسترسی به خط انتقال ، لازم است .

روشهای رایج برای دسترسی به خط انتقال عبارت اند از :

روش دسترسی چندگانه تشخیص حامل باتشخیص برخورد (CSMA/CD)

روش عبور نشانه (Token passing)

#### 1-5-3- روش دسترسی چندگانه تشخیص حامل باتشخیص برخورد (CSMA/CD)

این روش شبیه روش صحبت در یک اتاق شلوغ است . در چنین اتاقی شخصی که می خواهد صحبت کند باید با گوش دادن ، مطمئن شود که فرد دیگری در حال صحبت نیست و سپس اقدام به صحبت کند . اگر شخص دیگری در حال صحبت کردن است ، نفر اول باید تا پایان صحبت شخص دوم سکوت کند . این شخص ، پس از اتمام صحبت فردی که زودتر از دیگران شروع به صحبت کرده است ، می تواند به صحبت خود ادامه دهد و بقیه باید تا پایان صحبت منتظر بمانند . هر گاه پس از برقراری سکوت ، دوفنر با هم شروع به صحبت کنند ، هر دو سکوت کرده ، پس از طی یک زمان کوتاه نامشخص ، یکی از آنها شروع به صحبت خواهد کرد . این دقیقاً روشی است که در CSMA/CD از آن استفاده می شود :

کامپیوتر « تشخیص می دهد » که کابل آزاد است یعنی ترافیکی در کابل وجود ندارد .  
(Sense)

کامپیوتر می تواند داده ها را ارسال نماید.

اگر داده ها در کابل وجود داشته باشند ، تا زمانی که داده ها به مقصد خود برسند و کابل مجدداً آزاد گردد ، هیچ کامپیوتر ای داده ای را انتقال نمی دهد .

اگر دو یا چند کامپیوتر دقیقاً به طور همزمان ، داده ها را ارسال نمایند ، برخورد (Collision) داده ها پیش خواهد آمد . وقتی چنین اتفاقی نیفتند ، دو کامپیوتر در گیر برای یک دوره زمانی تصادفی ، انتقال را متوقف می سازند و سپس سعی در ارسال مجدد می نمایند .

CSMA/CD به عنوان روش کشمش شناخته می شود زیرا کامپیوتر های شبکه برای به دست آوردن فرصتی در ارسال داده ها ، با هم رقابت یا کشمکش می کنند .

وجود تعداد زیادی کامپیوتر در شبکه ، موجب بروز ترافیک سنگین تر در شبکه می گردد . در ترافیک سنگین تر ، برخورد ها افزایش می یابند . پس از هر برخورد هر دو کامپیوتر باید برای ارسال مجدد داده ها تلاش نمایند ، که موجب پایین آمدن سرعت شبکه می گردد .

بروز برخوردها با افزایش تعداد کامپیوتر ها در شبکه افزایش می یابد . برنامه کاربردی بانکهای اطلاعاتی نسبت به برنامه دیگر در ایجاد ترافیک سنگین تر شبکه ، نیز نقش دارند . بنابراین ، شبکه با روش دسترسی CSMA/CD با کاربران زیادی که چندین برنامه کاربردی بانکهای اطلاعاتی را اجرا می کنند ، ممکن است شبکه را به حد توقف ( سرعت بسیار کند و آهسته ) بکشاند .

### 2-5-3- روش عبور نشانه (Token passing)

در عبور نشانه ، بسته خاصی به نام (Token) دور کابل حلقوی ، کامپیوتر به کامپیوتر گردش می کند . وقتی هر کامپیوتر ای در حلقه بخواهد داده ها را در طول شبکه ارسال نماید ، باید منتظر نشانه آزاد بماند . وقتی نشانه آزاد تشخیص داده شد ، کامپیوتر می تواند داده ها را انتقال دهد . داده ها به صورت بسته ها منتقل می شوند و اطلاعات اضافی مانند آدرس دهی به بسته ها متصل می گردد .

در حالی که نشانه از سوی یک کامپیوتر مورد استفاده قرار می گیرد ، سایر کامپیوتر ها نمی توانند داده ای منتقل نمایند . مزیت این روش در آن است که چون در هر لحظه فقط یک کامپیوتر می تواند از نشانه استفاده نماید ، کشمکش و برخوردی پیش نمی آید و حتماً پس از طی زمانی مشخص ، نوبت ارسال داده به هر کامپیوتر خواهد رسید .

خود آزمایی و تحقیق

توپولوژی چیست؟ انواع آن را شرح دهید.

پدیده برخورد یا Collision در کدام یک از انواع توپولوژی روی می دهد؟ چرا؟

در کدام یک از انواع توپولوژی، با قطع شدن قسمتی از کابل، کل شبکه از کار می افتد؟

انواع توپولوژی ها را از لحاظ مصرف کابل، سرعت، هزینه، عیب یابی و اشکال زدایی مقایسه کنید.

انواع محیط های انتقال سیمی یا کابلی را از لحاظ سرعت، امنیت، هزینه، مسافت و نویز بررسی کنید.

حداقل فاصله بین کابل شبکه و کابل برق باید چقدر باشد؟

عوامل موثر در تعیین نوع کابل را نام ببرید.

سرعت کدام یک از روش های دسترسی به خط بیشتر است؟ دلیل آن را بنویسید.

چه عواملی در سرعت دسترسی به خط موثر است؟

تحقیق کنید که آیا می توان در کابل کشی یک شبکه از همه انواع کابل (مانند Cat5، Cat6،

Fiber و ...) استفاده کرد؟ سرعت و راندمان شبکه در این حالت چگونه است؟

تحقیق کنید که برای اتصال چندین Switch یا HUB از چه نوع کابلی باید استفاده گردد؟

## فصل چهارم - معماری شبکه

هدف های رفتاری

انواع معماری شبکه و ویژگیهای آن ها را شرح دهد.  
تکنولوژی FDDI را تعریف کند.

معماری شبکه ، استانداردهایی که برای نحوه اتصال کامپیوتر ها با یکدیگر و نحوه ارسال اطلاعات تعریف شده است . در این استانداردها نوع کابل شبکه ، اتصالات ، توپولوژی ، نحوه دسترسی به خطوط انتقال و سرعت انتقال مشخص شده است .

4-1- انواع معماری شبکه و ویژگی های آن ها

چندین نوع معماری شبکه وجود دارد که هنگام راه اندازی شبکه از آن ها استفاده می شود .  
انواع معماری شبکه عبارتند از :

اترنت<sup>۱۳</sup>

Token Ring

4-1-1- اترنت

اترنت یکی از انواع متداول معماری شبکه است . در این معماری از روش CSMA/CD برای دسترسی به خط انتقال یا همان کابل شبکه استفاده می شود . توپولوژی پیش فرض برای اترنت ، توپولوژی فیزیکی خطی تعریفی شده است . توپولوژی های شبکه مثل توپولوژی خطی که از توپولوژی منطقی خطی استفاده می کنند از اترنت بهره می برند . نوع کابلی که در هر توپولوژی استفاده می شود نیز در قوانین همان توپولوژی مشخص شده است .  
توپولوژی های مختلف اترنت عبارتند از :

10Base2

10Base5

10BaseT

10Base FL

100VG-ANYLAN

100Base x

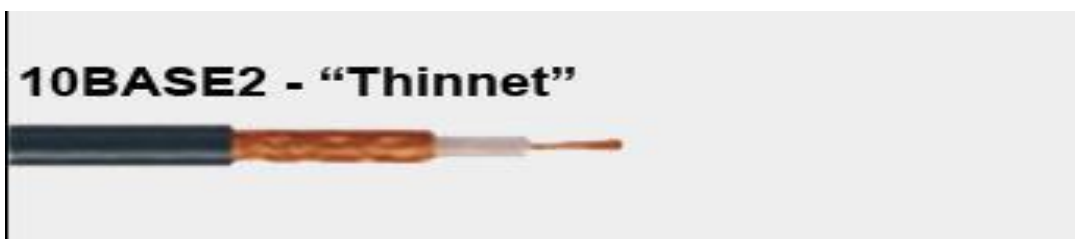
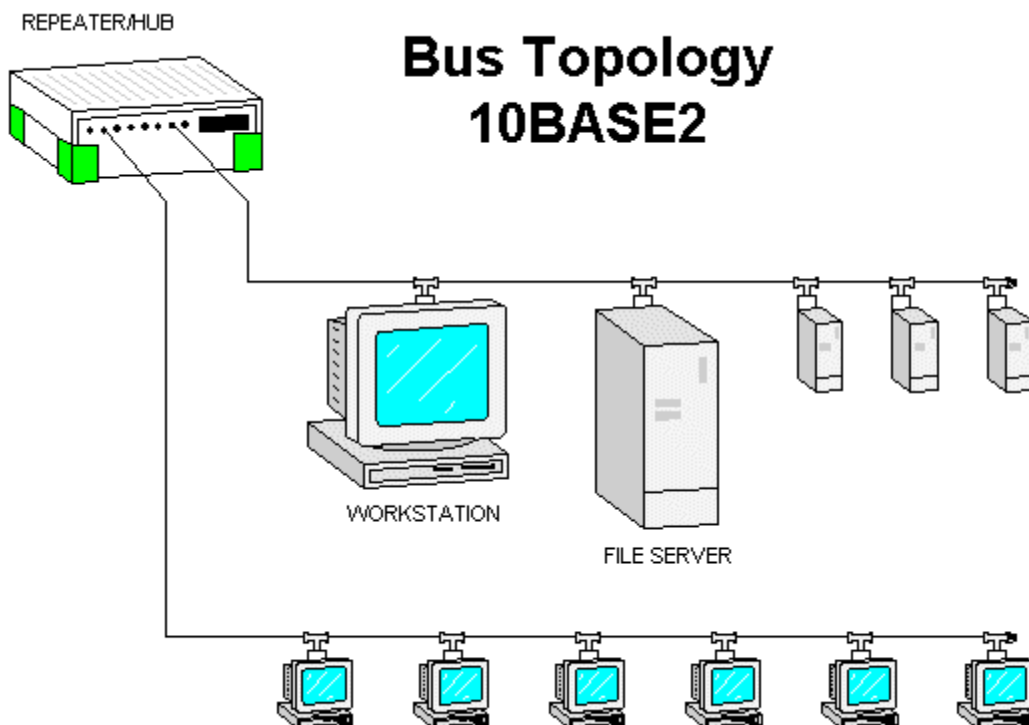
---

<sup>۱۳</sup> - Ethernet

تکته : در استانداردهایی که نام برده شد ، عدد اول نمایانگر سرعت انتقال است  
مثلاً 10Base2 با سرعت 10bps کار می کند. Base نشان دهنده Base band بودن توپولوژی و عبارت پس از آن نوع کابل را نشان می دهد.  
در معماری اترنت علاوه بر موارد ذکر شده نحوه ساخته شدن بسته های اطلاعاتی ، اندازه آن ها ، اطلاعات اضافی که باید در بسته های اطلاعاتی قرار گیرد و کابل کشی شبکه مشخص شده است . در ادامه برخی از استانداردهای متداول توضیح داده خواهد شد .  
استانداردهای IEEE

#### 10Base2 :

10Base 2 برای انتقال داده ها از کابل هم محور Thinnet استفاده می کند که مشخصات این کابل در فصل دوم توضیح داده شد . کانکتورهای این شبکه از نوع BNC بوده و دوسر کابل باید به وسیله ی Terminator مسدود شود تا شبکه فعال شود . از مزایای 10Base 2 نصب ساده و هزینه راه اندازی بسیار کم آن است . توپولوژی 10Base2 همان توپولوژی خطی است .  
قوانینی که در 10Base 2 باید رعایت شود ، عبارتند از :  
حداقل طول کابلی که کامپیوترها را به هم متصل می کند نباید کمتر از 0/5 متر باشد.  
برای اتصال T-connector به کامپیوتر نباید از استفاده کرد و باید آن را مستقیماً به کامپیوتر متصل نمود.  
فاصله اولین و آخرین کامپیوتر در شبکه نباید بیش از 185 متر باشد . این فاصله از روی اندازه کابل اندازه گیری می شود .  
با استفاده از هاب یا Repeater می توان حداکثر فاصله بین اولین و آخرین کامپیوتر را تا 925 متر افزایش داد کامپیوترها نباید خارج از این محدوده باشند.  
در فواصل بین هر دو Repeater نمی توان بیش از 30 دستگاه کامپیوتر به شبکه متصل کرد.  
ابتدا و انتهای کابل باید با Terminator مسدود شود . Terminator شبکه 10Base2 ، یک مقاومت 50 اهمی است که سیگنال های الکتریکی به وجود آمده در کابل شبکه را مصرف کرده و از باقی ماندن آن در شبکه جلوگیری می کند.  
برای دست یافتن به حداکثر فاصله کامپیوترها یعنی 925 متر، پنج Segment خواهیم داشت که با چهار دستگاه Repeater به هم متصل شده اند که فقط از سه Segment آن می توان استفاده کرد . این Segment ها شماره های 1، 2 و 5 هستند . این قانون به قانون 3-4-5 معروف است .



شکل 4-1

10Base 5 :

در 10Base 5 از کابل کواکسیال Thicknet برای اتصال کامپیوترها به یکدیگر استفاده می شود.

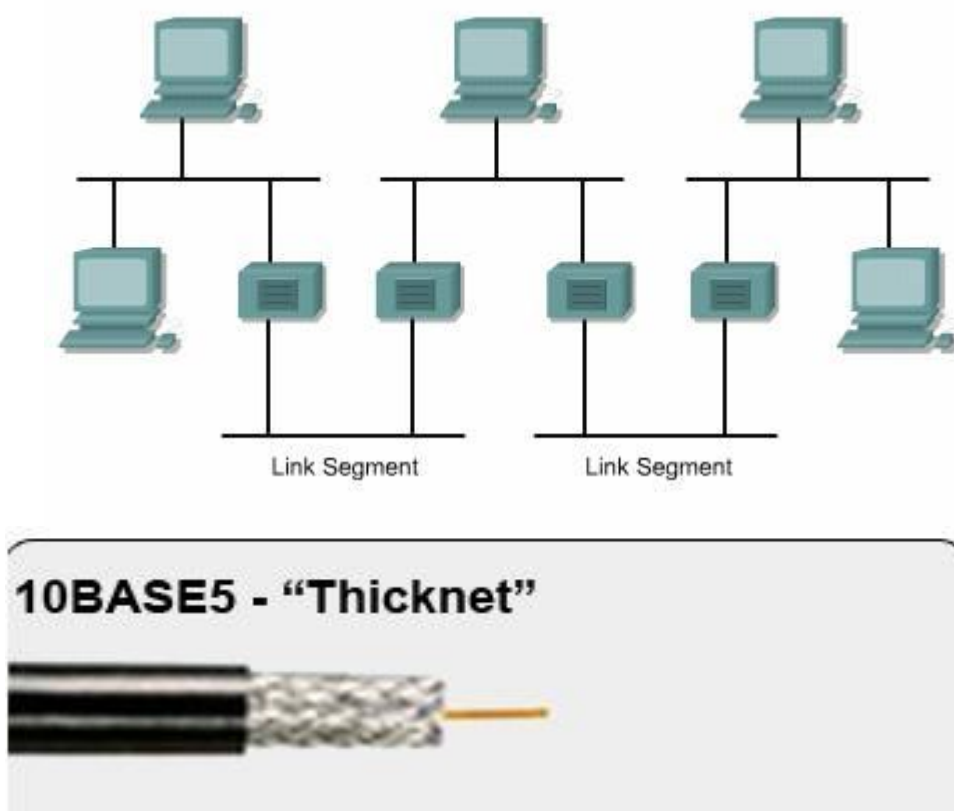
هر کامپیوتر به وسیله ی یک کابل AUT یا DIX به یک عدد Transceiver که به کابل شبکه متصل شده است ، وصل می شود و هر دو انتهای کابل با Terminator مسدود می شود . اولین مزیت :

10Base5 مسافت نسبتا زیادی است که تحت پوشش خود قرار میدهد . قوانینی که در مورد 10Base5 وجود دارد عبارتند از :

حداقل طول کابل که برای اتصال دو کامپیوتر استفاده می شود 2/5 متر است .

حداکثر طول کابل یا حداکثر فاصله بین اولین و آخرین کامپیوتر شبکه 500 متر است .

حداکثر فاصله بین اولین و آخرین کامپیوتر شبکه با استفاده از Repeater 2500 متر است یکی از Terminator ها باید به زمین متصل شود .  
اندازه کابلی که کامپیوتر را به Transceiver متصل می کند ، نباید بیشتر از 50 متر باشد .  
حداکثر تعداد کامپیوترها در هر Segment 100 دستگاه است .  
قانون 3-4-5 در مورد 10Base 5 نیز صادق است .



شکل 4-2

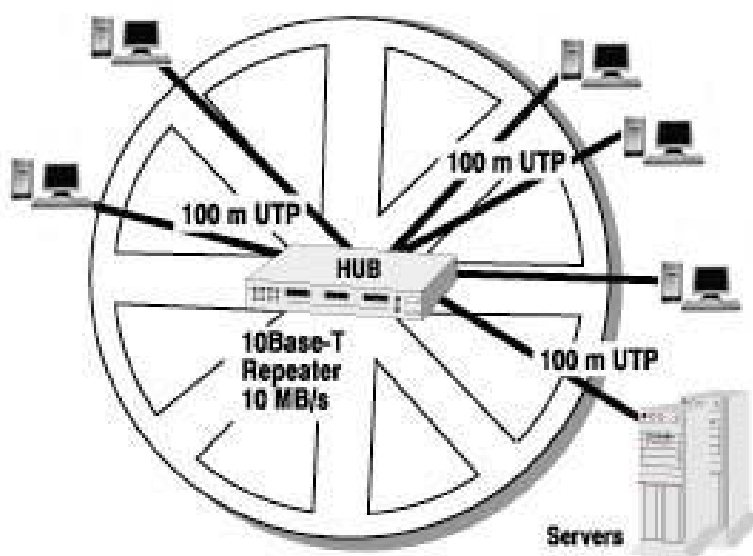
10Base T :

برای راه اندازی شبکه 10Base T از کابل های TP یا زوج به هم تاییده استفاده می شود که حداکثر سرعت آن 10Mbps است. در این استاندارد هر کامپیوتری که می خواهد به شبکه متصل شود مستقیماً به وسیله ی یک کابل به هاب وصل شده و هاب ، ارتباط کامپیوترها را برقرار می کند . اتصالات این توپولوژی از نوع RJ-45 است. Segment های مختلف می توانند به وسیله ی کابل های کواکسیال یا فیبر نوری به یکدیگر متصل شوند. برخی از انواع دستگاه هایی که می توانند جایگزین هاب شوند ، هوشمند بوده و می توانند ترافیک شبکه را کنترل کرده و

آن را کاهش دهند . از مشخصه های بارز این شبکه گران قیمت بودن هزینه راه اندازی و نصب آن است. 10BaseT در ظاهر یک شبکه ستاره ای است ولی عملکرد آن همانند شبکه های خطی می باشد در این مورد به طور خلاصه می توان گفت توپولوژی فیزیکی آن ، ستاره ای ولی توپولوژی منطقی آن خطی است .  
قوانین 10BaseT عبارتند از:

حداکثر تعداد کامپیوتری که این شبکه به هم متصل می کند ، 1024 دستگاه کامپیوتر است.

کابل ها باید از نوع زوج به تاییده Category3، Category4، یا Category5 باشند ( نوع کابل از نظر داشتن محافظ تفاوتی نمی کند ، می توان از هر دو کابل UTP یا STP استفاده کرد ).  
حداکثر فاصله هر کامپیوتر تا هاب ، 100 متر است .  
حداقل طول کابل ( فاصله بین کامپیوتر تا هاب ) 2/5 متر است .



شکل 3-4



## 10Base FL :

10Base FL یکی از خصوصیات شبکه اترنتی است که برای انتقال اطلاعات از فیبر نوری استفاده می کند . سرعت انتقال در این شبکه 10Mbps است . مهم ترین 10Base FL مسافت زیادی است که تحت پوشش قرار می دهد . این مسافت 2 کیلومتر است . از مزایای دیگر این شبکه این است که عوامل خارجی ، تأثیری روی اطلاعات داخل فیبر ندارند . به عبارت دیگر ، در فیبر نوری هم شنوایی و جود ندارد و اطلاعات سالم به مقصد می رسد .

دو استاندارد دیگر به نام های 10Base FB و 10Base FP نیز مورد استفاده قرار می گیرد . 10Base FB یک شبکه اترنت هم زمان است 14 و برای اتصال دو تقویت کننده فیبر نوری به یکدیگر که در مسیر بین دو ایستگاه قرار دارد ، استفاده می شود . استاندارد دیگر 10BASE FP است که یک شبکه ستاره ای با استفاده از فیبر نوری می باشد که برای Backbone شبکه ها مورد استفاده قرار می گیرد . در 10Base FP نور به جای سیگنال های الکترونیکی مسئولیت انتقال اطلاعات را برعهده دارد .

## 100Base X :

100BaseX شبکه همانند شبکه 10BaseT است ( سرعت این شبکه 100Mbps است ) با این تفاوت که 100BaseX با سه مدل کابل کشی متفاوت مورد استفاده قرار می گیرد . این سه مدل عبارتند از :

100Base TX: در این مدل از دو کابل category از نوع UTP یا STP به صورت همزمان استفاده می شود.

100Base FX: در این مدل از دورشته فیبر نوری در کنار هم استفاده می شود.

100Base T4: در این مدل 4 رشته کابل 5 یا 4, 3 Category در کنار هم استفاده می شود .

100Base X: بانام Fast Ethernet نیز شناخته می شود.

و 100BaseX این استاندارد ، شبکه ای را توضیح می دهد که در آن سرعت انتقال اطلاعات یک گیگابایت در ثانیه است و برای انتقال اطلاعات از فیبر نوری استفاده می شود. این استاندارد خود از چند قسمت تشکیل شده است که عبارتند از :

1000Base sx

1000Base LX/LH

1000Basezx

---

<sup>۱۴</sup> - Synchronous Ethernet

تفاوت استاندارد های ذکر شده در طول کابل ها و نوع فیبر نوری است که در آن ها استفاده می شود.

1000Base T :

در این استاندارد، از کابل های زوج به هم تاییده برای راه اندازی شبکه ای با سرعت یک گیگابیت در ثانیه استفاده می شود. این کابل ها از نوع Cat5 و کانکتورهای آن نیز از نوع RJ-45 است. نحوه ارسال اطلاعات در این استاندارد به گونه ای است که سیستم، توانایی انتقال اطلاعات با سرعت یک گیگابیت در ثانیه را پیدا می کند. کابل Cat5 نام دیگر کابل زوج به هم تاییده است.

محدودیت های اترنت :

یک شبکه اترنت دارای محدودیت های متفاوت از ابعاد گوناگون (بکارگیری تجهیزات) است. طول کابلی که تمام ایستگاهها بصورت اشتراکی از آن بعنوان محیط انتقال استفاده می نمایند یکی از شاخص ترین موارد در این زمینه است. سیگنال های الکتریکی در طول کابل بسرعت منتشر می گردند. همزمان با طی مسافتی، سیگنال ها ضعیف می گردند. وجود میدان های الکتریکی که توسط دستگاههای مجاور کابل نظیر لامپ های فلورسنت ایجاد می گردد، باعث تلف شدن سیگنال می گردد. طول کابل شبکه می بایست کوتاه بوده تا امکان دریافت سیگنال توسط دستگاه های موجود در دو نقطه ابتدائی و انتهائی کابل بصورت شفاف و با حداقل تاخیر زمانی فراهم گردد. همین امر باعث بروز محدودیت در طول کابل استفاده شده، می گردد

تولید کنندگان تجهیزات شبکه دستگاه های متفاوتی را بمنظور غلبه بر مشکلات و محدودیت گفته شده، طراحی و عرضه نموده اند. اغلب دستگاههای فوق مختص شبکه های اترنت نبوده ولی در سایر تکنولوژی های مرتبط با شبکه نقش مهمی را ایفاء می نمایند.

یکی از این دستگاهها پل ( Bridge ) می باشد :

Bridge :

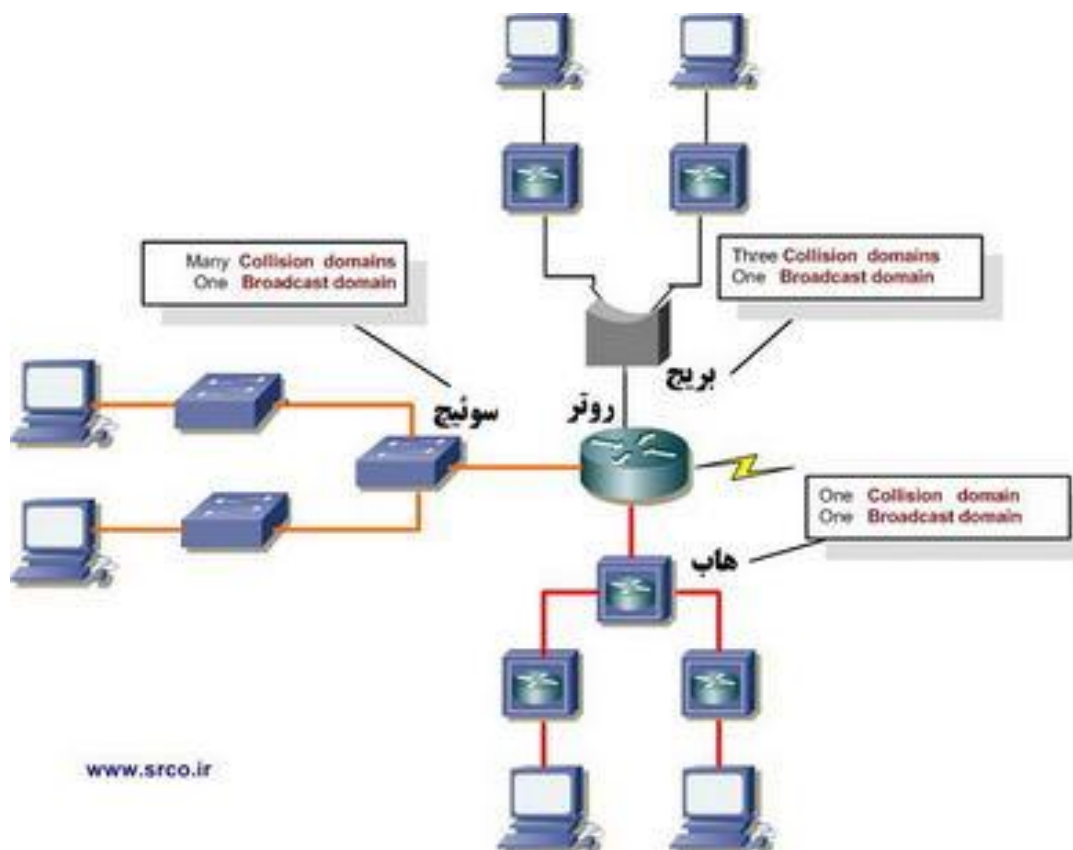
از واژه bridging قبل از پیاده سازی هاب و روتر، استفاده می گردید. بنابراین طبیعی است که برخی افراد از bridge به عنوان سوئیچ یاد کنند. در واقع، سوئیچ و bridge دارای عملکردی مشابه می باشند ( کلیات کار ). دو دستگاه فوق، collision domain در یک شبکه محلی را تفکیک می نمایند. این بدان معنی است که سوئیچ اساساً یک bridge چندین پورت با قدرک ادااراک بیشتری است. علی رغم وجود شباهت های زیاد بین سوئیچ و bridge، تفاوت هایی نیز در این رابطه وجود دارد. به عنوان نمونه سوئیچ ها به منظور انجام وظایف خود

دارای امکانات مدیریتی و قابلیت های پیشرفته ای می باشند . در اغلب موارد bridge صرفاً دارای یک ، دو و یا چهار پورت می باشد.

از bridge زمانی در شبکه استفاده می شود که هدف کاهش collision در broadcast domain و افزایش collision domain در شبکه است . در چنین وضعیتی bridge پهنای باند بیشتری را برای کاربران ارائه می نماید. یکی از مزایای اولیه bridging ، افزایش پهنای باند قابل دسترس بر روی یک سگمنت شبکه است ، چراکه با این کار تعداد دستگاه های موجود در یک collision domain کاهش می یابد .

استفاده از روتر ، سوئیچ و bridge در شبکه

شکل زیر نحوه استفاده از تجهیزات شبکه ای فوق را در یک شبکه فرضی نشان می دهد . در شکل فوق سه شبکه فرضی ( شبکه متصل شده از طریق هاب در قسمت پائین شکل ، شبکه متصل شده از طریق سوئیچ در قسمت سمت چپ شکل و شبکه متصل شده از طریق bridge در قسمت بالای شکل ) از طریق روتر به یکدیگر متصل شده اند .



## توضیحات :

همانگونه که در شکل فوق مشاهده می نمائید از روتر در مرکز شبکه استفاده شده است . علت این کار استفاده از فناوری های قدیمی تر نظیر هاب و bridge است . در صورتی که صرفاً از سوئیچ استفاده گردد ، در سناریوی فوق تغییرات عمده ای ایجاد خواهد شد .

در شبکه های جدید می توان سوئیچ را در مرکز شبکه قرار داد و از روتر برای اتصال شبکه های منطقی به یکدیگر استفاده نمود . در صورتی که قصد پیاده سازی اینچنین شبکه هائی را داشته باشیم ، می بایست شبکه های محلی مجازی ( VLANs ) را ایجاد نمود .

در قسمت بالای شکل فوق از یک bridge استفاده شده است تا به کمک آن هر دو هاب به روتر متصل شوند . همانگونه که در متن این مقاله اشاره گردید ، bridge باعث تفکیک collision domain می گردد ولی تمامی هاست های متصل شده به هر دو هاب همچنان در یک broadcast domain مشابه قرار می گیرند . همچنین ، bridge فوق صرفاً دو collision domain را ایجاد کرده است . بنابراین هر دستگاه متصل شده به یک هاب در یک collision domain مشابه قرار می گیرد .

در قسمت پائین شکل فوق ، سه عدد هاب متصل شده به هم به روتر متصل شده اند . وضعیت فوق باعث ایجاد یک collision domain بزرگ و یک broadcast domain بزرگ می شود ( یک بهم ریختگی بزرگ ) .

بهترین شبکه متصل شده به روتر ، شبکه متصل شده از طریق سوئیچ موجود در قسمت سمت چپ شکل فوق است . چرا ؟ چون هر پورت موجود بر روی سوئیچ باعث تفکیک collision domain می گردد . ولی این یک وضعیت مطلوب نمی باشد چون تمامی دستگاه ها همچنان در یک broadcast domain مشابه قرار داشته و می بایست به تمامی broadcast ارسالی گوش فرا دهند و اگر broadcast خیلی بزرگ باشد ، کاربران پهنای باند کمتری را داشته و می بایست broadcast بیشتری را پردازش نمایند . ماحصل این وضعیت ، کاهش زمان پاسخ شبکه به کاربران خواهد بود .

بهترین شبکه ، شبکه ای است که به درستی پیکربندی و منطبق بر نیاز یک سازمان باشد . سوئیچ ها به همراه روترها زمانی که به درستی در یک شبکه کنار هم قرار داده شوند ، طراحی شبکه بهترین وضعیت ممکن را پیدا خواهد کرد .

در شبکه فوق ، نه collision domain و نه broadcast domain وجود دارد .

مشاهده broadcast domain در شکل فوق ساده است چراکه روتر به صورت پیش فرض broadcast domain را تفکیک می نماید و از آنجائی که روتر فوق دارای سه اتصال است ، سه domain broadcast ایجاد می گردد .

مشاهده collision domain در شکل فوق به سادگی domain broadcast نمی باشد . تمامی

شبکه متصل شده از طریق هاب دارای یک collision domain است. شبکه متصل شده از طریق bridge شامل سه collision domain و شبکه متصل شده از طریق سوئیچ شامل پنج collision domain است (یکی برای هر پورت سوئیچ). بنابراین در مجموع نه collision domain در شبکه فوق وجود دارد.

در بخش دوم به بررسی طراحی یک مدل آدرس دهی IP منطبق بر طراحی شبکه خواهیم پرداخت.

## : Bridge

وسیله ایست که دو Lan مختلف یا دو سگمنت از یک Lan را که از پروتکل ارتباطی یکسانی استفاده می کنند، به یکدیگر متصل می سازد Bridge. توانایی کنترل ترافیک، فیلتر کردن بسته های داده و ... را دارد. توسط Bridge می توان یک Lan با تعداد ایستگاههای کاری زیاد را به سگمنت های کوچکتری تقسیم کرد که در نتیجه هر سگمنت مانند یک شبکه مستقل عمل کرده و برقراری ارتباط ایستگاهها راحت تر انجام می شود. هر گاه دو ایستگاه بطور همزمان اقدام به ارسال بسته های داده در شبکه کنند، تصادم (collision) رخ می دهد که مانع ارسال صحیح داده می شود و هر چه تعداد ایستگاهها بیشتر باشد، احتمال رخ دادن تصادم نیز بیشتر می گردد. Bridge با تقسیم شبکه به چندین سگمنت از احتمال رخ دادن تصادم می کاهد. همچنین اگر پیامی از یک ایستگاه برای ایستگاهی دیگر در همان سگمنت ارسال شود Bridge مانع انتشار پیام در سگمنت های دیگر شده و بار ترافیک سایر سگمنت ها را سنگین نمی کند.

## Token Ring 4-1-2

شبکه Token Ring از نظر ظاهری یک شبکه ستاره ای است ولی به صورت Token Passing کار می کند. در این شبکه یک حلقه منطقی به وجود می آید و Token در امتداد حلقه حرکت کرده و به کامپیوترها می رسد. هر کامپیوتری که به ارسال اطلاعات نیاز داشته باشد، Token را نگه داشته و اطلاعات خود را به سوی مقصد ارسال می کند. اطلاعات ارسال شده در همان حلقه مجازی و در امتداد حرکت Token مسیر خود را طی می کند تا به کامپیوتر مقصد برسد. کامپیوتر مقصد در صورت صحیح بودن اطلاعات ارسالی، در جواب یک بسته به نام Acknowledge به کامپیوتر مبدأ ارسال می کند. کامپیوتر مبدأ نیز Token اصلی را از بین برده و یک Token جدید تولید می نماید و آن را در امتداد مسیر Token قبلی به حرکت در می آورد. این روند به همین صورت ادامه خواهد یافت.

در شبکه Token Ring در محل اتصال کامپیوترها به جای هاب از دستگاهی به نام MAU استفاده می‌شود. سرعت انتقال اطلاعات در این شبکه 4Mbps یا 16Mbps است. کارت‌های 16Mbps می‌توانند با سرعت 4Mbps نیز فعالیت کنند.



شکل 4-4

در شبکه Token Ring از کابل‌های زوج به هم تاییده استفاده می‌شود. اگر از کابل UTP در این توپولوژی استفاده شود، حداکثر طول کابل می‌تواند 45 متر باشد و این شبکه فقط با سرعت 4 مگابیت در ثانیه کار می‌کند و اگر از کابل STP استفاده شود، حداکثر طول کابل 101 متر و با سرعت 16 مگابیت در ثانیه اطلاعات منتقل می‌شود.

#### FDDI 4-2

FDDI، تکنولوژی یک شبکه با سرعت 100 مگابیت در ثانیه است که برای ارتباط از فیبر نوری استفاده می‌کند. در این تکنولوژی به جای فیبر نوری می‌توان از کابل مسی نیز استفاده کرد ولی در صورت استفاده از کابل مسی حداکثر فاصله مجاز در شبکه کمتر می‌شود. FDDI به عنوان Backbone در محل‌هایی که تعداد زیادی کامپیوتر در آن قرار دارد، استفاده می‌شود. از جمله این محیط‌ها می‌توان به دانشگاه‌ها اشاره کرد. در FDDI می‌توان 500 گره را در مسافت 100 کیلومتر به یکدیگر متصل کرد. توپولوژی فیزیکی این شبکه حلقوی است. نحوه به وجود آمدن این حلقه به این صورت است که یک حلقه 100 کیلومتری از فیبر نوری ساخته می‌شود و در هر 2 کیلومتر یک تقویت کننده قرار می‌گیرد. برای جلوگیری از اختلالاتی که در اثر قطع شدن فیبر نوری به وجود می‌آید، از دو حلقه فیبر نوری در کنار هم استفاده می‌شود تا در صورتی که یکی از رشته‌ها قطع شود، رشته دوم وارد عمل شده و جایگزین رشته اول شود.

### خود آزمایی و تحقیق

- 1- انواع معماری شبکه را نام ببرید و ویژگیهای هر یک را از لحاظ حداقل و حداکثر طول کابل بین دو کامپیوتر، سرعت و نوع کابل و تجهیزات جانبی بررسی کنید.
- 2- FDDI چیست؟
- 3- برای جل گیری از اختلالاتی که در اثر قطع شدن فیبرنوری به وجود می آید، چه باید کرد؟
- 4- تفاوت اصلی استانداردهای IEEE در چیست؟
- 5- تحقیق کنید که تفاوت MAU و HUB در چیست؟