شبکه های کامپیوتری

مرتضی خدادادپور

mo_khodadad@yahoo.com
Telegram.me/chamranet

شبکه های کامپیوتری

- مجموعه ای از کامپیوترهای مستقل است که به نحوی با یکدیگر داده و اطلاعات رد و بدل می کنند.
- به مجموعه ای از کامپیوتر های مستقل و متصل به هم، شبکه گفته می شود.
- در سیستم های توزیع شده، کامپیوترها متصل هستند ولی مستقل نیستند ولی در شبکه علاوه بر اینکه کامپیوترها متصل به یکدیگرند ،از همدیگر مستقل نیز می باشند.
- یک شبکه کامپیوتری شامل دو یا بیش از دو کامپیوتر و ابزارهای جانبی مثل چاپگرها، اسکنرها و مانند اینها هستند که بطور مستقیم به منظور استفاده مشترک از سخت افزار، نرم افزار، منابع اطلاعاتی و ابزارهای متصل ایجاده شده است.
- تمامی تجهیزات سخت افزاری و نرم افزاری موجود در شبکه را منبع گویند .

اهداف شبکه های کامپیوتری

- **استفاده مشترک از منابع :**

استفاده مشترک از یک منبع اطلاعاتی یا امکانات جانبی رایانه، بدون توجه به محل جغرافیایی هریک از منابع .

- **کاهش هزینه:**

متمرکز نمودن منابع و استفاده مشترک از آنها و پرهیز از پخش آنها در واحدهای مختلف و استفاده اختصاصی هرکاربر در یک سازمان، کاهش هزینه را در پی خواهد داشت.

- **ارتباطات:**

کاربران می توانند از طریق نوآوریهای موجود مانند پست الکترونیکی و یا دیگر سیستم های اطلاع رسانی پیغام هایشان را مبادله کنند ؛ حتی امکان انتقال فایل نیز وجود دارد.

اهداف شبکه های کامپیوتری

- **قابلیت اطمینان:**

به این معنا که می توان از منابع گوناگون اطلاعاتی و سیستم ها در شبکه، نسخه های دوم و پشتیبان تهیه کرد و در صورت عدم دسترسی به یکی از منابع اطلاعاتی، از نسخه های پشتیبان استفاده کرد.

- **کاهش زمان :**

یکی دیگر از اهداف ایجاد شبکه های رایانه ای، ایجاد ارتباط قوی بین کاربران از راه دور است ؛ یعنی بدون محدودیت جغرافیایی تبادل اطلاعات وجود داشته باشد. به این ترتیب زمان تبادل اطلاعات و استفاده از منابع ،خود بخود کاهش می یابد.

- **قابلیت توسعه:**

یک شبکه محلی می تواند بدون تغییر در ساختار، توسعه یابد و تبدیل به یک شبکه بزرگتر شود.

- **کامپیوترهای شخصی اگر چه خیلی قدرتمند هستند ولی با این وجود و بنا بر موارد زیر، برای انجام کارهای خیلی بزرگ در ادارات و بانکها، آنها را به صورت شبکه به هم وصل می کنند :**
  - **امکان دسترسی همه کاربران به اطلاعات اصلی در کامپیوتر اصلی (server)**
  - **امکان انتقال اطلاعات به صورت خودکار بین کامپیوتر های شبکه**
  - **امکان تبادل پیام بین کاربران شبکه**
  - **امکان اشتراک تجهیزات گران قیمت مثل چاپگر و پلاتر**

کاربرد شبکه های کامپیوتری

۱	دسترسی به بانک های اطلاعاتی راه دور	Remote Access
۲	پست الکترونیکی	E-Mail
۳	خدمات انتقال فایل	File Transfer
۴	ورود به سیستم از راه دور	Remote Login
۵	گروه های خبری	News Groups
۶	جستجوی اطلاعات مورد نیاز	Information Seek
۷	تبلیغات	Advertisement
۸	تجارت الکترونیکی	E-Commerce
۹	بانکداری الکترونیکی	E-Banking

کاربرد شبکه های کامپیوتری

Entertainment	سرگرمی و محاوره	۱۰
Electronic magazine	مجلات و روزنامه های الکترونیکی	۱۱
Face to Face Conversation	محاوره ی مستقیم از راه دور	۱۲
Teleconference	کنفرانس از راه دور (ویدئویی)	۱۳
People Finding	یافتن اشخاص مورد نظر در جهان	۱۴
Fax	تلفن و دورنگاراز طریق شبکه	۱۵
	رادیو و تلویزیون از طریق شبکه	۱۵
	آموزش از راه دور	۱۷
	ارائه مدون اطلاعات فنی و عملی	۱۸

اصطلاحات شبکه کامپیوتری

- **DTE** (Data Terminal Equipment): منبع و گیرنده داده ها را در شبکه های رایانه ای میگویند.
- **DCE** (Data Communication Equipment): تجهیزاتی که مشخصات الکتریکی داده ها را با مشخصات کانال داده ها تطبیق می دهد مانند مودم.
- **BW**(Band width): پهنای باند یامحدوده ای که درآن امواج آنالوگ بدون هیچ افتی حرکت میکنند.
- **Noise**: نویز یا پارازیت به امواج الکتریکی مزاحم می گویند که موجب اختلال درانتقال داده ها میشود.
- **Bps**: سرعت انتقال داده ها یا بیت در ثانیه.
- **Share**: به اشتراک گذاری داده ها و منابع سخت افزاری برای استفاده همه کامپیوتر های موجود در شبکه.

اصطلاحات شبکه کامپیوتری

- **WLAN**(Wireless Lan): شبکه های محلی بی سیم.
- **AP**(Access Point): دستگاهی که یک کامپیوتر بی سیم را به یک شبکه LAN وصل می کند.
- **Cell**: محدوده ای را که یک AP تحت پوشش دارد را سلول می گویند.
- **Protocol** : قوانین و روالهایی برای ارتباط هستند و یک شبکه برای برقراری ارتباط از این قوانین استفاده می کند.
- **OSI**: این استاندارد برای برقراری ارتباط دو رایانه وظایف را به هفت قسمت تقسیم کرده و به ۷ لایه OSI معروف شده اند و به ترتیب لایه های (فیزیکی - پیوند داده ها – شبکه- انتقال – جلسه - نمایش و کاربردی) می باشند.
- **CSMA/CD**: نوعی روش دسترسی به خط با استفاده از روش گوش دادن به خط.

اصطلاحات شبکه کامپیوتری

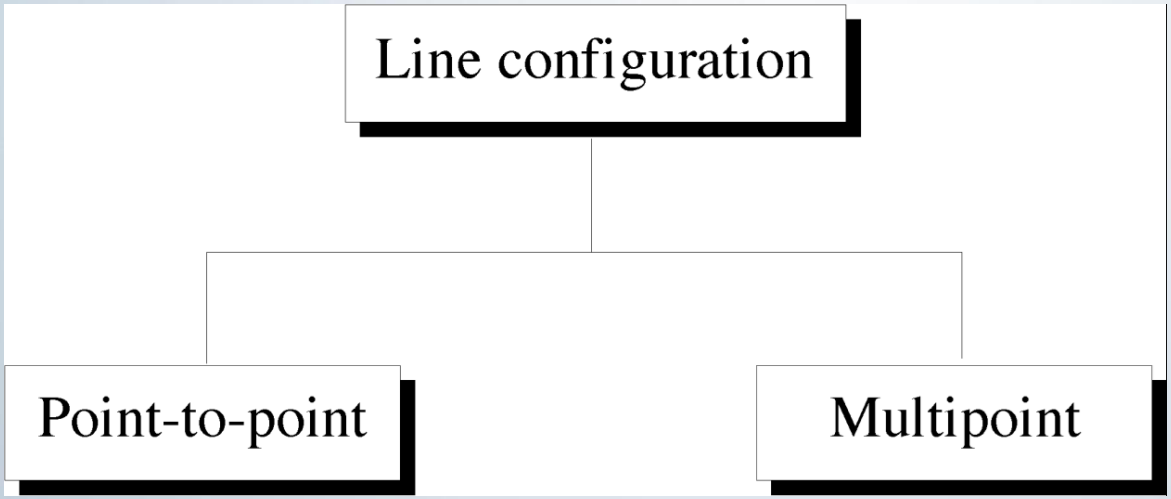
- **Token Ring**: روش عبور نشانه که در شبکه های حلقوی به کار می رود، از انواع روش دسترسی به خط است.
- **LAN**(Local area network):شبکه های محلی و کوچک.
- **MAN**(Metropolitan area network): شبکه های شهری.
- **WAN**(Wide area network): شبکه های گسترده همانند اینترنت.
- **Node**: به هر کامپیوتر وصل به شبکه، گره می گویند.
- **Server**: سرویس دهنده.
- **Client**: سرویس گیرنده.

اصطلاحات شبکه کامپیوتری

- **Peer-to-peer**: شبکه های نظیر به نظیر که در آن هر کامپیوتری هم سرویس دهنده هست و هم سرویس گیرنده.
- **Server-Based**: شبکه های بر اساس سرویس دهنده که در آن یک یا چند کامپیوتر فقط سرویس دهنده و بقیه کامپیوتر ها سرویس گیرنده هستند .
- **Topology**: توپولوژی به طرح فیزیکی شبکه و نحوه آرایش رایانه ها در کنار یکدیگر می گویند.
- **Collision**: برخورد یا لرزش سیگنال ها
- **NIC**: کارت شبکه.

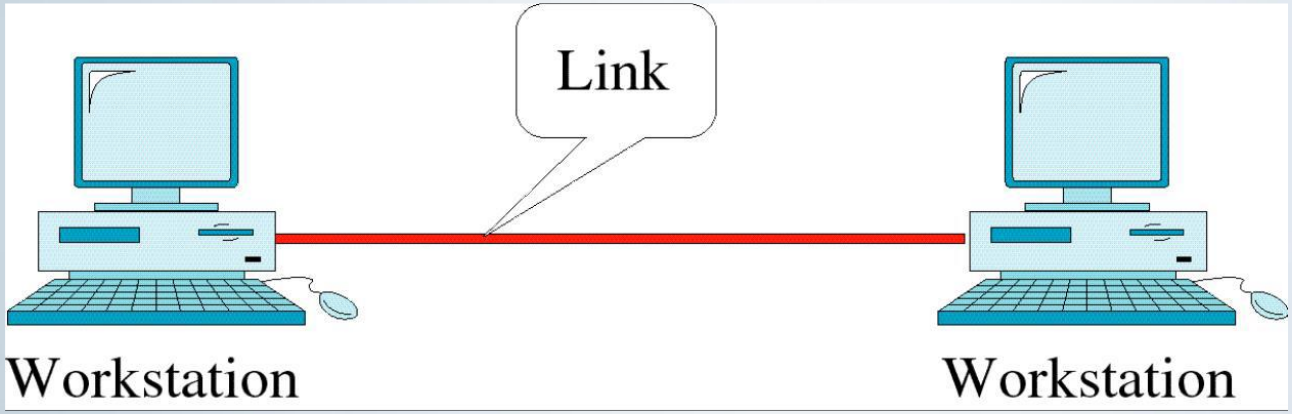
انواع اتصال

- پیکربندی خطوط به دو صورت نقطه به نقطه و یا چند نقطه ای امکان پذیر است



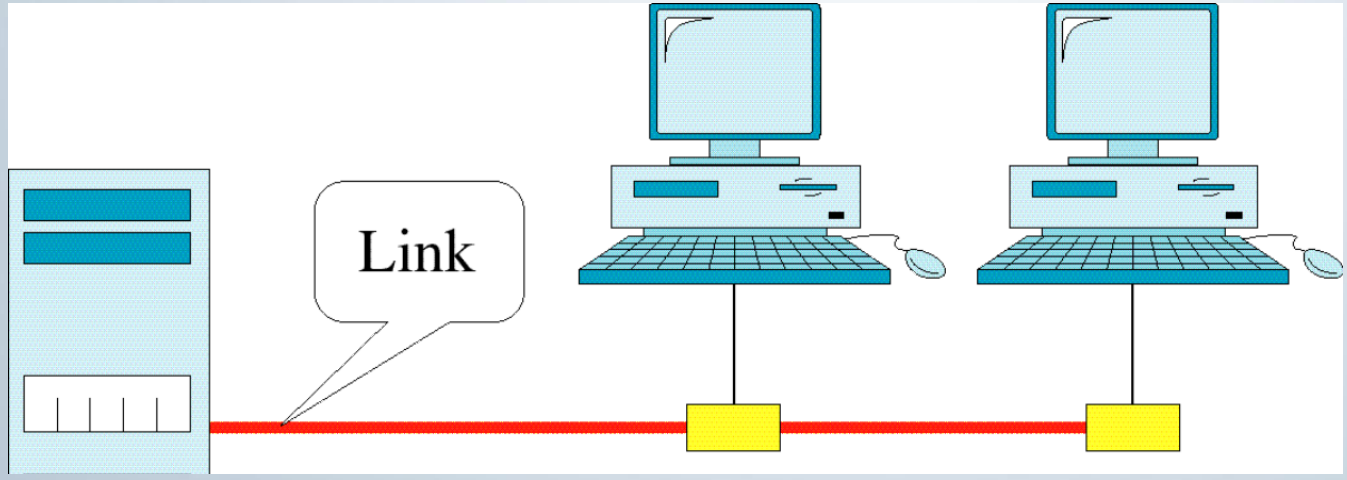
اتصال نقطه به نقطه

- پیکربندی خطوط به صورت نقطه به نقطه:



اتصال چند نقطه ای

- در حالت چند نقطه ای چون محیط اشتراکی است، بحث آدرس دهی مطرح است و اینکه چه کسی باید اطلاعات را بگیرد. بحث دیگری که مطرح است کنترل خط است و اینکه وقتی همه با هم صحبت می کنند ،تداخل اطلاعاتی پیش نیاید.



ابعاد تقسیم بندی شبکه های کامپیوتری

- شبکه های کامپیوتری را بر اساس مولفه های متفاوتی تقسیم بندی می نمایند. در ادامه به برخی از متداولترین تقسیم بندی های موجود اشاره می گردد .
  - تقسیم بندی شبکه براساس نوع وظایف
  - تقسیم بندی شبکه از بعد جغرافیایی
  - تقسیم بندی شبکه ها از بعد تکنولوژی انتقال
  - تقسیم بندی شبکه ها از بعد توپولوژی
  - تقسیم بندی شبکه از بعد نوع سوئیچینگ

براساس نوع وظایف

- کامپیوترهای موجود در شبکه را با توجه به نوع وظایف مربوطه به دو گروه عمده تقسیم می کنند :

  server – سرویس دهندگان

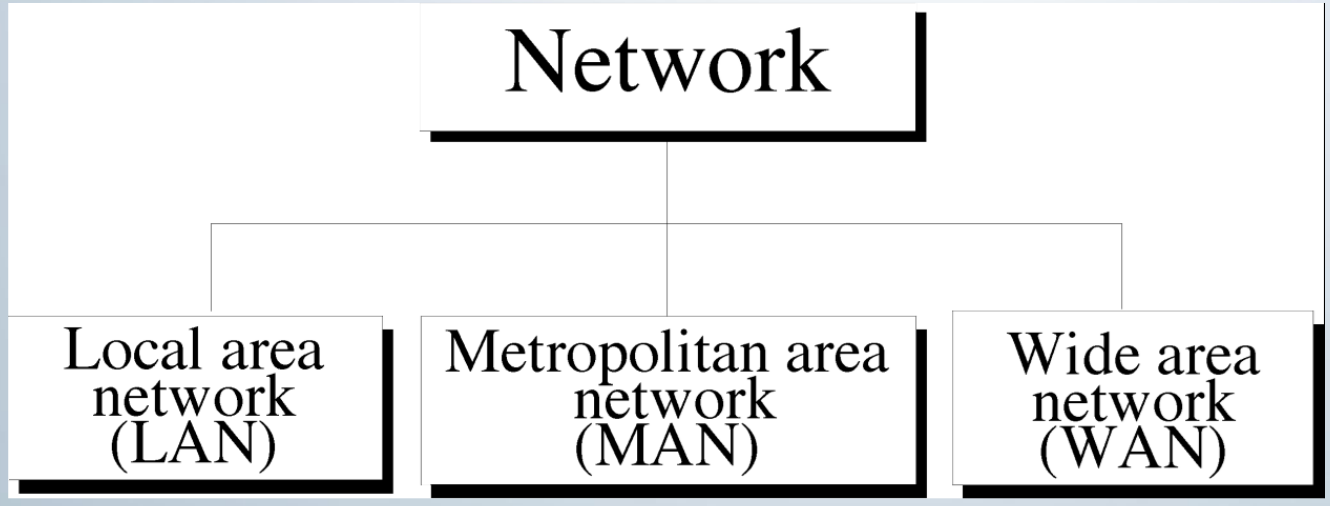
  client – سرویس گیرندگان

- کامپیوترهائی در شبکه که برای سایر کامپیوترها سرویس ها و خدماتی را ارائه می نمایند، سرویس دهنده نامیده می گردند.

- کامپیوترهائی که از خدمات و سرویس های ارائه شده توسط سرویس دهندگان استفاده می کنند، سرویس گیرنده نامیده می شوند .

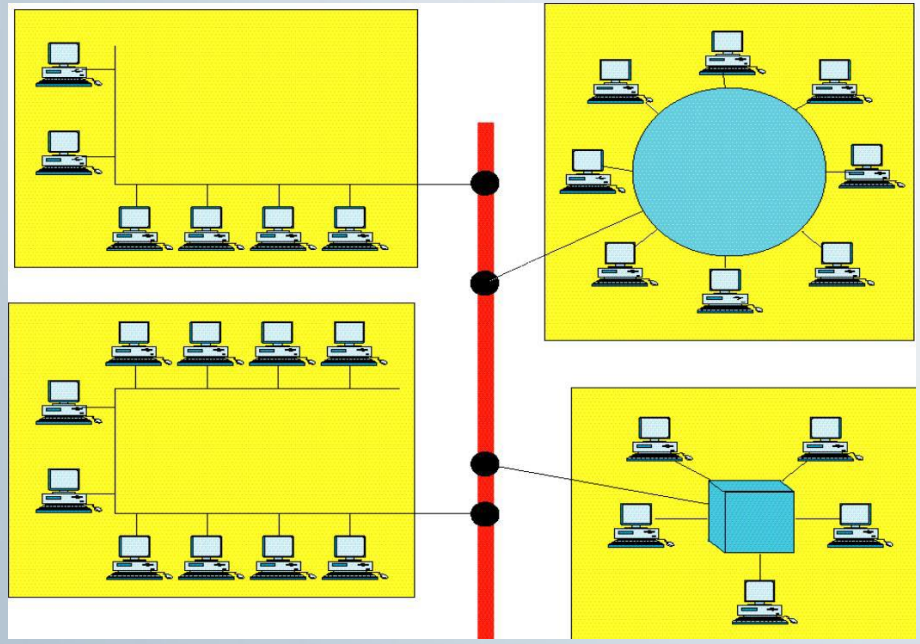
براساس بعد جغرافیایی

- شبکه های کامپیوتری با توجه به حوزه جغرافیائی تحت پوشش به سه گروه تقسیم می گردند:
  - LAN: شبکه های محلی
  - MAN: شبکه های متوسط
  - WAN: شبکه های گسترده



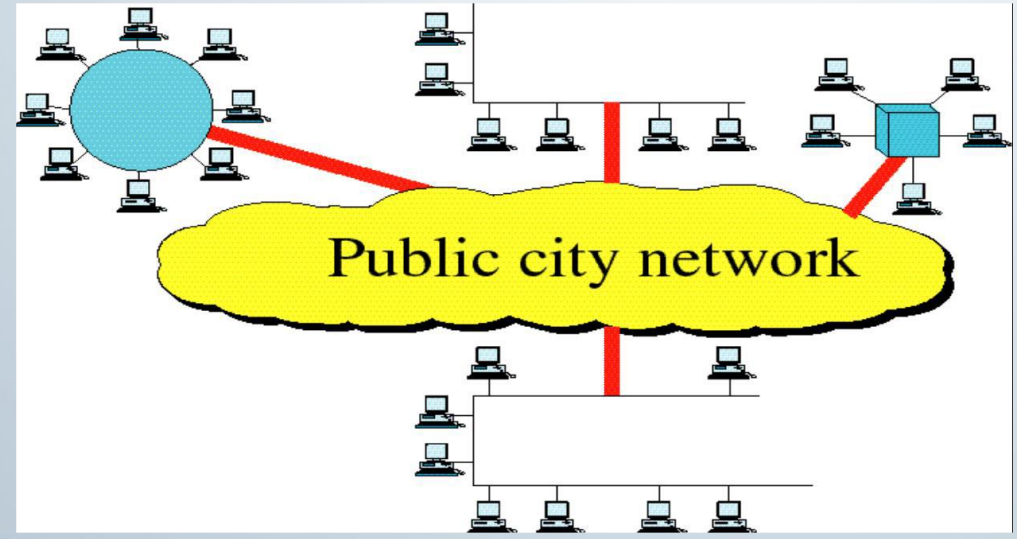
شبکه های LAN

- حوزه جغرافیائی که توسط این نوع از شبکه ها پوشش داده می شود، یک محیط کوچک نظیر یک ساختمان اداری است. این نوع از شبکه ها دارای ویژگی های زیر می باشند :
- توانائی ارسال اطلاعات با سرعت بالا
- محدودیت فاصله
- قابلیت استفاده از محیط مخابراتی ارزان نظیر خطوط تلفن بمنظور ارسال اطلاعات
- نرخ پایین خطاء در ارسال اطلاعات با توجه به محدود بودن فاصله



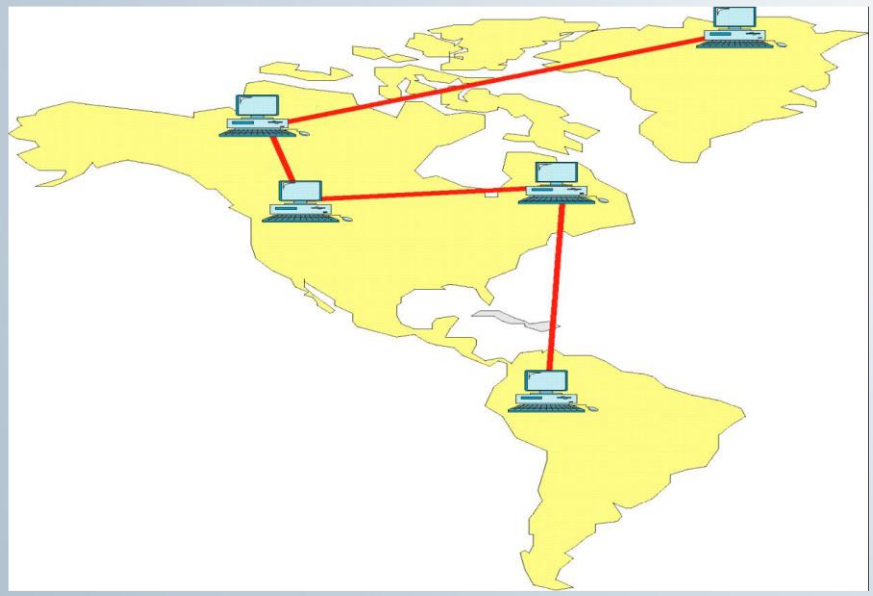
شبکه های MAN

- حوزه جغرافیائی که توسط این نوع شبکه ها پوشش داده می شود، در حد و اندازه یک شهر و یا شهرستان است. ویژگی های این نوع از شبکه ها بشرح زیر است :
- پیچیدگی بیشتر نسبت به شبکه های محلی
- برای اتصال شبکه های کوچکتر محلی به یکدیگر استفاده می شوند
- به هر دو صورت خصوصی و یا عمومی اداره و مدیریت شوند



شبکه های WAN

- حوزه جغرافیائی که توسط این نوع شبکه ها پوشش داده می شود ، در حد و اندازه کشور و قاره است. ویژگی این نوع شبکه ها بشرح زیر است :
- قابلیت ارسال اطلاعات بین کشورها و قاره ها
- قابلیت ایجاد ارتباط بین شبکه های Lan
- سرعت پایین ارسال اطلاعات نسبت به شبکه های Lan
- نرخ خطای بالا با توجه به گستردگی محدوده تحت پوشش
- وسعت بسیار زیاد
- امکان استفاده از تجهیزات متفاوت



براساس تکنولوژی انتقال

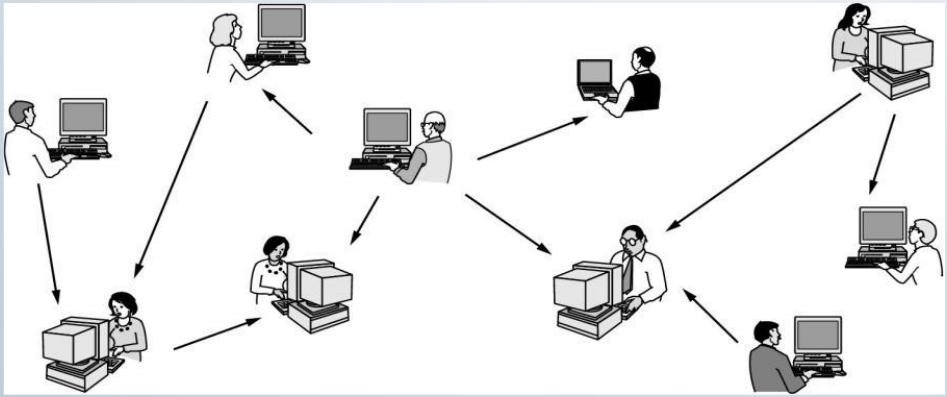
- شبکه ها را از نظر تکنولوژی انتقال یعنی چگونگی دسترسی کامپیوترها به کانال یا رسانه انتقال به دو دسته تقسیم می کنند:
  - پخش همگانی (broad cast) یا چند نقطه ای (multipoint)
  - نقطه به نقطه (Point-to-point)

پخش همگانی:

- در این روش همه ایستگاه ها به یک کانال مشترک متصلند و برای ارسال داده باید اطلاعات خود را بر روی این کانال قرار دهند و برای دریافت داده باید به کانال گوش دهند.
- امنیت پایین: دریافت اطلاعات توسط دیگر گره ها به علت مشترک بودن کانال. راه حل: رمزگذاری اطلاعات.
- کارایی نسبتا پایین: با توجه به مشترک بودن کانال برای ارسال اطلاعات، به هر کامپیوتر درصد کمی از پهنای باند کانال می رسد.
- مدیریت پیچیده کانال: باید قوانینی وضع شود تا به تمامی ایستگاه ها اجازه ارسال داده شود بنابراین به نرم افزاری پیچیده برای اداره این قوانین مانند کنترل برخورد اطلاعات نیاز داریم.
- قابلیت اطمینان پایین کانال: با قطع یا خرابی کانال، ارتباط تمامی گره ها با یکدیگر از بین میرود.

شبکه نقطه به نقطه

- در این شبکه بین هر دو گره درون شبکه یک کانال وجود دارد که این کانال فقط مختص آن دو ایستگاه است.
- ما بین ایستگاه های مختلف مسیرهای متفاوتی وجود دارد بر خلاف شبکه های پخش همگانی که فقط یک کانال و یا یک مسیر وجود دارد.
- انتخاب مسیر بین فرستنده و گیرنده توسط مسیریابی انجام می شود.
- امروزه از هر دو نوع شبکه در کاربردهای گوناگون استفاده می شود

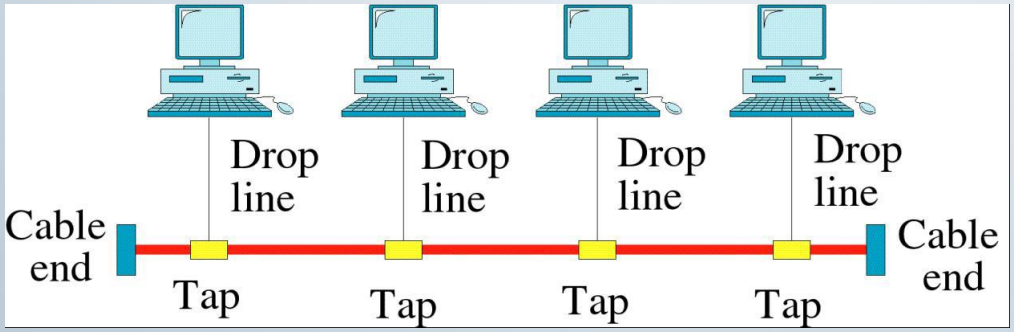


براساس توپولوژی

- چگونگی اتصال واقعی گره ها به یکدیگر توسط رسانه انتقال یا کانال را توپولوژی می گویند.
- به عبارت دیگر توپولوژی، ساختار یک شبکه را بیان می کند
- انواع توپولوژی:
  - گذرگاه مشترک (BUS)
  - ستاره ای (STAR)
  - حلقه (RING)
  - درخت (TREE)
  - مش(MECSH)
  - ترکیبی (HYBRID)

توپولوژی BUS

- در این توپولوژی همه کامپیوترها مستقیماً به یک کانال مشترک متصل هستند:
- **مزایا و معایب:**
  - برپاسازی ساده و هزینه آن ارزان می باشد.
  - در صورت قطع شدن یا خرابی کانال مشترک کل شبکه از کار می افتد.
  - تعداد کامپیوترها و طول کانال مشترک محدود است.
  - خطایابی و رفع اشکال در این شبکه ها مشکل است.
  - این نوع توپولوژی از توپولوژی های منسوخ شده می باشد



توپولوژی Ring

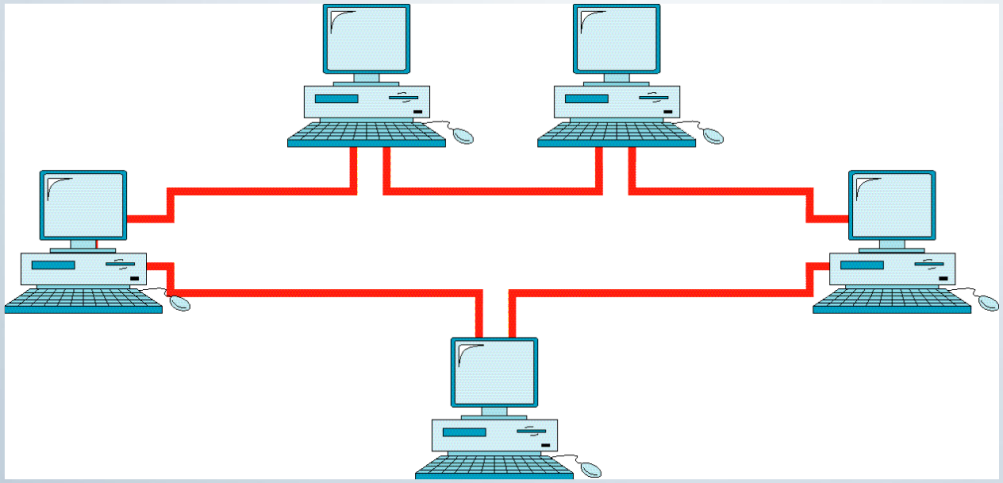
- در این توپولوژی همه کامپیوترها از طریق یک حلقه و به صورت نقطه به نقطه به یکدیگر وصل می شوند
- **مزایا :** کم بودن طول کابل.
  - نیاز به فضای خاص جهت انشعابات در کابل کشی نخواهد بود.
  - مناسب جهت فیبر نوری.
- در این توپولوژی به علت این که هر کامپیوتر یک بار اطلاعات را دریافت کرده و دوباره تکرار می کند پدیده تضعیف وجود ندارد.

توپولوژی Ring

- **معایب:** اشکال در یک گره باعث اشکال در تمام شبکه می شود.

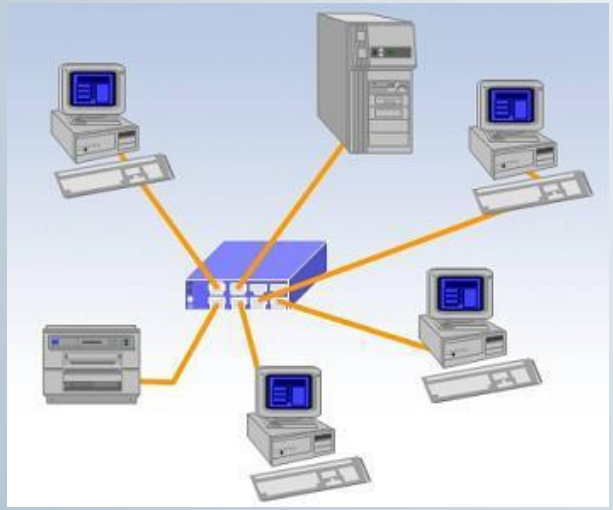
  اشکال زدایی مشکل.

  تغییر در ساختار شبکه مشکل است.



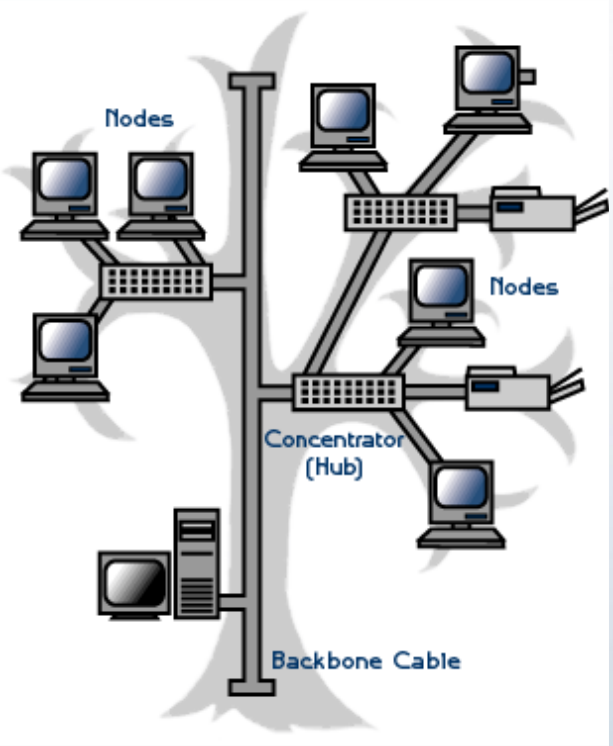
توپولوژی Star

- در این توپولوژی هر گره از طریق یک کانال اختصاصی نقطه به نقطه مستقیماً به یک ایستگاه مرکزی به نام سوییچ یا هاب متصل می شود.
- ارتباط گره ها با یکدیگر از طریق ایستگاه مرکزی انجام می شود.
- در صورت خرابی یا قطع شدن هر کانال کل شبکه از کار نمی افتد اما در صورت خرابی ایستگاه مرکزی کل شبکه از کار می افتد.
- در این توپولوژی تعداد کانال زیادی استفاده می شود



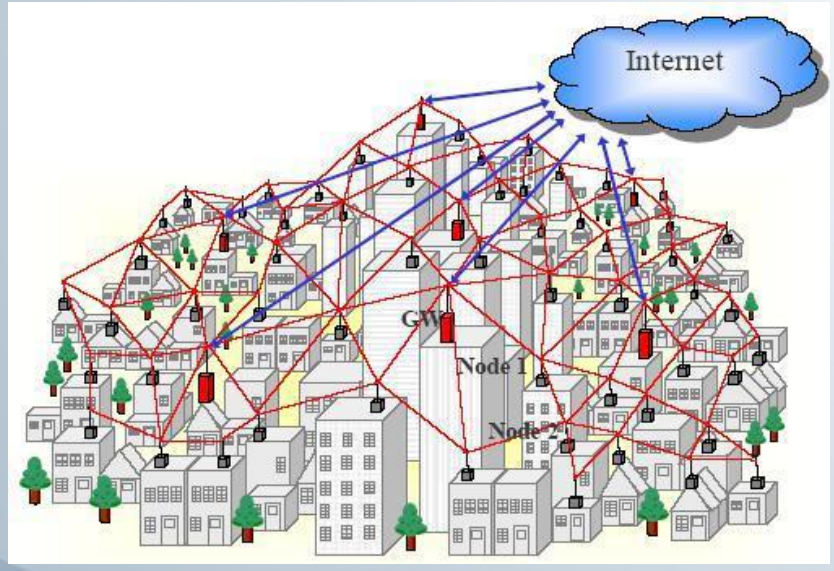
توپولوژی Tree

- این توپولوژی گسترش یافته شبکه ستاره ای و مبتنی بر کانال نقطه به نقطه است. به طوری که تعدادی هاب به یکدیگر اتصال دارند و کامپیوترها به هاب ها متصل هستند.



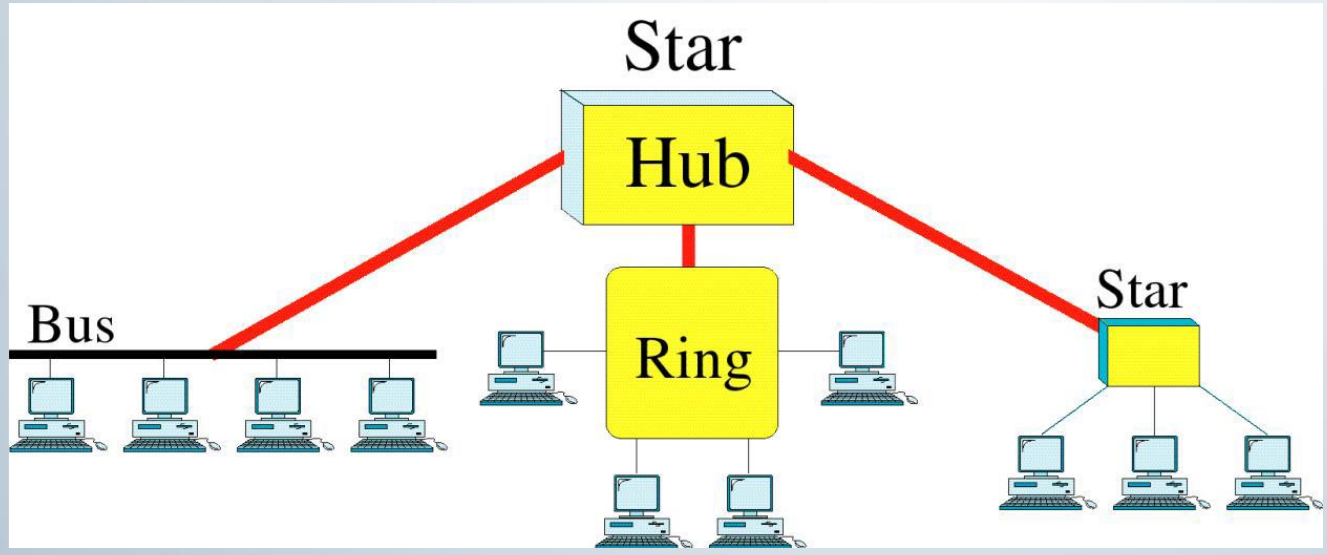
توپولوژی Mesh

- در این توپولوژی هر گره مستقیماً از طریق کانال نقطه به نقطه به هر کامپیوتر دیگر در شبکه اتصال دارد.
- سرعت انتقال داده بالا می باشد.
- قابلیت اطمینان بالا (با خرابی چند کانال کل شبکه از کار نمی افتد)
- عدم وجود مشکل ترافیک در شبکه.
- برپاسازی شبکه مش مشکل و پیچیده و هزینه بر است.
- قابلیت گسترش و افزودن کامپیوترهای جدید به این شبکه مشکل است



توپولوژی Hybrid

- شبکه های بزرگ معمولاً از اتصال چندین توپولوژی مختلف تشکیل شده اند. این توپولوژی بزرگ را به نام توپولوژی ترکیبی می شناسند.

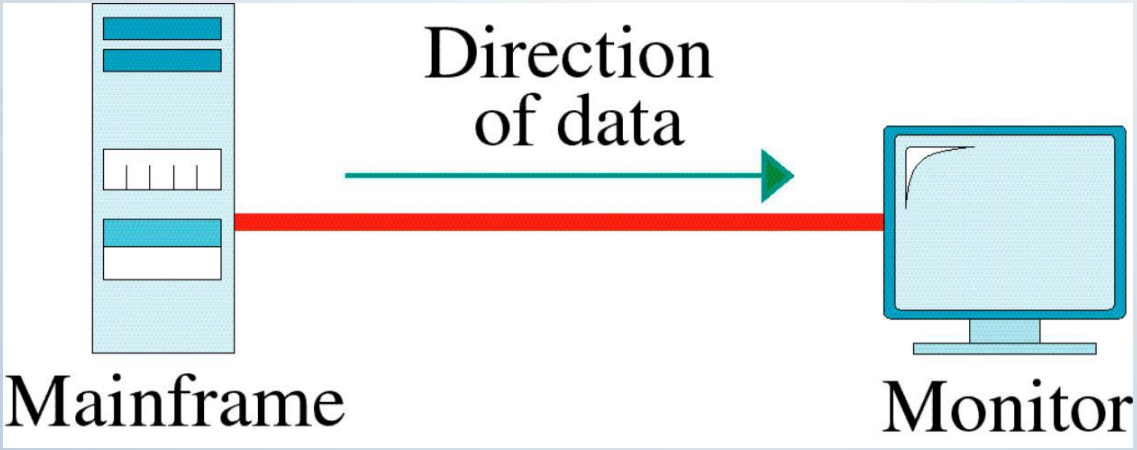


انواع ارتباط میان دو ایستگاه

- **Simplex**: ارتباط یکطرفه

- یکطرف همیشه گیرنده و یکطرف همیشه فرستنده

- مثال: پخش امواج تلویزیونی توسط فرستنده تلویزیون توسط گیرنده ها

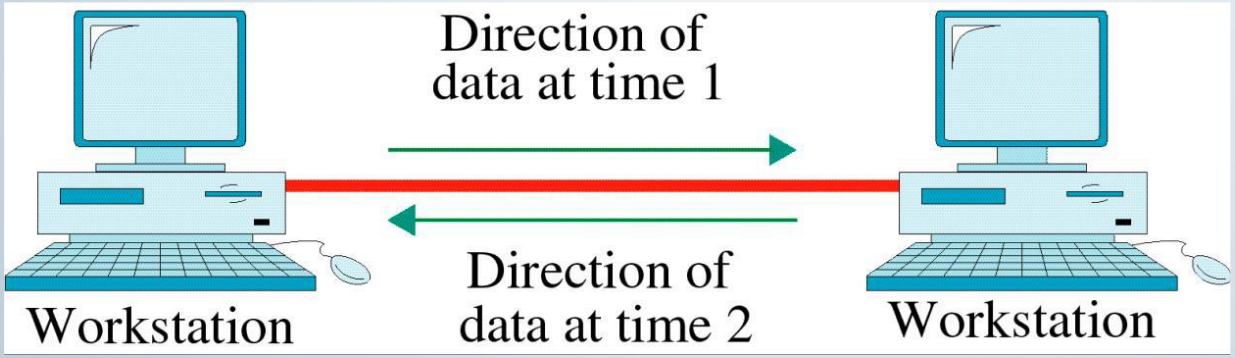


انواع ارتباط میان دو ایستگاه

- **Half duplex**: ارتباط دوطرفه غیرهمزمان

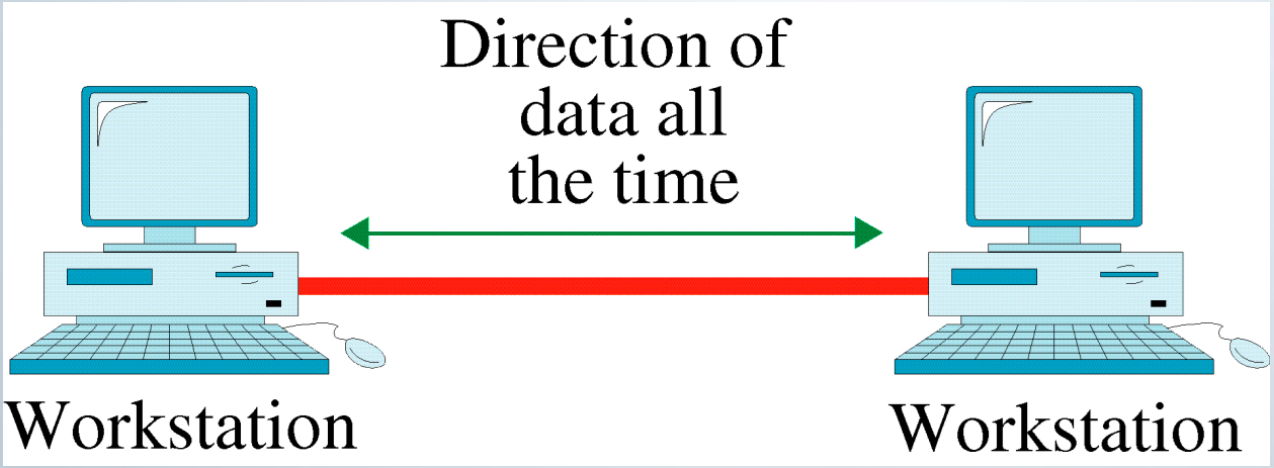
- هر دو ماشین هم میتوانند فرستنده باشند و هم گیرنده ولی نه بصورت همزمان

- مثال:کانال ارتباط و انتقال داده توسط دو دستگاه بی سیم



انواع ارتباط میان دو ایستگاه

- **Full duplex**: ارتباط دوطرفه همزمان
  - ارتباط دو طرفه همزمان
  - مثال:کانال انتقال صوت و داده توسط دو دستگاه تلفن، خطوط ماکروویو



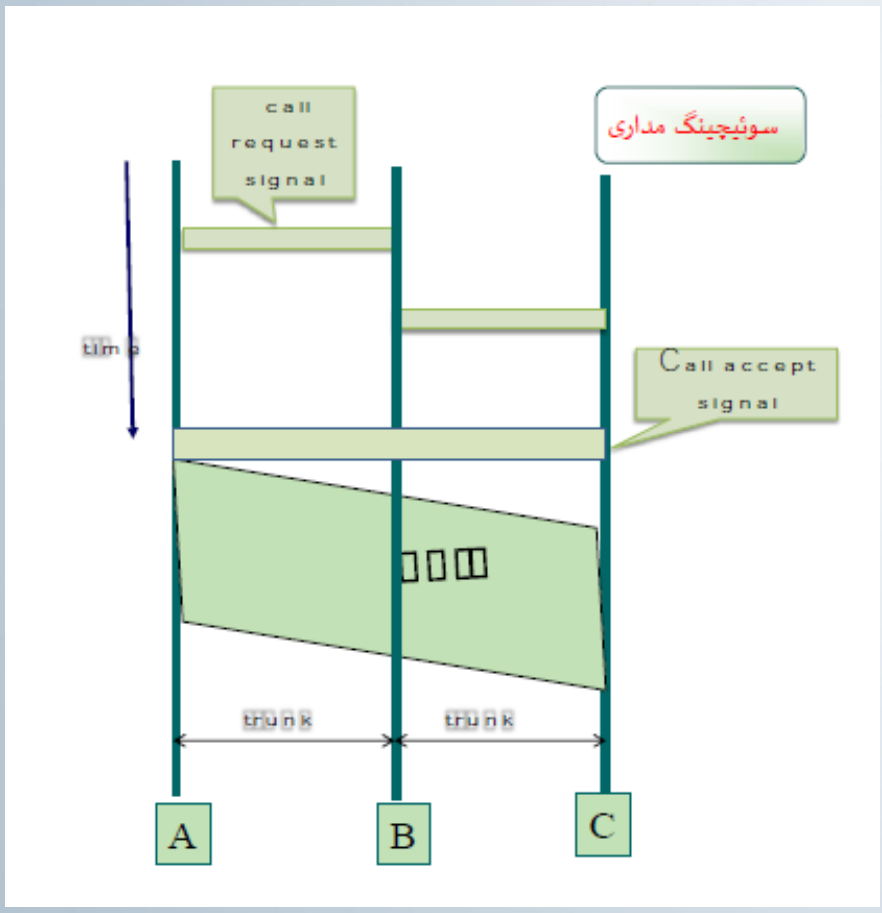
براساس نوع سوییچینگ

- در شبکه های کامپیوتری دو نوع مختلف سوئیچینگ وجود دارد :
  - سوئیچینگ مداری Circuit Switching
  - سوئیچینگ بسته و سلول Packet Switching / Cell Switching

سوییچینگ مداری

- برای ایجاد یک مدار اختصاصی و مسیر فیزیکی بین دستگاه فرستنده و گیرنده از روش سوئیچینگ مداری در لایه فیزیکی استفاده میشود دارای سه مرحله است:
  - مرحله برقراری ارتباط بین فرستنده و گیرنده
  - مرحله انتقال داده
  - مرحله قطع ارتباط
- این مدار فقط مختص فرستنده و گیرنده است ودیگر کامپیوترها نمی توانند از این مدار استفاده کنند.مثالی از این روش سوئیچینگ، انتقال صدای بلادرنگ مابین دو تلفن است که در شبکه عمومی سوئیچ تلفن بکار می رود.

معایب سوییچینگ مداری



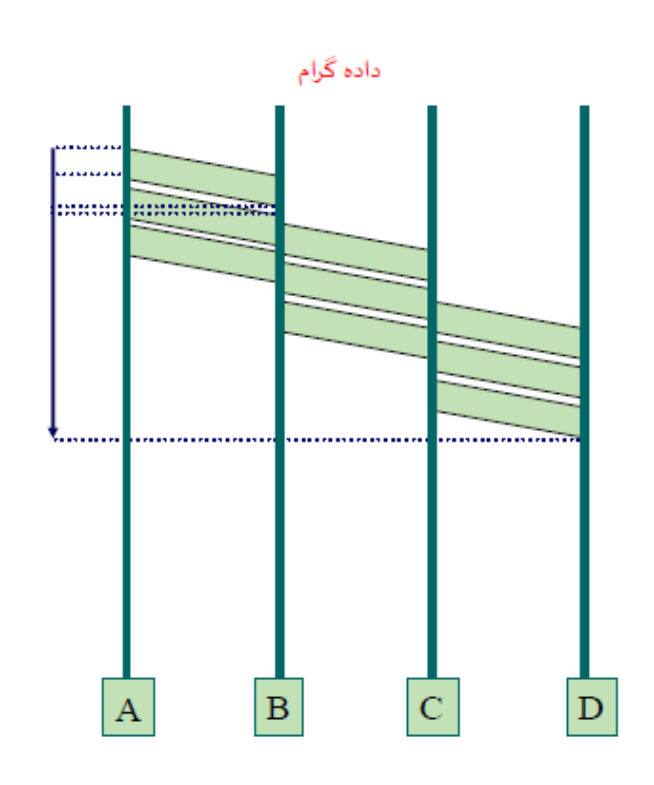
- نیاز به زمان قابل توجهی برای برقراری ارتباط بین فرستنده و گیرنده
- عدم امکان برقراری ارتباط توسط ماشین های دیگر با دو ماشین فرستنده و گیرنده هنگام اشغال بودن کانال توسط دو ماشین

سوییچینگ بسته و سلول

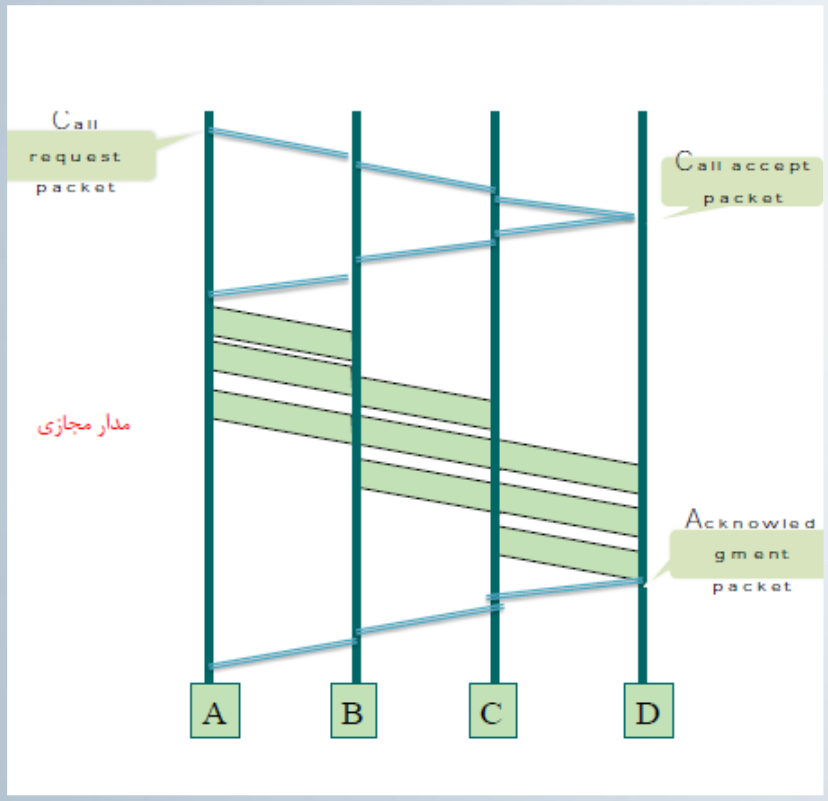
- شکستن پیام توسط ایستگاه فرستنده به قطعات کوچکتری به نام بسته و ارسال هر بسته به همراه اطلاعات لازم برای بازسازی آن به طور جداگانه به مراکز سوئیچ است.
- هر سوئیچ با دریافت کامل بسته می تواند آن را هدایت کند در حالی که می تواند به طور همزمان بسته بعدی را دریافت کند.
- بسته ها در هر سوئیچ ابتدا ذخیره می شود و سپس با بررسی سر فصل آن و جدول مسیریابی به سمت مناسب هدایت می شوند.
- دو روش سوئیچینگ بسته ای وجود دارد:
  - مدار مجازی (virtual circuit)
  - داده گرام (datagram)

سوییچینگ بسته و سلول – داده گرام

- ارسال بسته های اطلاعاتی با استفاده از آدرسهای IP مبدأ و مقصد در شبکه
- انجام مسیریابی جداگانه برای هر بسته
- توزیع و هدایت بسته ها روی مسیرهای متفاوت بر اساس شرایط توپولوژیکی و ترافیکی لحظه ای شبکه
- امکان دریافت بسته بدون ترتیب ارسال شده در مقصد
- لزوم نظارتهای ویژه بر گم شدن و یا تکراری بودن بسته در لایه های بالاتر



سوییچینگ بسته و سلول – مدار مجازی



- ارسال بسته های اطلاعاتی بدون نیاز به اطلاع از آدرسهای IP مبدأ و مقصد
- عدم اجرای الگوریتم مسیریابی جهت هدایت بسته های اطلاعاتی از مبدأ به مقصد
- دریافت بسته به ترتیب ارسال شده در مقصد
- عدم احتمال گم شدن بسته ها در عمل مسیریابی در شبکه

مقایسه داده گرام و مدار مجازی

موضوع	داده گرام	مدار مجازی
برقراری مدار	نیازی نیست	نیاز است
آدرس دهی	هر بسته شامل آدرس مبدأ و مقصد	هر بسته شامل یک شناسه(برای آدرس مبدأ و مقصد)
مسیر یابی	هر بسته مستقلا مسیریابی می شود	در ابتدا مسیریابی میشود ولی بعد بسته ها بر اساس شناسه مسیر را دنبال می کند
نوع ارتباط	بدون اتصال	اتصال گرا
دریافت بسته توسط گیرنده	بدون ترتیب	مرتب شده
اطلاعات وضعیت مسیر	مسیریاب نیازی به نگهداری اطلاعات ندارد	شناسه بایستی در جدول هر سوئیچ ذخیره شود
تاثیر خرابی مسیریاب	بدون تأثیر، البته بعضی از بسته ها از بین میرود	موثر، زیرا مدار مجازی از بین می رود
ارائه کیفیت سرویس ها	مشکل	ساده
کنترل ازدحام	مشکل	ساده

لایه بندی و ساختار لایه ای

- لایه چیست؟
  - به منظور تفکیک وظایف و عملیات لازم برای انتقال داده، تعدادی لایه در یک سیستم شبکه تعریف می شود که هر لایه وظیفه خاصی را برای انتقال داده بر عهده دارد ومجموعه لایه ها با کمک یکدیگر عمل انتقال داده به صورت صحیح را تضمین می کنند.
- هدف ساختار لایه ای:
  - کاهش پیچیدگی شبکه
  - افزایش انعطاف پذیری در مقابل تغییرات احتمالی

ویژگی لایه بندی

- هر لایه برروی لایه دیگری قرار دارد و با آن در ارتباط است
- هر لایه شبکه وظایف خاص خود را به عهده دارد و از لایه های دیگر مستقل می باشد
- هر لایه ازسرویس لایه پایین تر خود استفاده می نماید و به لایه بالاتر خود سرویس می دهد.
- هر لایه شبکه برای انجام وظایف خود از یکسری قواعد و قراردادهای استاندارد استفاده می نماید که به آن پروتکل گفته میشود.
- مجموع لایه ها و پروتکل های یک شبکه را معماری شبکه می گویند.

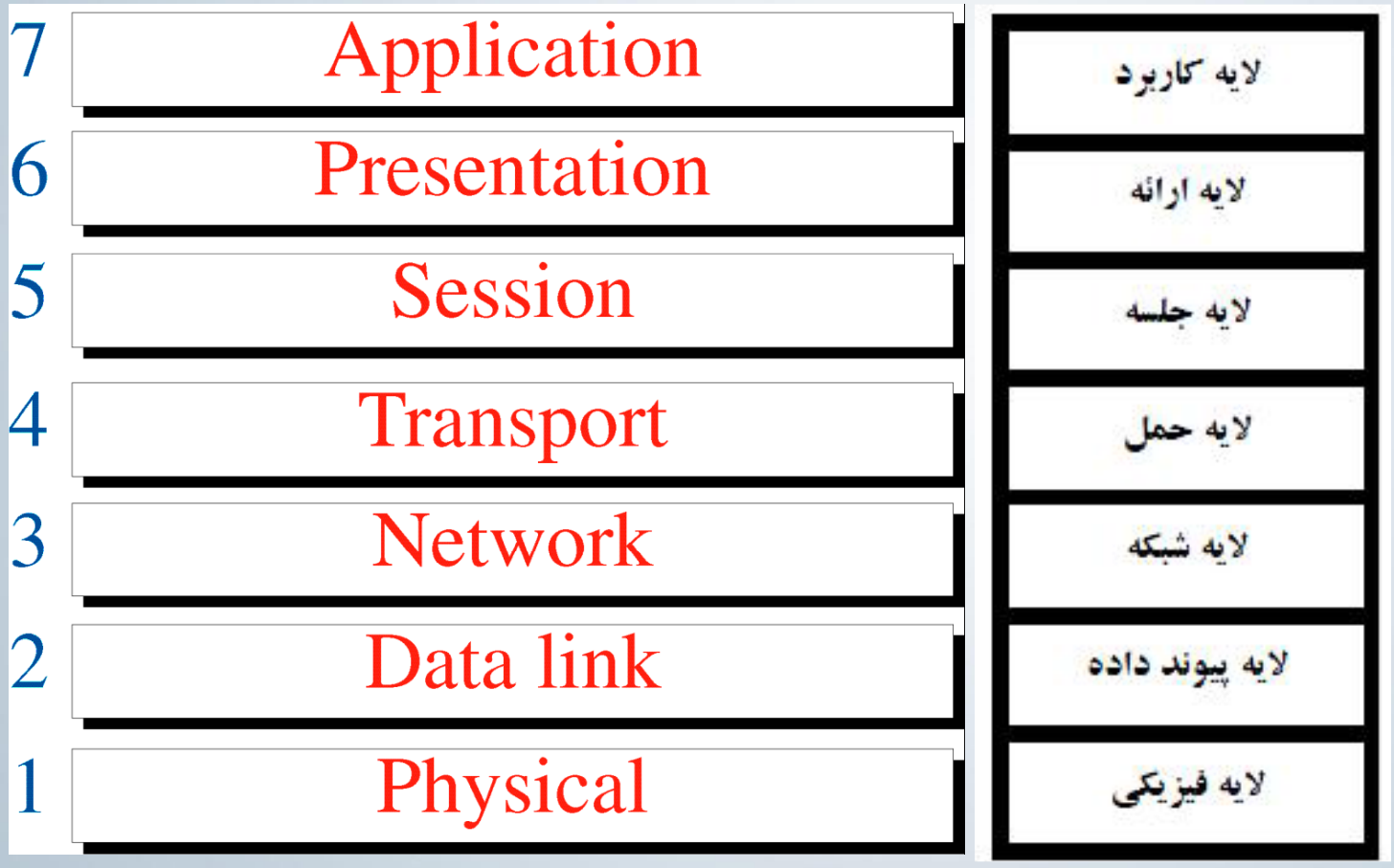
مشکلات لایه بندی

- نیاز به مکانیسمی برای برقراری و قطع ارتباط
- عدم تطابق سرعت لایه های فرستنده و گیرند ه
- محدودیت اندازه بسته ها
- وقوع خطا در بسته های دریافتی
- عدم رعایت ترتیب بسته ها

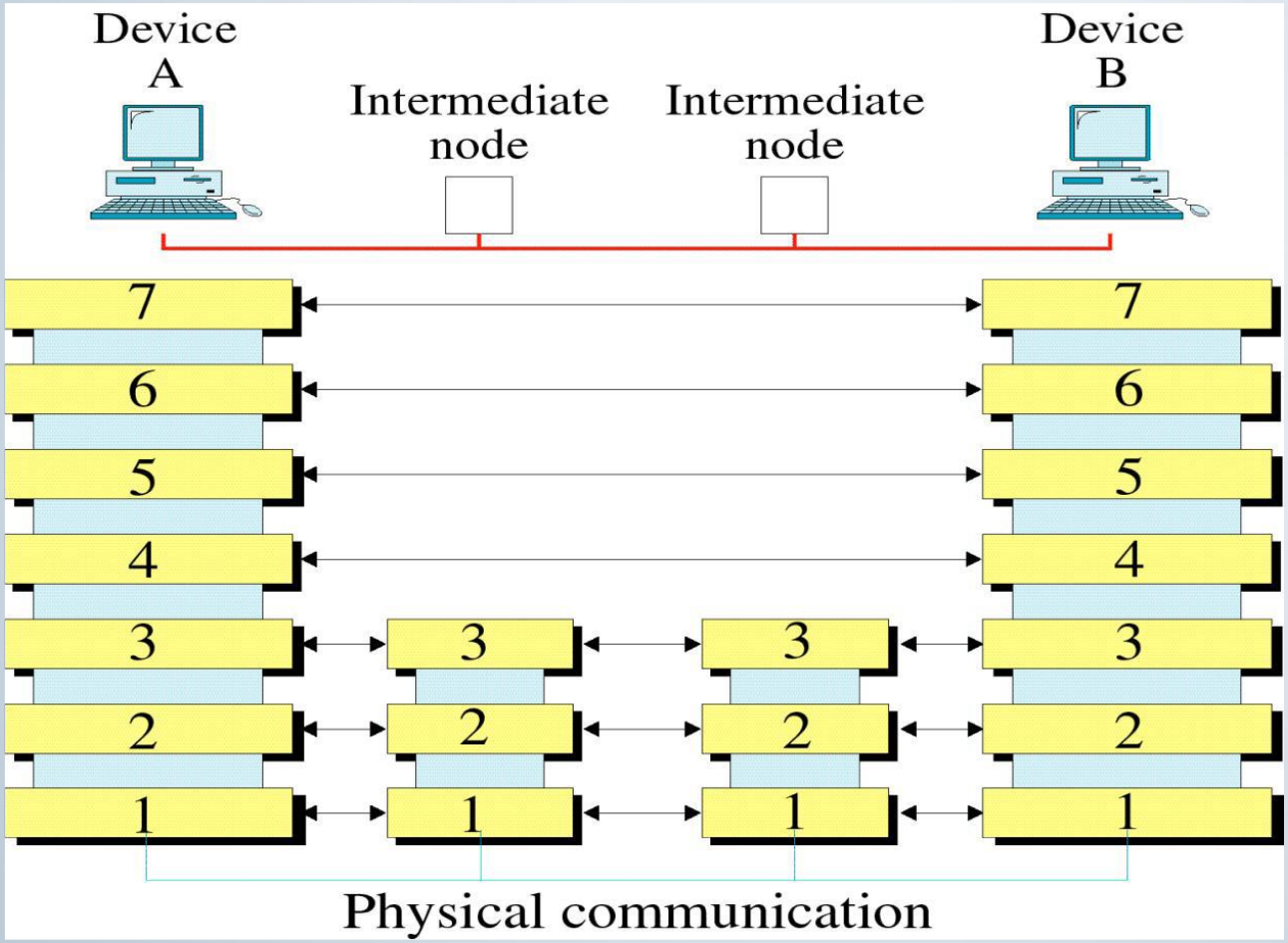
مدل OSI

- این مدل، مدلی هفت از وظایف شبکه است و لایه ها کاملا مستقل از یکدیگر می باشند و ارتباط بین لایه ها از طریق Interface برقرار می شود.
- هر لایه وظیفه دارد که به لایه های بالاتر سرویس بدهد و جزئیات لایه های زیرین را برای لایه های بالایی پنهان نگهدارد.
- با استفاده از مدل مرجع OSI امکان اتصال سیستم های مختلف و برقراری ارتباط بین آنها بدون نیاز به اعمال تغییرات در منطق سخت افزار و نرم افزار پایینی آنها وجود دارد.
- هر لایه پروتکل خاص خود را دارد.
- مجموعه ای از قوانین وقواعد خاص و مشترک که طرفین یک ارتباط ملزم به اجرای آن هستند تا بتوانند از اطلاعات یکدیگر به طور صحیح وکامل استفاده نمایند را پروتکل می گویند

لایه های مدل OSI



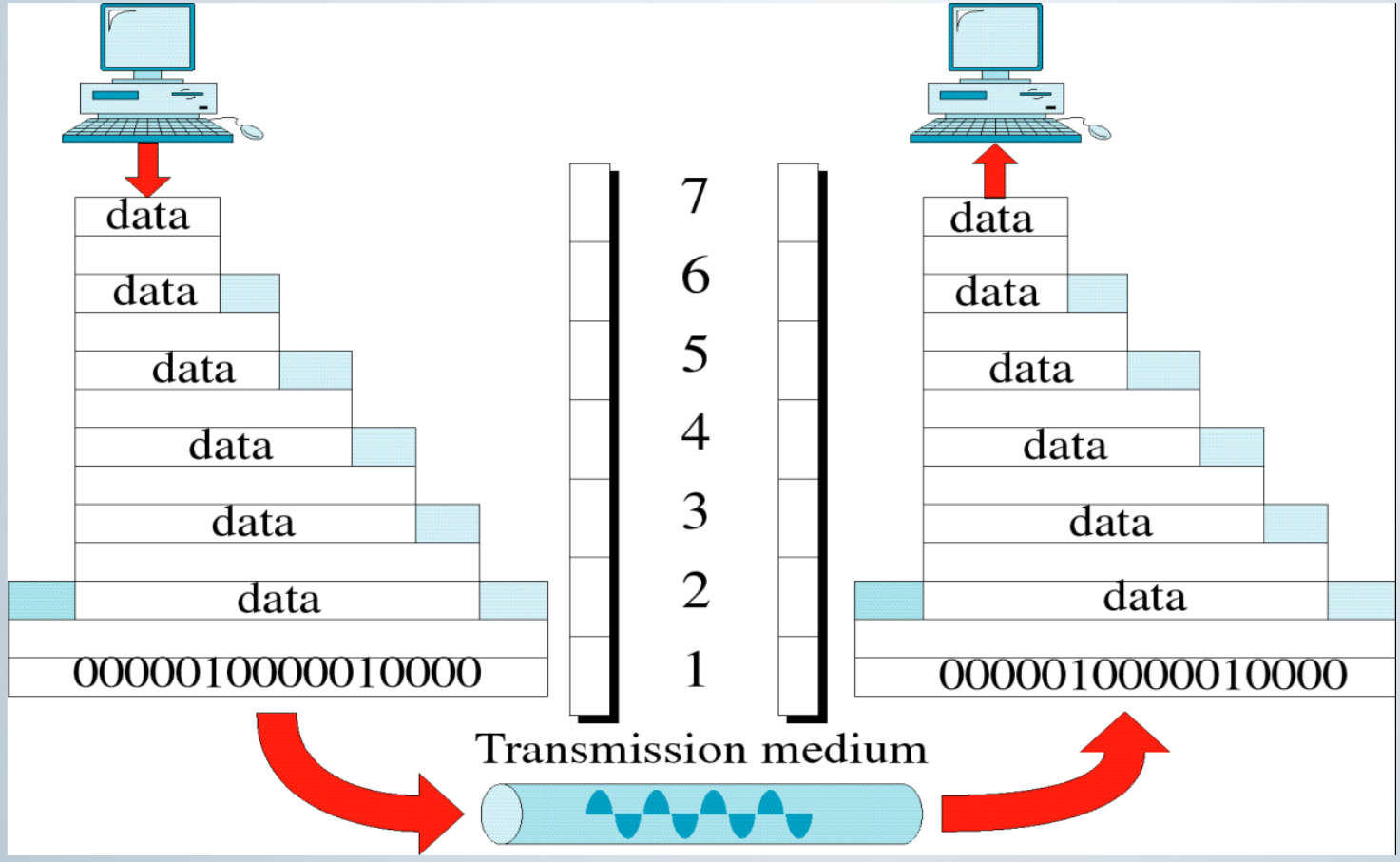
مدل OSI


Device
A
Intermediate
node
Intermediate
node
Device
B
7
6
5
4
3
2
1
3
2
1
3
2
1
7
6
5
4
3
2
1
Physical communication

مدل OSI

- لایه های متناظر ماشین A و ماشین B می توانند با هم ارتباط برقرار کنند. پس هر لایه با لایه متناظر یک پروتکل یکسان دارد.
- هیچ لایه ای نمی تواند مستقیما اطلاعات را روی محیط ارتباطی قرار دهد و برای انتقال اطلاعات ، ابتدا لایه ۷ به لایه ۶، لایه ۶ به لایه ۵ و به همین ترتیب انتقال می دهند و اطلاعات را روی محیط ارتباطی قرار می دهند.
- هر لایه برای انجام دادن کار باید یک سری اطلاعات کنترلی داشته باشد تا گیرنده بتواند بر حسب آن اطلاعات کنترلی کار را انجام دهد. که هر لایه یک سری اطلاعات کنترلی به داده ها اضافه می کند و به لایه بعدی می فرستد.

مدل OSI

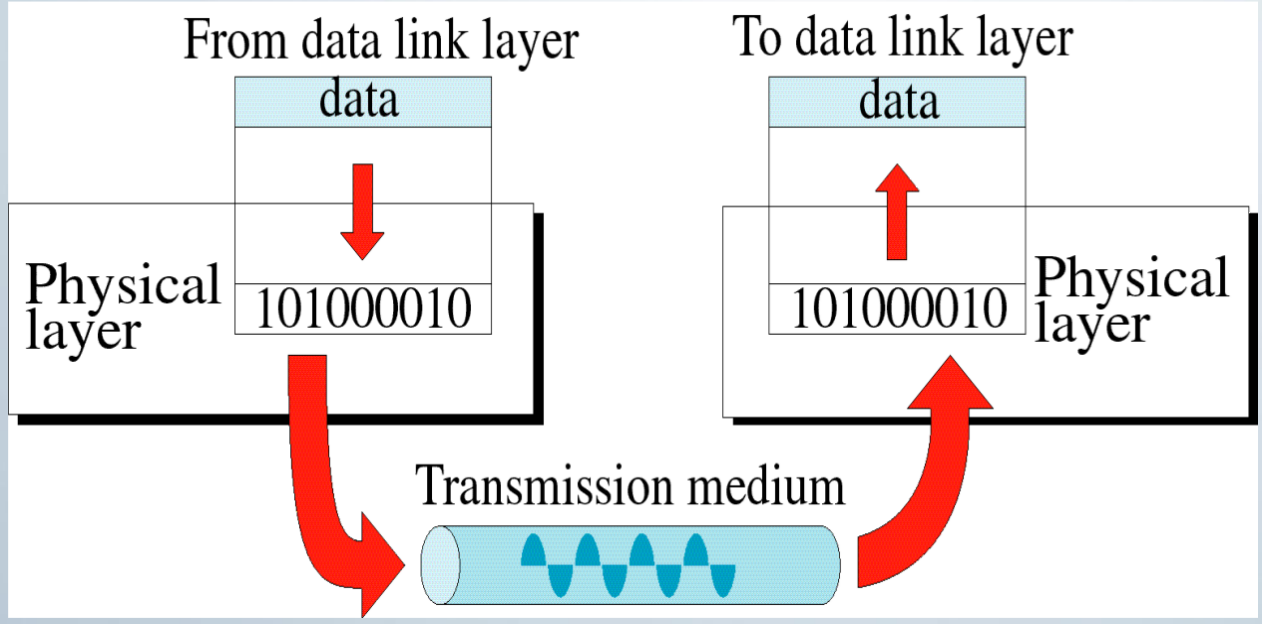

data
data
data
data
data
data
0000010000010000
7
6
5
4
3
2
1
Transmission medium
data
data
data
data
data
data
0000010000010000

لایه فیزیکی (Physical Layer)

- این لایه وظیفه گرفتن اطلاعات از لایه بالاتر (صفر و یک) و تبدیل آن به سیگنال متناسب با محیط را برعهده دارد. در لایه فیزیکی مستقیما با صفر و یک سروکار داریم. عرض بیت ، انواع Codingو سیگنال های آنالوگ و دیجیتال در این لایه مطرح می شود.
- واحد تبادل داده های انتقالی : بیت
- مسائل مطرح در این لایه:
  - ساختار کانالهای اتصالی
  - نقطه به نقطه یا پخشی
- ارسال داده ها در کانال : ارسال کاملاً یک طرفه(Simplex)،ارسال یک طرفه(Half Duplex)، ارسال دوطرفه (Full Duplex)

لایه فیزیکی (Physical Layer)

- توپولوژی
- نوع سیگنال : آنالوگ و دیجیتال
- واسط ارتباطی
- محیط ارسال



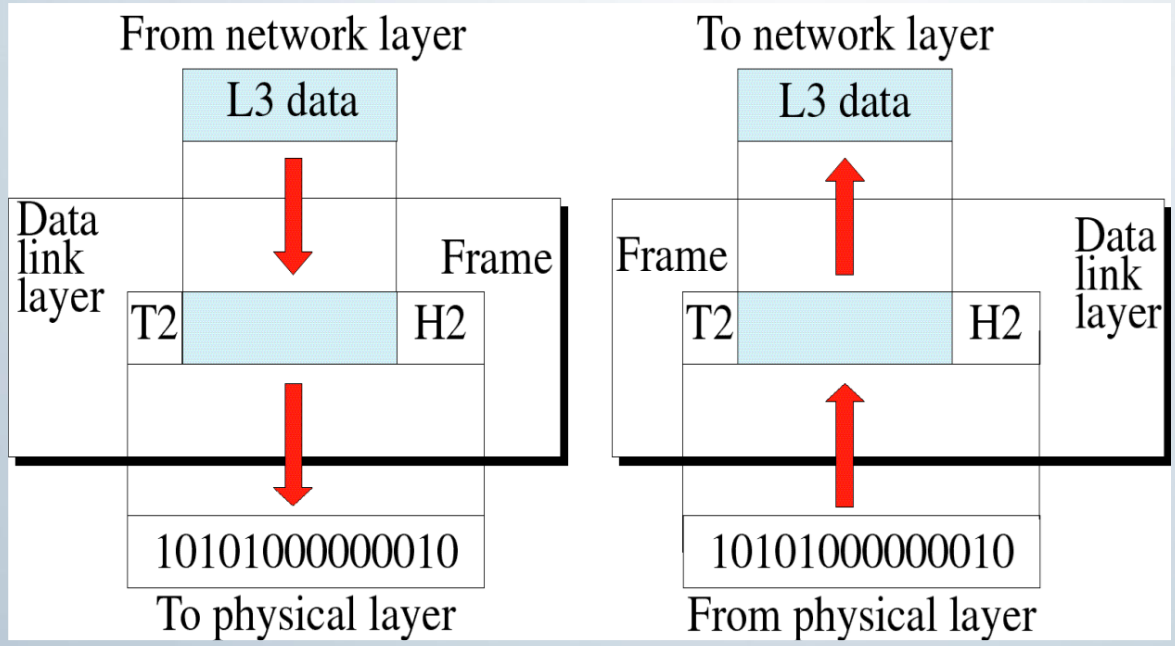
لایه پیوند لایه ها (Data link Layer)

- وظیفه این لایه آدرس دهی فیزیکی، تعیین نحوه دسترسی به رسانه و مدیریت کانال است. لایه فیزیکی به کمک این لایه به یک لینک ارتباطی قابل اطمینان تبدیل می شود.
- واحد تبادل داده های انتقالی : فریم
- سایر وظایف لایه پیوند داده:
  - شناسایی ابتدا و انتهای فریم(Framing)
  - تطبیق سرعت فرستنده و گیرنده (Flow Control):
    - مشکل عدم آمادگی CPU به علت پردازش وقفه قبلی
    - مشکل عدم فضای کافی در بافر

لایه پیوند لایه ها (Data link Layer)

- تشخیص خطا (Error Detection)
- تصحیح خطا (Error Correction)

- کنترل دسترسی: وقتی که دو یا چند وسیله به لینک مشترکی متصل می شوند باید مشخص شود در هر لحظه چه کسی می تواند از آن لینک استفاده کند.

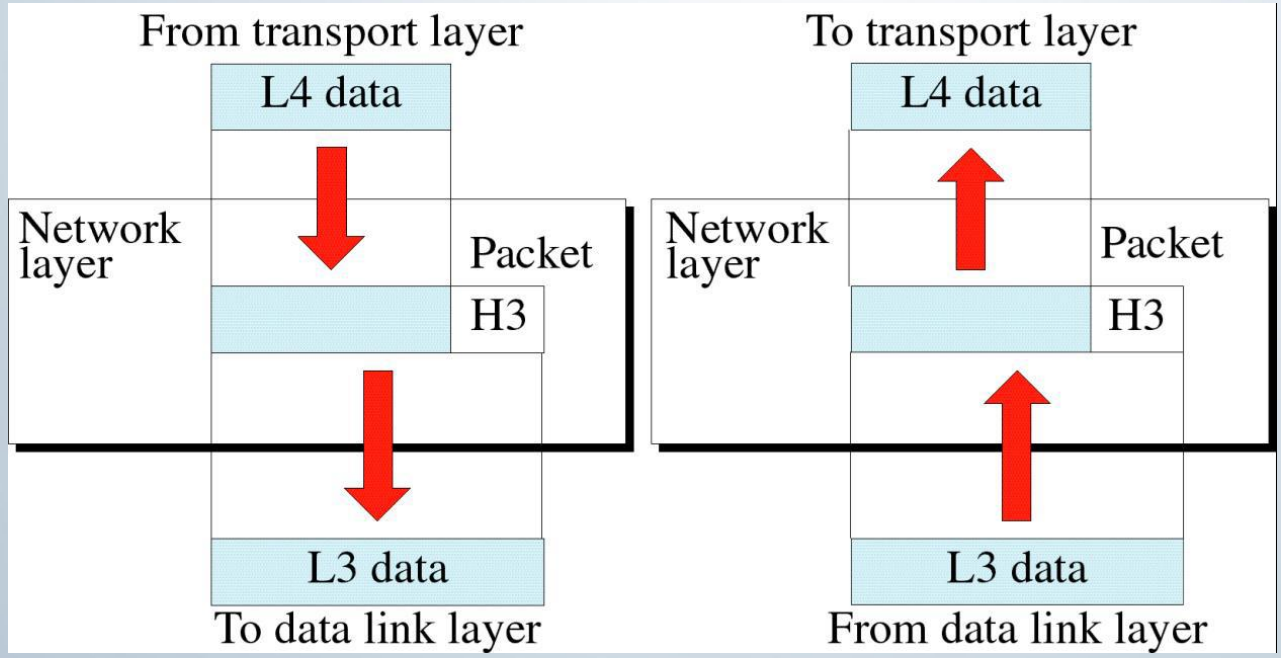


لایه شبکه (Network Layer)

- **این لایه مسئول تحویل بسته های اطلاعات از ماشین مبدا در یک شبکه به ماشین مقصد در شبکه دیگر است.**
- **واحد تبادل داده های انتقالی : بسته (Packet)**
- **سایر وظایف لایه :**
  - **مسیریابی در شبکه (Network Routing)**
  - **جلو بردن (پیش بری) بسته ها در شبکه (Packet Forwarding)**
  - **جلوگیری از ازدحام (Congestion Control)**
  - **آدرس دهی (Addressing)**

لایه شبکه (Network Layer)

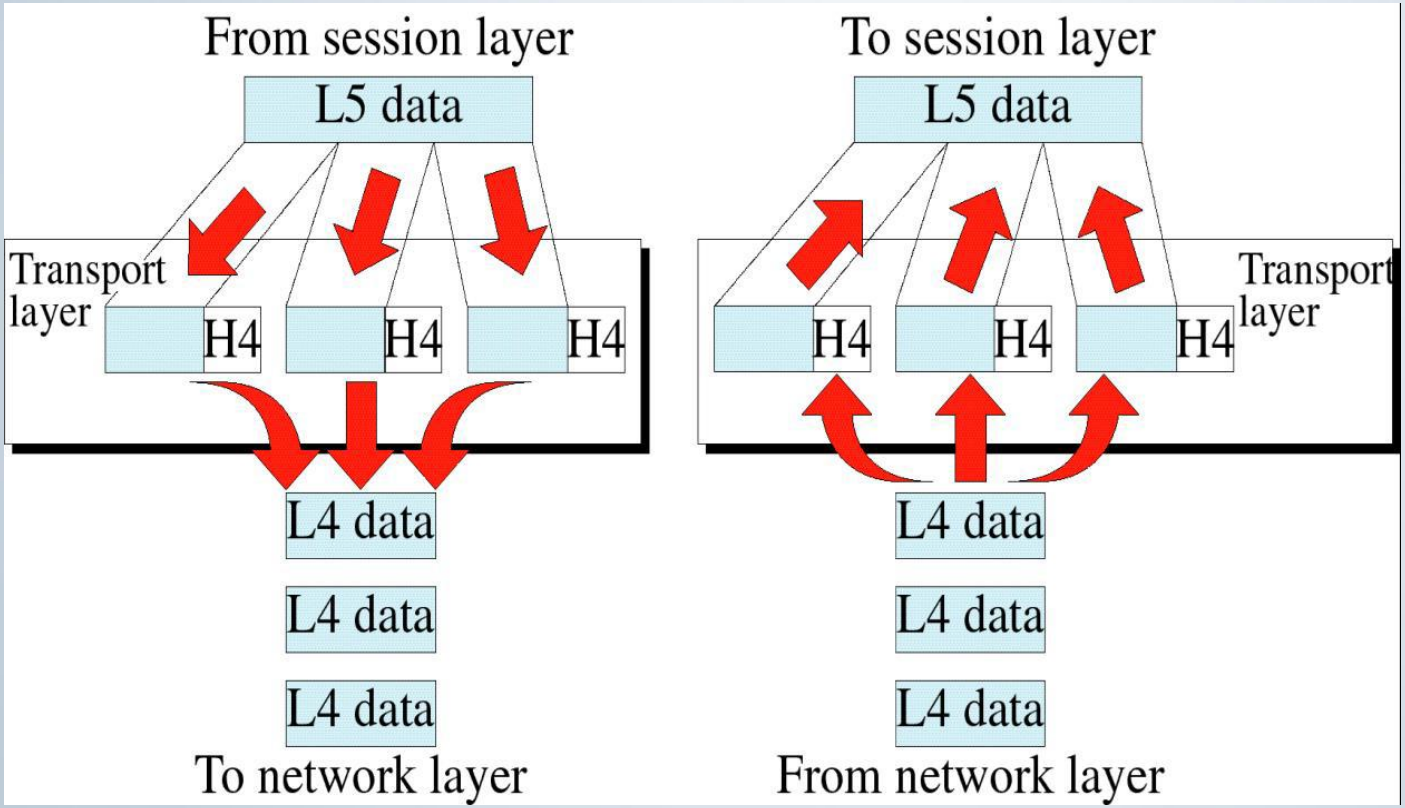
- تطبیق پروتکل ها در ارتباطات بین شبکه ای (Internetworking)
- به عبارت دیگر اتصال دو شبکه که ۳ لایه پایین آن ها متفاوت است به وسیله روتر
- کنترل جریان بین کامپیوتر و واسط شبکه(Flow Control)



لایه انتقال (Transport Layer)

- امکان خطا در لایه Network وجود دارد. زیرا هیچ لایه ای ، لایه بالاتر را کنترل نمی کند پس لایه شبکه لایه امنی نیست و به همین دلیل لایه انتقال مطرح می شود تا به این لایه امنیت بیشتری دهد.
- واحد انتقال داده: پیغام (Message)
- وظایف:
- تقسیم پیغام به بسته ها و بالعکس و شماره گذاری بسته ها (fragmentation / Defragmentation)
- تطبیق سرعت میزبان های سریع و کند (Flow Control)
- تضمین دریافت صحیح داده ها با سرویس دهی مستقل از نوع شبکه برای ارسال پیغام های لایه پنجم به مقصد.

لایه انتقال (Transport Layer)

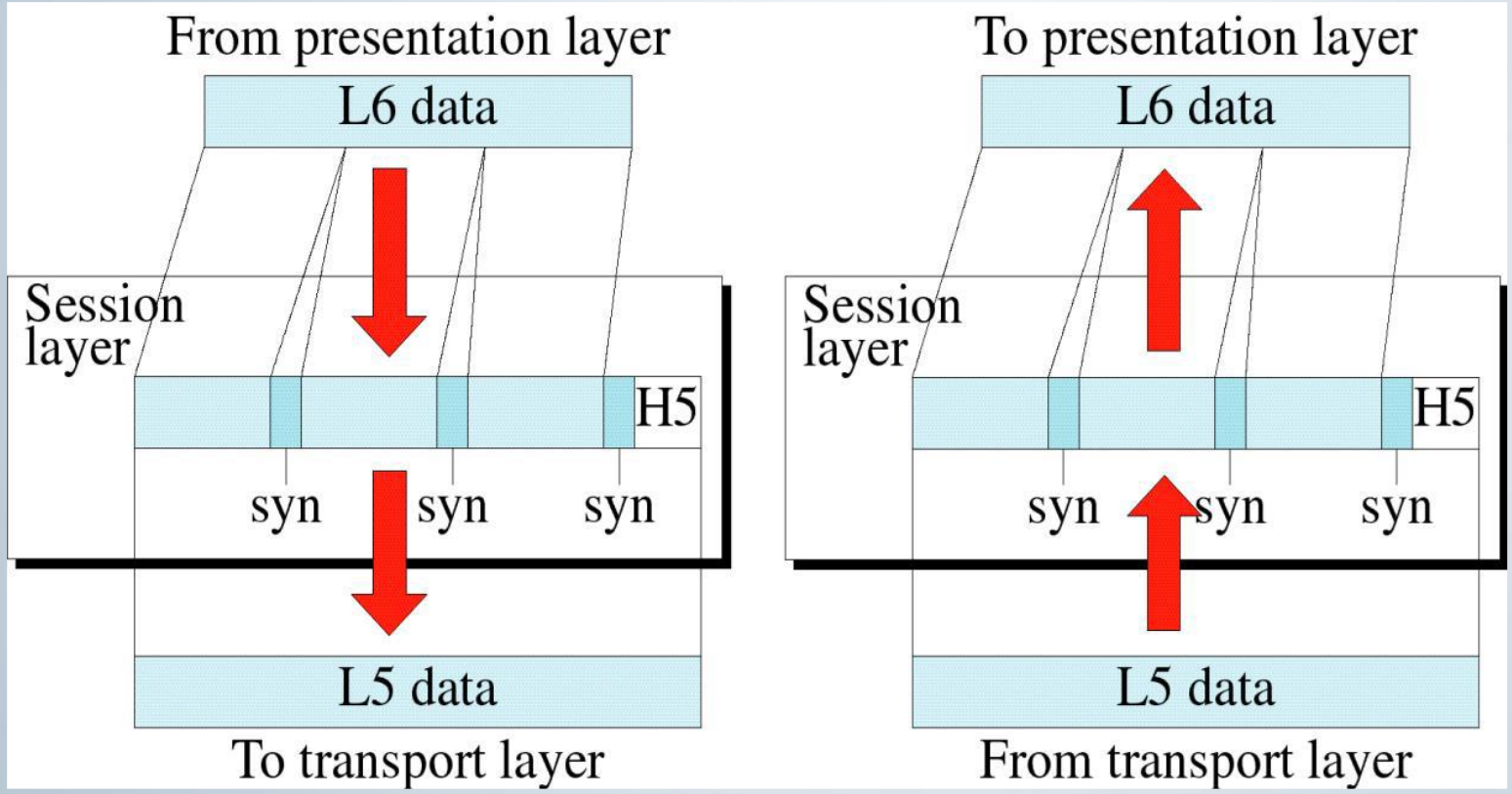


لایه جلسه (Session Layer)

- کنترل ، سازماندهی، مدیریت و همگام سازی برقراری جلسه بین کامپیوترهای میزبان
- واحد انتقال داده: پیغام
- دیگر وظایف:
  - مدیریت نشانه
  - همزمانی
- چنانچه در حین ارسال ارتباط قطع شود، باید انتقال اطلاعات دوباره ازسرگرفته شود.

برای رفع این مشکل، لایه جلسه با کمک امکانات همزمانی قادر میباشد که در صورت قطع ارتباط فقط از همان نقطهٔ قطع قبلی، دوباره اطلاعات را ارسال کند.

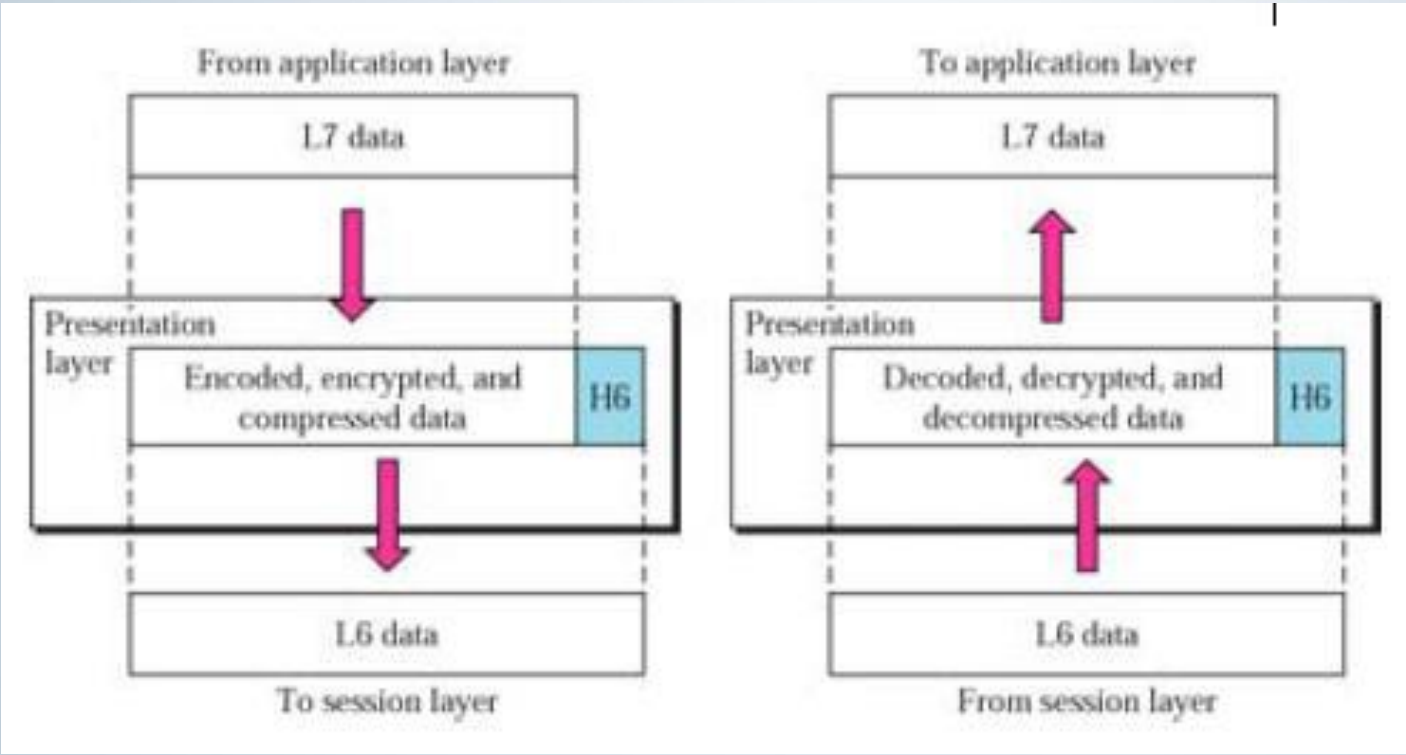
لایه جلسه (Session Layer)



لایه ارائه (Presentation Layer)

- این لایه به قواعد و معنای اطلاعات فرستاده شده مربوط می‌شود.
- واحد انتقال داده: پیغام
- وظایف:
  - فشرده سازی و باز کردن کدها (Compression / Decompression)
  - رمز نگاری و رمزگشایی به منظور ایجاد امنیت و محرمانگی (Encryption / Decryption)
  - تبدیل کدینگ های مختلف به یکدیگر

لایه ارائه (Presentation Layer)

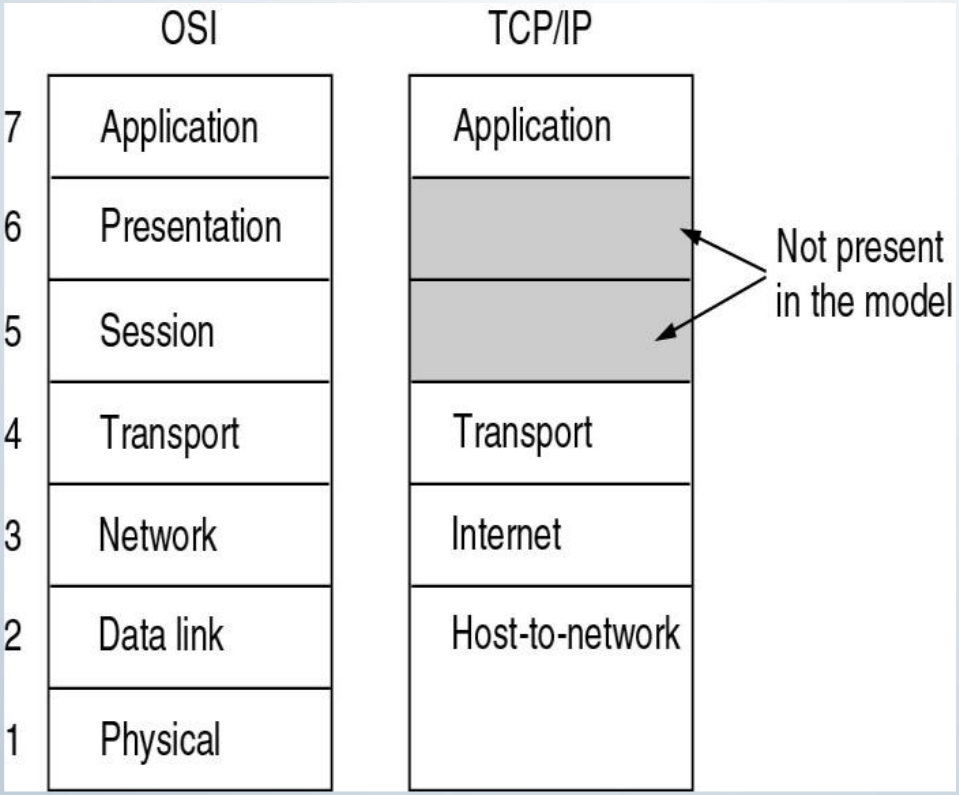


لایه کاربرد (Application Layer)

- کاربران شبکه از طریق امکانات و پروتکل های این لایه قادر به استفاده ازسرویس شبکه می باشند .
- واحد انتقال داده: پیغام
- ایجاد محیط مناسب جهت ارتباط برنامه های کاربردی کاربر انتهایی با سرویس های توزیع اطلاعات شبکه ای مانند FTP,Telnet و ...
- نرم افزار های کاربردی متنوع:
  - پست الکترونیکی، انتقال فایل، اتصال از راه دور به یک ماشین و ...

مدل TCP/IP

- مدل ۴ لایه ای است و دلیل نامگذاری این است که داده ها بزرگ هستند(TCP)پس از طریق IP ارسال می شوند. پس به همین دلیل به آن TCP/IPمی گویند.

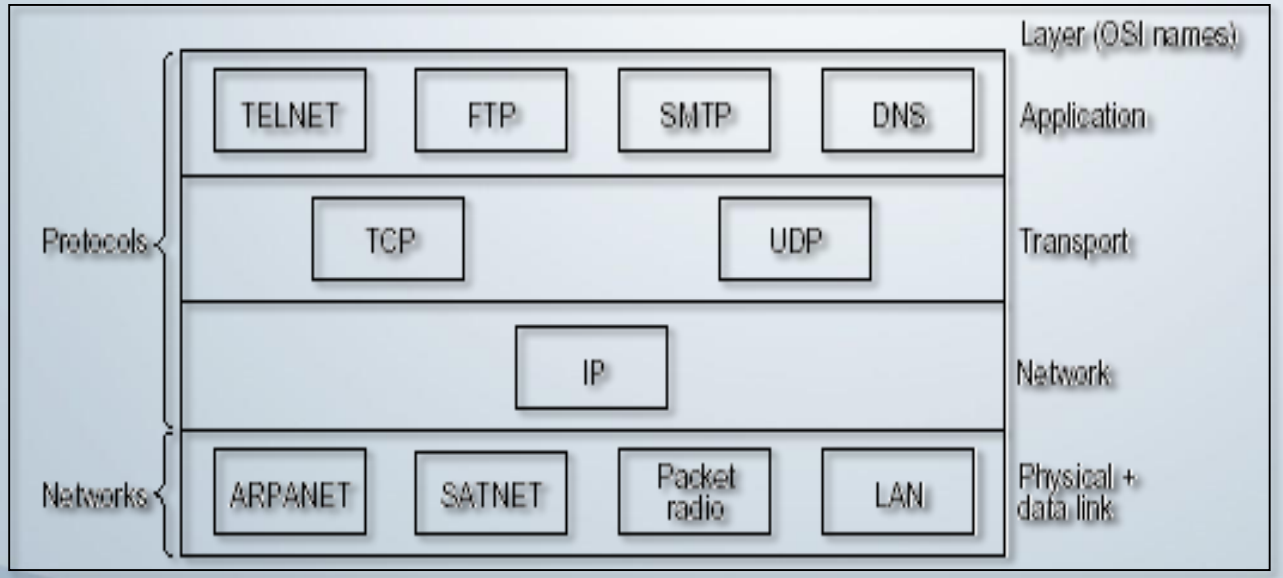


مدل TCP/IP

- لایه میزبان به شبکه (Network Interface)
- لایه اینترنت (Internet layer)
- لایه انتقال (Transport layer)
- لایه کاربرد(Application layer)

لایه میزبان به شبکه (Network Interface)

- بیان می‌کند که میزبان با استفاده از بعضی از قراردادها به شبکه متصل شود. بنابراین می‌تواند بسته‌های IP را از طریق آن ارسال کند.
- پروتکلهائی که در لایه اول از مدل TCP/IP تعریف می شوند، می توانند مبتنی بر ارسال رشته بیت یا مبتنی بر ارسال رشته بایت باشند.



لایه اینترنت(Internet Layer)

- **وظایف این لایه شبیه لایه شبکه در مدل OSI است و مهمترین وظیفه آن مسیریابی و آدرس دهی است.**
- **پروتکل های مورد استفاده در این لایه :** IP , BOOTP , ARP , RARP , RIP , ICMP

لایه انتقال(Transport Layer)

- برقراری ارتباط از طریق یک سرویس اتصال گرا و مطمئن با ماشینهای انتهایی یا میزبان.
- ارسال و یا دریافت داده های تحویلی به این لایه توسط برنامه های کاربردی و از طریق توابع سیستمی است.
- این لایه شامل دو قرارداد به شرح زیر می‌باشد:
- TCP (قرارداد کنترل انتقال): قرارداد قابل اعتماد و اتصالگرایی است که اجازه می‌دهد رشته‌ای از بایتهایی که از یک ماشین شروع به حرکت می‌کنند، بدون خطا به ماشین دیگری در لایه اینترنت تحویل شوند.
- UDP (قرارداد داده گرام کاربر): یک قرارداد غیر قابل اعتماد و بی اتصال برای کاربردهایی که در آن تحویل سریع مهمتر از تحویل صحیح می‌باشد، بطور گسترده مورد استفاده قرار می‌گیرد.

لایه کاربرد(Application Layer)

- لایه کاربرد در بالای لایه انتقال قرار دارد و شامل تمام قراردادهای لایه بالاتر می‌باشد.
- در حقیقت کار هر سه لایه نمایش، جلسه و کاربرد در مدل OSI را انجام می دهد.
- خدماتی که در این لایه صورت می گیرد در قالب پروتکلهای استاندارد زیر به کاربر ارائه می شود :
  - شبیه سازی ترمینال
  - انتقال فایل یا FTP
  - مدیریت پست الکترونیکی
  - خدمات انتقال صفحات

خدمات هرلایه به لایه‌های بالاتر:

- خدمات اتصال‌گرا (پیاده‌سازی بر اساس مدل تلفن)
  - قابل اعتماد
    - دنباله‌های پیام
    - رشته‌های بایتی ← انتقال فایل
  - غیر قابل اعتماد
- بی‌اتصال (پیاده‌سازی بر اساس مدل پست)
  - قابل اعتماد
  - غیر قابل اعتماد ← خدمات داده‌گرام
  - خدمات درخواست و پاسخ

اختلافات OSI و TCP/IP

- هر دو مدل به صورت لایه ای طراحی شده اند.
- هر دو مدل دارای لایه های انتقال و شبکه شبیه یکدیگر هستند.
- مدل TCP/IP ، لایه ارائه و جلسه OSI را در لایه کاربردی ادغام کرده است.
- مدل TCP/IP لایه پیوند داده و فیزیکی را در یک لایه قرار داده است.
- مدل TCP/IPبه علت تعداد لایه های کمتر ساده تر به نظر می رسد.
- پرتوکل TCP/IP استاندارد اینترنت است.

آدرس IP

- برای شناسایی هر سیستم در شبکه دو آدرس یکتا تعریف شده است.
  - آدرس IP که ۳۲ بیتی است و به صورت دهدهی نمایش داده میشود.
  - آدرس فیزیکی (MAC) که در لایه پیوند دادهها قرار دارد.
- هرآدرس IP دارای طول کلی چهار بایت می باشد که از ۲ قسمت تشکیل شده است که عبارتند از:
  - بخش مشخص کننده شبکه(Net ID)
  - بخش مشخص کننده میزبان (Host ID)
  - آدرس زیر شبکه (درصورت لزوم)

آدرس IP

- آدرس IP یک عدد ۳۲ بیتی منحصر به فرد و جهانی است که به هر کامپیوتر یا مسیریاب متصل به اینترنت نسبت داده می شود.
- برقراری ارتباط در یک شبکه ، مستلزم مشخص شدن آدرس کامپیوترهای مبداء و مقصد است. آدرس هریک از دستگاه های درگیر در فرآیند ارتباط ، توسط عدد منحصربفرد IP مشخص میگردند.
- در این روش نمادگذاری هر عدد باینری به ۴ بایت ۸ بیتی مجزا تقسیم شده که توسط نقطه از یکدیگر جدا می شوند و هر بایت توسط یک عدد دسیمال (صفر تا ۲۵۵)نمایش داده می شود.

آدرس IP

- آدرس IP به پنج کلاس مختلف A,B,C,D,E تقسیم می شوند.
- برای این که مشخص شود هر دستگاه متصل به شبکه متعلق به کدام کلاس است عدد دسیمال اول نشان دهنده کلاس یک آدرس است.
- کلاس های A,B,C دارای دو قسمت شماره شبکه (Network ID) و شماره میزبان (Host ID) است.
- قسمت شماره شبکه برای مشخص کردن شبکه ای است که دستگاه (کامپیوتر یا مسیریاب) به آن متصل است.
- شماره میزبان ، شماره آن دستگاه متصل به شبکه است.

آدرس IP

- آدرس IP می تواند یکی از انواع زیر باشد :

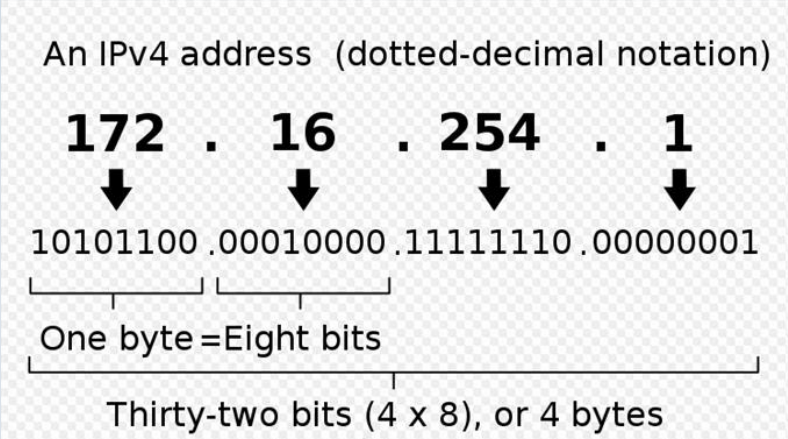
- Unicast: به یک اینترفیس شبکه متصل شده به یک شبکه مبتنی برIP نسبت داده می شود.

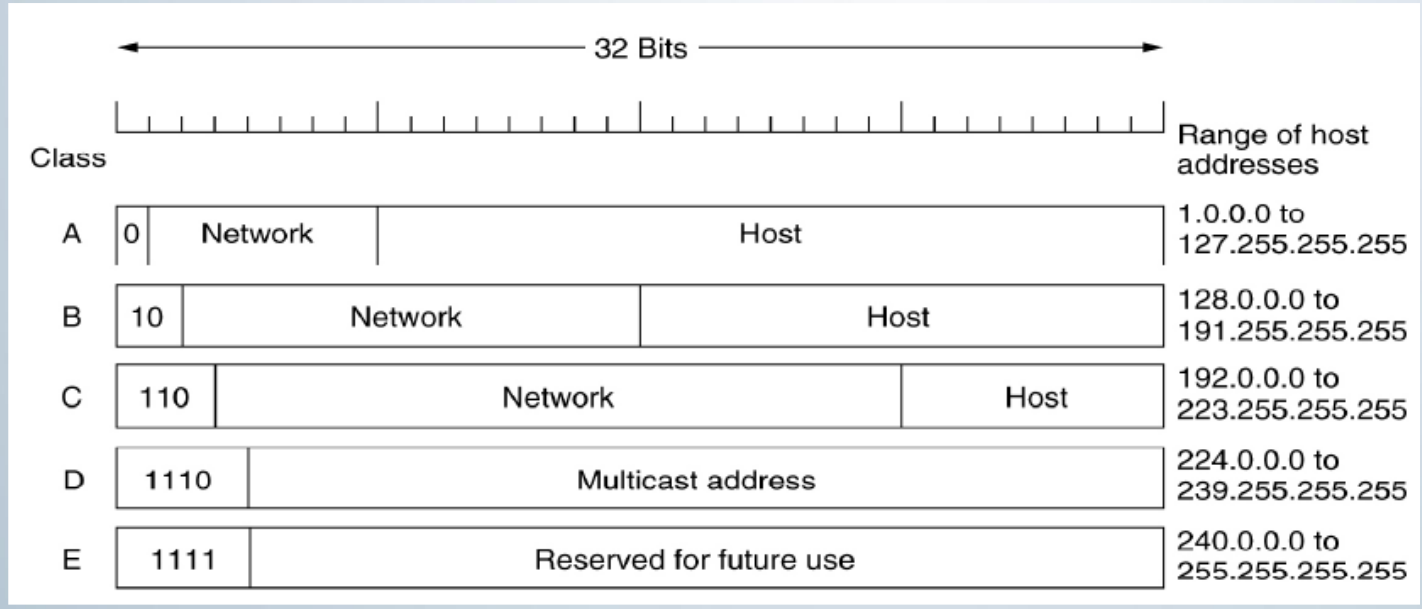
در ارتباطات "یک به یک" (One-To-One) استفاده می گردند .

- Broadcast: به منظور پردازش توسط هرگره موجود بر روی سگمنت یکسان شبکه ، طراحی شده است. در ارتباطات از نوع "یک به همه" (one-to-everyone) استفاده می گردند .

- Multicast: آدرسی است که یک و یا چندین گره را قادر به گوش دادن به سگمنت های مشابه و یا متفاوت می نماید. ارتباط از نوع "یک به چند" (one-to-many) را فراهم می نمایند .

کلاس بندی آدرس IP

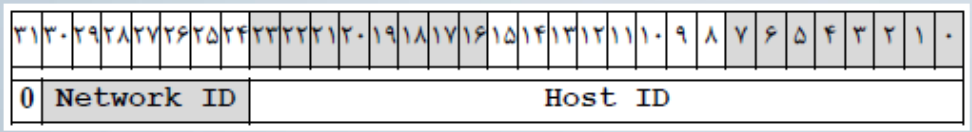




کلاس A

- در کلاس A پر ارزشترین بیت آدرس مقدار صفر دارد و این بیت کلاس A را از دیگر کلاس ها متمایز می کند.۷ بیت بعدی"مشخصه آدرس شبکه"و ۲۴ بیت باقیمانده"آدرس ماشین میزبان"را تعیین می کند. بنابراین در کلاس A بایت پر ارزش در محدوده صفرتا۱۲۷ تغییر می کند. چون با ۲۴ بیت می توان حدود ۱۷ میلیون ماشین میزبان را آدرس دهی کرد. مشخصه شبکه در این کلاس به هیچ وجه نمی تواند اعداد صفریا ۱۲۷ انتخاب شود چرا که این دو عدد در شبکه رزرو شده هستند بنابراین تعداد شبکه‌هایی که در جهان می توانند از کلاس A استفاده کنند۱۲۶ تا است . با نگاهی ساده به یک آدرس IP که در قالب ده دهی نوشته شده است براحتی می توان کلاس آن را تشخیص داد اگر عدد سمت چپ آدرس بین صفرتا ۱۲۷ باشدآن آدرس متعلق به کلاس A است.امروزه اختصاص آدرسهای کلاس A غیر ممکن است چرا که همهٔ آنها توسط پیشگامان شبکه قبلا تملیک شده اند.

Class	Start	End	CIDR	Bit	Subnet mask
Class A	**0.0.0.0**	**127.255.255.255**	**/8**	**0**	**255.0.0.0**



کلاس B

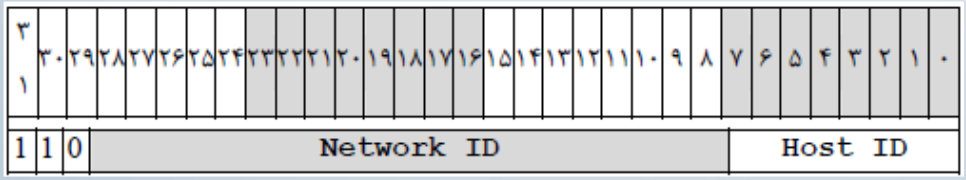
- هرگاه دو بیت پر ارزش از آدرس IP مقدار ۱۰ داشته باشد آن آدرس از کلاس B خواهد بود. ۱۴ بیت باقیمانده از ۲ بایت سمت چپ آدرس شبکه را تعیین می کند و دو بایت اول از سمت راست (۱۶ بیت) آدرس ماشین میزبان خواهد بود. در آدرس کلاس های B تعداد ۱۶۳۸۲ شبکه گوناگون قابل تعریف است و هر شبکه می تواند ۶۵۵۳۴ ماشین میزبان تعریف کند. اختصاص آدرس‌های کلاس B برای شبکه های بسیار عظیم مناسب است. هر چند تعداد این شبکه در جهان می تواند تا حدود شانزده هزار عدد باشد و لیکن امروزه عملا نمی‌توان آدرس کلاس B گرفت چرا که تقریبا همه آنها رزرو شده اند. اگر آدرسIP به صورت ده دهی نوشته شود و عدد سمت چپ آن بین ۱۲۸ تا ۱۹۱ باشد آن آدرس متعلق به کلاس B خواهد بود.

Class	Start	End	CIDR	Bit	Subnet mask
Class B	**128.0.0.0**	**191.255.255.255**	**/16**	**10**	**255.255.0.0**

کلاس C

- کلاس C مناسبترین و پرکاربردترین کلاس از آدرسهای IP است. همانگونه که در شکل مشخص است در این کلاس سه بیت پر ارزش از هر آدرس دارای مقدار ۱۱۰ است و ۲۱ بیت بعدی از سه بایت سمت چپ برای تعیین هویت شبکه مورد نظر بکار رفته است. بنابراین در این کلاس می توان حدود دو میلیون شبکه را در جهان آدرس‌دهی کرد و هر شبکه می تواند تا ۲۵۴ عدد ماشین میزبان تعریف کند. برای تشخیص آدرسهای کلاس C به عدد سمت چپ از آدرس IP که به صورت دهدهی نوشته شده است نگاه کنید، اگر عدد سمت چپ آن بین۱۹۲ تا ۲۲۳ بود آن آدرس از کلاس C خواهد بود:

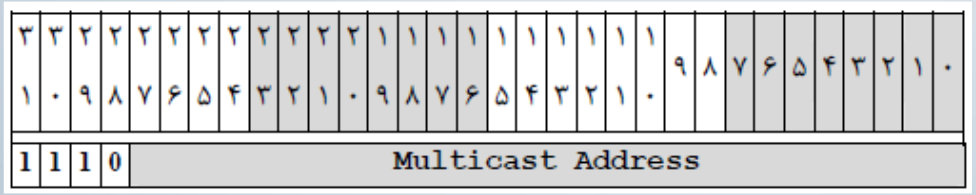
Class	Start	End	CIDR	Bit	Subnet mask
Class C	**192.0.0.0**	**223.255.255.255**	**/24**	**110**	**255.255.255.0**



کلاس D

- در این کلاس چهار بیت پرارزش دارای مقدار ۱۱۱۰ است. ۲۸ بیت باقیمانده از کل آدرس برای تعیین آدرسهای "چند پخشی" است. این آدرسها برای ارسال یک دیتا گرام واحد به طور همزمان برای چندین ماشین میزبان کاربرد دارد و به منظور عملیات رسانه ای و چند پخشی مورد استفاده قرار میگیرد و اگر عدد سمت چپ آن بین۲۲۴ تا ۲۳۹ بود آن آدرس از کلاس D خواهد بود.
- کاربرد این آدرسها Multi cast در ویدئو کنفرانس ها می باشد که یک نفر می خواهد سرویس اطلاعات را به جمعی از کاربران بفرستد نه برای یک شخص خاص.

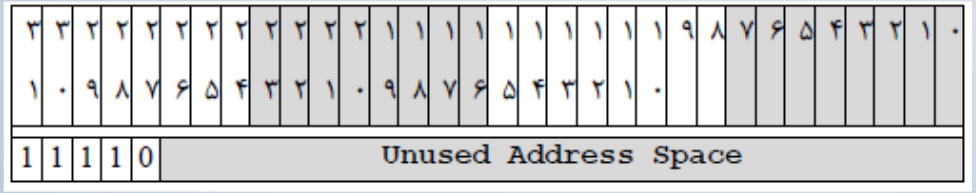
Class	Start	End	CIDR	Bit	Subnet mask
Class D	**224.0.0.0**	**239.255.255.255**	**/4**	**1110**	**-**



کلاس E

- فعلا این دسته از آدرسها که ۵ بیت پر ارزش آنها در سمت چپ معادل ۱۱۱۱۰ است کاربرد خاصی ندارند و به منظور استفاده در آینده بدون استفاده رها شده‌اند.
- البته گاهی به صورت آزمایشی از این آدرسها استفاده شده ولی هرگز جهانی و فراگیر نشدند اگر عدد بین۲۴۰ تا ۲۵۵ بود آن آدرس از کلاس E خواهد بود.

Class	Start	End	CIDR	Bit	Subnet mask
Class E	**240.0.0.0**	**255.255.255.255**	**/4**	**1111**	**-**



انواع آدرس IP

- معتبر (Valid): در شبکه اینترنت به نام شبکه سرویس دهنده یا سرویس گیرنده که از آن IP استفاده می کند تعریف شده است و شناخته شده می باشد و کلیه بسته های اینترنتی با آن نشانی ها به سمت شبکه‌ای که آن IP متعلق به آن است مسیر دهی می‌شود. (در قالب ip آدرس بگنجد)
- غیرمعتبر(Invalid): در شبکه اینترنت مسیردهی نمیشود و به طور خاص برای شبکه‌ای تعریف نشده است (متعلق به شبکه‌ای نیست) و جهت مصارف داخلی و ارتباطات داخل شبکه‌ای بکار می‌رود.

10.x.x.x	10.x.x.x
172.16.0.0	172.31.0.0
192.168.1.0	192.168.255.0

- سیستمی که آدرس نامعتبر دارد برای تماس با دنیای بیرون نیاز به یک آدرس معتبر که از دنیای بیرون شناخته شده است دارد. برای ترجمه‌ی آدرس نامعتبر به آدرس معتبر (برای اتصال با دنیای بیرون) از NAT استفاده می‌شود.

انواع آدرس IP

- **پویا (Dynamic): با هر بار وصل شدن به شبکه داخلی و یا اینترنت تغییر می‌کند و در هر شبکه توسط (DHCP Server) به کامپیوترها در شبکه اختصاص داده می‌شود. یعنی وقتی شما به اینترنت و یا شبکه داخلی وصل می‌شوید، DHCP به شما یک نشانی آی‌پی اختصاص می‌دهد.**

- **ایستا (Static): با هر بار وصل‌شدن به شبکه داخلی و یا اینترنت تغییر نمی‌کند.**
- **DHCP Server می‌تواند یک سرویس در سیستم‌عامل‌های سرور باشد یا یک قطعه سخت‌افزاری مانند مسیریاب (Router) و یا نقطه دسترسی (Access Point) در شبکه باشد.**

انواع آدرس IP

- **خصوصی (Private address): برای تعیین شبکه های محلی استفاده میشود و برای استفاده از آنها احتیاج به هیچ مجوزی نیست.**

- **عمومی (public address): برای تعیین شبکه های عمومی استفاده میشود و باید از سازمان IANA مجوز داشت**

Private IP Address		
Class A	**10.0.0.0**	**10.255.255.255**
Class B	**172.16.0.0**	**172.31.255.255**
Class C	**192.168.0.0**	**192.168.255.255**

(Classless Inter-Domain Routing) **CIDR**

- **مسیریابی بر اساس آدرس های بدون کلاس:**

یک روش است برای تخصیص دادن یک مقدار از آدرس به یک کمپانی و یا مشتری.

Subnet Mask: 255.192. 0.0/10

11111111.11000000.00000000.00000000 : 8+2+0+0 =10

- نشان slash به معنای این است که چه مقدار bits روشن است

- بیشترین مقدار cidr می تواند ۳۲/ باشد اما باتوجه به اینکه بایستی حداقل ۲ بیت برای host Bits نگه داشت ، بیشترین مقدار می تواند ۳۰/ باشد.

CIDR

Subnet Mask	CIDR value	Subnet Mask	CIDR value
255.0.0.0	**/8**	255.255.240.0	**/20**
255.128.0.0	**/9**	255.255.248.0	**/21**
255.192.0.0	**/10**	255.255.252.0	**/22**
255.224.0.0	**/11**	255.255.254.0	**/23**
255.240.0.0	**/12**	255.255.255.0	**/24**
255.248.0.0	**/13**	255.255.255.128	**/25**
255.252.0.0	**/14**	255.255.255.192	**/26**
255.254.0.0	**/15**	255.255.255.224	**/27**
255.255.0.0	**/16**	255.255.255.240	**/28**
255.255.128.0	**/17**	255.255.255.248	**/29**
255.255.192.0	**/18**	255.255.255.252	**/30**
255.255.224.0	**/19**		

Subnet Mask

- Subnet Mask مشخص میکند که محدوده شبکه ای که کامپیوترشما در آن قرار دارد کجاست.
- به عنوان مثال 255.255.255.0 شبکه ای مشتمل بر ۲۵۴ کامپیوتر است (2-256).
- اگر Subnet به همراه یک IP باشد می توان فهمید IP کامپیوترهای آن شبکه درچه محدوده ای است. مثلا 192.168.1.20 با Subnet ، 255.255.255.0 نشان می دهد کامپیوترهای آن شبکه می توانند IP در محدوده 192.168.1.1 تا 192.168.1.254 داشته باشند .
- اولین آدرس (192.168.1.0) به عنوان آدرس شبکه و آخرین آدرس (192.168.1.255) به عنوان آدرس Broadcast آن شبکه می باشد. این دو آدرس غیر قابل استفاده می باشند.
- Broadcast : از این نوع آدرس ها جهت انتشار بسته های اطلاعاتی برای تمامی دستگاه های موجود بر روی یک شبکه استفاده می گردد .

Subnet Mask

- به صورت قراردادی برای کلاس های IP A,B,C ، Subnet Mask های زیر تعیین گردیده اند.

A	255	0	0	0
	Net	Host	Host	Host
B	255	255	0	0
	Net	Net	Host	Host
C	255	255	255	0
	Net	Net	Net	Host

اعدادی که در subnet mask قابل استفاده اند

Binary	
00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

قوانین استفاده

* ترتیب قرارگیری مهم است
* وقتی یک عدد غیر از ۲۵۵ آمد باید

بعد از آن حتما ۰ باشد

X.0,0,0
255.X.0.0
255.255.X.0
255.255.255.X

255.255.255.0

255.255.252.0

255.252.255.0

IP زیرشبکه

- هر IP از دو قسمت تشکیل شده است که قسمت اول متعلق به آدرس شبکه (Network Address) و قسمت دوم متعلق به آدرس میزبان (Host Address) است.
- Network Address: هر سیستم موجود بر روی شبکه مشابه , به عنوان بخشی از آدرس IP آن در نظر گرفته می شود. بطور مثال ۱۰.۲۰.۲۰.۲۰ با توجه به اینکه IP از کلاس A میباشد عدد ۱۰ مشخص کننده آدرس شبکه در این IP است
- Host Address: هر سیستم موجود بر روی شبکه را مشخص می کند. آدرس هاست بصورت منحصر بفرد میباشد زیرا این آدرس نشان دهنده یک سیستم خاص بر روی شبکه میباشد. بطور مثال ۱۰.۲۰.۲۰.۲۰ اعداد ۲۰.۲۰.۲۰ آدرس هاست را نشان میدهد.

Subneting

- برای آنکه بتوان زیر شبکه‌ها را تفکیک کرد جدای از قسمت آدرس شبکه(که کل شبکه شرکت شما را تعیین هویت می‌کند) باید به گونه‌ای در بخش "شناسه ماشین میزبان" (Host ID) زیر شبکه ها نیز مشخص شوند.
- این کار از طریق مفهومی به نام " الگوی زیر شبکه" (Subnet Mask) انجام می گیرد.
- به عمل قرض دادن بیتهای Net ID به Host ID در اصطلاح Subneting گفته می شود.
- در واقع عمل Subneting بر روی Host ID صورت می گیرد.
- بیت های Net ID همگی یک می باشد و بیت های Host ID می توانند صفر و یا یک باشند و با تغییر در این بیت ها ، آدرس های IP مختلف ساخته می شود.

Network Address	اولین آدرس IP هر subnet
First Address	اولین آدرس قابل استفاده IP هر subnet
Last Address	آخرین آدرس قابل استفاده IP هر subnet
Broadcast Address	آخرین آدرس IP هر subnet

بدست آوردن مقادیر NA,FA,LA,BA

IP : 192.168.1.10
Subnet : 255.255.255.0

۱- تبدیل به باینری:

IP : 11000000.10101000.00000001.00001010

SM : 11111111.11111111.11111111.00000000

۲- AND کردن دو مقدار بدست آمده:

- تبدیل از باینری به دهدهی: 11000000.10101000.00000001.00000000

NA: 192 . 168 . 1 . 0

- یک کردن اولین صفر از سمت راست : 11000000.10101000.00000001.00000001

FA: 192 . 168 . 1 . 1

- یک رقم کمتر از (BA): 11000000.10101000.00000001.11111110

LA: 192 . 168 . 1 . 254

- تا هرجا یک بود را می نویسیم و بعد از آن صفرها را تبدیل به یک می کنیم:

11000000.10101000.00000001.11111111

BA: 192 . 168 . 1 . 255

بدست آوردن مقادیر NA,FA,LA,BA

IP : 192.168.1.100
Subnet : 255.255.255.252

IP : 11000000.10101000.00000001.01100100

SM : 11111111.11111111.11111111.11111100

11000000.10101000.00000001.01100100

NA: 192 . 168 . 1 . 100

11000000.10101000.00000001.01100101

FA: 192 . 168 . 1 . 101

11000000.10101000.00000001.01100110

LA: 192 . 168 . 1 . 102

11000000.10101000.00000001.01100111

BA: 192 . 168 . 1 . 103

Subneting

- زمانی که عملیات Subneting را بر روی یک IP انجام می دهیم، علاوه بر بدست آوردن مقادیر قبل ، می توان مقادیر زیر را بدست آورد:
  - چه مقدار subnets میتوانیم داشته باشیم؟
  - چه مقدار هاست در هر subnet موجود می باشد ؟
  - چه هاست هایی قابل قبول است؟

Subneting

- چه مقدار subnet می توانیم داشته باشیم

برای بدست آوردن تعداد subnet از فرمول زیر استفاده می کنیم:

2^n ---> 2^8=256

n تعداد بیتهای تعلق گرفته به قسمت network address است.

- چه مقدار هاست در هر subnet موجود می باشد

برای بدست آوردن هاست از فرمول زیر استفاده می کنیم:

(2^n)-2 ----> (2^6)-2=62

در هر subnet شصت و دو هاست موجود میباشد و **2-** همان network address و broad cast address می باشد که قابل استفاده نیستند.

- چه **host** هایی قابل قبول است ؟

- همیشه اعدادی که بین subnet address و broadcast address می باشند هاست های قابل قبول هستند

قوانین مشخصه شبکه (Network ID)

- در زمان استفاده از مشخصه شبکه ، قوانین زیر رعایت می گردد:
- مشخصه شبکه نمی تواند با ۱۲۷ بعنوان اولین Octet آغاز گردد. تمامی آدرس های IP:127.x.x.x بعنوان آدرس های Loopback رزو شده می باشند .
- تمامی بیت های مشخصه شبکه ، نمی تواند ارزش یک را داشته باشد. مشخصه های شبکه که مقدار تمامی بیت های آن یک است ، بمنظور آدرس های Broadcast رزو شده اند .
- تمامی بیت های مشخصه شبکه ، نمی تواند ارزش صفر را داشته باشد. مشخصه های شبکه که مقدار تمامی بیت های آن صفر است ، یک میزبان بر روی شبکه محلی را مشخص می نمایند.
- مشخصه شبکه در شبکه های مبتنی بر IP عمومی ، می بایست منحصربفرد باشد .

Class	First Network ID	Last Network ID	Net's
A	1.0.0.0	126.0.0.0	126
B	128.0.0.0	191.255.0.0	16.384
C	192.0.0.0	223.255.255.0	2.097.152

قوانین مشخصه های میزبان (Host ID)

- در زمان استفاده از مشخصه میزبان ، قوانین زیر رعایت می گردد :
- تمامی بیت ها ی مشخصه میزبان ، نمی تواند ارزش یک را داشته باشد . مشخصه های میزبان که مقدار تمامی بیت های آن یک است ، برای آدرس های Broadcast رزو شده اند .
- تمامی بیت های مشخصه میزبان، نمی تواند ارزش صفر را داشته باشد. مشخصه های میزبان که مقدار تمامی بیت های آن صفر است ، برای ارائه IP مربوط به مشخصه های شبکه ، رزو شده اند .
- مشخصه میزبان می بایست در شبکه، منحصر بفرد باشد .
- جدول زیر محدوده کلاس های آدرس دهی برای مشخصه میزبان را نشان می دهد.

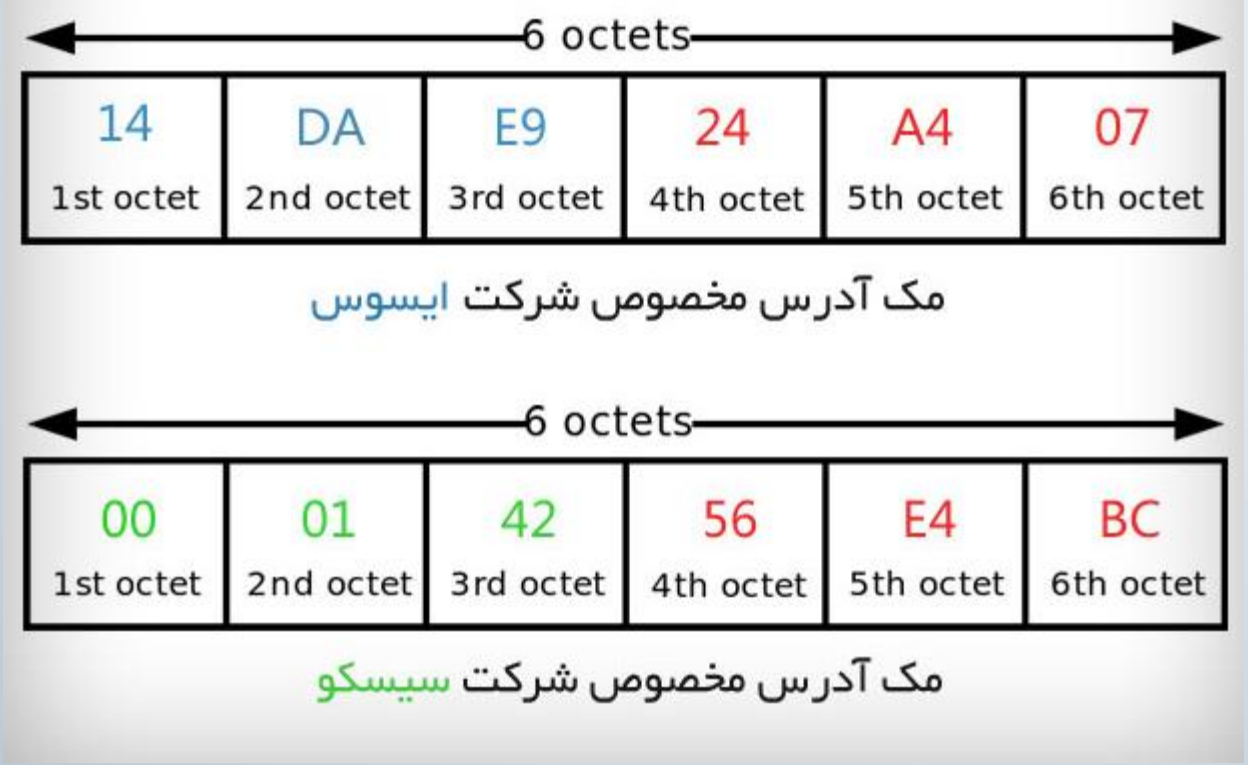
Class	First Host ID	Last Host ID	Host's
A	w.0.0.1	w.255.255.254	16.777.214
B	w.x.0.1	w.x.255.254	65.534
C	w.x.y.1	w.x.y.254	254

آدرس فیزیکی (MAC Address)

- مخفف عبارت Media Access Control Address به معنای "زیرلایه کنترل دسترسی به رسانه" بوده و یک آدرس فیزیکی ۶ یا ۸ بایتی است که توسط سازنده‌های کارت‌های واسط شبکه بر روی حافظه آن (اغلب بر روی رام حافظه فقط خواندنی) ذخیره می‌کنند.
- آدرس مک معمولاً آدرس فیزیکی نیز خوانده می‌شود.
- تمامی دستگاه‌هایی که به هر طریقی به یک شبکه متصل می‌شوند (از جمله تلفن‌های هوشمند، مودم‌های خانگی، لپ تاپ‌ها و...) دارای یک مک آدرس جداگانه هستند.
- متشکل از ۶ بخش ۸ بیتی است که هر بایت توسط یک جفت کاراکتر هگزادسیمال نشان داده می‌شود.هربخش توسط کاراکترهای دونقطه(:) یا خط تیره(-) و گاهاً نقطه(.) از یکدیگر جدا می‌شوند.

D0-DF-9A-C8-9F-6B

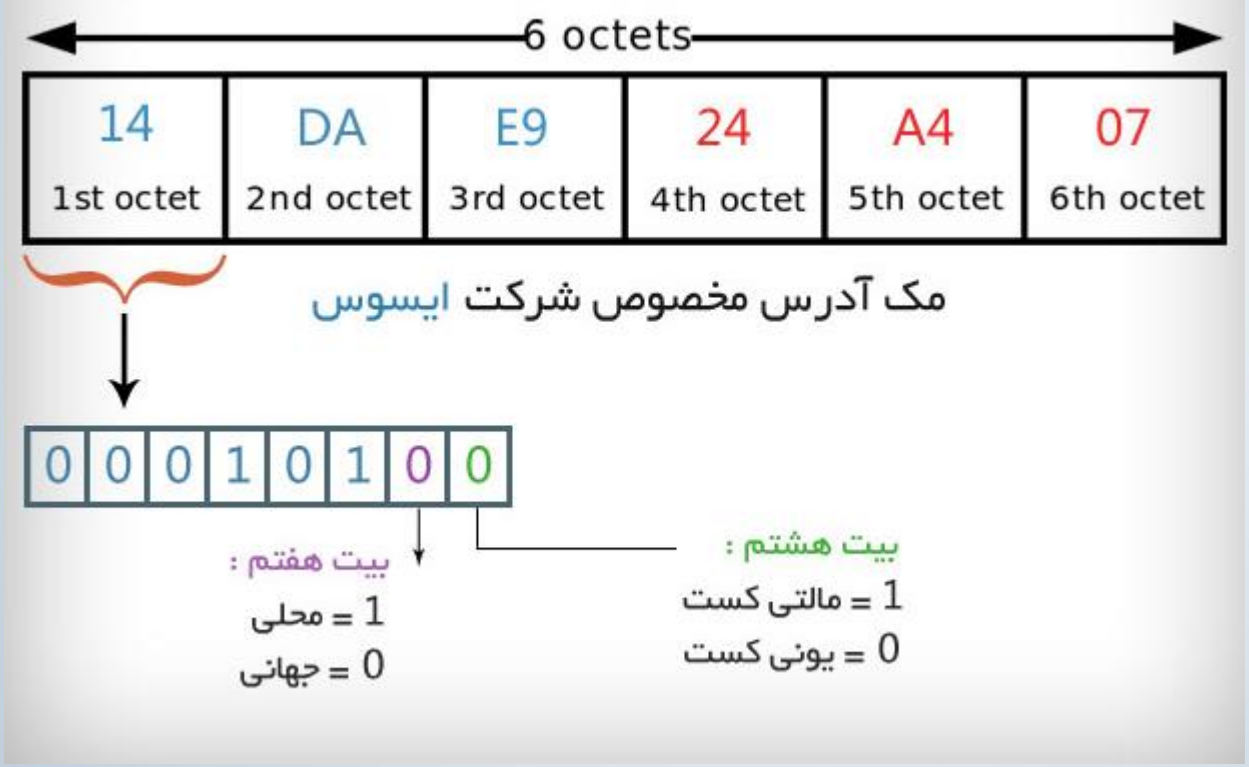
تشریح MAC Address



تشریح MAC Address

- آدرس دهی مک به صورت کلی به دو نوع محلی(Locally) و جهانی (Universally) تقسیم می‌شوند. در نوع محلی آدرس مک توسط مدیر شبکه تعیین می‌شود و در نوع جهانی این آدرس از پیش توسط شرکت سازنده تعیین می‌شود.
- محلی یا جهانی بودن آدرس از طریق هفتمین بیت بایت اول تشخیص داده می‌شود. درصورتی که هفتمین بیت بایت اول یک باشد، آدرس مک ما به صورت محلی است و تمامی کارت‌های شبکه که توسط شرکت‌ها ساخته می‌شوند بیت هفتم بایت اول آن‌ها بر روی صفر تنظیم می‌شود.

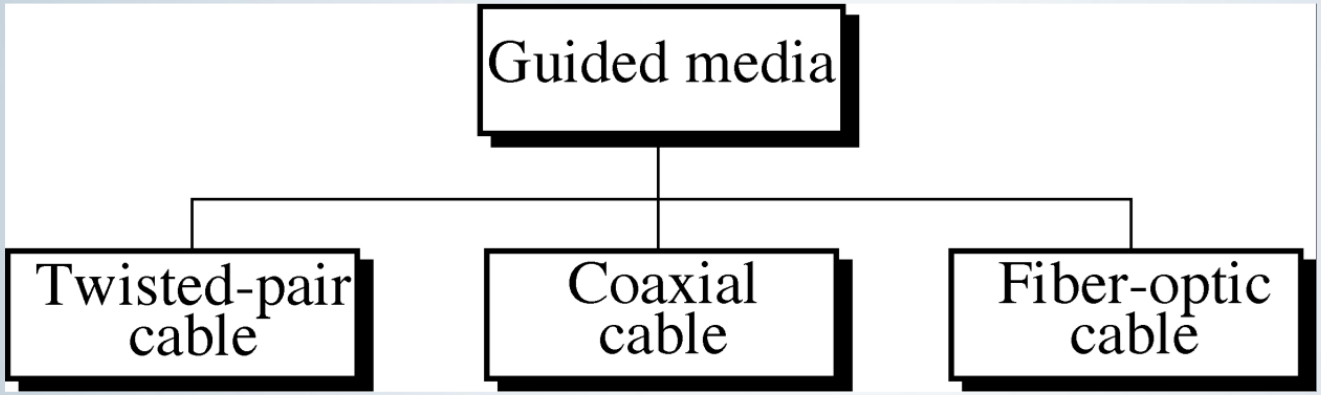
تشریح MAC Address



لایه فیزیکی

- **وظیفه سخت افزار انتقال در لایه فیزیکی: انتقال بیتهای داده بر روی کانال فیزیکی بدون توجه به نوع و محتوای دادها**
- **انتقال داده در کامپیوترها و دیگر اجزای کامپیوتری از طریق رسانه انتقال یا کانال انجام می شود.**
- **رسانه انتقال در پایین لایه فیزیکی قرار می گیرد و مستقیماً توسط لایه فیزیکی کنترل می شود.**
- **کابل شبکه، رسانه ای است که از طریق آن، اطلاعات از یک دستگاه موجود در شبکه به دستگاه دیگرانتقال می یابد .انواع مختلفی از کابلها بطور معمول در شبکه های LAN استفاده می شوند . در برخی موارد شبکه تنها از یک نوع کابل استفاده می کند، اما گاه انواعی از کابلها در شبکه به کار گرفته می شود. غیر از عامل توپولوژی، پروتکل و اندازه شبکه نیز در انتخاب کابل شبکه مؤثرند.**

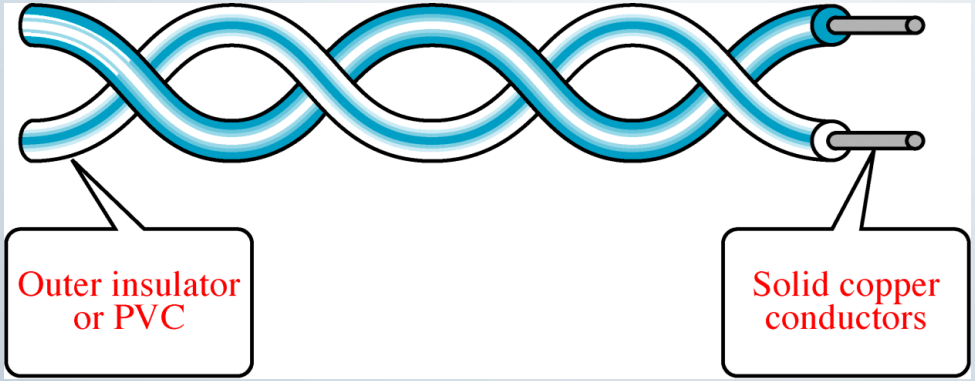
محیط های رایج انتقال اطلاعات



- کابل زوج یه هم تابیده
- کابل کواکسیال
- فیبرهای نوری
- بی سیم

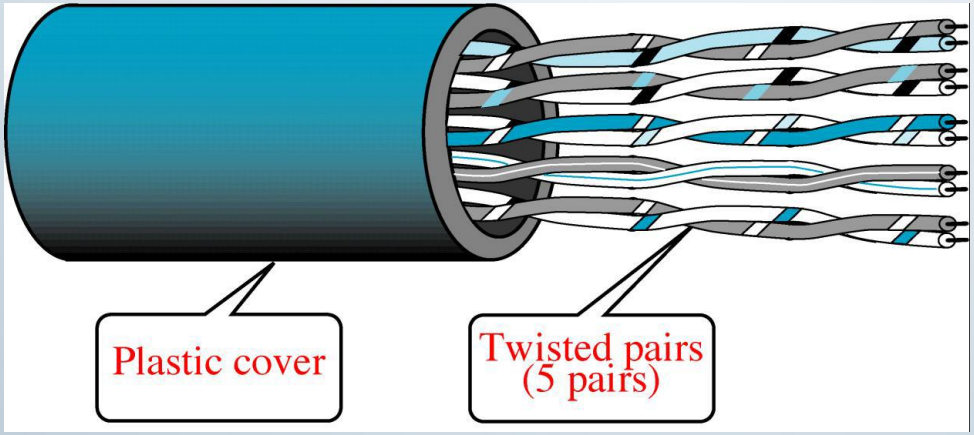
کابل های Twisted-Pair

- یکی از قدیمی ترین رسانه های انتقال می باشد که شامل دو سیم مسی عایق دار است که به صورت مارپیچ بهم تابیده شده اند.
- علت اصلی تابیدن سیم‌ها، کاهش اثر آنتن در دریافت سیگنال اغتشاش بیرونی می‌باشد.



کابل های Twisted-Pair

- تقسیم بندی کابل های زوج به هم تابیده :
  - Shielded Twisted-Pair (STP)
  - Un Shielded Twisted-Pair (UTP)
- در نوع اول ، یک پوشش روی کابل ها وجود دارد که اثر نویز را کم می کند و در کار های صنعتی از این نوع کابل استفاده می گردد و گران تر از نوع دوم می باشد.



کابل های Twisted-Pair

- UTP :

- دارای گونه ها و رده های مختلفی از رده یک CAT1 تا رده هفتCAT7

- هر چه رده UTP بالاتر می رود تعداد پیچش آن بیشتر شده و در مقابل نویز مقاوم تر می شود.

نوع	نرخ انتقال	فرکانس	بیشترین طول	تعداد جفت	کاربرد
Cat1	1 Mbps	1 MHz	90 meters	1 pair	Telephone and ISDN
Cat2	4 Mbps	1 MHz	90 meters	2 pairs	Token ring
Cat3	10 Mbps	16 MHz	100 meters	3 or 4 pairs	10BaseT (Can reach 100 Mbps with 100VGAnyLAN)
Cat4	16 Mbps	16 MHz	100 meters	4 pairs	Token ring
Cat5	10 Mbps 1 Gbps if using all 4 pairs	100 MHz	100 meters	4 pairs	10BaseT and 100BaseT 155 Mbps ATM Gigabit Ethernet
Cat5e	1000 Mbps	100 MHz	100 meters	4 pairs	Gigabit Ethernet
Cat6	4-10 Gbps	250 MHz	100 meters	4 pairs	Gigabit Ethernet, uses all 4 pairs

کابل های Twisted-Pair

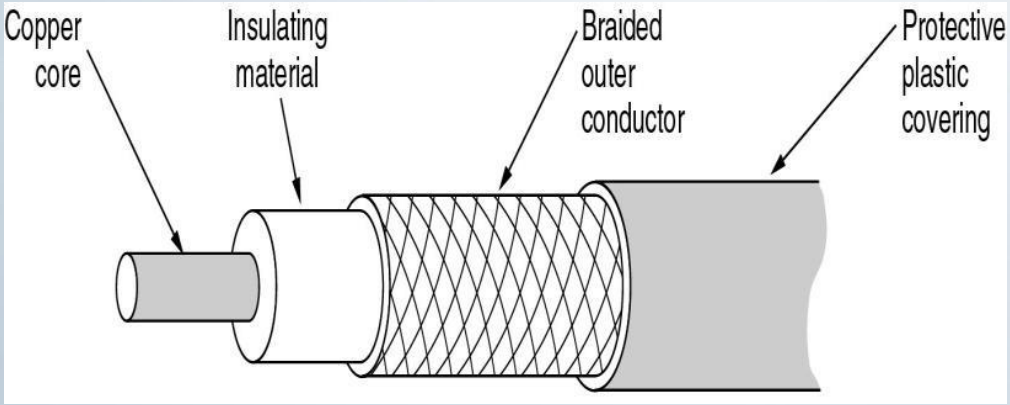
- کاربردهای کابل Twisted-Pair
  - سیم کشی عادی
  - شبکه تلفن
  - بین ساختمان ها
  - شبکه های LAN

کابل های Twisted-Pair

- **مزایا:**
  - **سادگی و نصب آسان**
  - **انعطاف پذیری مناسب**
  - **دارای وزن کم بوده و براحتی بهم تابیده می گردند.**
- **معایب:**
  - **پایین بودن پهنای باند (نسبت به دیگر رسانه های انتقال)**
  - **نویزپذیری زیاد در محیط های الکتریکی**
  - **نیاز به تکرارگر در مسافت های کوتاه (تضعیف زیاد)**
  - **وجود پدیده تشعشع بدین معنی که زوج سیم مانند آنتن عمل کرده و باعث انتشار اطلاعات درون خود به محیط خارج می شود لذا در مقابل استراق سمع امنیت ندارد.**

کابل Coaxial

- Conducting Core: هسته مرکزی آن معمولاً از یک رشته سیم جامد مسی تشکیل می گردد.
- Insulation: عایقی معمولاً از جنس pvc یا تفلون است.
- Copper Wire Mesh: آن از سیم های بافته شده تشکیل می شود و کار آن جمع آوری امواج الکترومغناطیسی است.
- Jacket: جنس آن اغلب از پلاستیک بوده و نگهدارنده خارجی سیم در برابر خطرات فیزیکی است.



کابل Coaxial

- انواع کابل Coaxial

  - کابل های ۱۱ اهمی : انتقال اطلاعات در آن های به صورت Digital است .

  - کابل های ۱۱ اهمی : انتقال اطلاعات در آن های به صورت Analog است .

- کاربرد کابل های Coaxial

  - تلویزیون (Television Distribution) به دلیل پهنای باند بالا .

  - بین مراکز تلفن (Long distance Telephone Transmission)

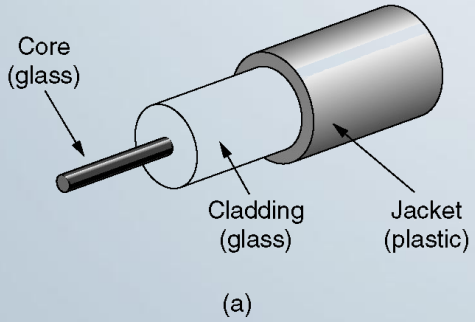
  - شبکه های LAN: با سرعت ۱۰ مگابیت که از کابل ۵۰ اهمی دیجیتال است و محدودیت کابل و پهنای باند ندارد .

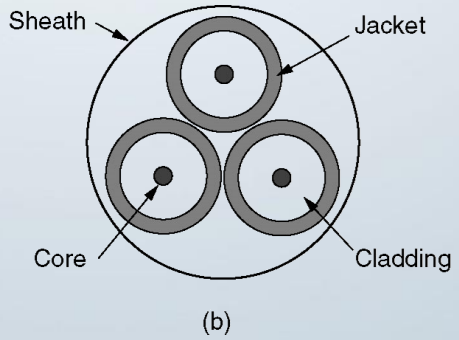
کابل Coaxial

- مزایای کابل های کواکس :
  - قابلیت اعتماد بالا
  - ظرفیت بالای انتقال ، حداکثر پهنای باند ۳۰۰ مگاهرتز
  - دوام و پایداری خوب
  - پایین بودن مخارج نگهداری
  - قابل استفاده در سیستم های آنالوگ و دیجیتال
  - هزینه پائین در زمان توسعه
- معایب کابل های کواکس :
  - مخارج بالای نصب
  - نصب مشکل تر نسبت به کابل های بهم تابیده
  - محدودیت فاصله
  - نیاز به استفاده از عناصر خاص برای انشعابات

فیبر نوری Fibre Optic

- فیبر نوری از ترکیبات خاص پلاستیک فشرده یا سیلیس ساخته می شوند و میتواند پالس های نور را از یک سمت به سمت دیگر هدایت کند.
- 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 آن ها است.
- Coating لایه محافظ فیبر است، بعضی اوقات فقط یک PVC پلاستیک است که روی cladding قرار میگیرد و گاهی از یک مایعی ژله مانند برای محافظت در برابر حشرات(جوندگان...)،آب(آب به داخل کابل نفوذ نکند)، آتش(اگر یک نقطه آتش گرفت بقیه کابل آتش نگیرد)و... نیز استفاده میشود.

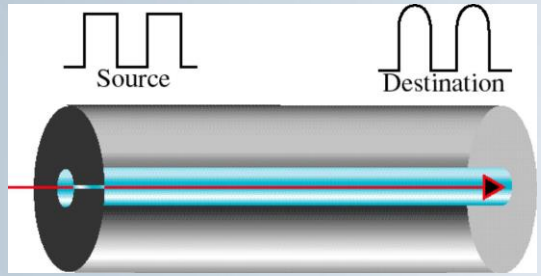




ویژگی های فیبر نوری

- پهنای باند بالا یا ظرفیت بیشتر (صد ها گیگابیت در ثانیه)
- سایز و وزن کم .
- تضعیف کم .
- ایزوله بودن در برابر امواج الکترومغناطیسی . (از نور استفاده می شود و نور به دلیل اینکه باری ندارد ، میدانی بوجود نمی آورد)
- برای افزایش برد انتقال اطلاعات در صورت تضعیف ، از تکرار کننده یا تقویت کننده استفاده می شود.
- کابل ارزان اما مبدل ها و اتصالات گران.
- امنیت اطلاعات

انواع فیبر های نوری

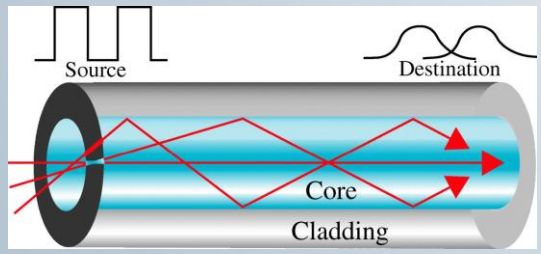


Single Mode

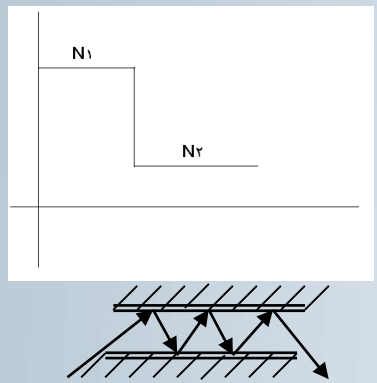
- هسته باریکتر.
- تلفات کم.
- تنها از مولد لیزری می توان استفاده کرد (پروتکل موج).
- برای نرخ چند ده گیگا(سرعت زیاد).
- فواصل طولانی(یک رشته پالس نوری منفرد در تارمی توان ارسال نمود).

Multi Mode

- می توان از LED استفاده کرد.
- چندین پالس نوری با زوایای مختلف در داخل فیبر منتقل می گردد.
- سرعت کم.
- برد کم.
- تلفات زیاد.
- در فواصل کوتاه استفاده میشود.



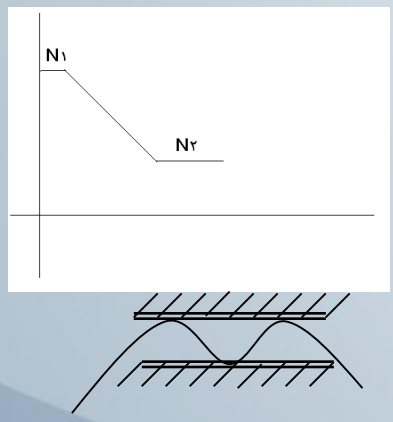
انواع فیبر نوری



Multi Mode:

Step Index Multi Mode:

- ضریب شکست در مرز هسته و روکش به صورت ناگهانی تغییر می کند .
- قطر هسته بین 50 تا 100 میکرون است.
- مشکل پهن شدگی پالس در زمان وارد شدن .
- تلفات زیاد.
- پرتو هایی که زاویه بیشتری نسبت به خط قائم دارند مسیر کوتاهتر با تضعیف کمتری طی می کنند .



Graded Index Multi Mode:

- ضریب شکست به صورت تدریجی کاهش می یابد.
- قطر هسته بین 50تا 62.5 میکرون است.
- تلفات کم.

انواع فیبر نوری

- Indoor:
  - تعداد Coreکمتر.
  - ارزان.
  - انعطاف پذیری زیاد.
  - محافظ کمتر.
- Outdoor:
  - دارای محافظ ضد آب ، آتش ، حشره (حلقه ی استیل) و... .
  - تعداد coreزیاد.
  - انعطاف پذیری کم.
  - گران.

- افقی:
  - ارزان تر.
  - Coatingخاص نیست.

- عمودی:
  - Coatingوزن فیبر را نگه میداردتا بر اثر وزن و طول زیاد نشکند.
  - گرانتر.

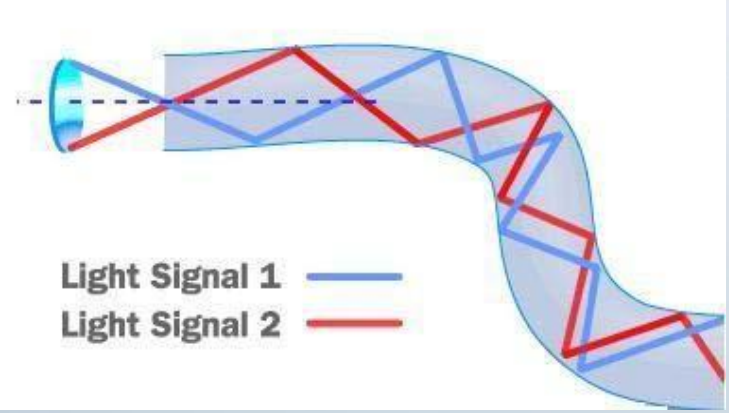
فیبر نوری

اجزای سیستم انتقال نوری عبارتند از:

منبع نور: دیود نوری معمولی یا لیزری که وظیفه آن تبدیل سیگنال الکتریکی موجود در کامپیوترها به نور است.

رسانه انتقال: فیبر نوری که انتقال دهنده نور است.

گیرنده نوری یا آشکارساز : فتودیود یا دیود حساس به نور که وظیفه آن تبدیل سیگنال های نوری به سیگنال های الکتریکی قابل فهم برای کامپیوترها است.



بی سیم

- در شبکه های بی سیم رسانه انتقال فضای آزاد است.
- عمل انتقال داده توسط سیگنال ها و امواج الکترومغناطیسی و از طریق فضای آزاد انجام می شود.
- با توجه به محدوده فرکانس به امواج زیر تقسیم می شوند:
  - امواج رادیویی
  - امواج ماکرویو
  - امواج مادون قرمز
  - بلوتوث

بی سیم

- امواج الکترومغناطیسی در محدوده فرکانس بین 3 KHZ تا 1 GHZ **امواج رادیویی** نامیده می شوند. این امواج در تمام جهات منتشر می شوند و نیازی به این نیست که آنتن فرستند و گیرنده روبروی هم باشد. مانند امواج رادیویی FM
- امواج الکترومغناطیسی در محدوده فرکانس بین 1GHZ تا 300 GHZ را **امواج مایکروویو** می نامند. این امواج به صورت مستقیم منتشر می شوند بنابراین آنتن فرستنده و گیرنده بایستی دقیقاً روبروی یکدیگر باشند.
- امواج الکترومغناطیسی در محدوده فرکانس بین 300 GHZ تا 400 THZ را به نام سیگنال های **مادون قرمز** می نامند. به علت فرکانس بالا این امواج نمی توانند از دیوار و یا جسم سخت عبور کنند

بی سیم

- **بلوتوث، امواج الکترومغناطیسی با فرکانس 2.4 GHZ است که برای استفاده از این محدوده فرکانس، نیازی به کسب اجازه رسمی نیست.**
- **از بلوتوث برای ارتباط و انتقال داده در فواصل کوتاه از 10 CM تا 10 M استفاده می شود.**
- **بر عکس سیگنال های مادون قرمز ، بلوتوث از دیوارها و اجسام غیرفلزی عبور می کند.**
- **شبکه های بی سیم نسبت به نویز بسیار حساس هستند و به صورت پخش همگانی منتشر می شوند و معمولاً امنیت پایینی دارند**

بی سیم

نوع کانال	پهنای باند	خطا	پیاده سازی	قیمت	توضیح
خطوط تلفن معمولی	کم (حدود ۴ KH)	**زیاد**	ساده	ارزان	از قبل وجود دارد
زوج سیم	متوسط (حدود چند ده تا صد مگاهرتز)	**متوسط**	ساده	ارزان	برای فواصل کوتاه مناسب است
کواکس	حدود چند صد مگاهرتز	**کم**	متوسط	متوسط	
فیبرهای نوری	حدود چند گیگا هرتز	**بسیار کم**	پیچیده	متوسط	بهترین کارایی
کانالهای ماهواره	حدود چند صد مگا هرتز	**متوسط**	**بسیار پیچیده**	گران	در همه جا تحت پوشش
کانالهای رادیویی	حدود چند مگا هرتز	**زیاد**	نسبتا پیچیده	نسبتا گران	در جایی که کابل کشی عقلایی نیست مناسب می باشد .

پهنای باند

- در اصطلاح مخابراتی پهنای باند یک رسانه انتقال محدوده فرکانسی است که آن رسانه می تواند منتقل کند.
- در اصطلاح شبکه های کامپیوتری حداکثر مقدار اطلاعاتی است که در واحد زمان از یک نقطه به نقطه دیگر می تواند انتقال یابد پهنای باند می گویند.
- پهنای باند یکی از خواص فیزیکی رسانه انتقال است و معمولاً به شکل، نوع، ضخامت و طول آن بستگی دارد.
- محدود کردن پهنای باند باعث محدود شدن نرخ انتقال اطلاعات خواهد شد.
- واحد پهنای باند بیت بر ثانیه است.

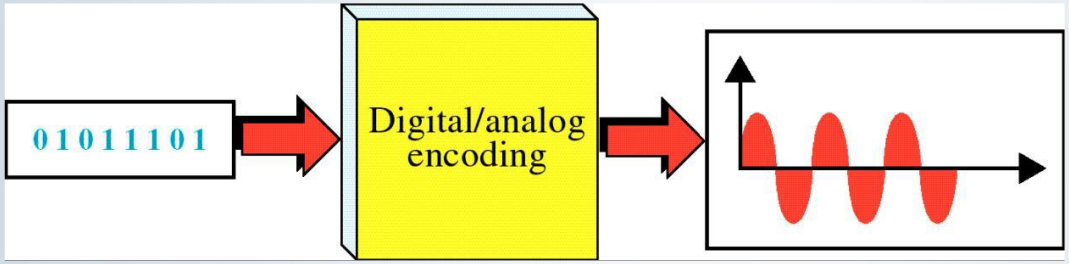
کدگذاری

- **کد گذاری اطلاعات** (Encoding):
- **در لایه فیزیکی ورودی به صورت صفر و یک است و خروجی سیگنال متناسب با محیط می باشد .**

- **تکنیک های مختلف کد گذاری :**
  - **ورودی داده دیجیتال و خروجی سیگنال آنالوگ باشد.(مانند مودم)**
  - **ورودی داده دیجیتال و خروجی سیگنال دیجیتال باشد . (مانند تلویزیون)**
  - **ورودی داده آنالوگ و خروجی سیگنال آنالوگ باشد.(مانند تلفن)**

دیجیتال به آنالوگ

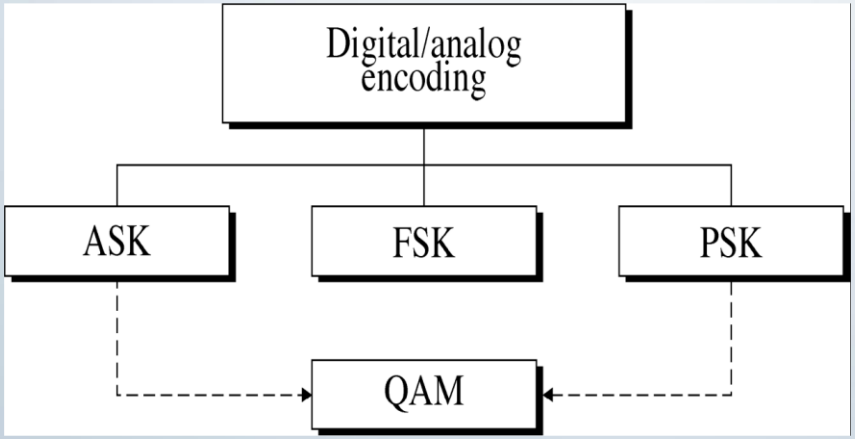
- در این حالت همانطور که گفته شد ورودی صفر و یک و خروجی سیگنال متناسب با محیط می باشد



- پارامتر کلیدی برای کد گذاری اطلاعات در محیط آنالوگ عبارتند از :
  - **A**: دامنه
  - **P**: تعداد تکرار ها در واحد زمان(فرکانس).
  - **F**: اختلاف نسبی نسبت به زمان (فاز)

دیجیتال به آنالوگ

- روش های تبدیل نمادهای صفر و یک به نمادهای آنالوگ :
  - **ASK**: از ویژگی دامنه برای ساختن نمادهای آنالوگ استفاده می کند .
  - **FSK**: از ویژگی فرکانس برای ساختن نمادهای آنالوگ استفاده می کند .
  - **PSK**: از ویژگی فاز برای ساختن نمادهای آنالوگ استفاده می کند .
  - **QAM**: از ترکیبی از ویژگی دامنه و فاز برای ساختن نمادهای آنالوگ استفاده می کند



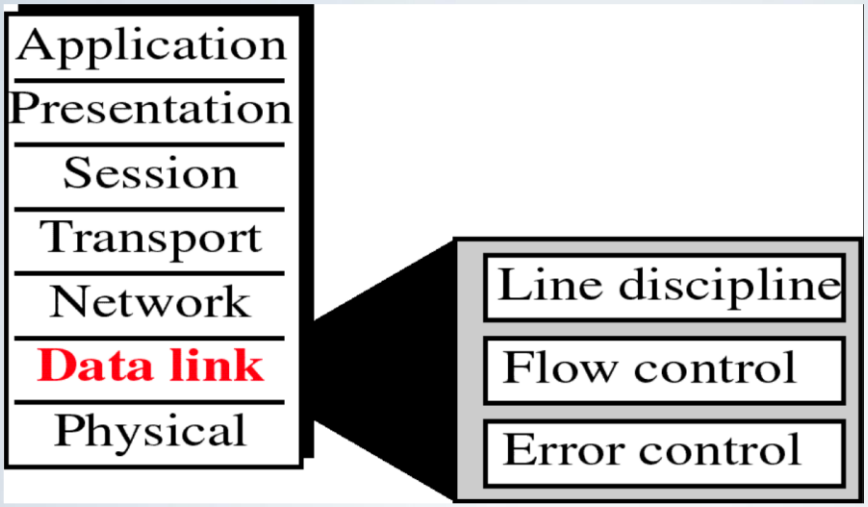
دیجیتال به آنالوگ

- **ASK:**
  - **در این حالت ، نمادها را با ویژگی های دامنه مشخص می کنیم و فرکانس و فاز ثابت می باشد . یعنی دامنه را تغییر می دهیم.**
- **PSK:**
  - **در FSK از ویژگی فرکانس برای ساختن نمادها استفاده می گردد . در اینجا نمادها بر اساس تغییر فرکانس ساخته می شوند و گیرنده به راحتی تفاوت بین بیت های صفر و یک را متوجه می شود.**
- **FSK:**
  - **در این حالت فرکانس و دامنه های بیت های صفر و یک با هم برابرند ولی فاز ها متفاوت می باشند . در این حالت نمادها با فاز های متفاوت ساخته می شوند .**

لایه پیوند داده (Datalink Layer)

- لایه پیوند داده وظایف متعددی را به عهده دارد بنابراین سازمان ISO آن را به دو زیر لایه MAC (Media Access Control) و LLC (Logical Link Control) تقسیم کرد.
- زیر لایه MAC با لایه فیزیکی و زیر لایه LLC با لایه شبکه ارتباط دارد
- به طور خلاصه وظیفه زیر لایه LLC مدیریت ارتباطات میان دو کامپیوتر در یک کانال و همچنین پنهان نگه داشتن توپولوژی و سخت افزار فیزیکی از دید لایه بالاتر است.
- وظیفه لایه MAC تعیین نحوه و چگونگی دسترسی به کانال، چگونگی انتقال صحیح داده و به عبارت کلی تر مدیریت کانال است.

لایه پیوند داده (Datalink Layer)



- قسمت Line Discipline مشخص می کند که چه کسی اول اطلاغات را بفرستد .
- قسمت Flow Control مشخص می کند که چه مقدار اطلاعات بفرستیم تا گیرنده قادر به دریافت آن باشد .
- قسمت Error Control مشخص می کند که خطا چگونه تشکیل داده شود .

وظائف کلی پیوند داده

- لایه پیوند داده دارای شش وظیفه اصلی است که به تفکیک بررسی خواهد شد.
  - ارائه سرویس به لایه بالاتر
  - قرار دادن آدرس فیزیکی در فریم اطلاعاتی در شبکه های LAN
  - فریم بندی (Framing)
  - کنترل خطا (Error Control)
  - کنترل جریان (Flow Control)
  - مدیریت کانال

ارائه سرویس به لایه بالاتر

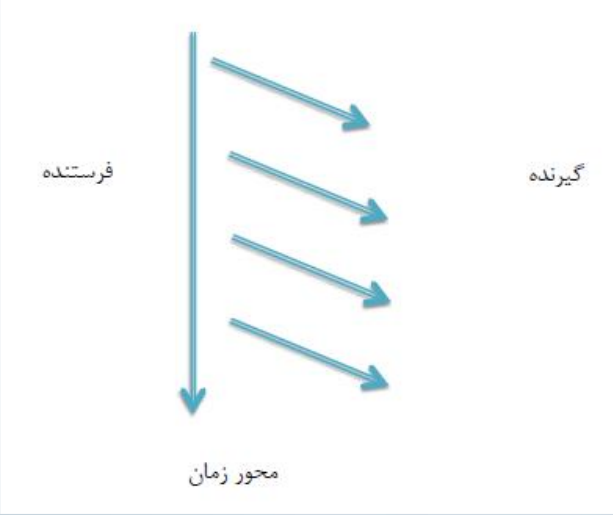
- لایه بالای پیوند داده، لایه شبکه است.
- بنابراین زیر لایه LLC وظیفه ارائه سرویس به لایه شبکه را به عهده دارد.
- ارائه سرویس به سه طریق امکان پذیر است:
  - سرویس بدون اتصال بدون دریافت پیغام پاسخ از گیرنده
  - سرویس بدون اتصال همراه با دریافت پیغام پاسخ از گیرنده
  - سرویس اتصال گرا

ارائه سرویس به لایه بالاتر

- **سرویس بدون اتصال بدون دریافت پیغام پاسخ از گیرنده**
- **در این نوع سرویس در ابتدا هیچ اتصالی بین فرستنده و گیرنده برقرار نمی شود و فرستنده اطلاعات را به صورت فریم های متوالی و مستقل برای گیرنده ارسال می کند.**
- **فرستنده هیچ گاه منتظر پیغام در یافت فریم ACK از سمت گیرنده نمی ماند .**
- **فرستنده هیچگاه خاموش بودن گیرنده یا آمادگی دریافت اطلاعات توسط گیرنده رابررسی نمی کند.**
- **بنابراین تضمینی برای دریافت فریم توسط گیرنده یا دریافت صحیح آن و یا حفظ ترتیب دریافت فریم ها وجود ندارد.**

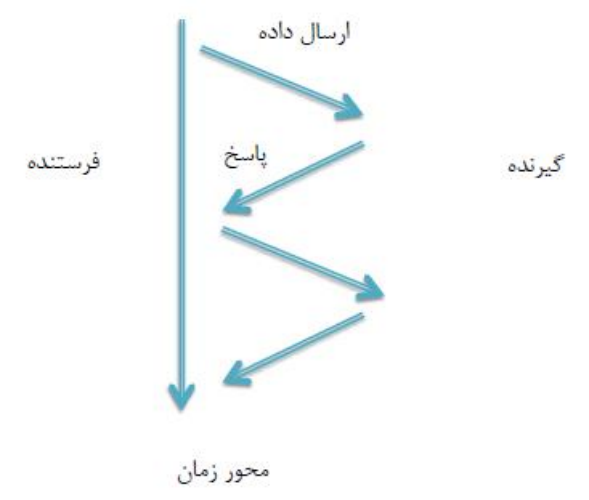
ارائه سرویس به لایه بالاتر

- قابلیت اطمینان این روش در مقابل خطا پایین است بنابراین بایستی در کانال های مطمئن مانند فیبرنوری از این سرویس استفاده شود.
- نرخ انتقال داده در این سرویس بالا است و برای کاربردهای بلادرنگ (real time) و یا سرویس هایی که درآنها تاخیر مهم است به کار میرود.مثال:گوش دادن به رادیو به صورت online است.



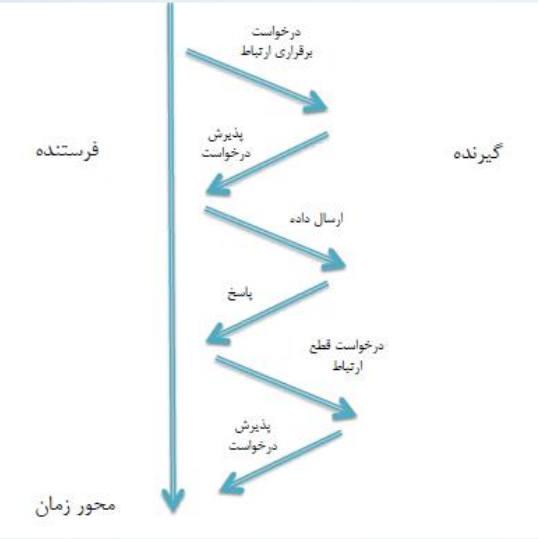
ارائه سرویس به لایه بالاتر

- **سرویس بدون اتصال همراه با دریافت پیغام پاسخ از گیرنده**
- **در این سرویس هیچ اتصال اولیه ای بین فرستنده و گیرنده برقرار نمی شود.**
- **اما بعد از ارسال هر فریم فرستنده منتظر دریافت پاسخ (دریافت سالم یا خطادار فریم) از سمت گیرنده می ماند.**
- **فرستنده اگر در فاصله معینی پاسخی دریافت نکند فریم را دوباره ارسال می کند**
- **با توجه به قابلیت اطمینان بالا در این روش می توان آن را در کانال های بی سیم که ذاتاً نویزپذیر هستند به کار برد.**



ارائه سرویس به لایه بالاتر

- **سرویس اتصال گرا**
- **در این سرویس علاوه بر اتصال اولیه بین فرستنده و گیرنده و انتقال فریم داده همراه با دریافت پاسخ از گیرنده، در انتها اتصال اولیه قطع می شود.**
- **بنابراین در این روش قبل از ارسال هر فریم اطلاعاتی روشن بودن گیرنده و آمادگی آن برای دریافت اطلاعات بررسی می شود.**
- **قابلیت اطمینان این سرویس بسیار بالا است.**
- **نرخ انتقال داده در این روش نسبت به دو روش دیگر پایین تر است.**



فریم بندی

- فریم بندی یعنی این که لایه پیوند داده فرستنده، اطلاعات را در یک قالب مشخص و مورد توافق فرستنده و گیرنده قرار دهد و مرز ابتدا و انتهای آن قالب را مشخص کند.

فیلد شروع فریم	فیلد آدرس	فیلد طول	داده	فیلد کنترل خطا	فیلد انتهای فریم

کنترل خطا

- در هنگام انتقال داده ممکن است به علت وجود نویز درمحیط، داده های ارسالی دچار تغییر شده و گیرنده آنها را خطادار دریافت کند . باید به طریقی گیرنده متوجه دریافت خطادار داده ها شود تا از آنها استفاده نکند.
- منظور از کنترل خطا، امور مربوط به شناسایی یا تشخیص خطا (کشف وجود خطا(Error Detection)) و تصحیح آن (کشف موقعیت بیت خطا (Error Correction)) می باشد.

مکانیزم کشف خطا

- در مکانیزم کشف خطا، گیرنده متوجه وقوع خطا می شود ولی نمی تواند آن خطا را تصحیح کند. پس باید از فرستنده درخواست کند تا آن اطلاعات را دوباره ارسال کند.
- در مکانیزم تصحیح خطا، گیرنده علاوه بر کشف خطا می تواند خطای رخ داده را تصحیح کند.
- مکانیزم های کشف / تصحیح خطا توسط لایه پیوند داده فرستنده بر روی فریم قرار می گیرد.

مکانیزم های تشخیص خطا

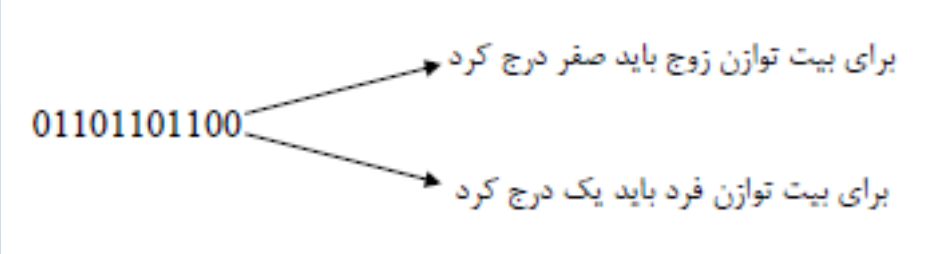
- روشهای کشف خطا
  - اضافه کردن بیت توازن به داده ها
  - کد همینگ Hamming
  - روش Checksum
  - کدهای کشف خطای CRC

بیت توازن

ساده ترین روش تشخیص خطا استفاده از یک بیت اضافی به اسم Parity است

اگر Parity زوج داشته باشیم مقدار این بیت طوری انتخاب خواهد شد که همراه کل مجموعه بیت ها، تعداد بیت های یک زوج باشد. و اگر Parity فرد داشته باشیم طوری بیت های یک را انتخاب می کنیم که تعداد آنها فرد باشد.

مثال:



ضعف این روش در این است که اگر تعداد خطاهای اتفاق افتاده مضربی از دو باشد در (بیت توازن زوج) دیگر نمی توان خطا را تشخیص داد.

کد همینگ

تعداد اختلاف بین بیتهای متناظر در رشته هم طول را **فاصله همینگ** گویند.

مثال: ۰۱۱۰۱۰۱

۱۰۱۰۰۱۰

فاصله همینگ دو عدد بالا برابر ۵ می باشد.

- اگر برای چند رشته بخواهیم فاصله همینگ را بدست آوریم کوچکترین فاصله بین جفت، جفت آنها را به عنوان فاصله همینگ دسته اعداد در نظر می گیریم.
- اگر فاصله همینگ برابر $d+1$ باشد تا d بیت خطا در انها را می توان تشخیص داد.
- اگر فاصله همینگ برابر $2d+1$ باشد تا d خطا را می توان اصلاح کرد.

checksum

- در این مکانیزم کشف خطا، لایه پیوند داده فرستنده تک تک بایت های فریم داده را با یکدیگر جمع کرده، مکمل یک گرفته و آن را به عنوان checksum یک بایتی در انتهای فریم ارسال می کند.
- لایه پیوند گیرنده با دریافت فریم داده تمامی بایت های آن را از جمله checksum با یکدیگر جمع می کند.
- در صورتی که حاصل غیر صفر باشد حتماً فریم خطادار است زیرا حاصل جمع یک عدد با مکمل یک آن عدد برابر صفر است.

CRC

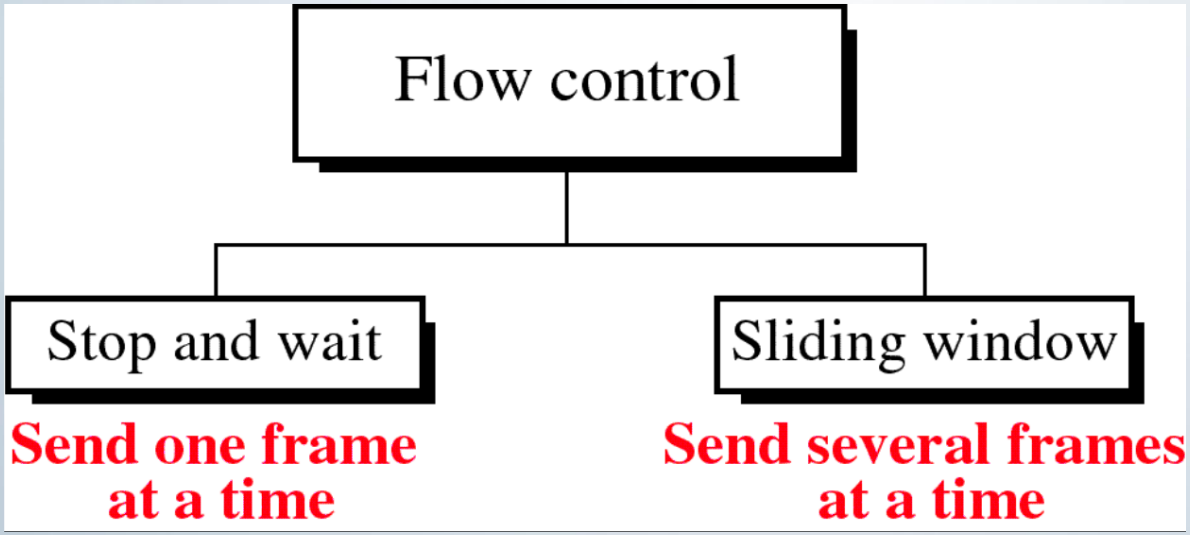
- در این مکانیزم کشف خطا، لایه پیوند داده فرستنده بایت های فریم داده را بر یک چند جمله ای مولد (یک عدد باینری) تقسیم کرده و باقیمانده را به عنوان CRC در انتهای فریم ارسال می کند.
- لایه پیوند گیرنده با تقسیم داده دریافتی بر همان چند جمله ای مورد توافق فرستنده و گیرنده و به دست آوردن باقی مانده، متوجه خطا یا عدم وقوع خطا می شود.

روش های کنترل خطا

- Automatic Repeat Request (ARQ) : خود سیستم خطا را تشخیص می دهد و درخواست ارسال مجدد می کند . دو روش برای این کار وجود دارد:
- Idle RQ (نوع ارتباط Half Duplex است): در این روش فرستنده صبر می کند تا مطمئن شود فریم یا کارکتر قبلی رسیده است (به طور صحیح) یا خیر و نهایتا" یا داده بعدی را می فرستد و یا قبلی را دوباره ارسال می کند.
- Continuous RQ (نوع ارتباط Full Duplex است):در این روش K فریم بدون انتظار بدون انتظار برای پاسخ پشت سر هم ارسال می شود فریم های ارسالی شماره ترتیب دارند . به موازات ارسال پاسخ با شماره ترتیب بر می گردند.

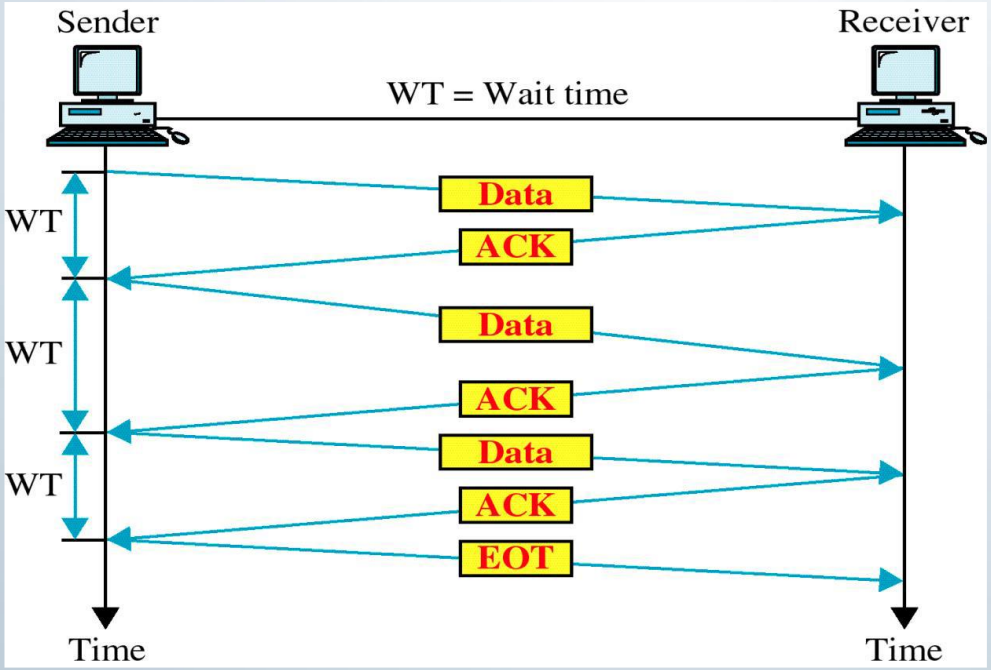
کنترل جریان

- وقتی که فرستنده حجم زیادی از اطلاعات را می فرستد و گیرنده نمی تواند آن را دریافت کند ، بخشی از اطلاعات از بین خواهد رفت . برای جلوگیری از این مشکل دو روش ارائه شده است .



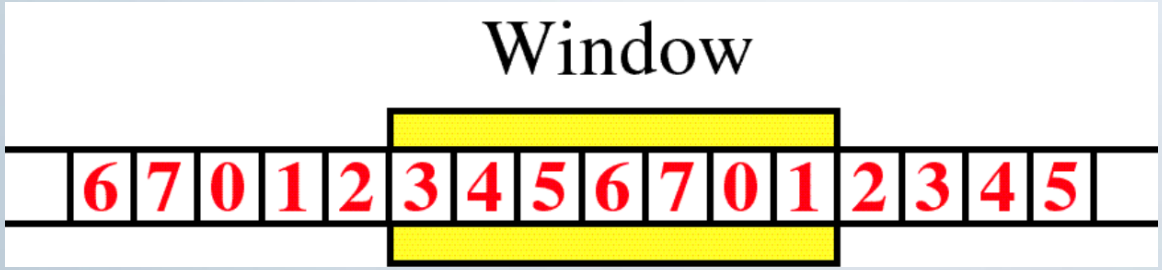
روش توقف / انتظار

- در این روش یک فریم از طرف فرستنده ارسال می شود و صبر می کند تا تأییدیه دریافت فریم بیاید و بعد فریم بعدی را ارسال می کند . در این روش ، گیرنده دقیقا فرستنده را کنترل می کند و پس از فرستادن هر فریم ، تأییدیه آن را ارسال می کند. در واقع در این روش در آن واحد یک فریم بیشتر منتقل نمی شود.



روش پنجره لغزان

- در این روش فرستنده برای اینکه زیاد بیکار نماند ، چندین Frame را به طور هم زمان ارسال می کند بدون اینکه تأییدیه ای بیاید. گیرنده تعداد فریم ها را محدود می کند . مثلا گیرنده می گوید که در آن واحد می تواند ۱۰ فریم را دریافت کند و نه بیشتر و فرستنده هم ۱۰ فریم بیشتر نمی تواند بفرستد . به این ترتیب ، گیرنده می تواند فرستنده را کنترل کند.



زیر لایه MAC

- وظیفه اصلی لایه MAC کنترل دسترسی ماشین ها به لایه فیزیکی (کانال ارتباطی) است. هنگام ارسال اطلاعات برروی کابل، در صورت نبود مدیریت بر لایه فیزیکی، ممکن است مشکلاتی در روند ارسال و دریافت اطلاعات به وجود آید. مثلا ارسال اطلاعات توسط دو یا چند ماشین به صورت همزمان بر روی یک کانال صورت گیرد.
- پارامترهای مربوط به یک کانال ارتباطی:
- Delay: مدت زمانی که یک فرستنده باید صبر کند تا کانال در اختیارش گزارده شود
- Through put: هیچ گاه کابل نباید بیکار یا خالی باشد.

تخصیص کانال

- تخصیص کانال در شبکه های محلی و گسترده به دو صورت انجام می پذیرد :
  - پویا
  - ایستا: که به صورت زیر می باشد:
    - FDM (تسهیم‌سازی فرکانسی): یکی از روشهای مرسوم برای تخصیص یک کانال است که در آنها استفاده کننده‌ها با هم رقابت دارند. به اینصورت که اگر N کاربر داشته باشیم، پهنای باند را به N قسمت مساوی تقسیم می‌کنیم که به هر کاربر یک قسمت اختصاص می‌یابد و از آنجائی که هر کاربر از یک باند فرکانسی مخصوص به خود استفاده می کند، بنابراین بین کاربران برخوردی صورت نمی‌گیرد.

تخصیص کانال

- پویا: که به صورت زیر می باشد:
  - مدل ایستگاه
  - فرض کانال منفرد
  - فرض برخورد
  - زمانی
    - زمان پیوسته
    - زمان برهه‌ای
  - وضعیت حامل
    - تشخیص وضعیت‌های حامل
    - عدم تشخیص وضعیت حامل

تخصیص کانال

- مدل ایستگاه

- این مدل شامل N ایستگاه مستقل که هر کدام شامل یک برنامه یا کاربری که قابهایی را برای انتقال ایجاد می کند، هستند.

- فرض کانال منفرد

- یک کانال منفرد برای تمام ارتباطات در دسترس می باشد. به این معنا که تمام ایستگاهها از طریق آن می توانند پیامی را دریافت و یا ارسال کنند.
- ایستگاهها از نظر سخت‌افزار یکسانند، ولی ممکن است از نظر نرم‌افزار اولویتهایی را برای آنها ایجاد کنند.

- فرض برخورد

- اگر ۲ قاب بطور همزمان با هم فرستاده شوند، از نظر زمانی با یکدیگر تداخل کرده و سیگنال حاصل نامفهوم خواهد بود، به این اتفاق برخورد گویند.

تخصیص کانال

- زمان پیوسته

- انتقال قاب را می‌توان در هر زمانی آغاز کرد و ساعتی وجود ندارد که زمان را به فاصله‌های زمانی گسسته تقسیم کند.

- زمان برهه‌ای

- زمان به فواصل مجزایی (برهه) تقسیم می‌شود. انتقال قاب همواره از ابتدای یک مقطع زمانی شروع می‌شود.

تخصیص کانال

- تشخیص وضعیتهای حامل

- ایستگاهها می توانند تشخیص دهند که آیا یک کانال قبل از اینکه مورد استفاده قرار گیرد اشغال است یا خیر. اگر کانال اشغال باشد هیچ ایستگاهی نمی‌تواند از آن استفاده کند تا آزاد شود.

- عدم تشخیص وضعیت حامل

- ایستگاهها نمی‌توانند وضعیت کانال را قبل از استفاده تشخیص دهند. آنها پس از شروع به انتقال می‌توانند تعیین کنند که آیا انتقال موفق بوده است یا خیر.

لایه شبکه (Network Layer)

Forwarding: هدایت ؛ وقتی بسته ای وارد مسیریاب می شود باید یک گام به سمت مقصد به پیش رانده شود . از روی جداول درون مسیریاب تشخیص داده می شود که هر بسته ورودی از کدام درگاه خروجی خارج شود. این تصمیم گیری یا براساس آدرس مقصد و یا شماره ارتباط انجام می شود.

ROUTING: مسیریابی، پیدا کردن بهترین یا مناسب ترین مسیر بین مبدا و مقصد است از دیگر وظائف این لایه است . این کار یا به ازای هر بسته تکرار می شود. نتیجه عملیات مسیریابی، به روز رسانی جداول درون مسیریابها است.

لایه شبکه

کنترل ازدحام: اگر همزمان بسته های زیادی در زیر شبکه وجود داشته باشند ، عبور مشکل می شود. کنترل این ازدهام نیز از وظایف لایه شبکه است .

تطبیق پروتکل ها : لینکهای ورودی و خروجی مسیریابها ممکن است دارای پروتکل ها و استانداردهای متفاوت و متعلق به شبکه های مختلف باشند . وظیفه دیگر مسیریابها تطبیق پروتکل و یا نگاشت بسته های اطلاعاتی از یک پروتکل به پروتکل دیگر می باشد.

بطور کلی کیفیت خدمات (تاخیر ، زمان انتقال و...) به لایه شبکه مربوط می شود.

لایه شبکه

سرویسهایی که لایه شبکه به لایه انتقال می دهد بر دو نوع است:

اتصال‌گرا: قبل از آنکه بسته ها فرستاده شود باید یک مسیر از منبع به مقصد ایجاد شود. این اتصال مدار مجازی نامیده می شود. شبکه های سوئیچ تلفنی از این مکانیزم استفاده می کنند

بی‌اتصال: اگر خدمات بدون اتصال باشد، بسته ها به شبکه جداگانه وارد شده و جدا از یکدیگر مسیریابی می شوند. اینترنت از این روش استفاده می کند.

مسیریابی

هنگامی که بسته‌های اطلاعاتی روی شبکه منتشر می‌شود باید مکانیزمی برای هدایت بسته‌ها از مبدا به مقصد وجود داشته باشد، تا میان شبکه‌ها با توپولوژی‌ها و ساختارهای مختلف بتوانند حرکت کنند که به این عمل هدایت، همان **مسیریابی** گفته می‌شود.

الگوریت مسیریابی: الگوریتم مسیریابی، بخشی از نرم افزار لایه شبکه است که تعیین می کند بسته ورودی به کدام خط خروجی باید منتقل شود.

الگوریتم های مسیریابی

هر یک از الگوریتم های مسیریابی به طور کلی ۶ ویژگی داشته باشند.

- صحت عملکرد: الگوریتم باید صحیح عمل کند.
- سادگی
- قابلیت تحمل: خرابی سخت افزار و نرم افزار تاثیری بر عملکرد شبکه نگذارد. (شبکه را از کار نیاندازد)
- پایداری: الگوریتم همگرا باشد زیرا اگر چنین شرطی وجود نداشته باشد در حلقه ابدی گرفتار خواهد شد.
- بهینه بودن: منابع به صورت عادلانه تقسیم شوند.
- عدالت و مساوات

الگوریتم های مسیریابی

الگوریتم های مسیریابی به ۲ گروه اصلی تقسیم می شوند:

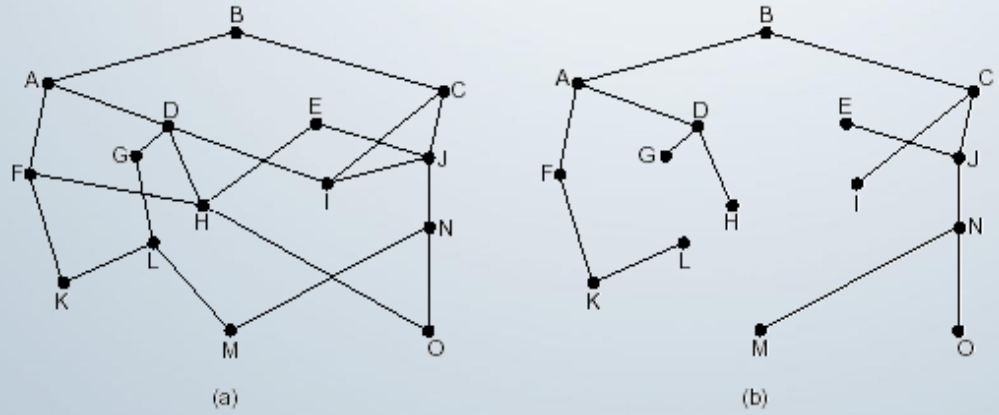
- **الگوریتمهای غیر وِفقی (ایستا):** تصمیمات مسیریابی خود را بر اندازه گیری یا تخمین توپولوژی و ترافیک فعلی بنا نمی نهند، در عوض برای انتخاب یک مسیر مورد استفاده از قبل محاسبه و از خط خارج می شود و هنگامی که شبکه راه اندازی شد،به شبکه بار می شود.
- **الگوریتمهای وِفقی (پویا):** الگوریتم وفقی تصمیمات مسیریابی خود را بر اساس تغییرات در توپولوژی وترافیک تغییر می دهند.

اصل بهینگی

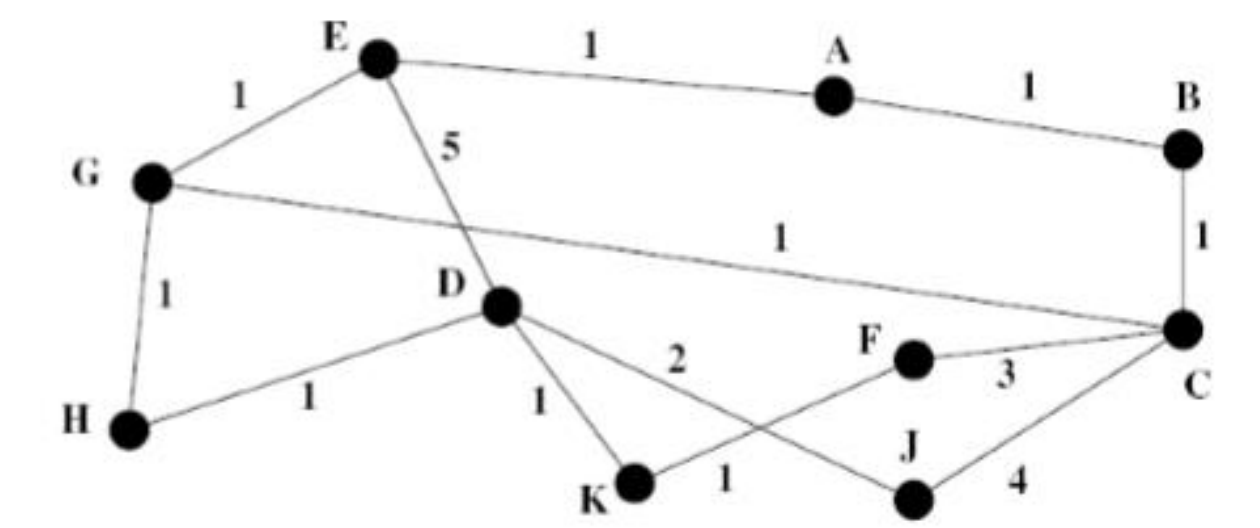
- اگر بین مبدا و مقصدی یک مسیر بهینه باشد، این مسیر به عنوان بهترین مسیر برگشت هم به حساب می آید .

- اگر مسیر یاب J از مسیر یاب I به مسیر یاب K در مسیر بهینه ای قرار گیرد آنگاه مسیر بهینه ای از J به K نیز در همان مسیر قرار می گیرد .

نتیجه ای که از این اصل دریافت می شود، این است که ما می توانیم ببینیم که مجموعه ای از مسیرهای بهینه از تمام منابع به یک مقصد معین ، به شکل درختی می باشد که ریشه آن مقصد است لذا چنین درختی را sink tree می نامیم .



هزینه در مسیریابی



الگوریتم مسیریابی ابتدا کوتاه ترین مسیر(Shortest Path)

در این الگوریتم هر گره دارای یک برچسب دو قسمتی است که حاوی فاصله آن با گره مبدا و نام گره ایست که آن گره را به گره مبدا متصل می کند. (با فاصله مذکور)

همچنین هر گره در طی پیشرفت الگوریتم یکی از دو وضعیت زیر را دارد:

T (Tentative) یا موقتی

P (Permanent) یا دائمی

گره دائمی گره ایست که برچسب آن مطمئنا" کوتاه ترین مسیر تا مبدأ را نشان می دهد.

الگوریتم مسیریابی ابتدا کوتاه ترین مسیر(Shortest Path)

۱) برچسب همه گره ها تا مبدا را (- و ∞) قرار دهید (یعنی فاصله آن تا مبدا ∞ و از طریق گره نامشخص)

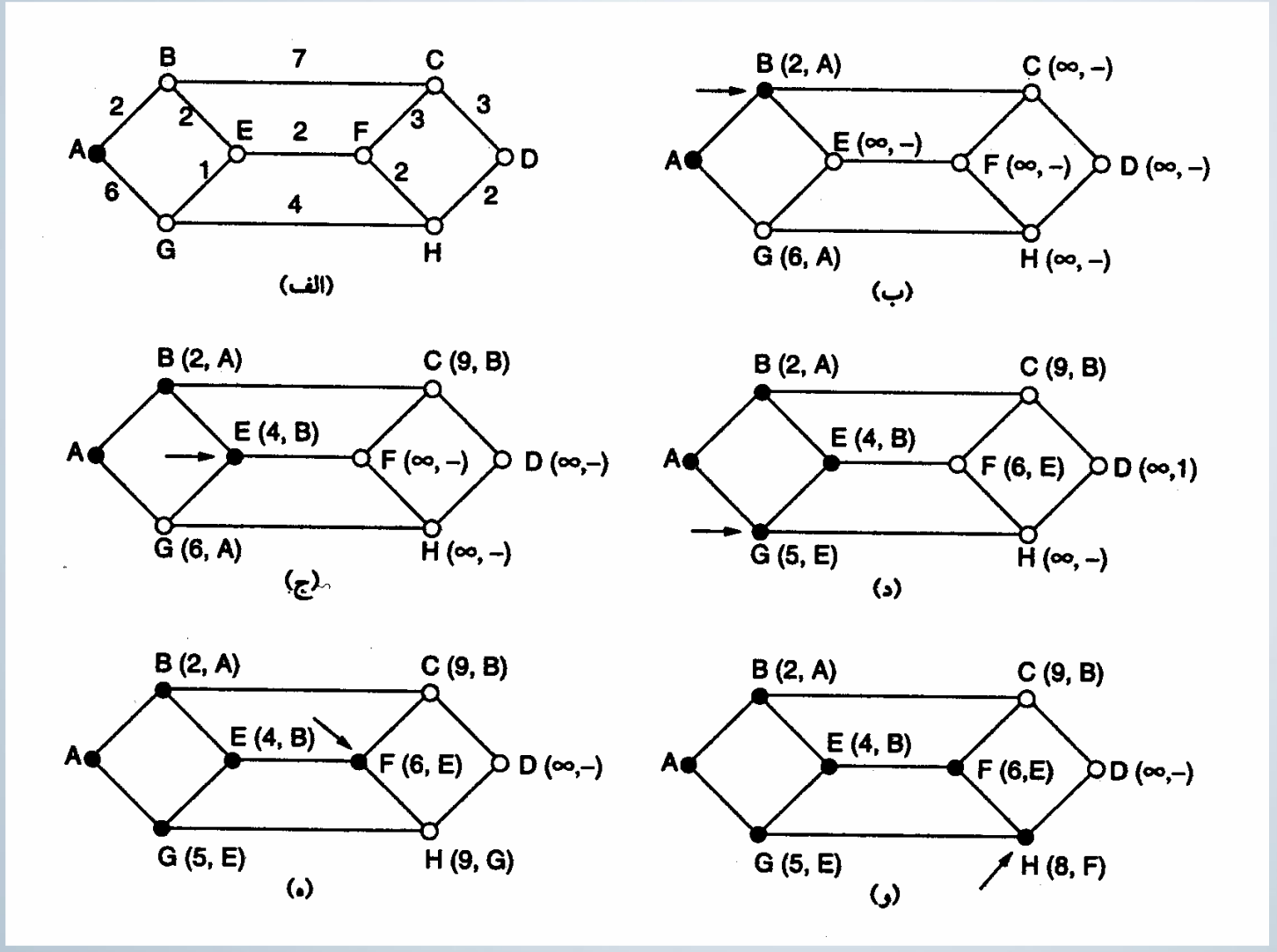
۲) از گره مبدا شروع می کنیم (فرقی کند؛ از مقصد هم می توانستیم شروع کرده و تا مبدا ادامه دهیم) آن را دائمی علامت بزنید . این گره را گره کار در نظر می گیریم.

۳) برای کلید همسایگان گره کار در صورتی که مجموع برچسب گره کار و فاصله گره کار تا آن گره از برچسب آن گره کوچکتر باشد . فاصله گره کار را (وزن LINK متصل را)تا گره مبدا جمع کنید و به همراه نام گره کار به عنوان برچسب گره همسایه قرار دهید.

۴) به کلیه گره های موقتی نگاه کنید. کوچکترین آن ها را پیدا کنید و به عنوان گره کار در نظر بگیرید و آن را به صورت دائمی علامت بزنید

۵) اگر همه گره ها دائمی نشده اند به قسمت ۳ مراجعه کنید.

الگوریتم مسیریابی ابتدا کوتاه ترین مسیر(Shortest Path)



الگوریتم مسیریابی بردار فاصله یا DVR

این الگوریتم، مسیریابی در شبکه را به صورت پویا انجام می دهد . در این الگوریتم هر مسیریاب در حافظه خود جدولی یا برداری دارد که در آن بهترین مسیر به هر مقصد را نگهداری می کند و خطی که برای رسیدن به آن مقصد لازم است را مشخص می کند. که به ازای هر مسیریاب موجود در زیر شبکه یک سطر در آن وجود دارد.

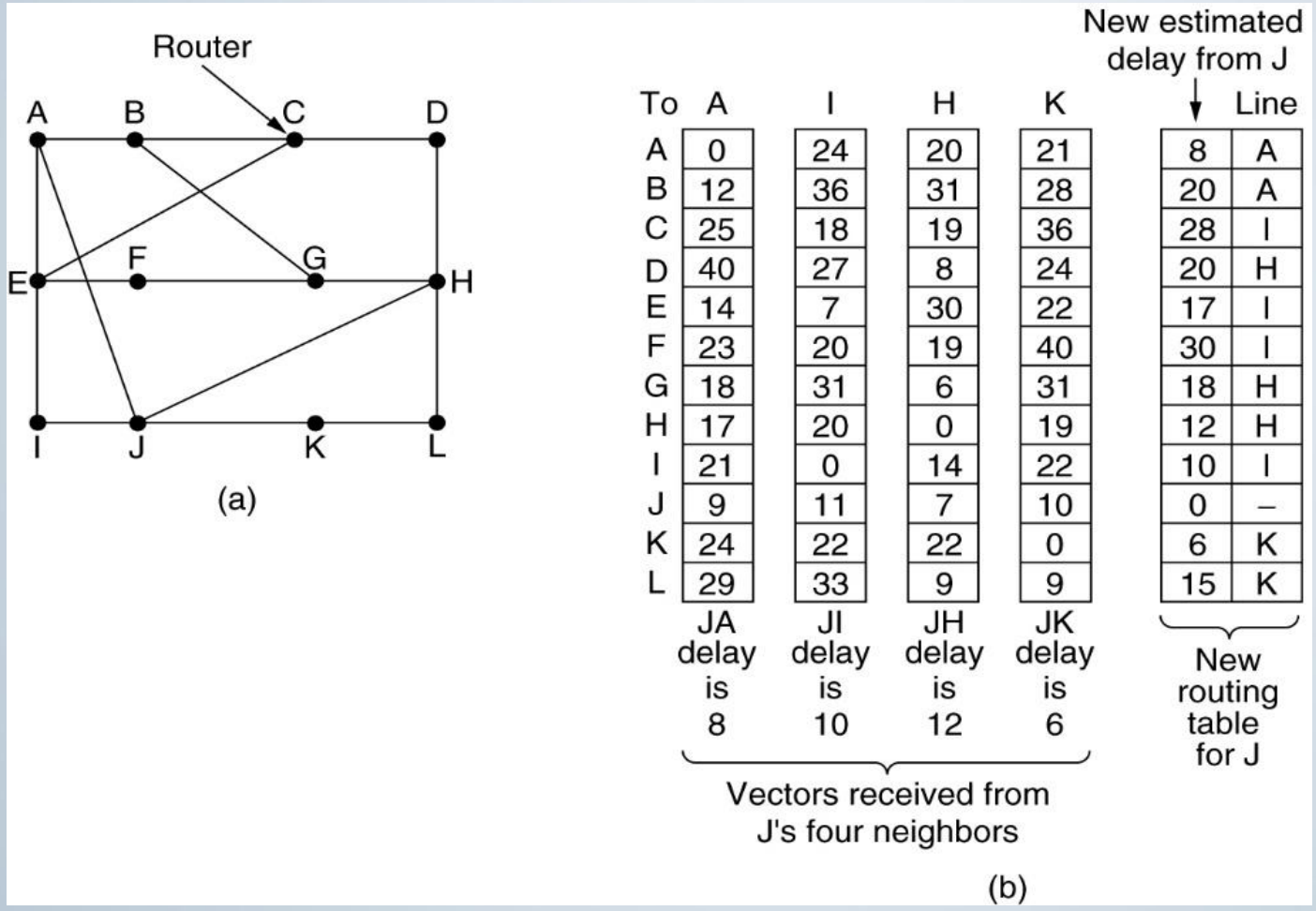
در هر سطر دو فیلد زیر وجود دارد:

۱- Link خروجی مناسب برای رسیدن به مقصد موردنظر

۲- تخمینی از زمان یا فاصله رسیدن به آن مقصد (این هزینه می تواند تعداد گام، تاخیر و یا هر پارامتر دیگر شبکه باشد.)

برای اینکه این جدول به روز نگاه داشته شود و آخرین تغییرات در آن اعمال شود، مسیریاب های موجود در شبکه در فاصله های زمانی مشخص این جدول را برای یکدیگر ارسال می کنند و همدیگر را از وجود مسیر های شکسته یا مسیر های تازه ایجاد شده مطلع می نمایند.

الگوریتم مسیریابی بردار فاصله یا DVR



الگوریتم مسیریابی بردار فاصله یا DVR

گره j ابتدا بردار فاصله چهار همسایه خود را (A, I, H, K) را دریافت می کند و بر اساس این چهار بردار و فاصله خود از این چهار گره بردار فاصله خود را به روز در می آورد.

نکته : این الگوریتم مشکلات اساسی دارد که باعث منسوخ شدن آن شده است. اگرچه از نظر تئوری الگوریتم درست عمل میکند.

مسیریابی حالت پیوند یا LS (Link State)

ایده مسیر یابی حالت پیوند در پنج بخش میانی بیان می شود . هر مسیر یاب باید :

۱- همسایه هایش را تشخیص داده و آدرسهای شبکه آنها را بداند.

۲- تأخیر یا هزینه تا همسایه هایش را اندازه گیری کند.

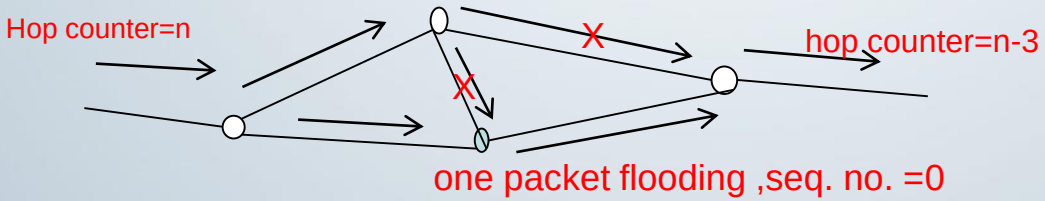
۳- ایجاد بسته ای که گویای تمام اطلاعات بدست آمده بالا باشد.

۴- این بسته ها را به تمام مسیریابها ارسال نماید.

۵- براساس الگوریتم کوتاهترین مسیر، کوتاهترین مسیر به هر مسیریاب دیگررا محاسبه کند.

الگوریتم سیل آسا (Flooding)

در این الگوریتم سیلی از بسته ها از مسیرهای مختلف در آن واحد به سمت مقصد (در واقع در همه جهات) ارسال می شود. هر مسیریاب موظف است با دریافت آن بسته یک نسخه از آن را به تمام پورت های خروجی ارسال کند. واضح است که در این الگوریتم بسته های تکراری از مسیرهای مختلف به کلیه گره ها خواهد رسید و تولید بسته های تکراری موجب ازدحام و اشباع شبکه خواهد شد . برای حل این مشکل پیشنهاداتی ارائه شده است:



الگوریتم سیل آسا (Flooding)

۱) یک شمارنده گام داشته باشیم و در Header بسته قرار دهیم و در هر گام یک واحد از آن کم کنیم و پس از صفر شدن آن، بسته را دور بریزیم.

۲) فهرست بسته های سیل آسای ارسالی از هر گره مبدا را از طریق شماره ترتیب آن نگهداری نمائید و از ارسال مجدد بسته های تکراری جلوگیری کنیم.

۳) برای اجتناب از طولانی شدن این لیست فقط کافی است آخرین بسته (بزرگترین شماره ترتیب) مربوط به هر گره مبدا را لیست کنیم.

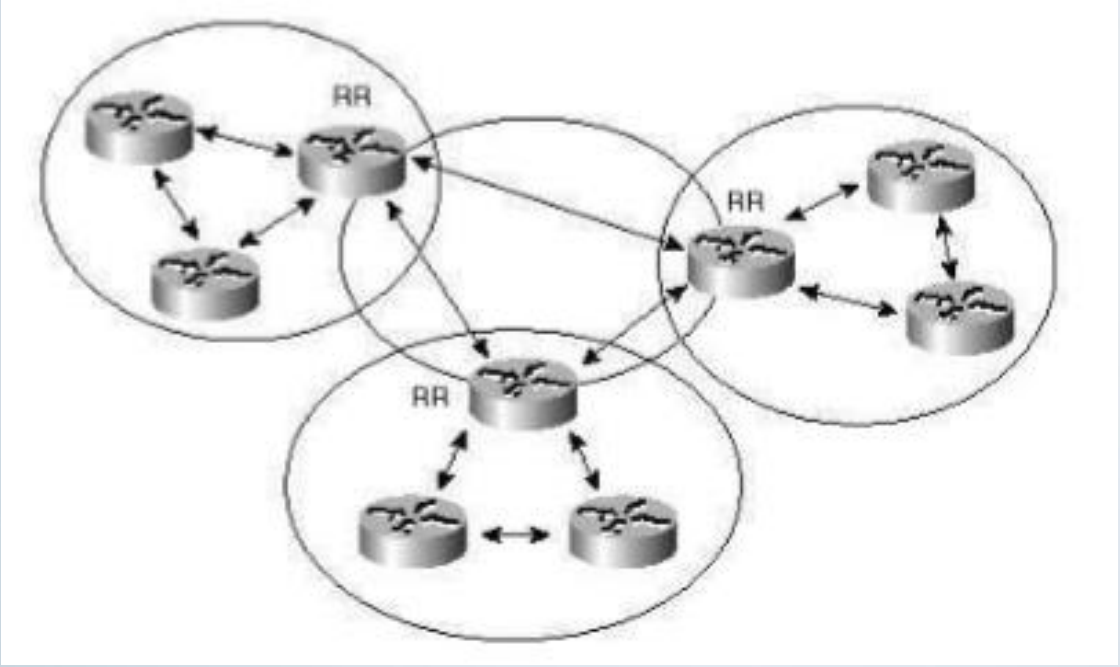
الگوریتم مسیریابی سلسله مراتبی

با استفاده از مسیریابی سلسله مراتبی مسیریابها به قسمتهایی تقسیم می شوند که آنها را نواحی می نامیم .

هر مسیریاب تمام جزئیات ناحیه خود را درباره اینکه چطور بسته ها به مقصد ارسال میشود، می داند ولی از ساختار داخلی سایر نواحی خبر ندارد.

هرگاه ماشینی بخواهد اطلاعاتی را به خارج از قسمت خود ارسال کند مسیریاب تقاضای او را به مسیریاب مرزی (مسیریابی که بین دو قسمت مجزا فعالیت می کند) تحویل می دهد و مسیریاب مرزی نیز به نوبه خود بسته را به مسیریاب های سطوح بالاتر که جزئیات بیشتری در مورد شبکه مقصد می دانند تحویل می دهد و این روند ادامه می یابد تا اینکه اطلاعات به شبکه مقصد برسد.

مسیریابی سلسله مراتبی



کنترل ازدحام

سیاست های مختلفی در لایه های مختلف شبکه برای کنترل و پیش گیری از ازدحام پیشنهاد شده است .

یک شبکه گسترده و یا کوچک کامپیوتری نیاز به مقرراتی جهت ساماندهی به مراجعات آن و قوانینی جهت جلوگیری از عدم کارآیی در شبکه دارد.

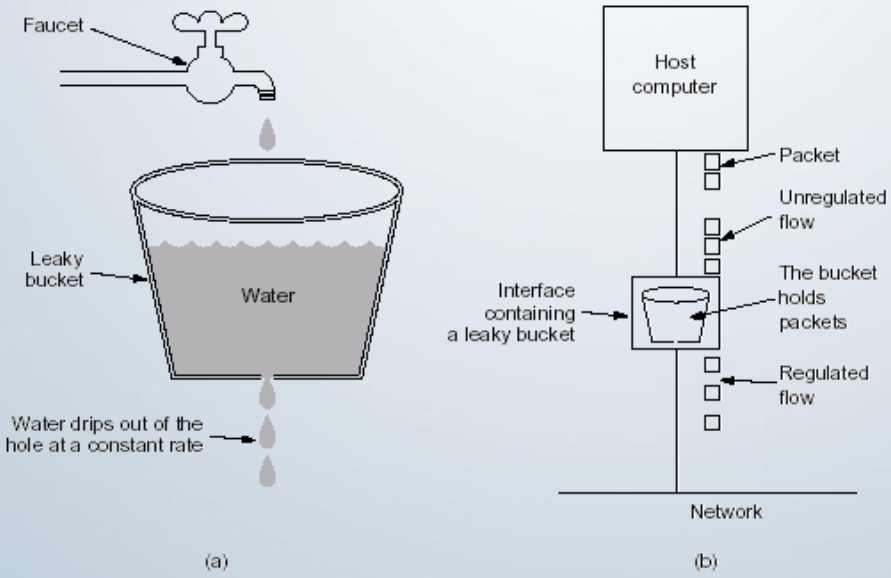
۱- الگوریتم سطل سوراخدار

۲- الگوریتم سطل نشانه

الگوریتم سطل سوراخدار

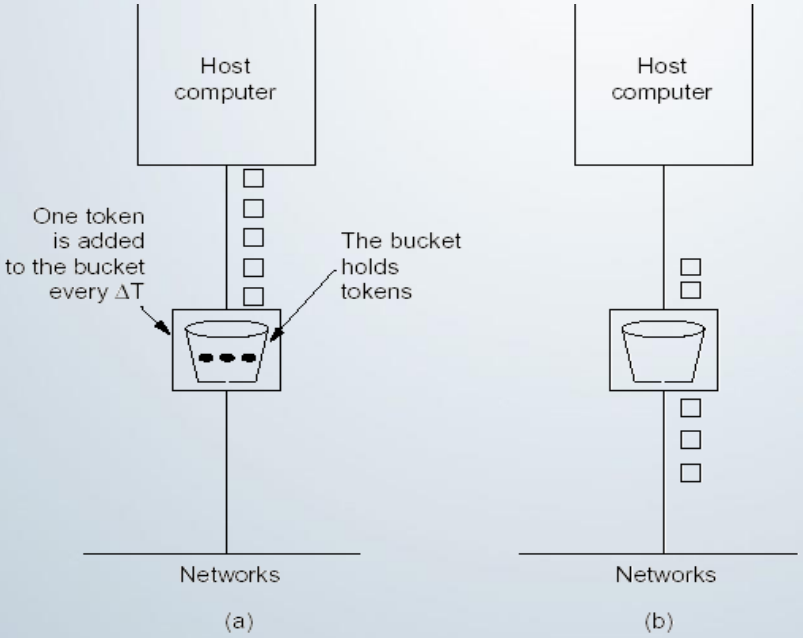
الگوریتم سطل سوراخدار الگوی خروجی ثابتی را با سرعت میانگین و بدون توجه به میزان ترافیک اجرا می کند.

هر میزبان بوسیله رابطی که حاوی سطح سوراخدار است ، که یک صف داخلی متناهی است به شبکه متصل می شود . اگر بسته ای به صف برسد و صف پر باشد آن بسته در نظر گرفته نمی شود



الگوریتم سطل نشانه

در این الگوریتم ، سطل سوراخدار ، نشانه ها را نگهداری می کند ، این نشانه ها توسط یک ساعت با سرعت یک نشانه ایجاد می شود. برای بسته ای که می خواهد منتقل شود یک بسته را ذخیره و سپس از بین می برد.



پروتکل اینترنت IP

جوهرهٔ اینترنت به گونه ای شکل گرفته است که مجموعه ای از شبکه های خودمختار را به همدیگر وصل می نماید. قراردادی که حمل و تردد بسته های اطلاعاتی و همچنین مسیریابی صحیح آنها را از مبدأ به مقصد ، مدیریت و سازماندهی می نماید پروتکل IP نام دارد.

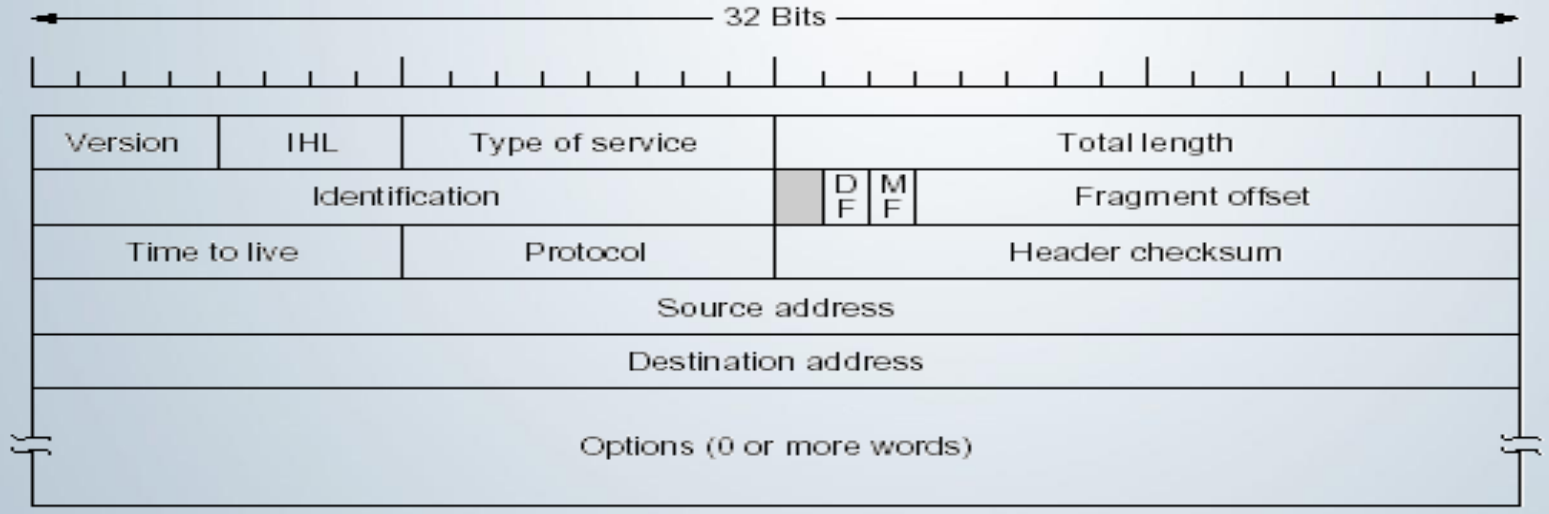
در حقیقت پروتکل IP که روی تمامی ماشینهای شبکه اینترنت وجود دارد بسته های اطلاعاتی را (بسته های IP) از مبداء تا مقصد هدایت می نماید، فارغ از آنکه آیا ماشینهای مبدأ و مقصد روی یک شبکه هستند یا چندین شبکهٔ دیگر بین آنها واقع شده است.

پروتکل اینترنت IP

پروتکل IP شامل ۲ بخش می باشد:

۱- سرایند : یک بخش ثابت ۲۰ بایتی و یک بخش اختیاری با طول متغیر می باشد.

۲- متن



فیلدهای بخش سرایند

- Version: مشخص می کند که بسته براساس چه نسخه ای از پروتکل IP سازماندهی و ارسال شده است
- IHL: بدین منظور در سرآیند تعبیه شده تا با کلمات ۳۲ بیتی، طول سرآیند را مشخص نمایند
- Type of service: بین طبقات مختلفی از service، تمایز ایجاد می کند
- Total Length: طول کل بسته را مشخص می نماید.
- Identification: مشخص می کند قطعه دریافتی به کدام دیتاگرام متعلق است.
- DF: به مسیریاب ها دستور می دهد که داده نگاشت را قطعه بندی نکند.
- MF: بیانگر قطعات بیشتر است. تمام این قطعات غیر از آخری باعث می شوند که این بیت مرتب شود.

فیلدهای بخش سرایند

- Fragment Offset: **مشخص می کند که قطعه در کجای داده نگاشت قرار دارد.**
- Time to live: **عمر شمارنده ای است که طول عمر بسته را محدود می کند.**
- Protocol: **تعیین می کند که داده نگاشت را به کدام فرآیند احتمال تحویل دهد .**
- Header checksum: **این جمع کنترلی برای تشخیص خطاهای حاصل از کلمات حافظه در یک مسیر یاب مفید است.**
- Source/ Destination Address: **شماره شبکه و شماره میزبان را نشان می دهد.**
- Options: **برای آزمایش، دیباگ، امنیت و سایر پارامترهای مشابه روی شبکه مورد استفاده قرار می‌گیرد.**

پروتکل های کنترل اینترنت

اینترنت علاوه بر IP که برای انتقال داده ها کاربرد دارد، چندین پروتکل کنترلی دیگر دارد که همگی در لایه شبکه به کار گرفته می شوند:

- ICMP
- ARP –
- RARP –
- BOOTP
- DHCP

ICMP

این پروتکل ، امکانات لازم جهت اشکال زدایی ، گزارش خطاها و همچنین مبادله اطلاعات محدود در بستر یک شبکه را ارائه می دهد . با توجه به اینکه icmp صرفا مسئول ارائه پیغامهای کنترلی و گزارش خطاها و نهایتا ارائه فیدبک های لازم در جهت تحقق یک وضعیت خاص است ، حاوی هیچگونه اطلاعاتی مبنی بر اعلام وصول بسته های اطلاعاتی نمی باشد.

عملکرد غیر منتظره در اینترنت توسط این پروتکل گزارش می‌شود. همچنین این پروتکل برای آزمایش و رفع عیب در شبکه به کار می‌رود.

پیامهای ICMP

نوع پیام	توصیف عملکرد
Destination unreachable	به هر دلیلی بسته را نمی‌توان به مقصد تحویل داد
Time exceeded	زمان حیات بسته به پایان رسیده است
Parameter problem	فیلدی از سرآیند بسته، مقدار نامعتبر داشته است
Redirect	حاوی اطلاعاتی در خصوص جغرافیای مسیر و اعلام اشتباه در مسیریابی
Echo	درخواست از یک ماشین تا اگر فعال است پاسخ دهد
Echo reply	پاسخ به پیام Echo بمنظور تایید فعالیت
Timestamp request	همانند پیام Echo به همراه مهر زمان
Timestamp reply	همانند پیام Echo Reply به همراه مهر زمان

ARP

ARP یا پروتکل تحلیل آدرس برای تجزیه و تحلیل آدرسها در شبکه بکار می‌رود.

همانطور که می‌دانیم آدرسهای فیزیکی توسط لایه پیوند داده دریافت و فهمیده می‌شوند. ولی این لایه از آدرسهای IP چیزی نمی‌داند. این پروتکل برای ترجمه آدرسهای IP به آدرسهای فیزیکی(MAC) بکار می‌رود.

RARP

پروتکل RARP عکس عمل ARP را انجام می‌دهد. یعنی آدرس فیزیکی را گرفته و آدرس IP متناظر با آن را برمی‌گرداند.

در این پروتکل هم می‌توان آدرسهای فیزیکی ماشینهای مختلف را بصورت فراگیر روی شبکه پخش کرد یا آدرس IP یک ماشین در تصویر حافظه جاسازی شود.

BOOTP

فریم های پخش فراگیر را به خارج از شبکه محلی هدایت می‌کند.

از پروتکل BOOTP برای راه اندازی ایستگاههای بدون دیسک استفاده می‌شود. این پروتکل می‌تواند به غیر از آدرس IP ایستگاه بدون دیسک، اطلاعات اضافه‌تری را مانند آدرس IP مسیریاب پیش‌فرض ، الگوی زیر شبکه و ... را به ایستگاهها ارائه دهد.

DHCP

مشکل جدی پروتکل BOOTP اینست که جدول نگاشت آدرسهای IP باید بصورت دستی تنظیم و پیکربندی شود. پروتکل DHCP این امکان را می‌دهد که آدرسهای IP را هم بصورت خودکار و هم بصورت دستی تنظیم نمود.

AS

شبکه اینترنت از تعداد بسیاری سیستم خود مختار (Autonomous System) یا اختصاراً AS تشکیل شده است.

مسیریابی درون یک AS را مسیریابی درونی و مسیریابی بین AS ها را مسیریابی خروجی یا بیرونی گویند.

OSPF

OSPF پروتکل مسیریابی درونی می باشد و بدین شکل عمل می‌کند:

مجموعه شبکه‌ها مسیریابها و خطوط ارتباطی را در قالب یک گراف جهت دار مدل برده و به هر کمان در گراف یک وزن می‌دهد که نشان دهنده پارامترهایی مانند تاخیر، فاصله و امثال آن است. سپس بر اساس وزن کمانها، مسیر بهینه را پیدا می‌کند.

این پروتکل از سه نوع شبکه و خطوط انتقال پشتیبانی می‌کند:

۱- خطوط نقطه به نقطه بین دو مسیریاب.

۲- شبکه‌های با دسترسی چندگانه از نوع پخش فراگیر(مثل LAN)

۳- شبکه‌های با دسترسی چندگانه از نوع غیر پخش فراگیر(مثل WAN)

OSPF چهار کلاس مسیریاب را به رسمیت می‌شناسد:

۱- مسیریابهای درونی

۲- مسیریابهای واقع در مرز دو ناحیه

۳- مسیریابهای ستون فقرات

۴- مسیریابهای مرزی AS که می‌توانند با مسیریابهای دیگر محاوره کنند.

انواع پیامهای OSPF

نوع پیام	توصیف عملکرد
Hello	از این پیام برای شناسایی همسایه‌ها استفاده می‌شود
Link state update	هزینه فرستنده پیام تا همسایه‌هایش را معین می‌کند
Link state ack	دریافت بسته Link State Update را تایید می‌کند
Database description	مسیر یاب با این پیام فهرست درایه‌های بهنگام‌سازی خود را اعلام می‌کند
Link state request	از شریک خود اطلاعاتی را درخواست می‌کند

BGP

برای مسیریابی بین AS ها از پروتکل BGP استفاده می‌شود. این پروتکل مبتنی بر الگوریتم بردار فاصله (DV) است.

ترافیک هر شبکه AS در یکی از سه رده زیر قرار می‌گیرد:

۱- شبکه‌های پایانی که فقط یک اتصال با گراف BGP دارند و نمی‌توانند ترافیک را از خود عبور بدهند.

۲- شبکه‌های چند اتصالی که می‌توانند ترافیک داده‌ها را منتقل کنند.

۳- شبکه‌های ترانزیت که در نقش ستون فقرات تمایل دارند بسته‌های دیگران را منتقل کنند.