شبکه‌های کامپیوتری

شناسنامه درس

نام درس:	شبکه‌های کامپیوتری
نام مؤلف:	اندرو تننبام
نام مترجم:	پدرام و ملکیان
شماره ویرایش:	چهارم
تعداد واحد:	۳
فصلهای مرجع درس:	فصل ۱ تا آخر فصل ۵
رشته تحصیلی:	مهندسی کامپیوتر، نرم‌افزار
گروه آموزشی:	کامپیوتر
طراح اسلایدهای خلاصه درس:	مهندس عصاری

فصل اول:

اصول و مبانی شبکه ها

رئوس مطالب فصل ۱ :

- تاریخچه شبکه‌ها
- اهداف و مزایای شبکه ها
- کاربردهای شبکه ها
- تقسیم‌بندی شبکه‌ها
- طراحی لایه‌ای
- خدمات اتصال‌گرا و بی‌اتصال
- مدل های مرجع
- مقایسه مدل های مرجع OSI و TCP/IP
- معایب مدل های مرجع OSI و TCP/IP
- سازمان های استاندارد در زمینه شبکه

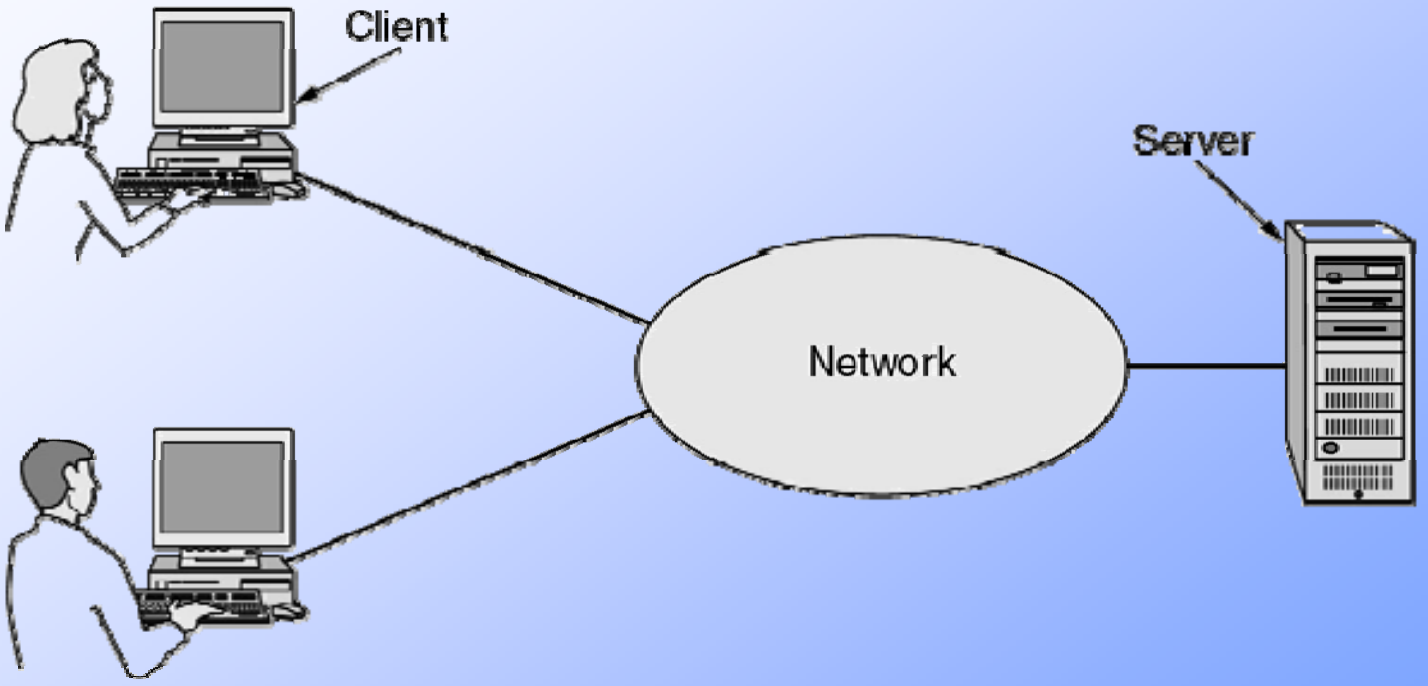
اهداف و مزایای شبکه های کامپیوتری :

1) اشتراک منابع
2) سهولت در انتقال داده
3) صرفه جوئی در هزینه ها
4) افزایش قابلیت اطمینان
5) افزایش سرعت
6) جنبه سرگرمی
7) ایجاد ارتباط بین کاربران

انواع شبکه ها از نظر ارائه سرویس و خدمات :

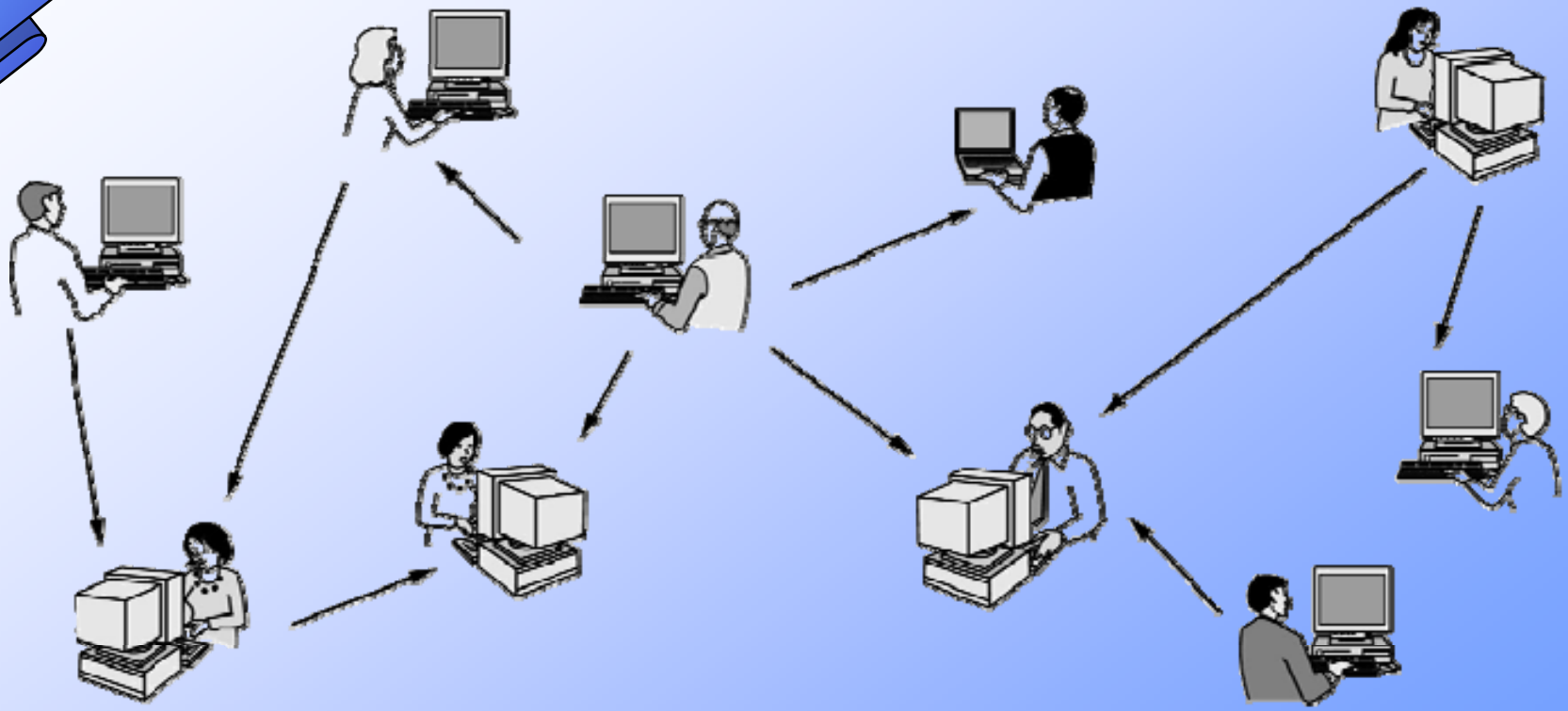
- مدل سرویس گیرنده_سرویس دهنده (مشتری_کارگزار / client - server)
- مدل نظیر به نظیر (peer to peer)

مدل client – server :



یک شبکه با یک سرور و دو کلاینت

مدل peer to peer :



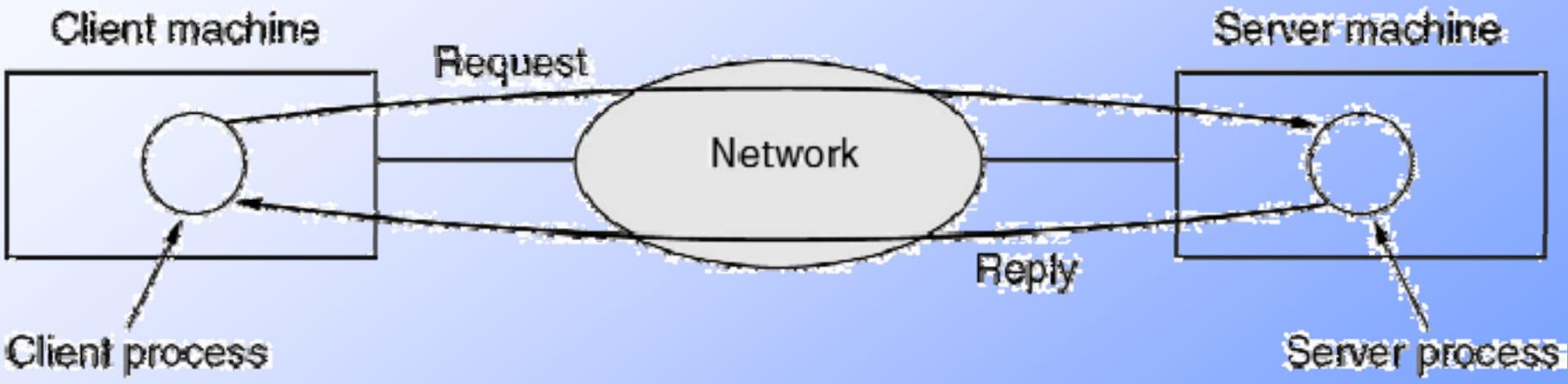
در سیستمهای نقطه به نقطه، کلاینت و یا سرور ثابت وجود ندارد

کاربردهای شبکه‌های کامپیوتری :

- کاربردهای تجاری
- کاربردهای خانگی
- کاربران در حرکت
- تبعات اجتماعی

کاربرد تجاری شبکه‌ها :

این کاربردها بر مبنای مدل کلاینت_سرور می‌باشد.



مدل کلاینت_سرور با درخواست و پاسخ همراه می‌باشد

کاربردهای خانگی :

- دسترسی به اطلاعات از راه دور
- ارتباط فرد با فرد
- سرگرمی های تعاملی (محاوره ای)
- تجارت الکترونیکی

کاربردهای خانگی :

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books on-line
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products on-line
P2P	Peer-to-peer	File sharing

برخی انواع تجارت الکترونیکی

کاربران شبکه‌های متحرک :

Wireless	Mobile	Applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in older, unwired buildings
Yes	Yes	Portable office: PDA for store inventory

ترکیبی از شبکه‌های بی‌سیم و کامپیوترهای سیار

تبعات اجتماعی :

- عدم اطمینان از صحت اطلاعات
- تجسس و دزدی اطلاعات شخصی
- ایجاد مزاحمت (ارسال spam به میل ها)
- نقض قانون کپی رایت

تقسیم‌بندی شبکه ها :

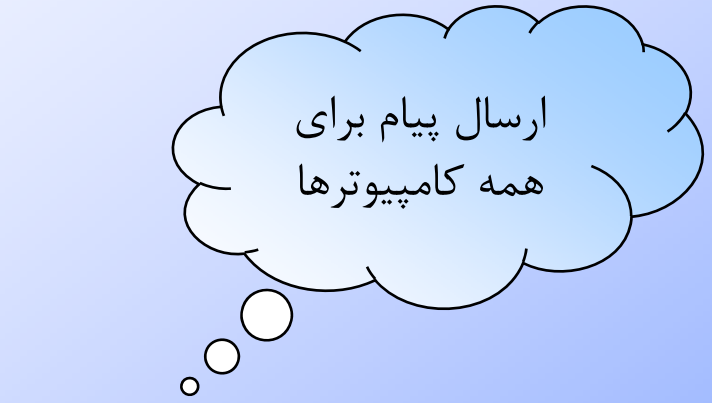
- ✓ از نقطه نظر تکنولوژی انتقال شبکه‌ها
- ✓ براساس اندازه شبکه

تفکیک شبکه‌ها از نقطه نظر تکنولوژی انتقال

- شبکه‌های پخشی (broadcast)
- شبکه‌های نظیر به نظیر (peer to peer)

شبکه‌های پخشی (Broadcast) :

- دارای یک کانال مشترک بین همه کامپیوترها
- حاوی بسته پیام
- بسته شامل متن پیام به همراه آدرس کامپیوتر مقصد



پخش یا broadcasting

پخش گروهی یا multicasting

شبکه‌های نظیر به نظیر (peer to peer) :

مسائل مطرح در این نوع از شبکه‌ها :

- مسیر جداگانه بین هر دو کامپیوتر
- کشف کوتاهترین مسیر بین هر دو سیستم

تقسیم‌بندی شبکه‌ها بر اساس اندازه آنها

- شبکه‌های محلی (Local Area Networks)
- شبکه‌های ناحیه‌ای (Metropolitan Area Networks)
- شبکه‌های گسترده (Wide Area Networks)
- شبکه‌های بی‌سیم (Wireless Networks)
- شبکه شبکه‌ها (internetwork)

فاصله پردازنده‌ها	محدوده پردازنده‌ها	مثال
1 m	به فاصله یک میز	شبکه شخصی
10 m	یک اتاق	شبکه محلی
100 m	یک ساختمان	" "
1 km	یک مجتمع	" "
10 km	یک شهر	شبکه شهری
100 km	یک کشور	شبکه گسترده
1000 km	یک قاره	" "
10,000 km	کره زمین	اینترنت

طبقه‌بندی شبکه‌ها براساس اندازه آنها

شبکه‌های محلی(Local Area Networks)

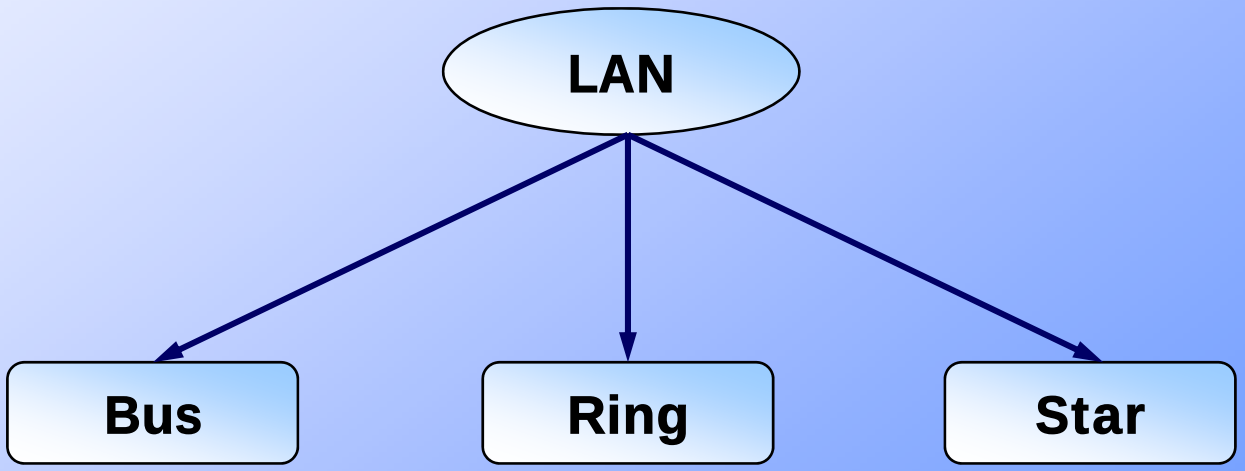
شبکه‌ای خصوصی برای متصل کردن کامپیوترهای یک شرکت و به اشتراک گذاشتن منابع و تبادل اطلاعات بین ایستگاههای کاری.

سه پارامتر مهم در شبکه‌های محلی:

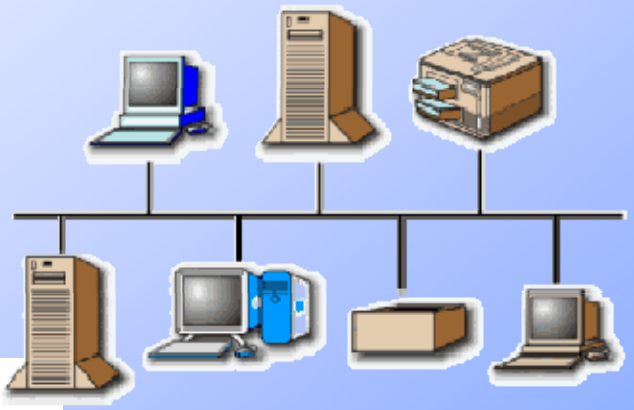
- اندازه
- فناوری انتقال اطلاعات
- توپولوژی

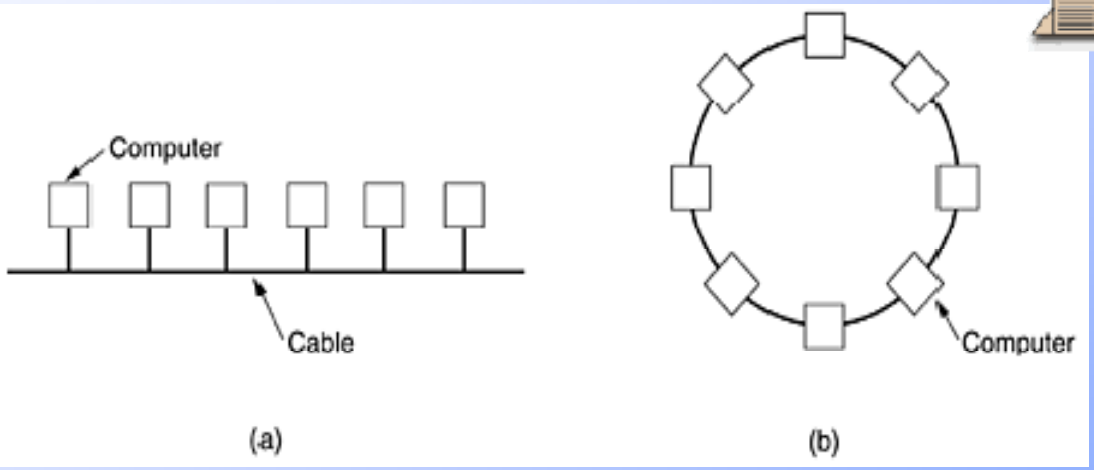
انواع توپولوژی یا همبندی‌های شبکه محلی:

- Bus (گذرگاه: وجود یک خط ارتباطی بین ایستگاه‌ها)
- Ring (حلقه: وجود کانال ارتباطی حلقوی)
- Star (ستاره: اتصال همه ایستگاه‌ها به یک وسیله هاب مرکزی و عدم ارتباط مستقیم ایستگاه‌ها با یکدیگر)



شبکه‌های محلی (LAN)

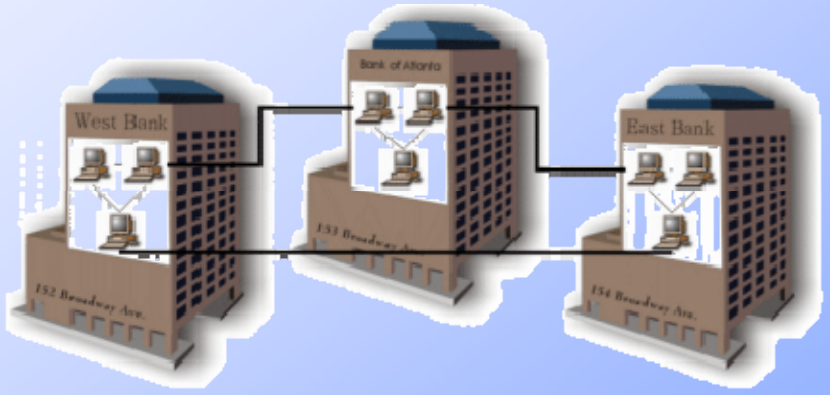




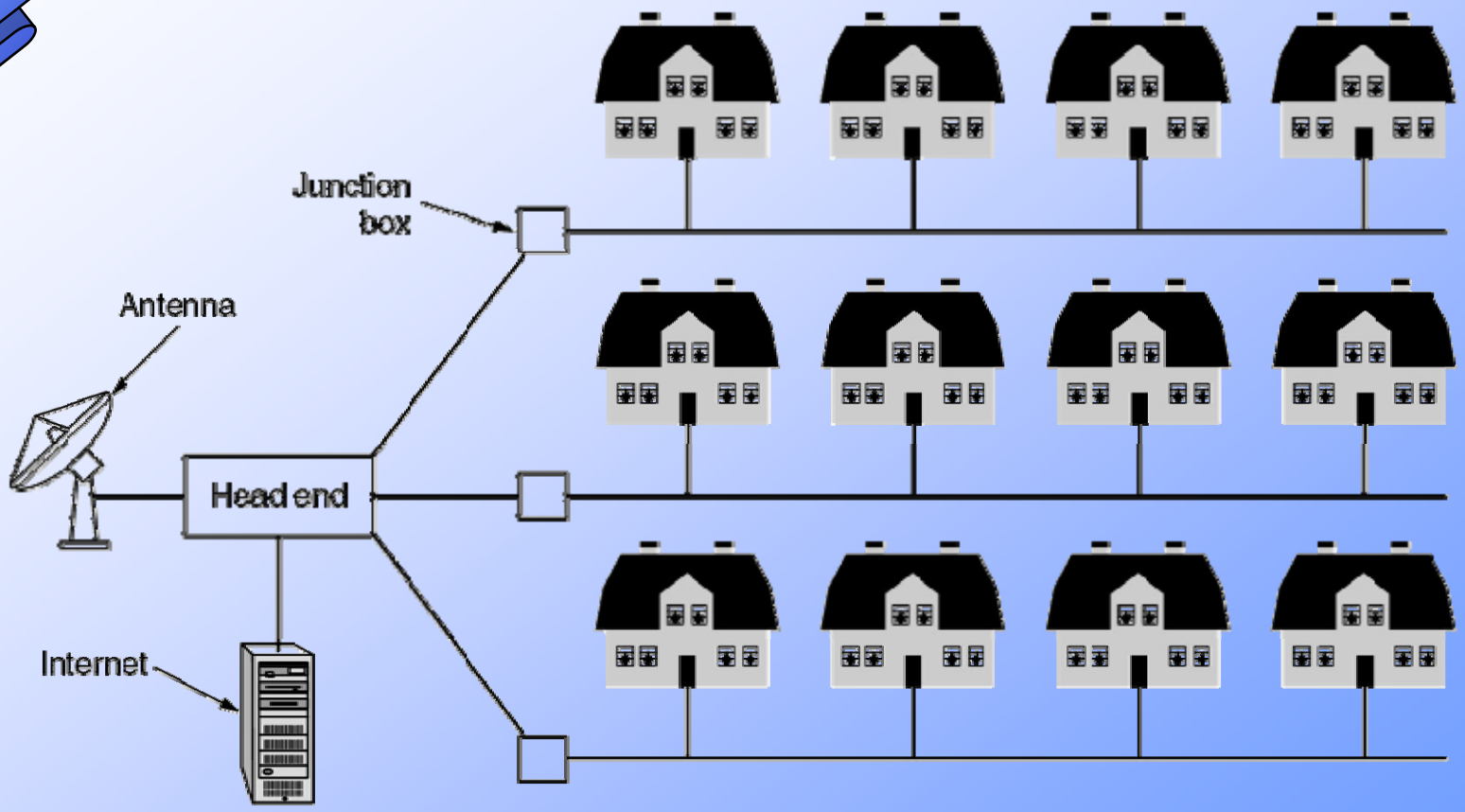
دو نوع شبکه پخشی : Bus (a) Ring (b)

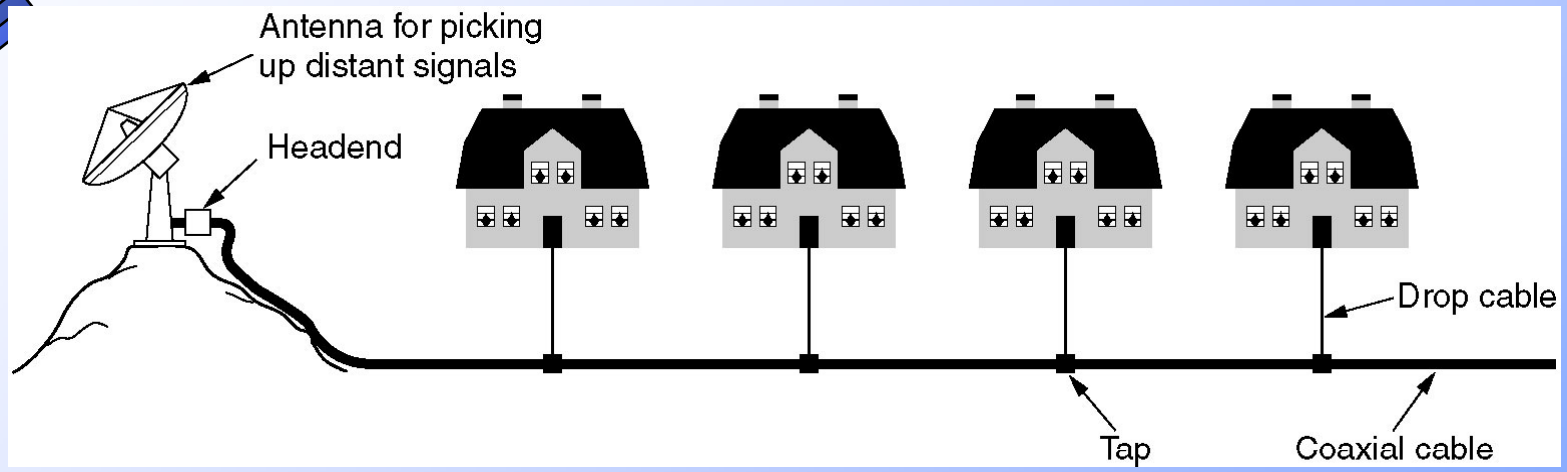
شبکه‌های ناحیه‌ای (Metropolitan Area Networks)

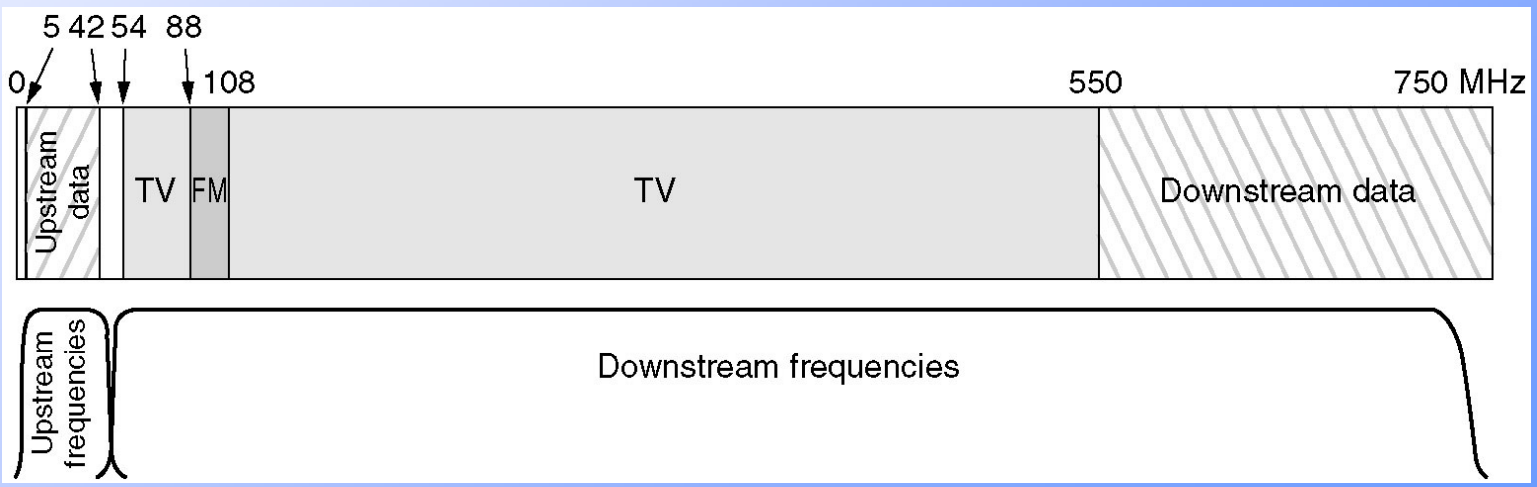
شبکه‌ای است در محدوده یک شهر که بهترین نمونه برای آن شبکه تلویزیون کابلی می‌باشد



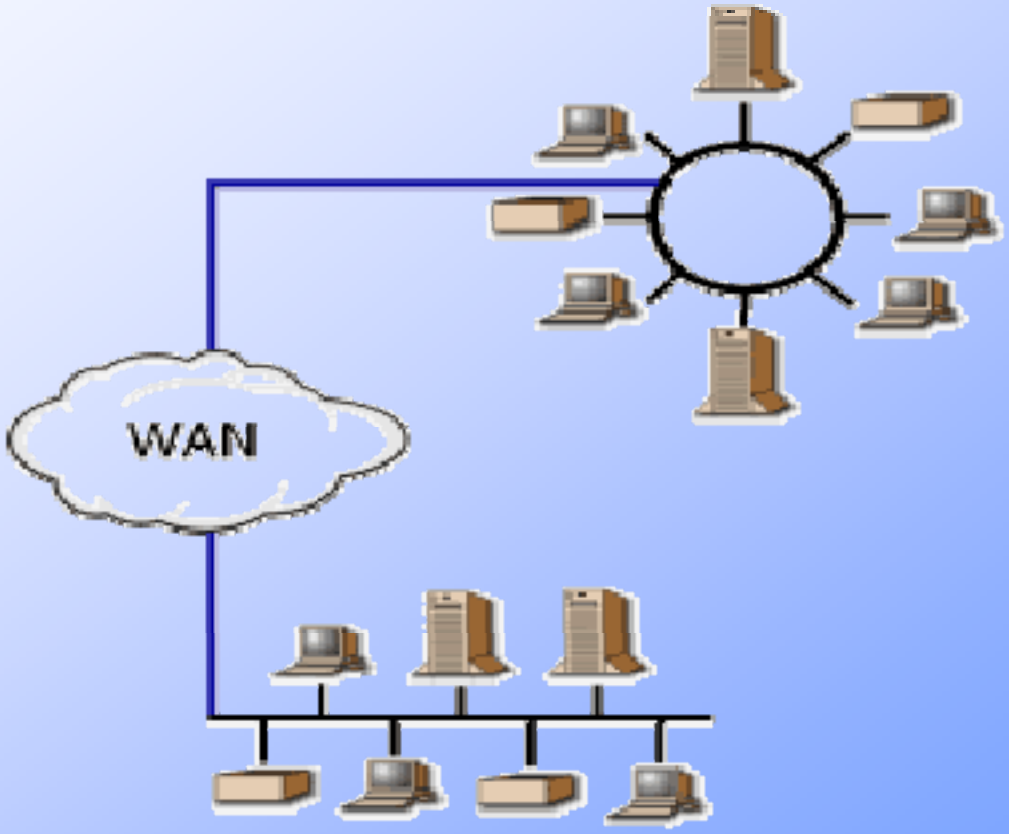
شبکه‌های ناحیه‌ای (MAN)




Antenna for picking
up distant signals
Headend
Drop cable
Tap
Coaxial cable


5 42 54 88
0
108
550
750 MHz
Upstream data
TV
FM
TV
Downstream data
Upstream frequencies
Downstream frequencies

شبکه‌های گسترده (Wide Area Networks)



اجزاء شبکه‌های گسترده

- ✓ میزبان (host)
- ✓ زیرشبکه‌ها (subnets)
  - خطوط انتقال
  - تجهیزات سوئیچینگ

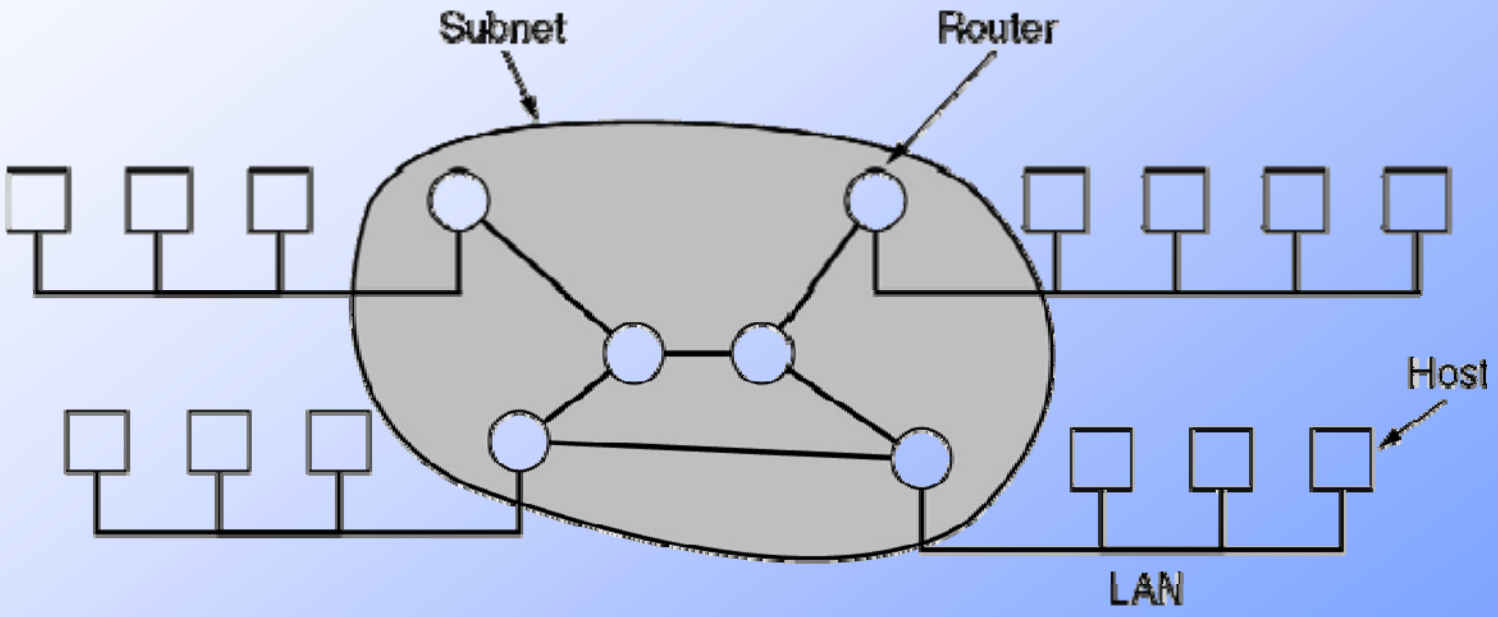
ابزار انتقال داده :

سیم مسی، فیبر نوری، امواج رادیویی

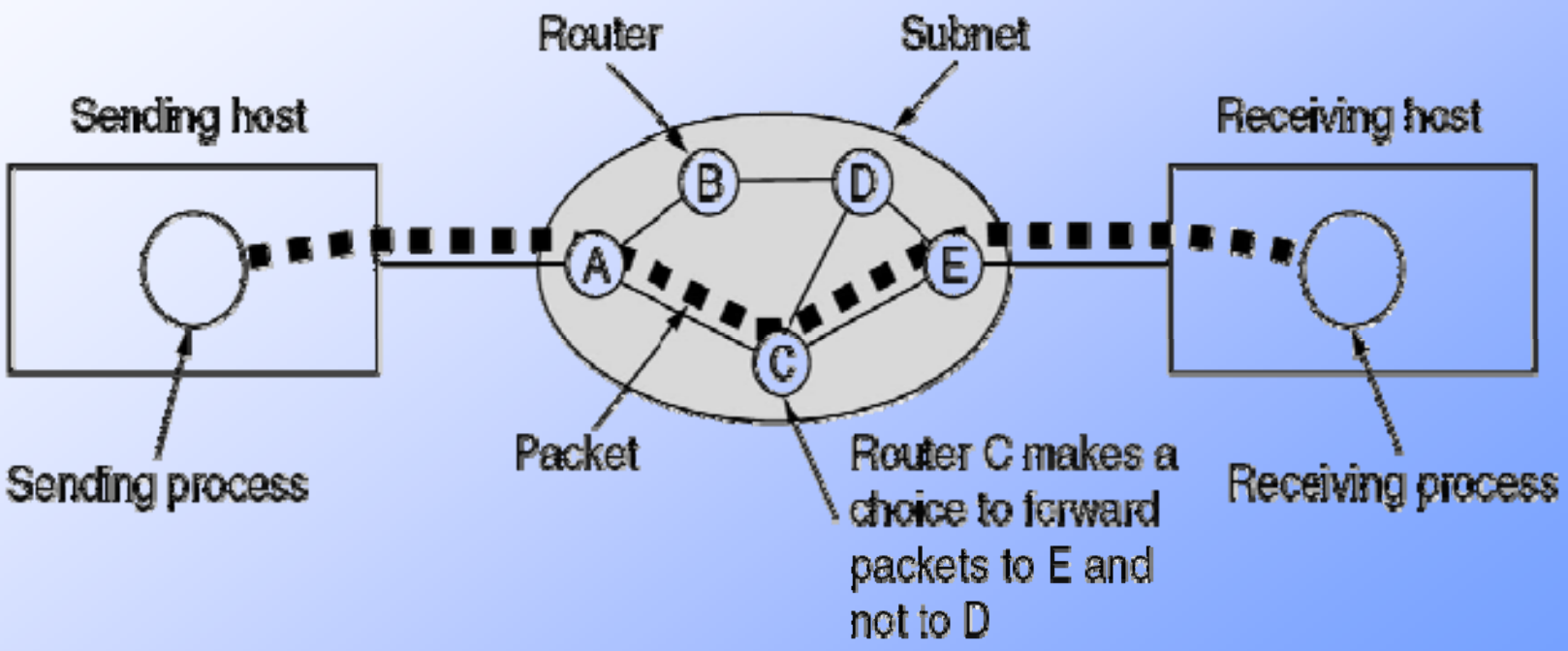
شامل مجموعه خطوط ارتباطی و مسیریابها

برقرای ارتباط بین خطوط

ارتباط بین hostها و زیر شبکه



ارتباط بین hostها و زیر شبکه



شبکه‌های بی‌سیم (Wireless Networks)

- ارتباطات بین سیستمی (Bluetooth)
- LAN بی‌سیم (IEEE 802.11)
- WAN بی‌سیم

- ارتباطات داخل سیستمی:

  برقراری ارتباطات بی سیم بین قطعات داخلی یک کامپیوتر

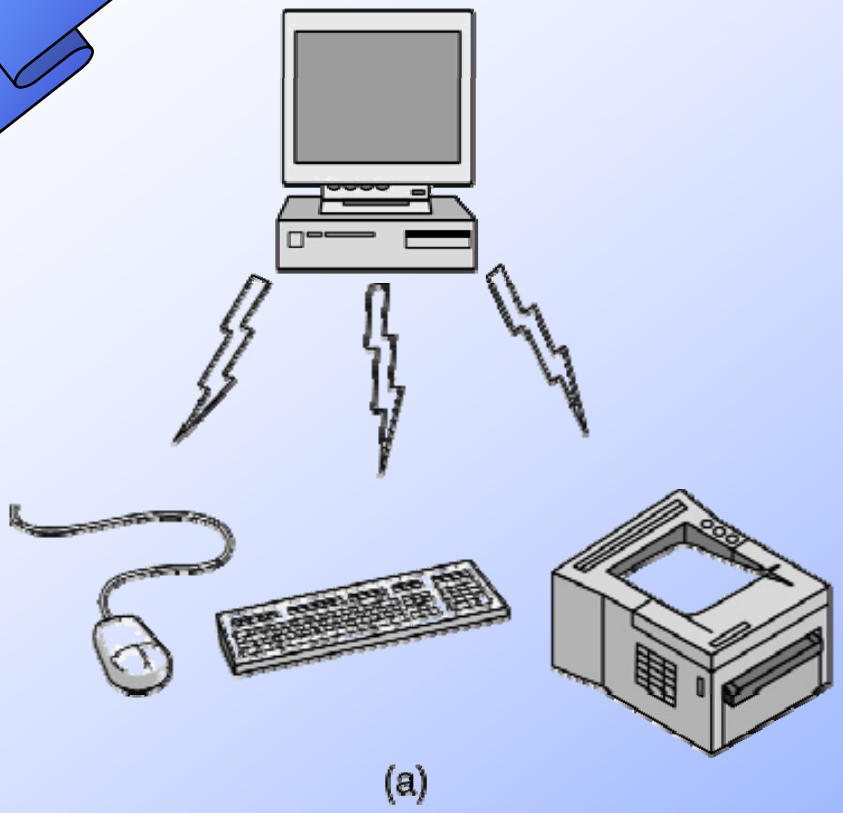
- LAN بی‌سیم:

  برقراری ارتباط بین کامپیوترها از طریق یک مودم رادیویی و یک آنتن

- WAN بی‌سیم:

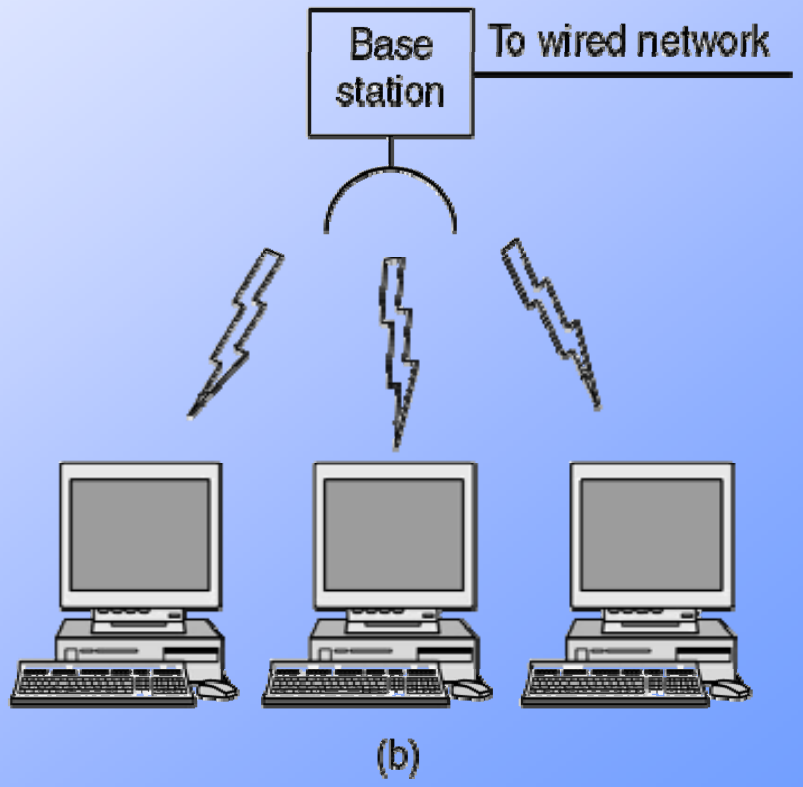
  با برد بیشتر و نرخ انتقال داده کمتر نسبت به LAN بی‌سیم از جمله شبکه تلفن همراه

شبکه‌های بی‌سیم



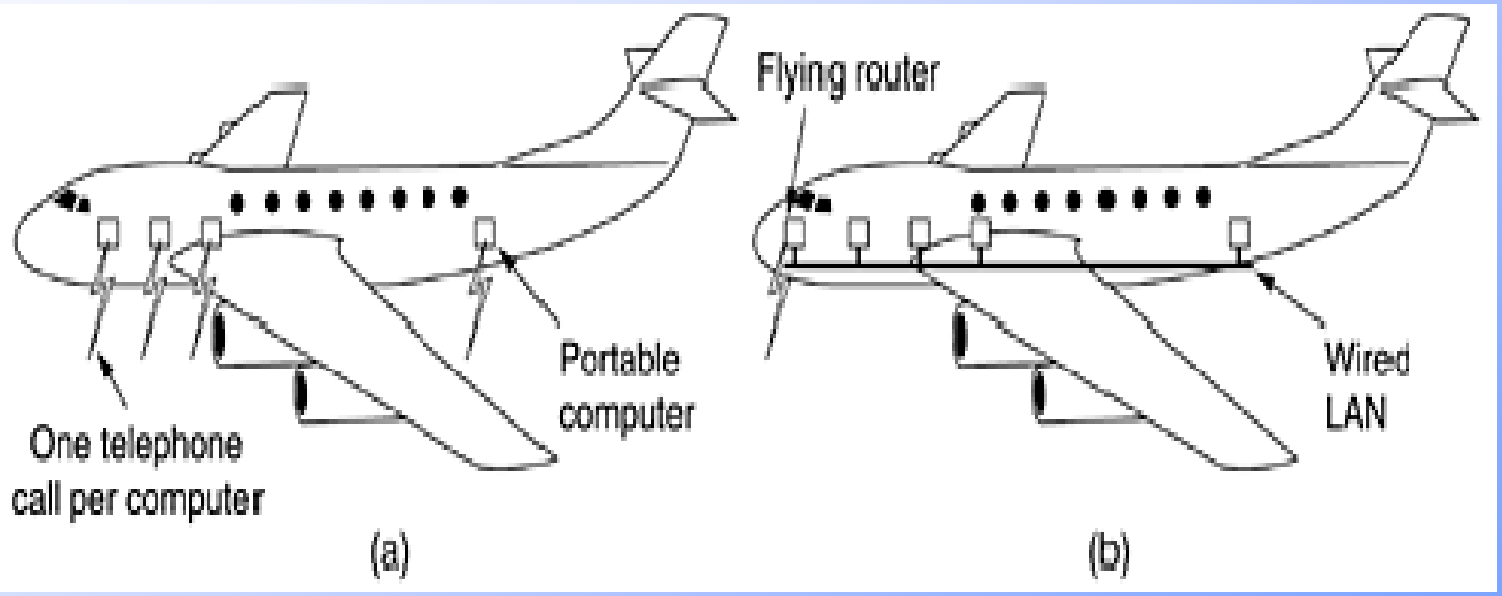
(a)

همبندی بلوتوث



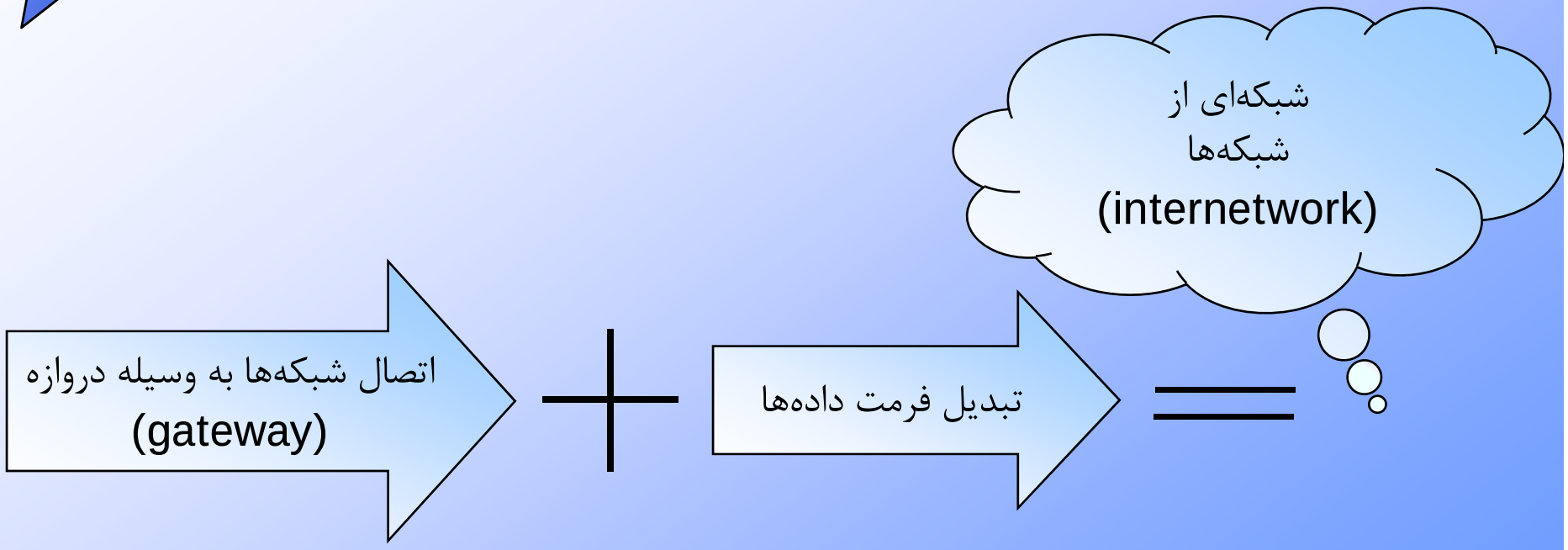
شبکه محلی بی‌سیم

شبکه‌های بی‌سیم



حالت (b) بهینه تر از حالت (a) است.

شبکه شبکه‌ها (internetwork)



نرم‌افزار شبکه

- پروتکل با ساختار سلسله مراتبی
- ارتباط بین سرویسها و پروتکل ها
- مقوله‌های طراحی در لایه‌ها
- خدمات اتصال‌گرا و خدمات بی‌اتصال
- مدل های مرجع شبکه (OSI و TCP/IP)

لزوم طراحی لایه‌ای ⟵ کاهش پیچیدگی های طراحی

مفاهیم کلی :

لایه: اجزاء تشکیل دهنده شبکه‌ها با ارائه سرویسهای خاص به لایه بالاتر

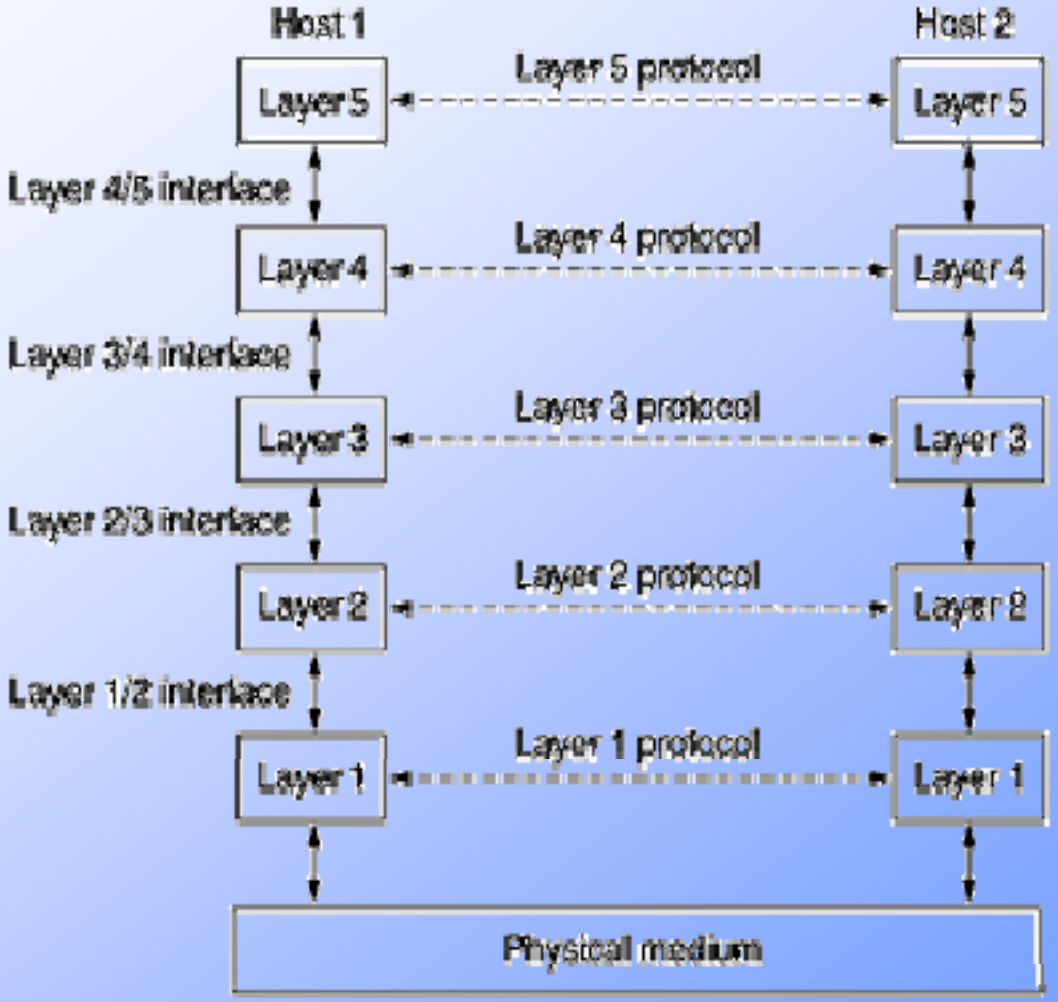
پروتکل: قواعد برقراری ارتباط یک لایه با لایه متناظرش

همتا(peer): تمام اجزاء موجود در یک لایه

واسط (interface): تعیین سرویس ها و عملکردهایی که هر لایه در اختیار لایه بالاتر قرار می‌دهد .

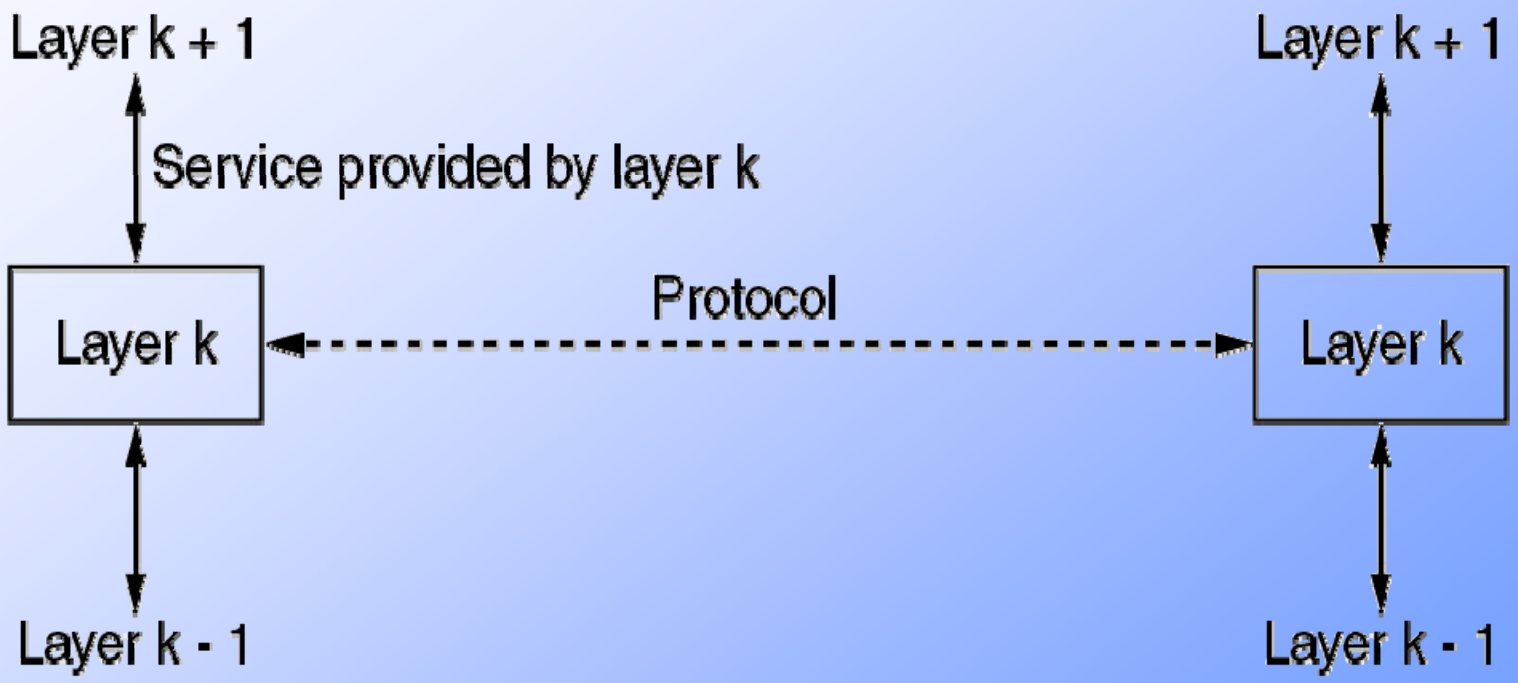
معماری شبکه (network architecture) : مجموعه لایه‌ها و پروتکل ها

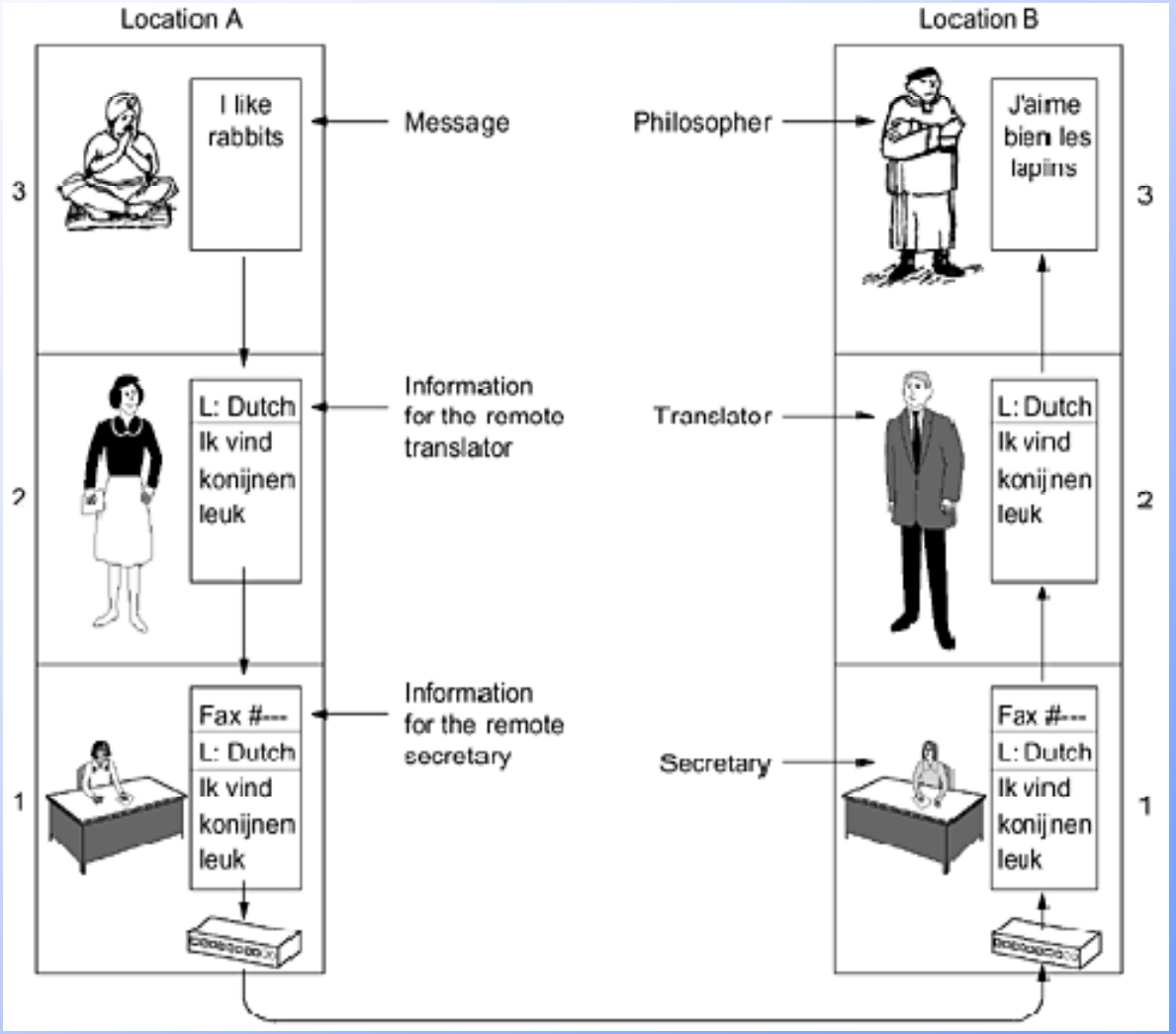
معماری شبکه (network architecture)



لایه‌ها، پروتکل‌ها و واسط‌ها

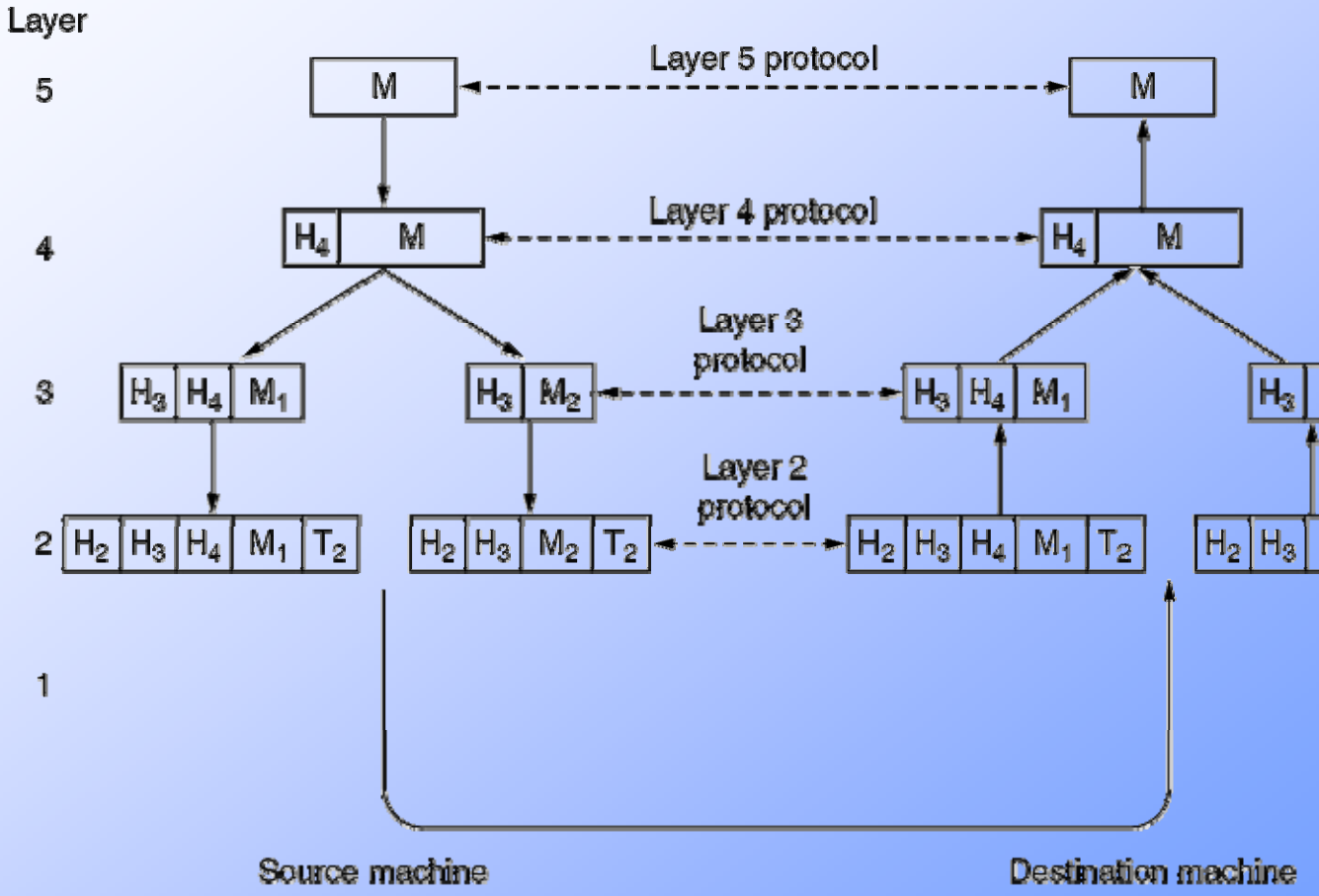
ارتباط سرویس‌ها با پروتکل‌ها





The philosopher-translator-secretary architecture.

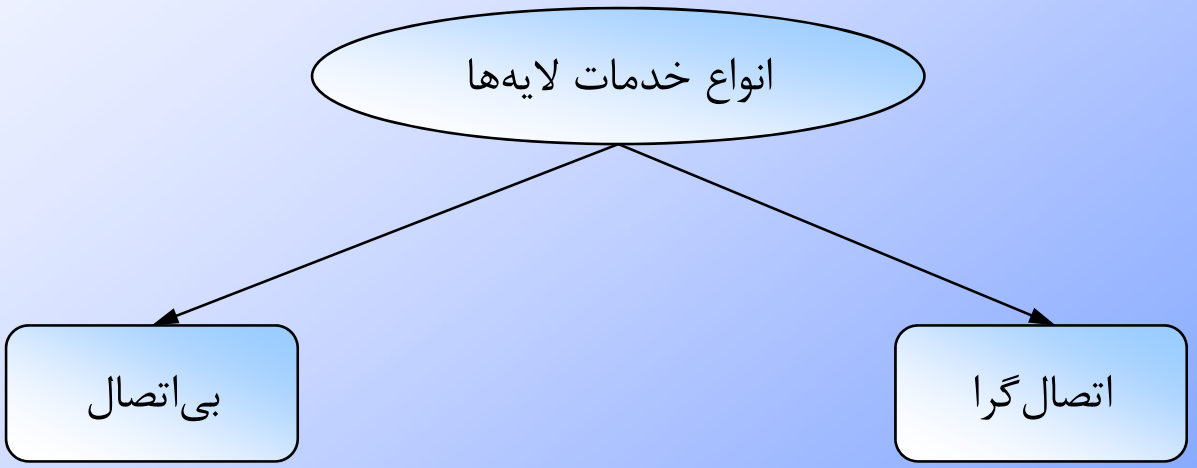
سلسله مراتب در پروتکل



نمونه‌ای از جریان اطلاعات که از ارتباط مجازی ۵ لایه پشتیبانی می‌نماید

مقوله‌های طراحی برای هر لایه

- آدرس دهی (Addressing)
- کنترل خطا (Error Control)
- کنترل جریان (Flow Control)
- تسهیم سازی (Multiplexing)
- مسیریابی (Routing)


انواع خدمات لايه‌ها
بی‌اتصال
اتصال گرا

خدماتی که هرلایه به لایه‌های بالاتر خود عرضه می‌کند:

- ✓ خدمات اتصال‌گرا **(پیاده‌سازی براساس مدل تلفن)**
  - ♦ ایجاد اتصال
  - ♦انتقال اطلاعات
  - ♦قطع اتصال
- ✓ بی‌اتصال **(پیاده‌سازی براساس مدل پست)**
  - ♦ غیر قابل اعتماد
  - ♦سرعت انتقال بالا

سرویس قابل اعتماد :

هیچ داده‌ای در حین انتقال از بین نرود ⟵ استفاده از تصدیق دریافت (Ack)

مدلهای مرجع

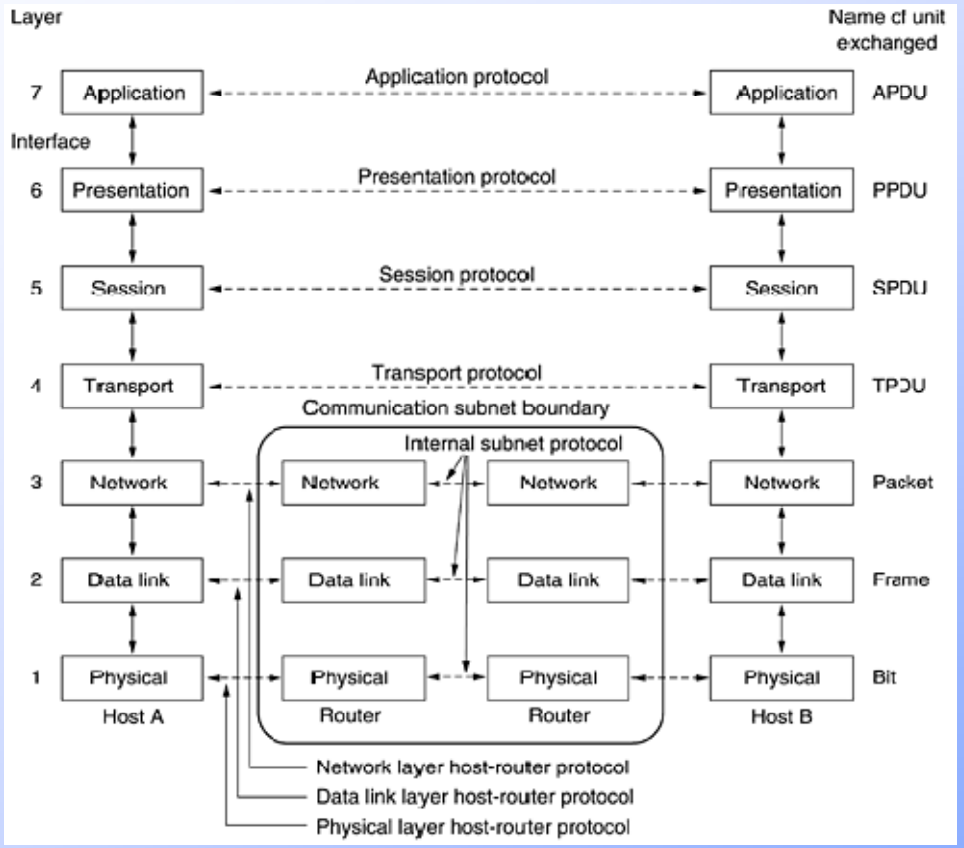
- ✓ مدل مرجع OSI
- ✓ مدل مرجع TCP/IP
- ✓ مقایسه مدل OSI با مدل TCP/IP
- ✓ نواقص مدل OSI
- ✓ نواقص مدل TCP/IP

اصول مدل مرجع OSI

- یک لایه، زمانی باید ایجاد شود که خدمت متفاوتی مورد نیاز است.
- هر لایه باید وظیفه مشخصی داشته باشد.
- وظیفه هر لایه بایستی با در نظر گرفتن پروتکل های جهانی تعریف گردد.
- مرزهای لایه باید برای کم کردن جریان اطلاعات از طریق رابط لایه‌ها انتخاب شوند.
- تعداد لایه‌ها باید به اندازه‌ای زیاد باشد که وظایف متمایز در یک لایه مشترک نباشد و به اندازه‌ای کم باشد که معماری آن ها نامناسب نگردد.

لایه‌های مدل مرجع OSI

- لایه فیزیکی (Physical layer)
- لایه پیوند داده‌ها (Data link layer)
- لایه شبکه (Network layer)
- لایه انتقال (Transport layer)
- لایه جلسه (Session layer)
- لایه نمایش (Presentation layer)
- لایه کاربرد (Application layer)

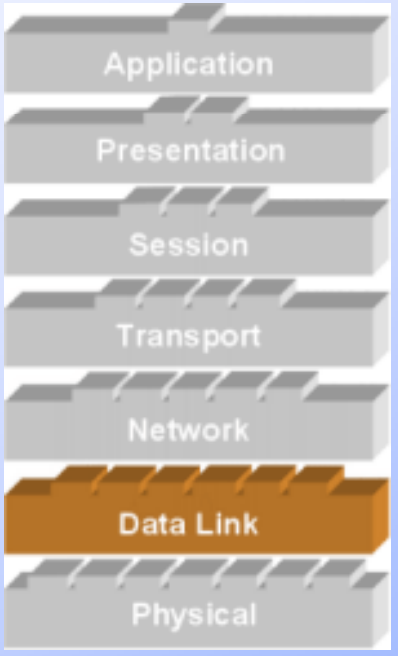


لایه فیزیکی (Physical layer)

وظیفه ارسال بیتهای خام(پردازش نشده) بر روی کانال ارتباطی و حصول اطمینان از ارسال درست بیت مورد نظر .

لایه پیوند داده‌ها (Data link layer)

این لایه وظیفه تبدیل وسایل انتقال اطلاعات خام به کانال ارتباطی بدون خطا از دید لایه شبکه را بر عهده دارد و حاوی زیرلایه خاصی به نام زیرلایه دستیابی شبکه (MAC) می‌باشد.



لایه شبکه (Network layer)

این لایه وظیفه کنترل زیر شبکه و چگونگی هدایت بسته‌های اطلاعاتی را از مبدأ به مقصد بر عهده دارد.

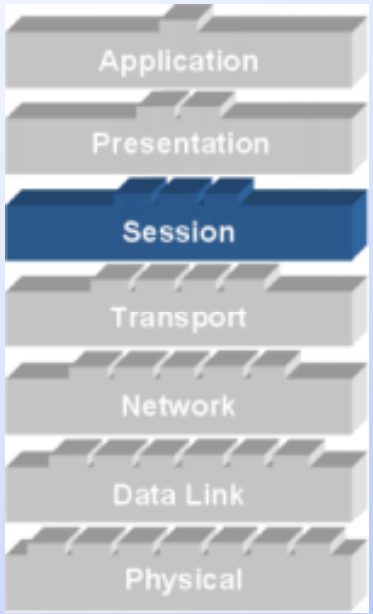
لایه انتقال (Transport layer)

وظیفه اصلی این لایه دریافت داده از لایه بالاتر و در صورت نیاز شکستن آن به اندازه‌های کوچکتر، فرستادن آنها به لایه شبکه و اطمینان حاصل کردن از اینکه داده‌ها بطورصحیح به طرف مقابل می‌رسد.

لایه جلسه (Session layer)

این لایه به کاربران در ماشینهای مختلف اجازه می‌دهد که جلساتی را بین خودشان برقرار کنند و خدمات گوناگونی مانند کنترل گفتگو ، مدیریت نشانه و همگام‌سازی را نیز ارائه می‌دهد.

مدیریت نشانه: به این معناست که دو طرف یک عمل بحرانی را در آن واحد انجام ندهند.

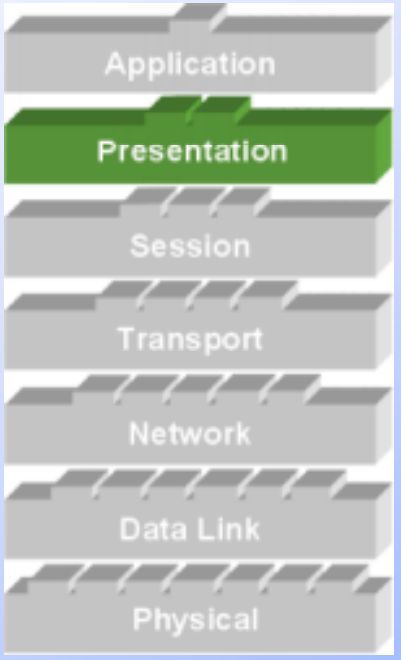


همگام سازی: همگام سازی کمک می‌کند که در هنگام ارسال یک فایل بزرگ، پس از بروز مشکل، انتقال دوباره از آخرین نقطه کنترلی، تکرار گردد.

لایه نمایش (Presentation layer)

این لایه به قواعد و معنای اطلاعات فرستاده شده مربوط می‌شود.

به طور کلی وظیفه اش قابل فهم کردن اطلاعات آمده از لایه کاربرد فرستنده برای لایه کاربرد گیرنده است.



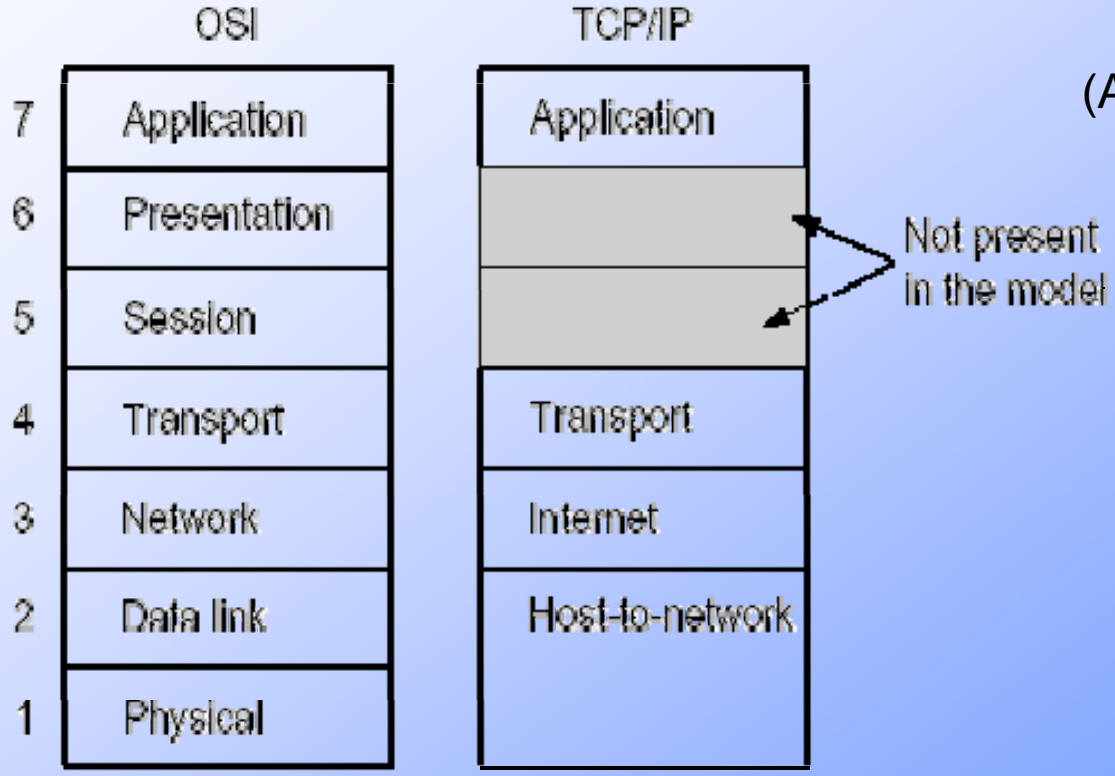
لایه کاربرد (Application layer)

این لایه شامل پروتکلهای گوناگونی که مورد نیاز عمومی کاربران است می‌باشد. از جمله پروتکلهایی که بطور گسترده مورد استفاده قرار می‌گیرد HTTP می‌باشد که اساس شبکه جهانی اینترنت می‌باشد.

از دیگر پروتکلهای این لایه می‌توان از پروتکل انتقال فایل (FTP) ، پست الکترونیکی (SMTP) و... نام برد.

لایه‌های مدل مرجع 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)

فقط بیان می‌کند که میزبان با استفاده از بعضی از پروتکل ها به شبکه متصل شود.

بنابراین می‌تواند بسته‌های IP را از طریق آن ارسال کند. این پروتکل از میزبان به میزبان و از شبکه به شبکه متفاوت است.

لایه اینترنت (internet layer)

وظیفه لایه اینترنت تحویل بسته های IP به جایی که مورد نظر است می باشد . در اینجا مسیریابی مسأله اصلی است، به همین دلیل می توان گفت که لایه اینترنت در مدل TCP/IP شبیه لایه شبکه در OSI می باشد.

لایه انتقال (Transport layer)

این لایه شامل دو پروتکل به شرح زیر می‌باشد:

- TCP (قرارداد کنترل انتقال):

پروتکل قابل اعتماد و اتصال گرایی است که اجازه می‌دهد رشته‌ای از بایت هایی که از یک ماشین شروع به حرکت می‌کنند، بدون خطا به ماشین دیگری در لایه اینترنت تحویل شوند.

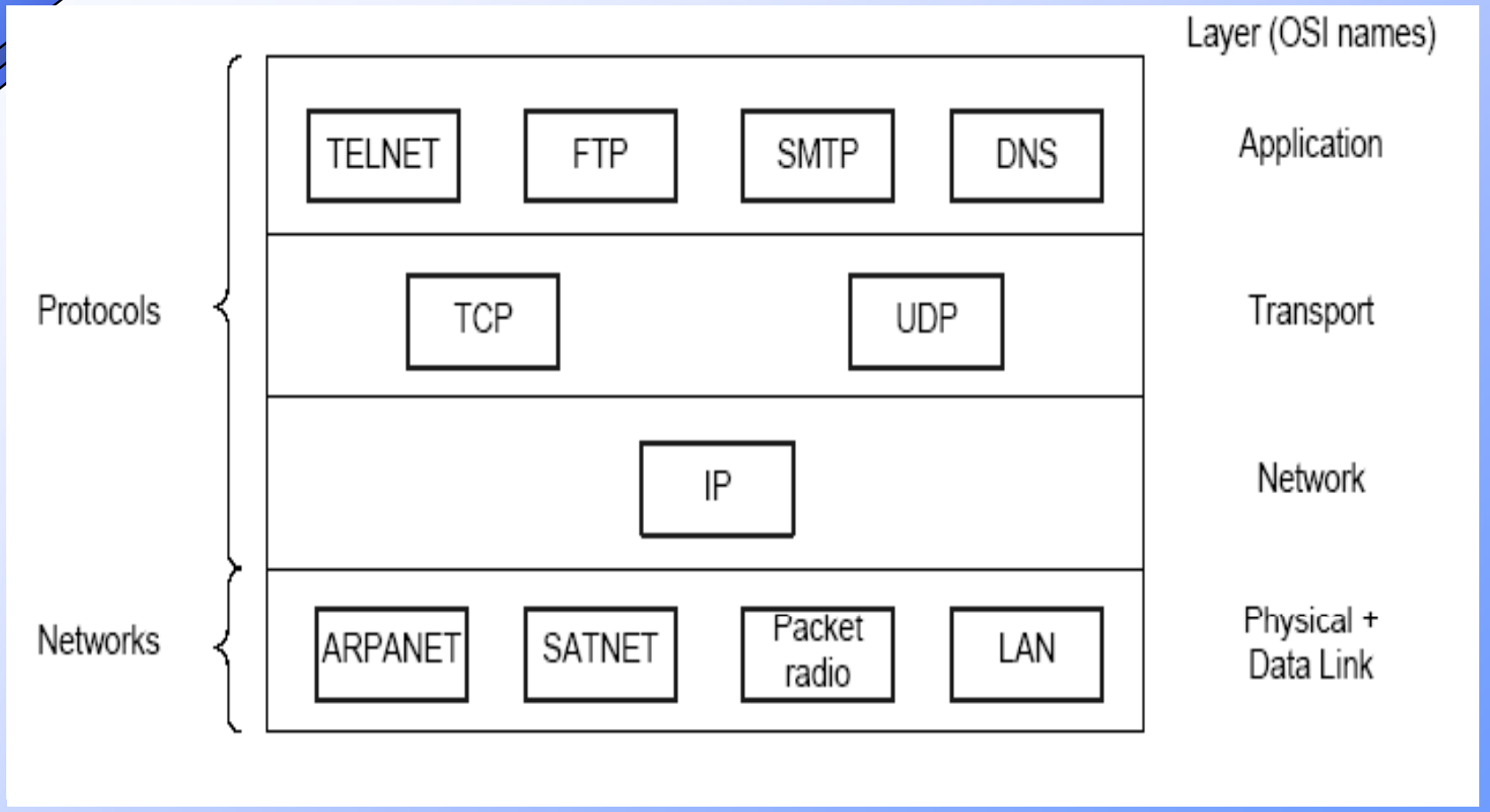
- UDP (پروتکل داده گرام کاربر):

یک پروتکل 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 پروتکلهای لایه بالاتر می‌باشد.

مدلهای اولیه، شامل پایانه مجازی (Telnet) و انتقال فایل (FTP) و پست الکترونیکی (SMTP) و ... بوده‌اند.



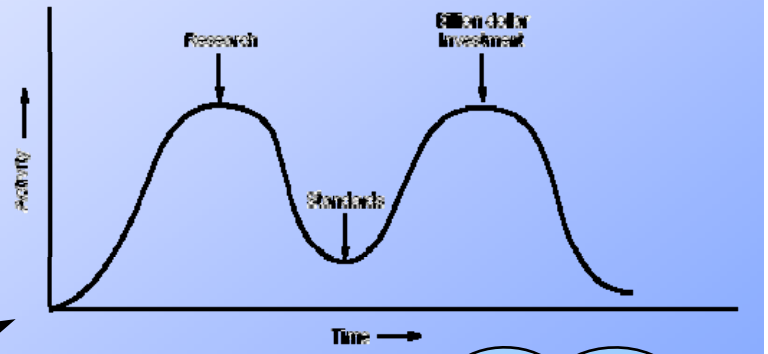
پروتکلها و شبکه‌ها در مدل اولیه TCP/IP

مقایسه مدل های مرجع OSI و TCP/IP

- هر دو بر اساس مفهوم پشته‌ای از پروتکل های مستقل پایه‌گذاری شده‌اند.
- عملکرد لایه‌ها در آنها مشابه به هم می‌باشد.
- تفاوت در تعداد لایه ها.
- مدل OSI هر دو ارتباط اتصالگرا و بی‌اتصال را در لایه شبکه و فقط اتصالگرا را در لایه انتقال پشتیبانی می‌کند. و مدل TCP/IP در لایه شبکه فقط از ارتباط بی اتصال و از هردو ارتباط در لایه انتقال پشتیبانی می‌کند.

معایب مدل مرجع OSI

مکاشفه دو فیل



- زمان بندی نادرست
- تکنولوژی نادرست
- پیاده سازی نادرست
- سیاست های نادرست

دومین دلیل عدم رشد OSI این است که هم مدل و هم پروتکل ناقص است.

نقدی بر مدل مرجع TCP/IP

- در این مدل مفاهیم خدمات، رابطه و پروتکل بطور واضح قابل تفکیک نیست.
- مدل TCP/IP یک مدل عمومی نیست و برای تشریح هر پشته‌ای از پروتکل ها به جز TCP/IP مفید نیست.
- لایه میزبان شبکه که در مورد پروتکل های لایه‌ای وجود داشت، بعنوان یک لایه محسوب نمی‌شود و تنها به عنوان یک رابط (بین لایه شبکه و پیوند داده) عمل می‌کند.
- در مدل TCP/IP تمایزی بین لایه‌های فیزیکی و پیوند داده‌ها نیست. در صورتیکه این دو لایه کاملاً از هم متمایز هستند.

سازمانهای استاندارد در زمینه شبکه

- ANSI
- IEEE
- ISO
- IEC
- IAB

یک سازمان خصوصی و غیرانتفاعی می‌باشد که وظیفه توسعه و هماهنگ سازی استانداردهای ملی را داراست.

مسئول تعریف و تدوین استانداردهای مخابراتی و ارتباطات داده‌ای است.

تمام موارد بجز موارد الکتریکی و الکترونیکی را پوشش می‌دهد. استانداردهای آن با سرنام ISO شناخته می‌شوند.

تمام استانداردهای بین‌المللی برای موارد الکتریکی و الکترونیکی تعریف می‌کند.

توسعه اینترنت را کنترل می‌کند که شامل دو کمیته IETF و IRTF می‌باشد.

Metric Units

Exp.	Explicit	Prefix	Exp.	Explicit	Prefix
10^{-3}	0.001	milli	10^{3}	1,000	Kilo
10^{-6}	0.000001	micro	10^{6}	1,000,000	Mega
10^{-9}	0.000000001	nano	10^{9}	1,000,000,000	Giga
10^{-12}	0.000000000001	pico	10^{12}	1,000,000,000,000	Tera
10^{-15}	0.000000000000001	femto	10^{15}	1,000,000,000,000,000	Peta
10^{-18}	0.000000000000000001	atto	10^{18}	1,000,000,000,000,000,000	Exa
10^{-21}	0.000000000000000000001	zepto	10^{21}	1,000,000,000,000,000,000,000	Zetta
10^{-24}	0.000000000000000000000001	yocto	10^{24}	1,000,000,000,000,000,000,000,000	Yotta

فصل دوم:

لایه فیزیکی

مبنای تئوریک در انتقال داده

- تحلیل فوریه
- سیگنال های با پهنای باند محدود
- بیشترین نرخ ارسال داده در کانال

تحلیل فوریه

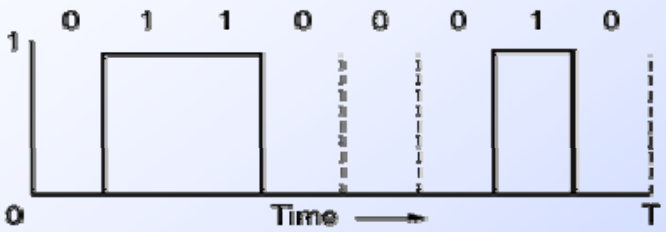
$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty}\left(a_n \sin\frac{2n\pi t}{T} + b_n \cos\frac{2n\pi t}{T}\right)$$

$$a_n = \frac{2}{T}\int_0^T g(t)\sin(2n\pi ft)\,dt$$

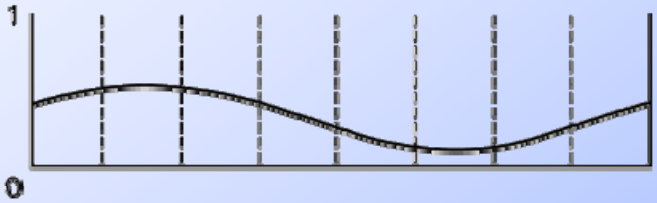
$$b_n = \frac{2}{T}\int_0^T g(t)\cos(2n\pi ft)\,dt$$

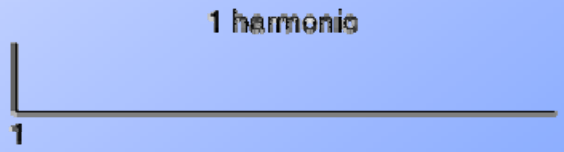
$$C = \frac{2}{T}\int_0^T g(t)dt$$

سیگنال های با پهنای باند محدود

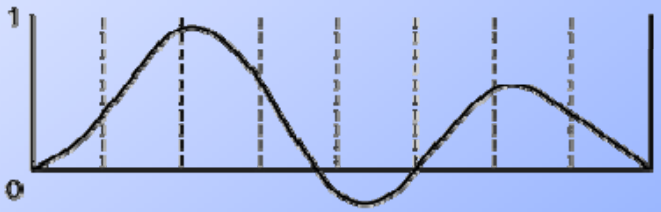


(a)





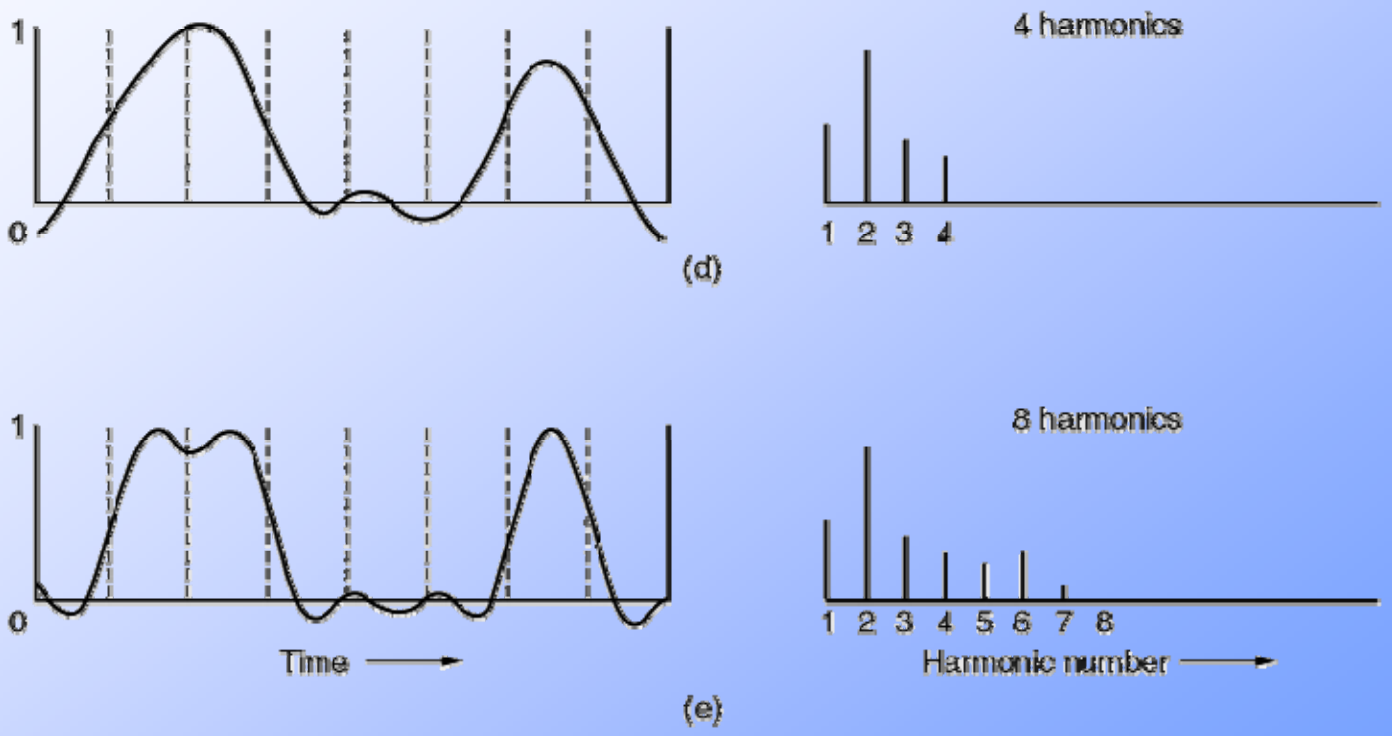
(b)



(c)

$$\sqrt{a_n^{\,2} + b_n^{\,2}}$$

سیگنال های با پهنای باند محدود



(d) – (e) Successive approximations to the original signal.

سیگنال های با پهنای باند محدود

Bps	T (msec)	First harmonic (Hz)	# Harmonics sent
300	26.67	37.5	80
600	13.33	75	40
1200	6.67	150	20
2400	3.33	300	10
4800	1.67	600	5
9600	0.83	1200	2
19200	0.42	2400	1
38400	0.21	4800	0

ارتباط بین نرخ داده و شماره هارمونیک در یک کانال تلفن معمولی

(در یک کانال صوتی حداکثر با سرعت 19.2 kbps می توان داده را منتقل کرد.)

بیشترین نرخ ارسال داده در کانال

نایکویست:

$$\text{حداکثر سرعت داده} = 2H \log_2 V \ bits/\sec$$

- V: تعداد سطوح مجزا
- H : پهنای باند کانال

شانون:

$$\text{حداکثر سرعت داده‌ها} = H \log_2 (1 + s/n)$$

محیط های انتقال داده:

- هدایت شده ⟵ سیم مسی ، فیبرنوری ، ...
- هدایت نشده ⟵ امواج رادیوئی (پخش در هوا)

الف) محیط های انتقال داده کابلی

۱- کابل جفت تابیده

۲- کابل کواکسیال

۳- فیبرهای نوری

۴- آداپتور واسط شبکه

۵- هاب های شبکه

۱) کابل جفت تابیده (Twisted Pair)

رسانه انتقالی است که بطور گسترده در مخابرات استفاده می‌شود و شامل چهار جفت سیم مسی عایق دار است که به صورت مارپیچ بهم تابیده شده اند.

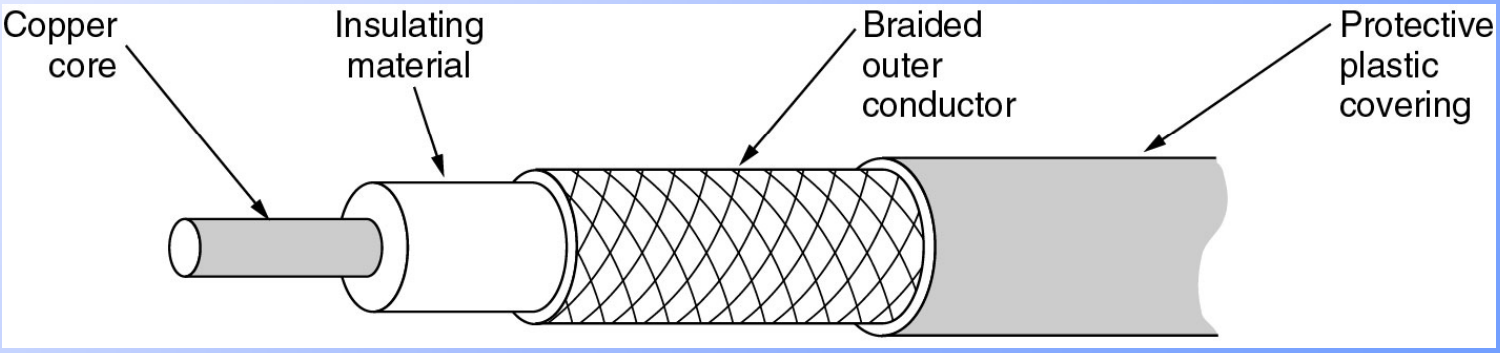
علت اصلی تابیدن سیم‌ها، کاهش اثر آنتن در دریافت سیگنال می‌باشد. (اولا میدانی در اطراف خود ایجاد نکنند. ثانیا اثرات نویز القا شده روی خود را خنثی کنند.)

(b) Category 5 UTP

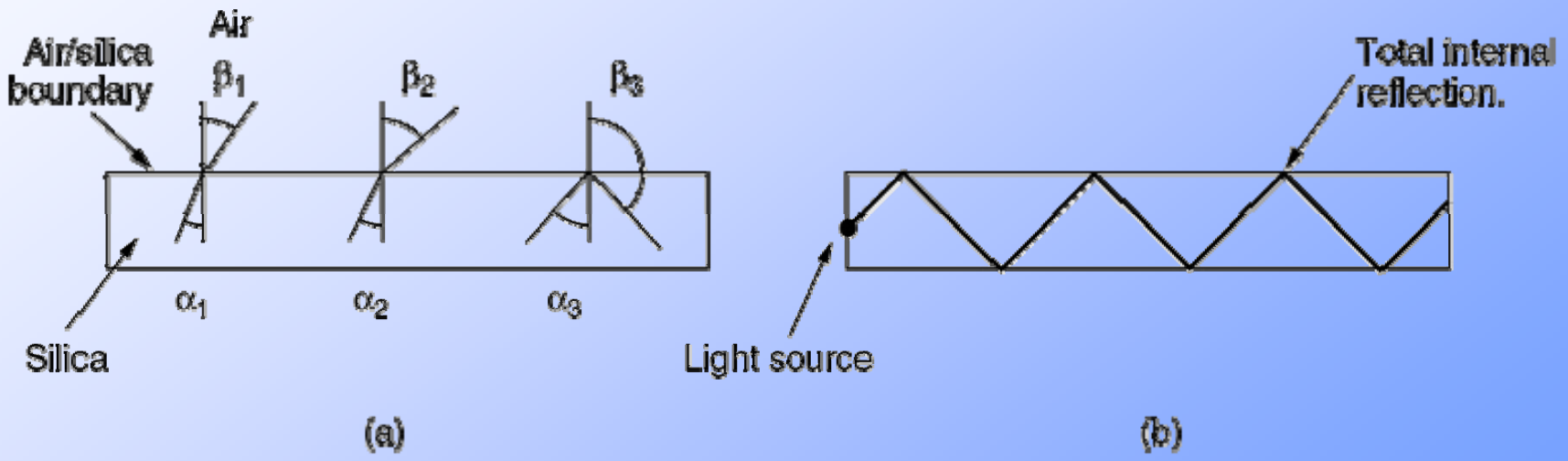
(a) Category 3 UTP

۲) کابل کواکسیال

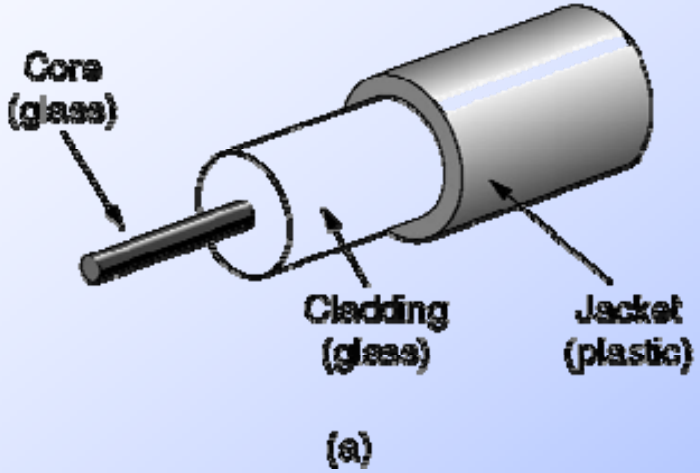
یکی از قدیمی ترین رسانه های انتقال می باشد. این نوع کابل به علت پوشش فلزی می‌تواند کارایی بیشتری را (از نظر سرعت و فاصله) نسبت به زوج تابیده فراهم کند.

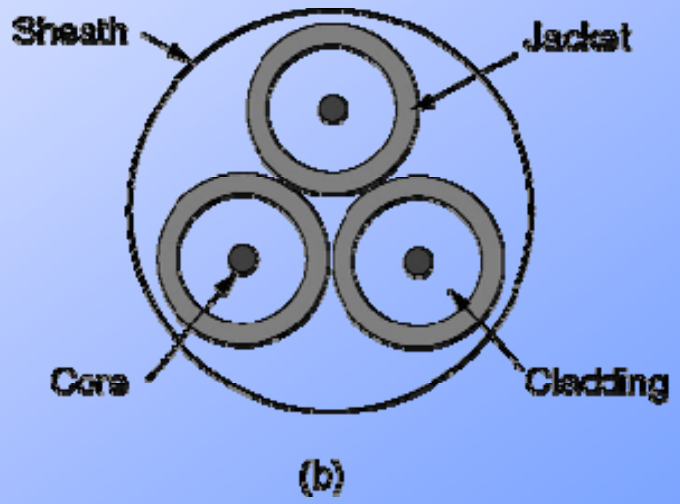


۳) فیبر نوری


Air
Air/silica boundary
β1
β2
β3
α1
α2
α3
Silica
(a)
Total internal reflection.
Light source
(b)

کابل های فیبرنوری





(a) Side view of a single fiber.
(b) End view of a sheath with three fibers.

فیبرهای نوری

سیستم انتقال نور دارای ۳ مؤلفه اصلی می‌باشد :

۱- منبع نور

۲- رسانه انتقال

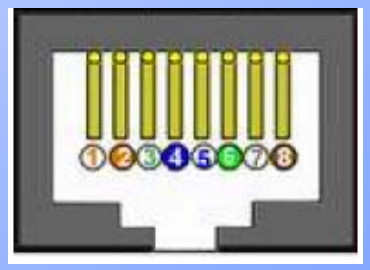
۳- آشکار ساز

۴) آداپتور واسط شبکه

ابزاری جهت ارتباط بین کامپیوتر و شبکه

انواع :

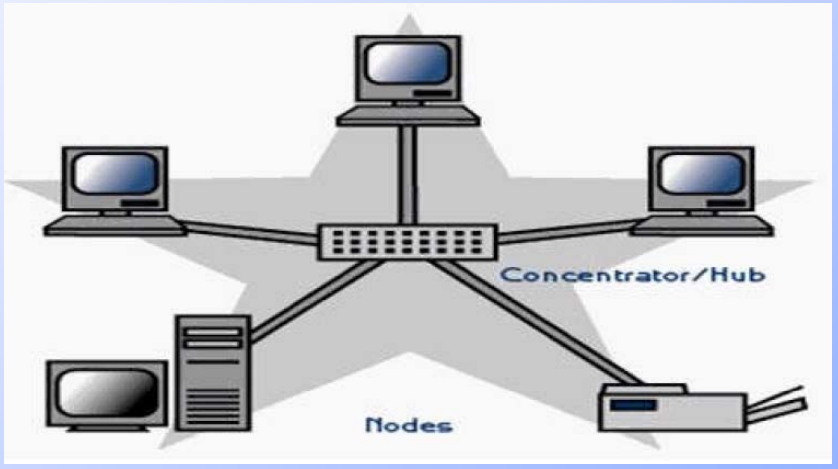
1) On-board روی مادربرد
2) نصب بر روی شیار های مادربرد ← PCI - ISA -
3) بی سیم



RJ45

۵) هاب های شبکه

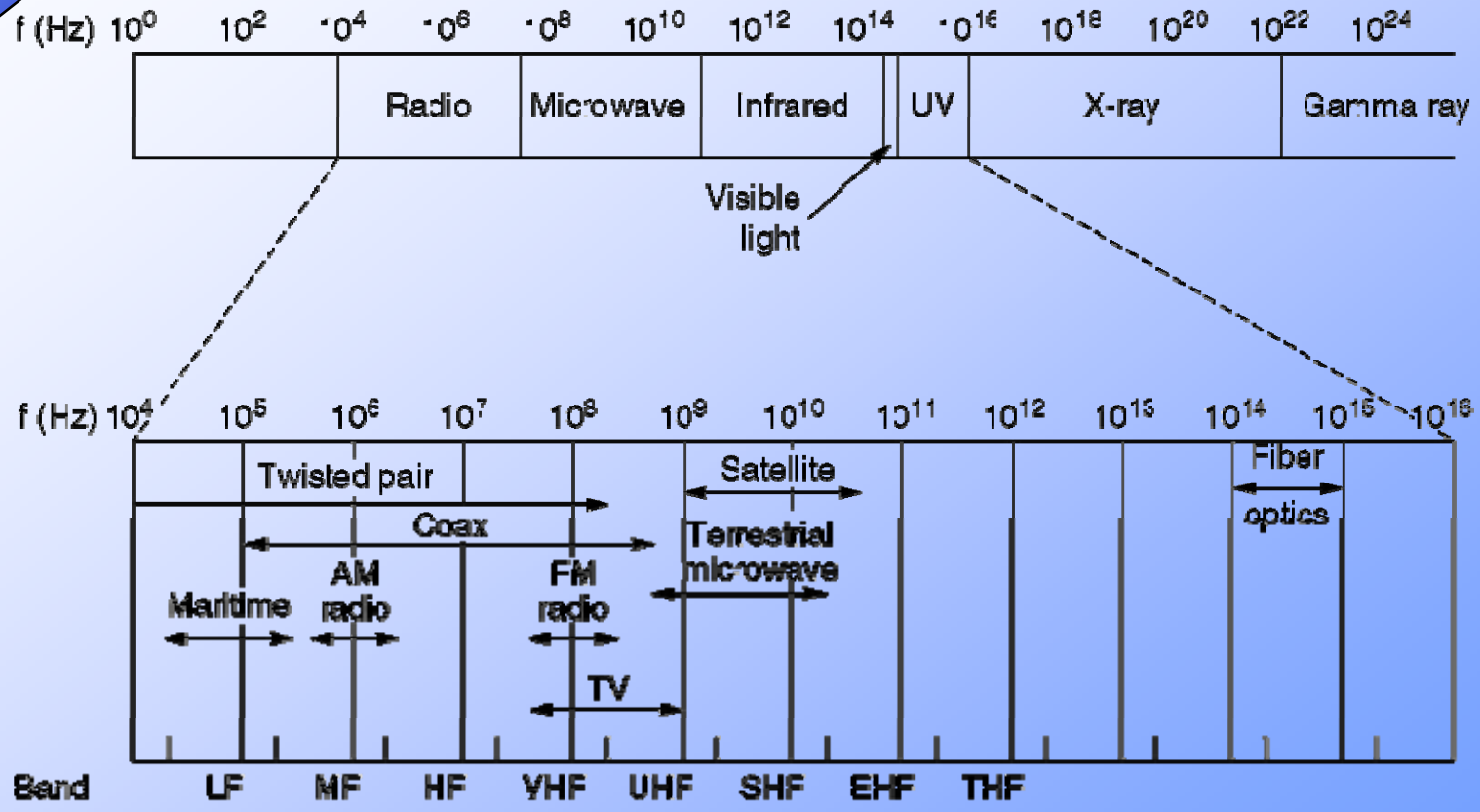
- ابزاری جهت اتصال کامپیوترهای یک شبکه ستاره ای.
- هاب سیگنال دریافتی را تقویت کرده و سپس به همه پورت های خروجی ارسال می کند.
- حداکثر فاصله بین hub و nodeها ۱۰۰متر.



ب) رسانه‌های انتقال بی سیم

- مخابرات رادیویی
- مخابرات ماکروویو
- امواج مادون قرمز و امواج میلیمتری
- مخابرات نوری
- ماهواره ها

طیف امواج الکترومغناطیس



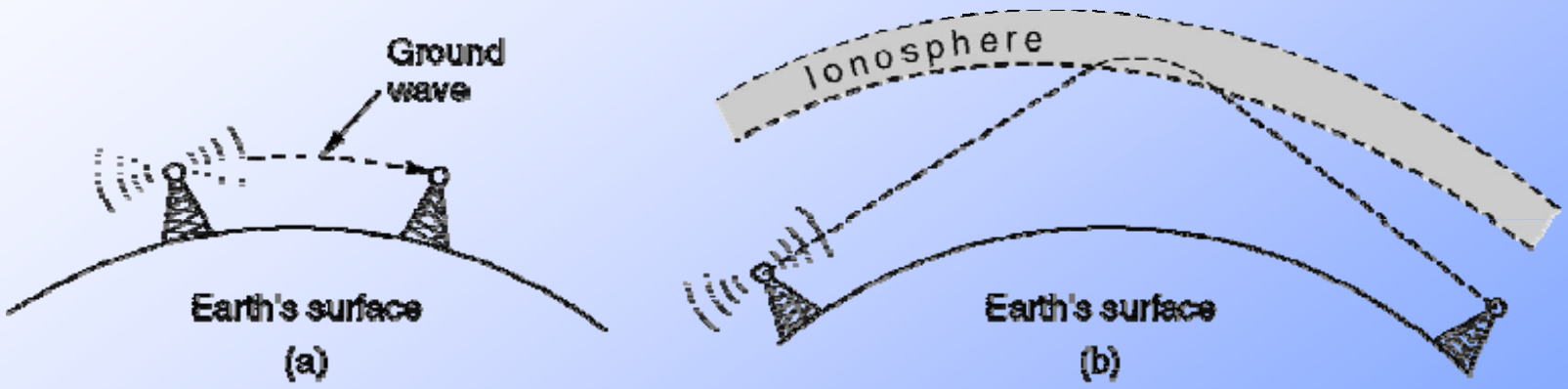
ELF = Extremely low frequency	MF = Medium frequency	UHF = Ultrahigh frequency
VF = Voice frequency	HF = High frequency	SHF = Superhigh frequency
VLF = Very low frequency	VHF = Very high frequency	EHF = Extremely high frequency
LF = Low frequency		

۱) مخابرات رادیویی

امواج رادیویی به آسانی تولید می‌شوند و می‌توانند مسافت های طولانی را طی کرده و به راحتی در ساختمان ها نفوذ نمایند.

این امواج بطورگسترده هم برای ارتباط درونی و هم برای ارتباط بیرونی مورد استفاده قرار می گیرند.

مخابرات رادیویی



(a)در باند VLF, LF, & MF امواج رادیویی از انحناء زمین تبعیت می‌کند.

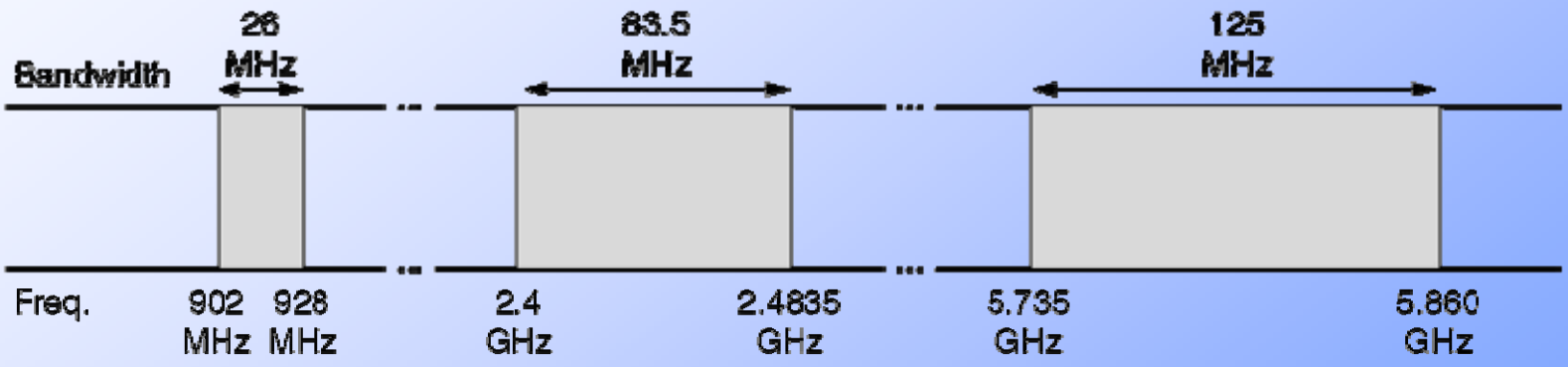
(b) در باند HF و VHF امواج رادیویی در مسیر مستقیم و با برخورد به یونوسفیر منعکس می‌گردد.

۲) مخابرات مایکروویو

امواج با فرکانس بالای 100MHZ تقریبا" به خط مستقیم حرکت می‌کنند لذا به سختی متمرکز می‌شوند ⟵ لزوم استفاده از آنتن های بشقابی

تمرکز تمام انرژی به یک پرتو کوچک توسط آنتن ، نسبت سیگنال به نویز را بالاتر خواهد برد ولی آنتن های فرستنده و گیرنده باید دقیقاً با یکدیگر تنظیم شده باشند.

سیاست ها در طیف مجاز کاربری الکترومغناطیس



باندهای ISM مجاز در ایالات متحده آمریکا

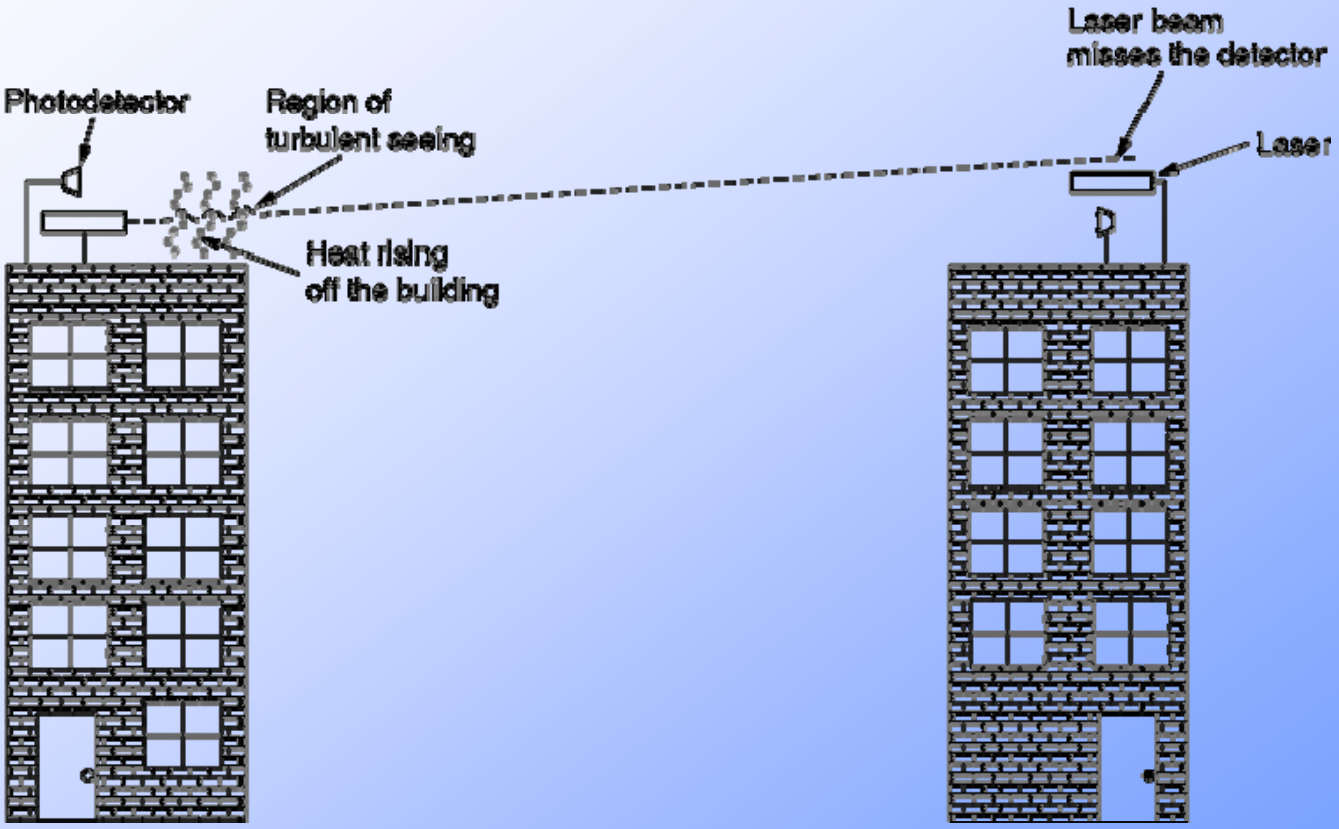
۳) امواج مادون قرمز

این امواج برای ارتباطات با بعد کم مورد استفاده قرار می‌گیرد.

این امواج جهت دار و ارزان هستند و ساخت آنها ساده می‌باشد.

عیب عمده آنها این است که از میان اشیای سخت و جامد عبور نمی‌کنند.

۴) انتقال موج نوری



یک سیستم دو سویه با دو لیزر در شکل نمایش داده شده است.

جریان جابجایی گرما در هوا قادر است در سیستم مخابرات لیزری اغتشاش ایجاد کند.

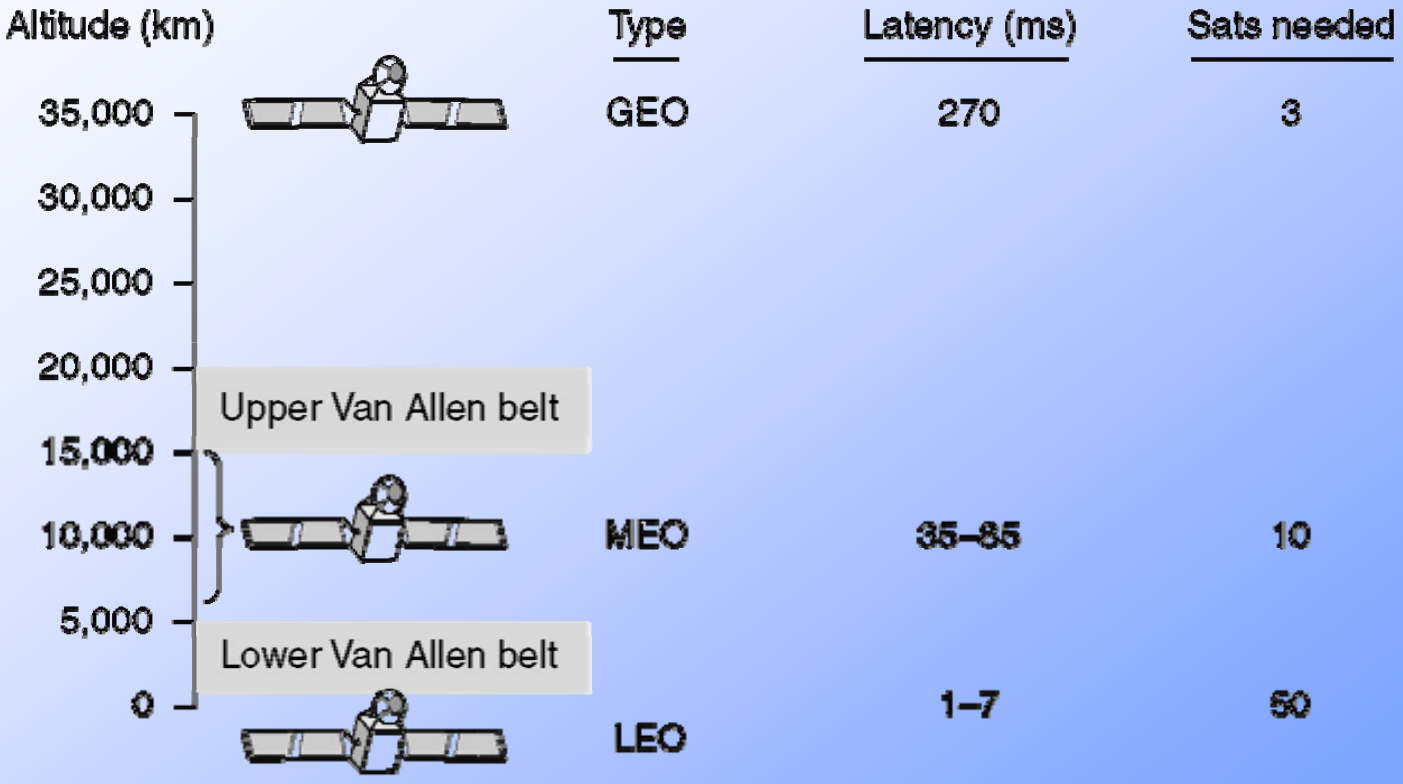
۵) ماهواره‌ها

ماهواره در واقع یک تکرارکننده مایکروویو بزرگ در فضاست.

سه ناحیه امن برای قرار گرفتن ماهواره‌ها وجود دارد:

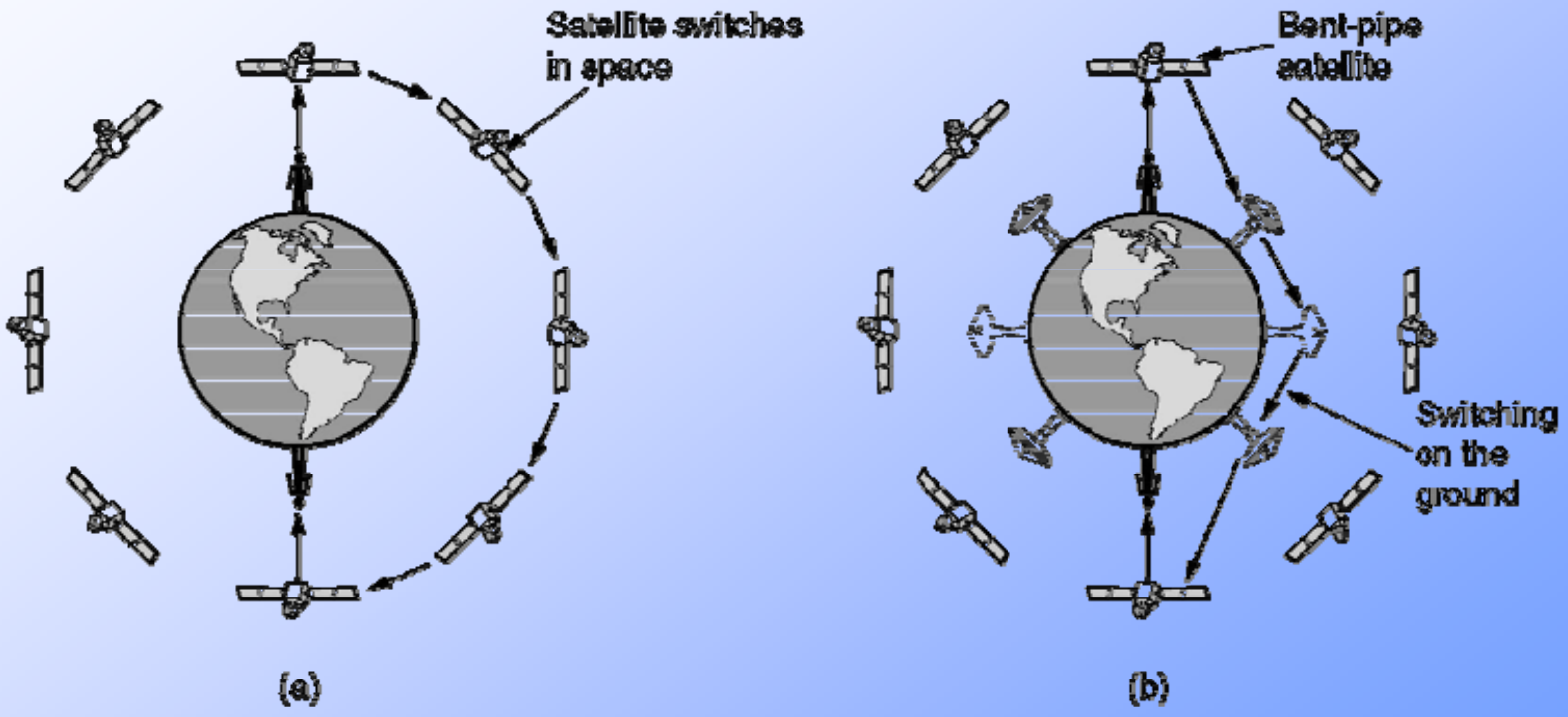
- ماهواره‌های زمین ثابت (GEO)
- ماهواره‌های مدارمتوسط(MEO)
- ماهواره‌های مدار پایین (LEO)

ماهواره‌های مخابراتی



ماهواره‌های مخابراتی و برخی از مشخصه‌های آنان شامل : ارتفاع از زمین، زمان تأخیر یک رفت و برگشت، و تعداد ماهواره‌های مورد نیاز در تأمین پوشش کامل زمین

پروژه Globalstar



(a) رله سیگنال در فضا

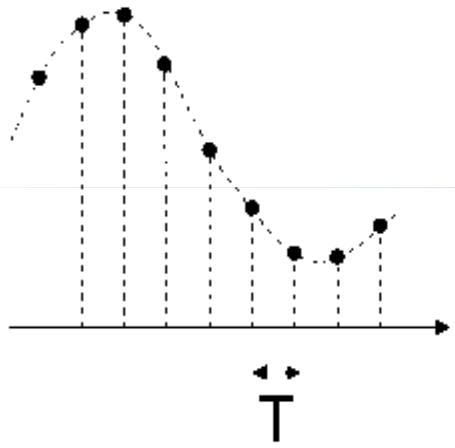
(b) رله سیگنال روی زمین (مورد استفاده در Globalstar)

ماهواره‌های مخابراتی

Band	Downlink	Uplink	Bandwidth	Problems
L	1.5 GHz	1.6 GHz	15 MHz	Low bandwidth; crowded
S	1.9 GHz	2.2 GHz	70 MHz	Low bandwidth; crowded
C	4.0 GHz	6.0 GHz	500 MHz	Terrestrial interference
Ku	11 GHz	14 GHz	500 MHz	Rain
Ka	20 GHz	30 GHz	3500 MHz	Rain, equipment cost

باندهای اصلی ماهواره

نمونه برداری (Sampling)



نظریهٔ نمونه برداری نایکوئیست :

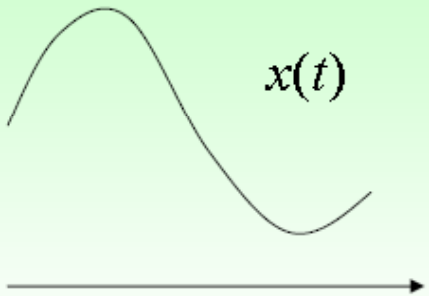
برای آنکه یک سیگنال با پهنای باند W از روی نمونه هایش به طور کامل بازسازی شود حداقل تعداد 2W نمونه در ثانیه لازم است.

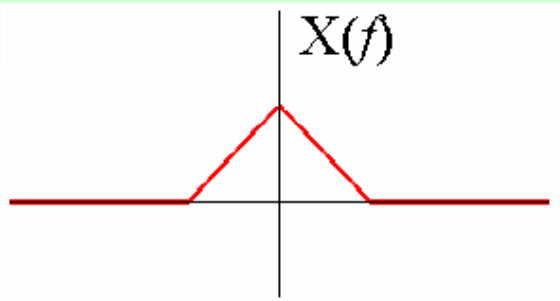
مثال: برای صدای با کیفیت تلفنی

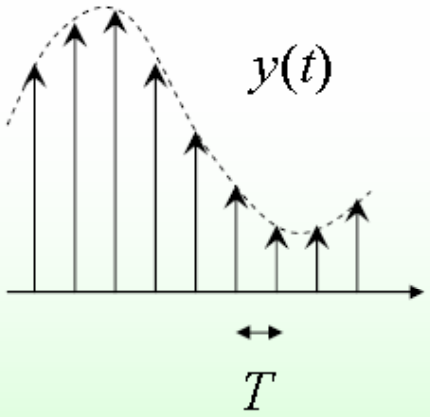
$$W = 3kHz \rightarrow R \geq 6000 \frac{\text{sample}}{\text{second}}$$

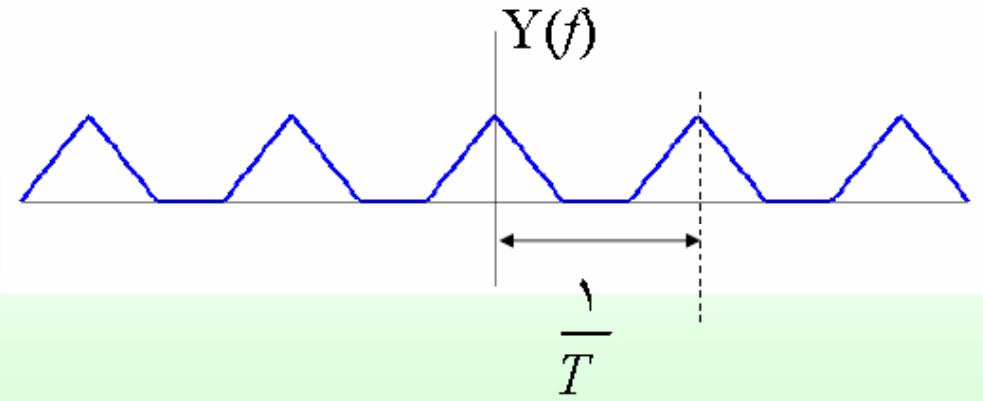
برای سیگنال تلویزیونی

$$W = 5MHz \rightarrow R \geq 10,000,000 \frac{\text{sample}}{\text{second}}$$

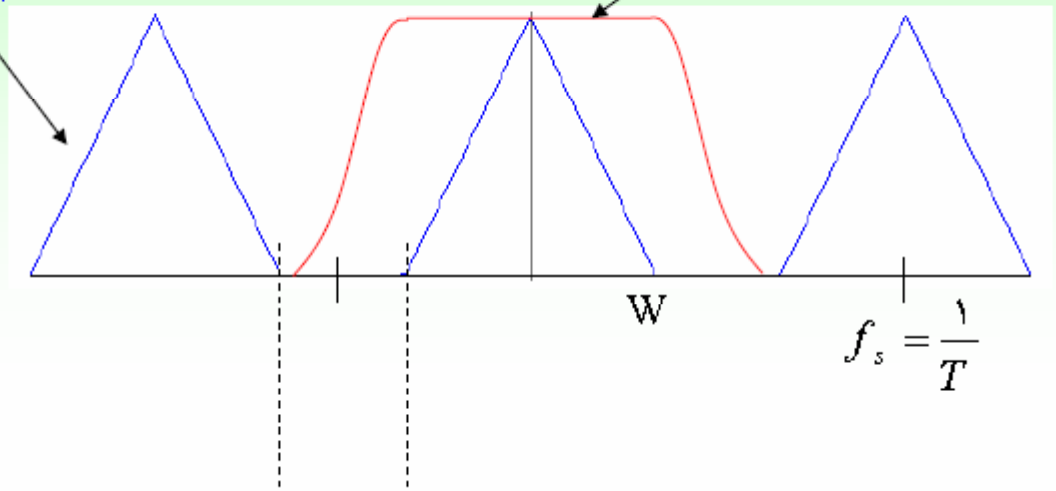








نمونه برداری در حوزهٔ زمان معادل است با تکرار طیف در حوزهٔ فرکانس(دورهٔ تناوب تکرار همان فرکانس نمونه برداری است.)



- ✓ شرط آنکه سیگنال اصلی از روی $y(t)$ قابل بازسازی باشد این است که $f_s \geq 2W$
- ✓ بازسازی توسط یک فیلتر پایین گذر صورت میگیرد.
- ✓ هرچه f_s بزرگتر انتخاب شود فاصلهٔ طیفها از هم بیشتر می شود در نتیجه امکان استفاده از فیلترهای غیر ایده آل نیز وجود خواهد داشت.
- ✓ استفاده از فیلترهای غیر ایده آل (گیرنده ساده تر) به بهای افزایش تعداد نمونه ها خواهد بود.
- ✓ بازسازی سیگنال بطور کامل وبدون تقریب است. افزایش نرخ نمونه برداری باعث افزایش دقت سیگنال بازسازی شده نخواهد شد و فقط باعث می شود فیلترساده تری درگیرنده استفاده شود.

Over sampling ($f_s>2W$)

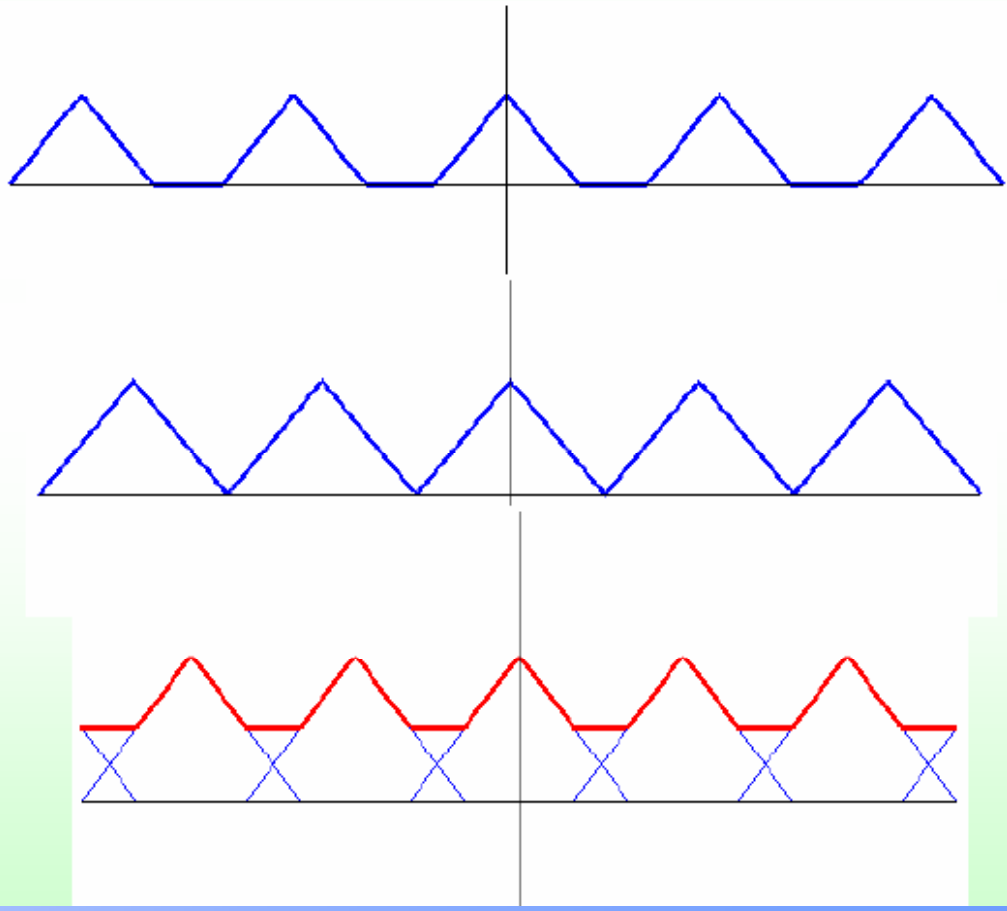
در این حالت میتوان از فیلترهای ساده تری استفاده کرد اما این کار به بهای افزایش پهنای باند تمام میشود

Critical sampling ($f_s=2W$)

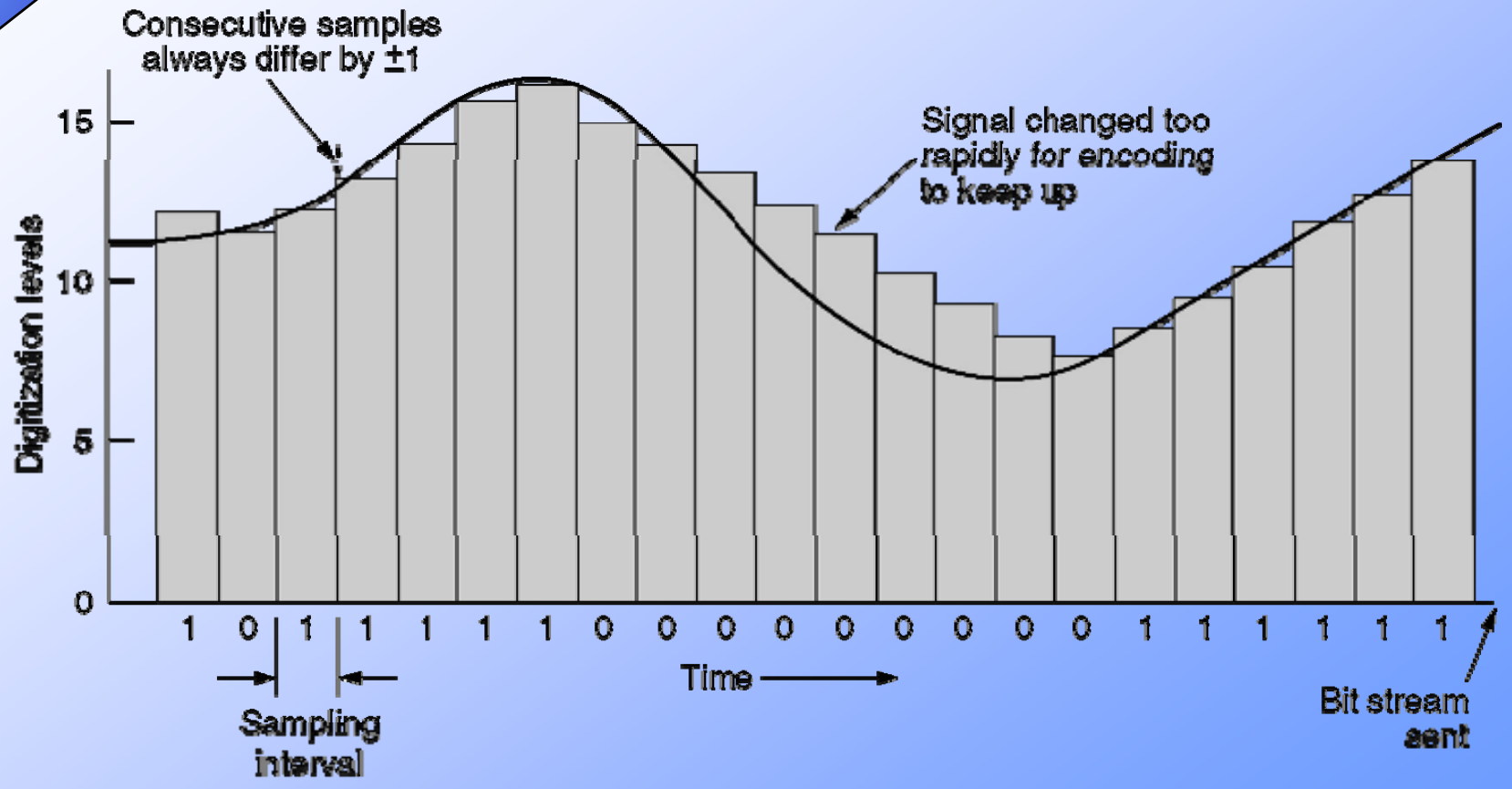
در این حالت بازسازی سیگنال تنها توسط فیلتر ایده آل ممکن است

Under sampling ($f_s<2W$)

بازسازی سیگنال ممکن نیست و سیگنال اعوجاج یافته است. این اعوجاج را aliasing میگویند.

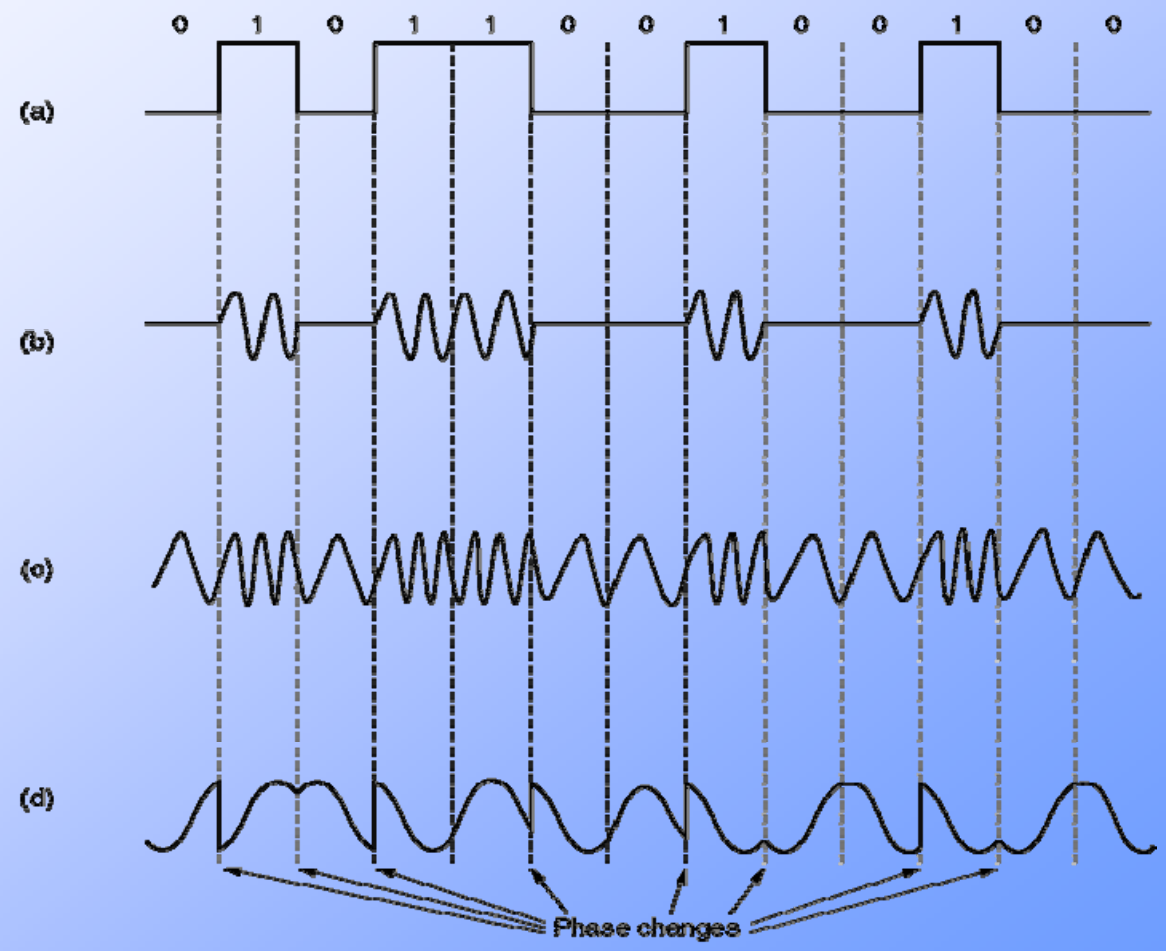


مدولاسیون دلتا (Delta modulation)



مدولاسیون های دیجیتال

$$x(t) = A\cos(\omega t + \varphi)$$



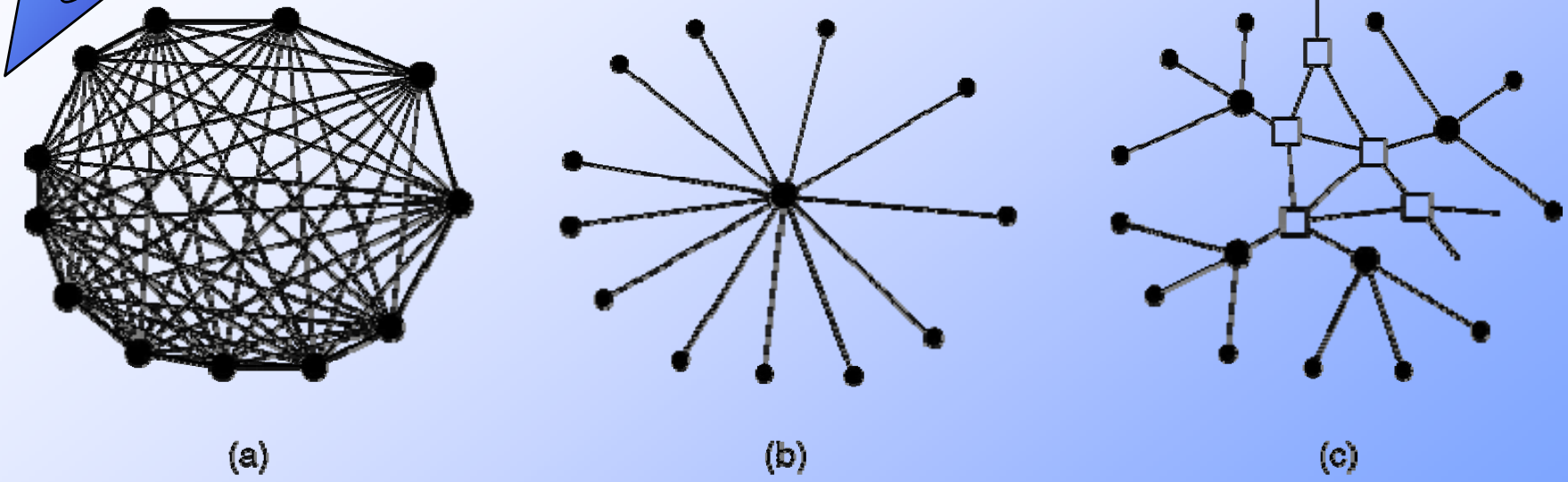
(a) A binary signal

(b)ASK(Amplitude Shift Keying)

(c)FSK(Frequency Shift Keying)

(d)PSK(Phase Shift Keying)

شبکه تلفن عمومی

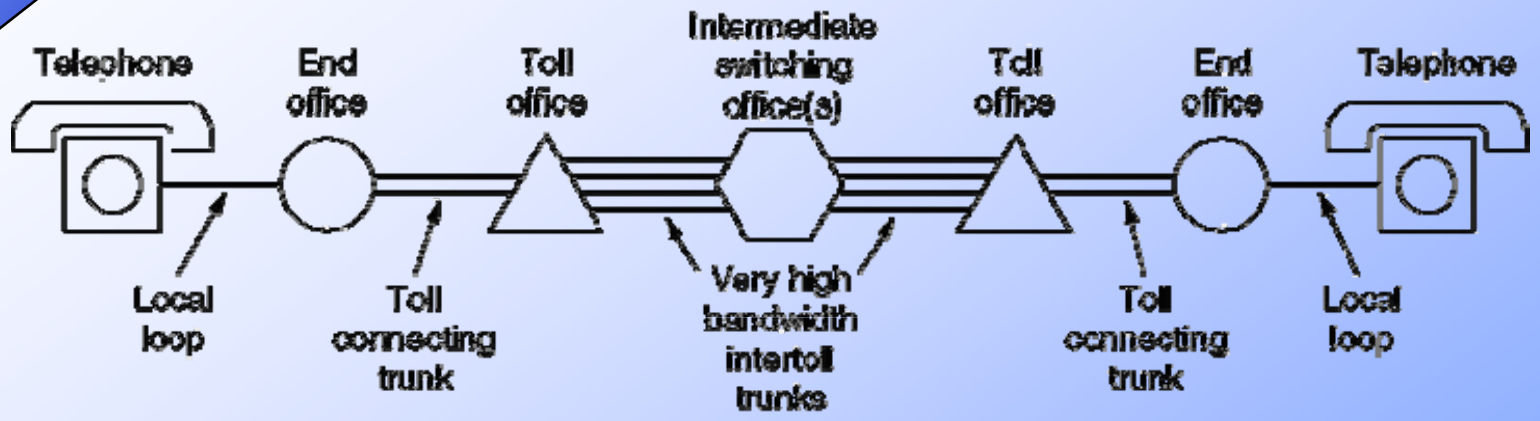


(a) شبکه کاملاً متصل

(b) سویچ مرکزی

(c) سلسله مراتبی دو سطحی

معماری سیستم تلفن



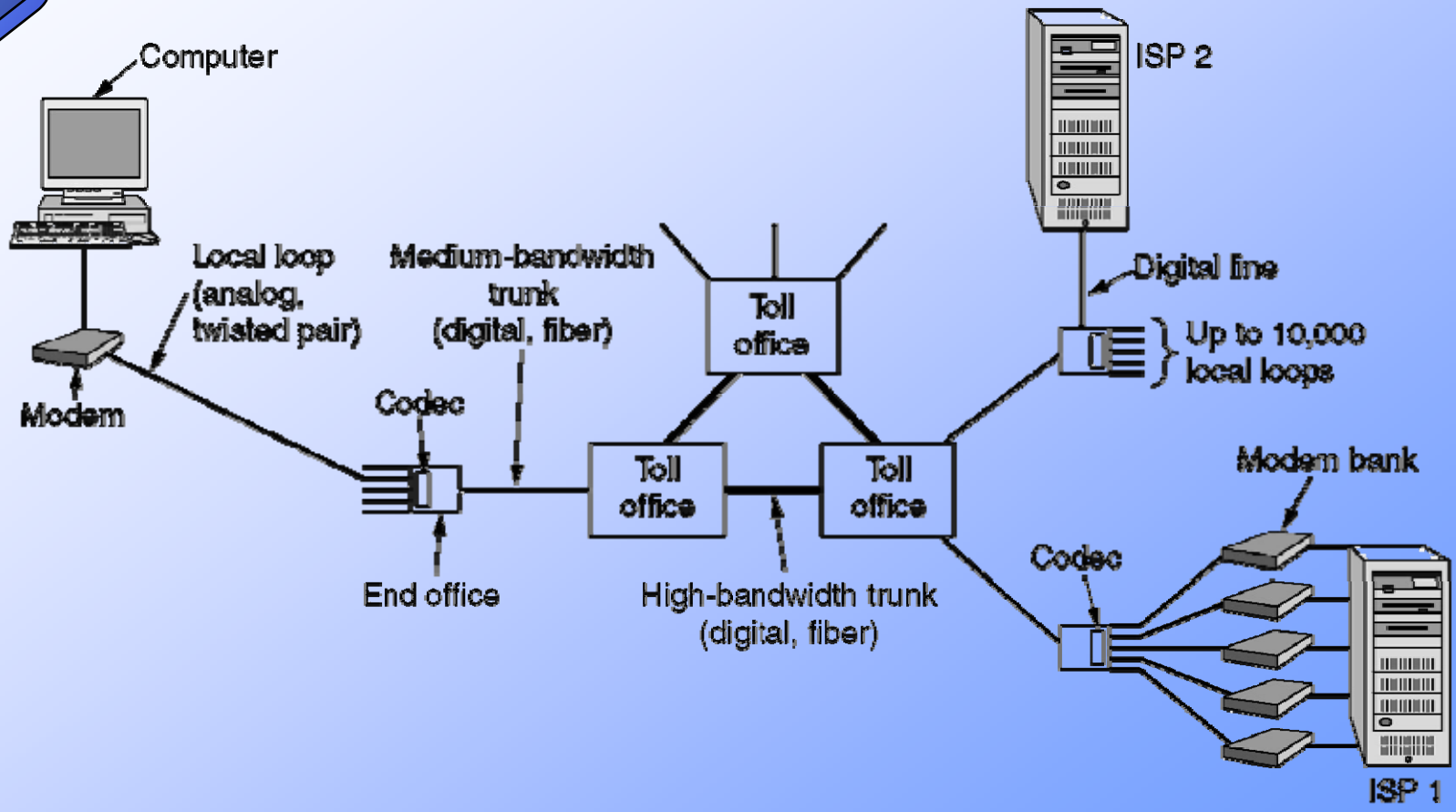
سه قسمت اصلی سیستم تلفن :

۱- حلقه‌های محلی (مدارهای پایانی)

۲- شاه سیم ها (ترانک ها)

۳- دفاتر راه گزینی (مراکز سوئیچینگ / ایستگاه های پایانی)

حلقه‌های محلی(Local Loop):



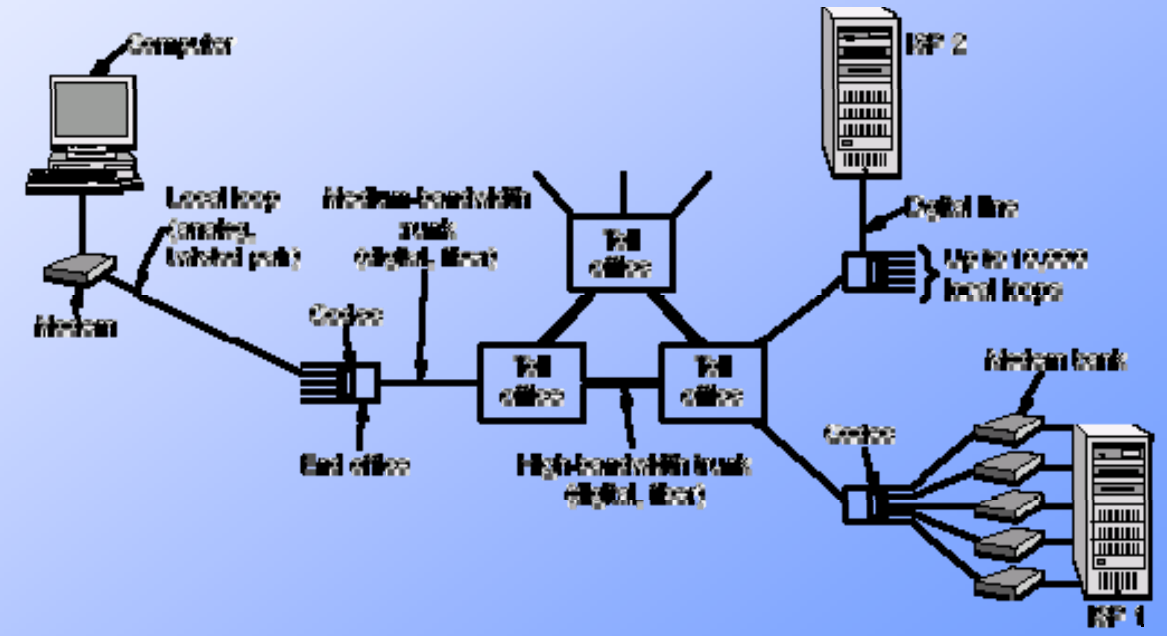
مشکلات انتقال سیگنال های الکتریکی در خطوط انتقال :

- تضعیف
- اعوجاج تاخیری
- اختلال (نویز)
  - اختلال گرمائی
  - اختلال القائی
  - اختلال ضربه ای

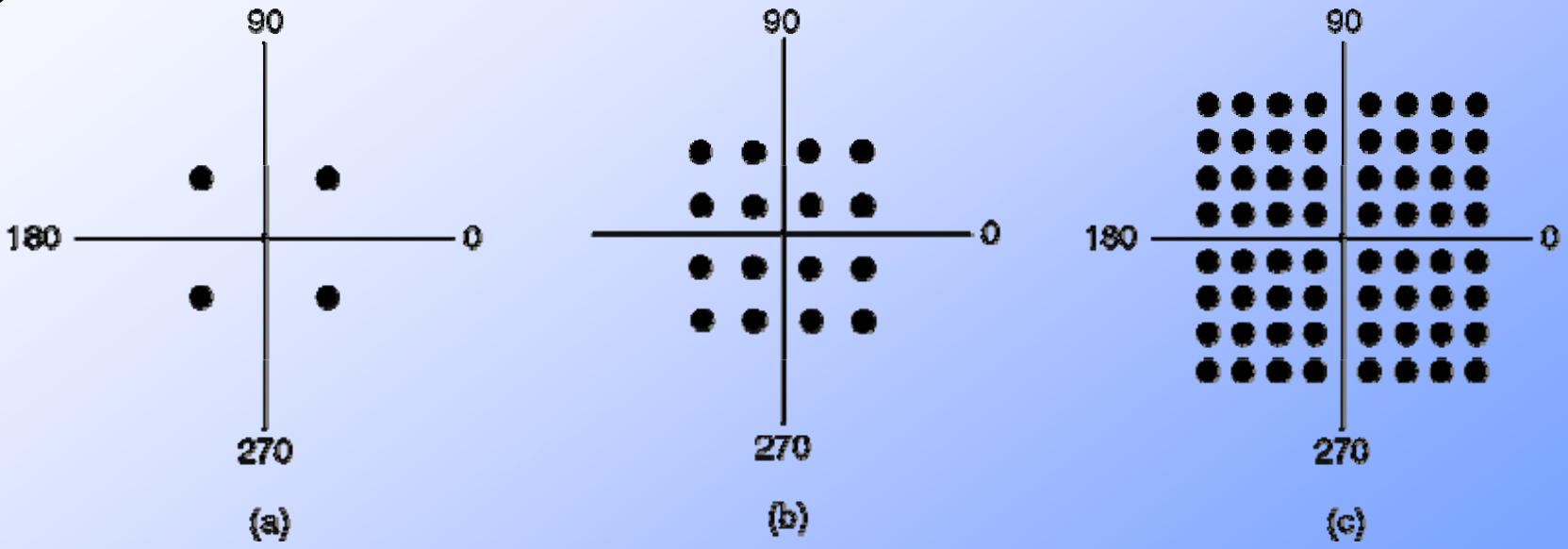
مودم ها

وسیله‌ای که یک رشته از بیت ها را بعنوان ورودی پذیرفته و بوسیله یک یا چند روش مدلاسیون، یک خروجی آنالوگ تولید می‌کند، مودم می‌نامیم.

یک مودم بین کامپیوتر (دیجیتال) و سیم تلفن قرار می‌گیرد.

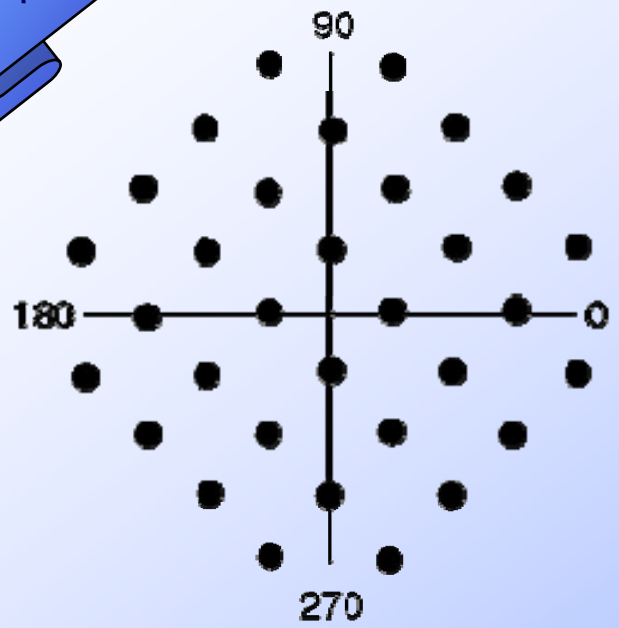


الگوی فلکی در مودم‌ها



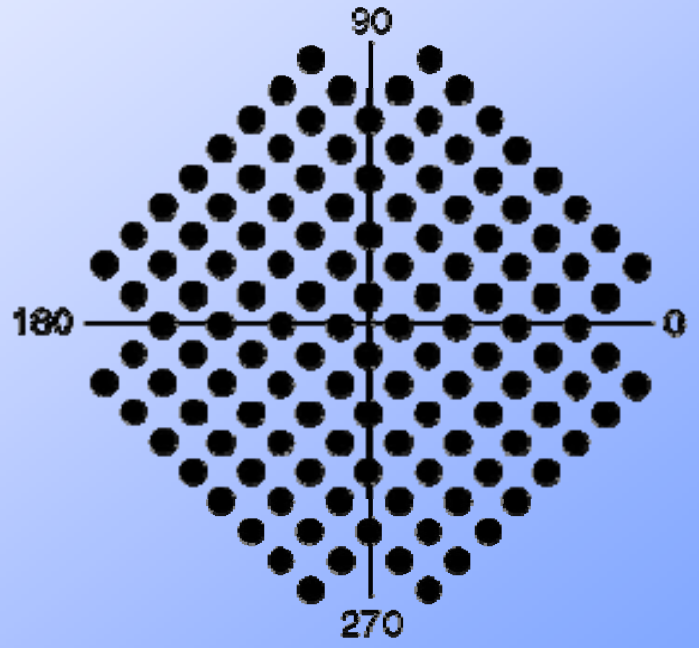
(a) QPSK (b) QAM-16 (c) QAM-64

دو استاندارد با نرخ باود ۲۴۰۰ در مودم‌ها



(a)

(a) V.32 for 9600 bps.



(b)

(b) V.32 bis for 14,400 bps.

خطوط اجاره‌ای (LEASED LINE)

یک خط اجاره‌ای یک اتصال تلفنی پایدار بین دو مکان می‌باشد که مقدار مشخصی از پهنای باند را برای همه زمان ها از قبل معین می‌کند.

خطوط اجاره‌ای می‌توانند آنالوگ یا دیجیتال باشند.

خطوط اجاره ای برای کاربردهای خاصی مفید است.

خط اجاره ای در آمریکا 1.544 Mbps
خط اجاره ای در اروپا 2.048 Mbps

خطوط اجاره ای به کانال های 64 Kbps تقسیم می شود.

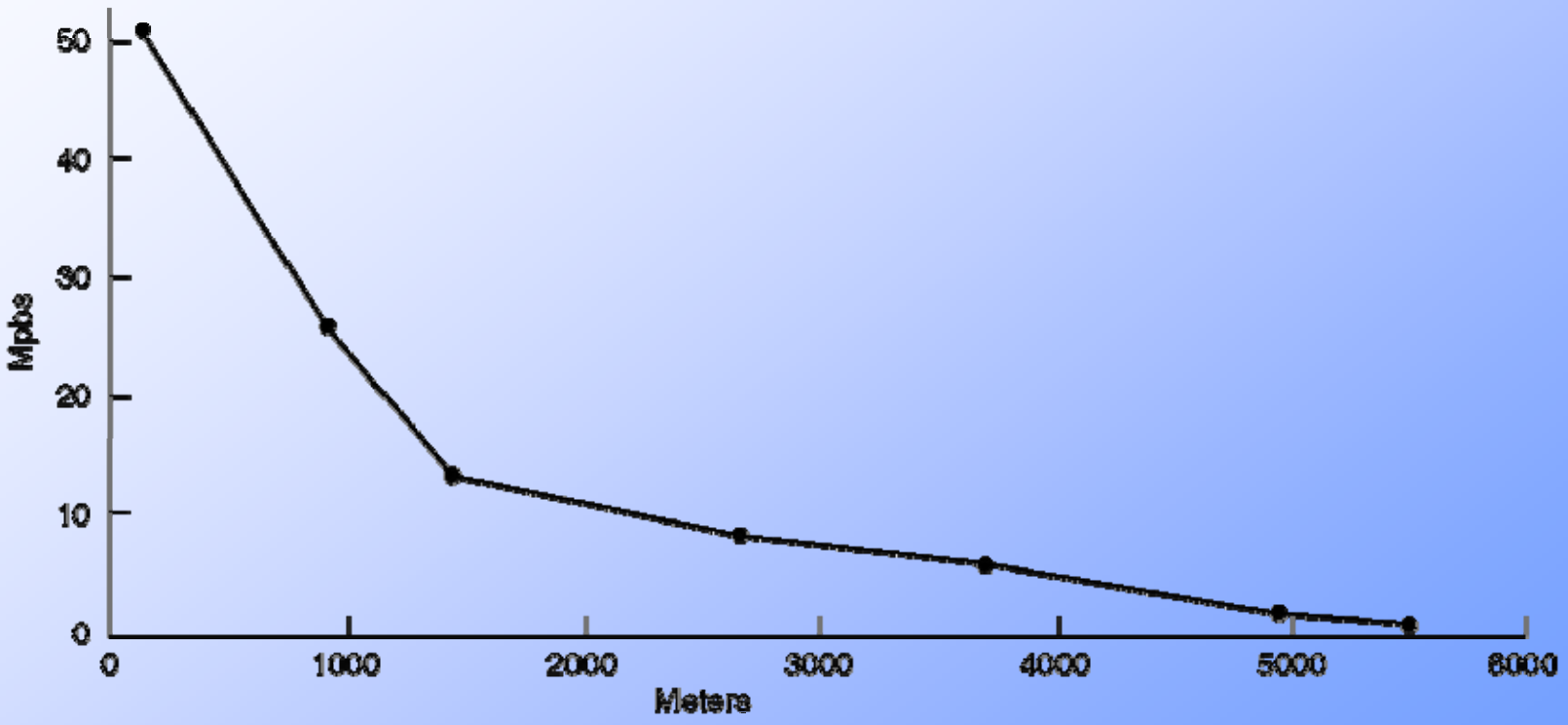
خطوط ADSL

اهداف :

- استفاده از تمام ظرفیت حلقه محلی (مدار پایانی)
- سریعتر بودن از خطوط تلفن 56 kbps
- عدم اختلال بین دستگاه های تلفن و فکس معمولی
- متصل بودن دائمی و داشتن هزینه ثابت

عوامل موثر در ظرفیت حلقه محلی
- طول خط
- ضخامت سیم
- کیفیت

عیب خطوط DSL



نمودار پهنای باند در سرویس DSL بر حسب فاصله در کابل cat 3 UTP

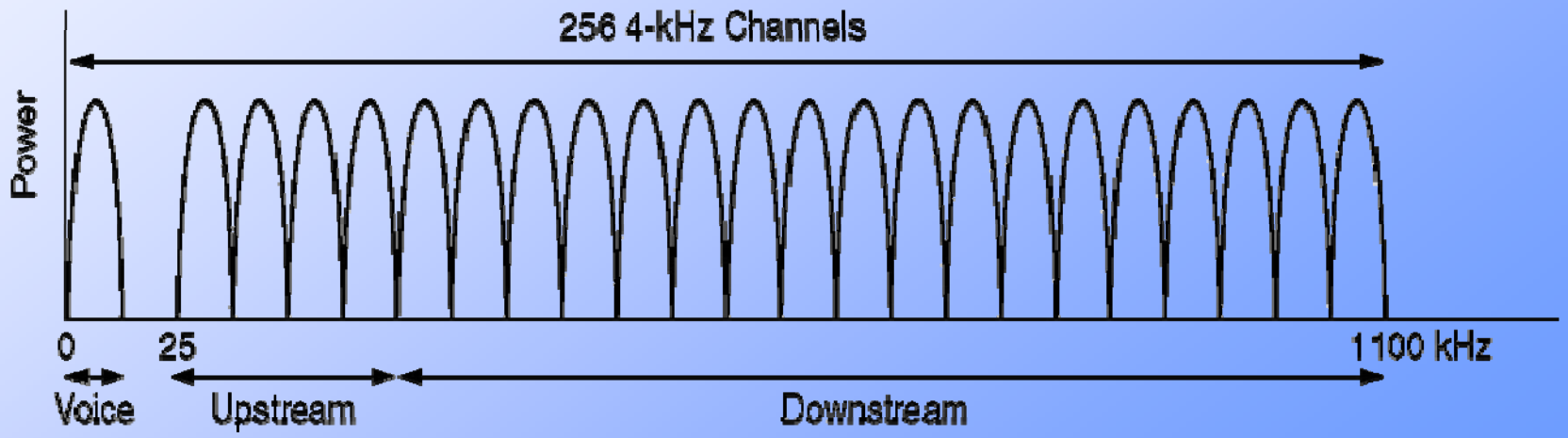
عملکرد ADSL با روش DMT

در اولین سرویس ADSL پهنای باند حلقه محلی به سه باند تقسیم شده بود:

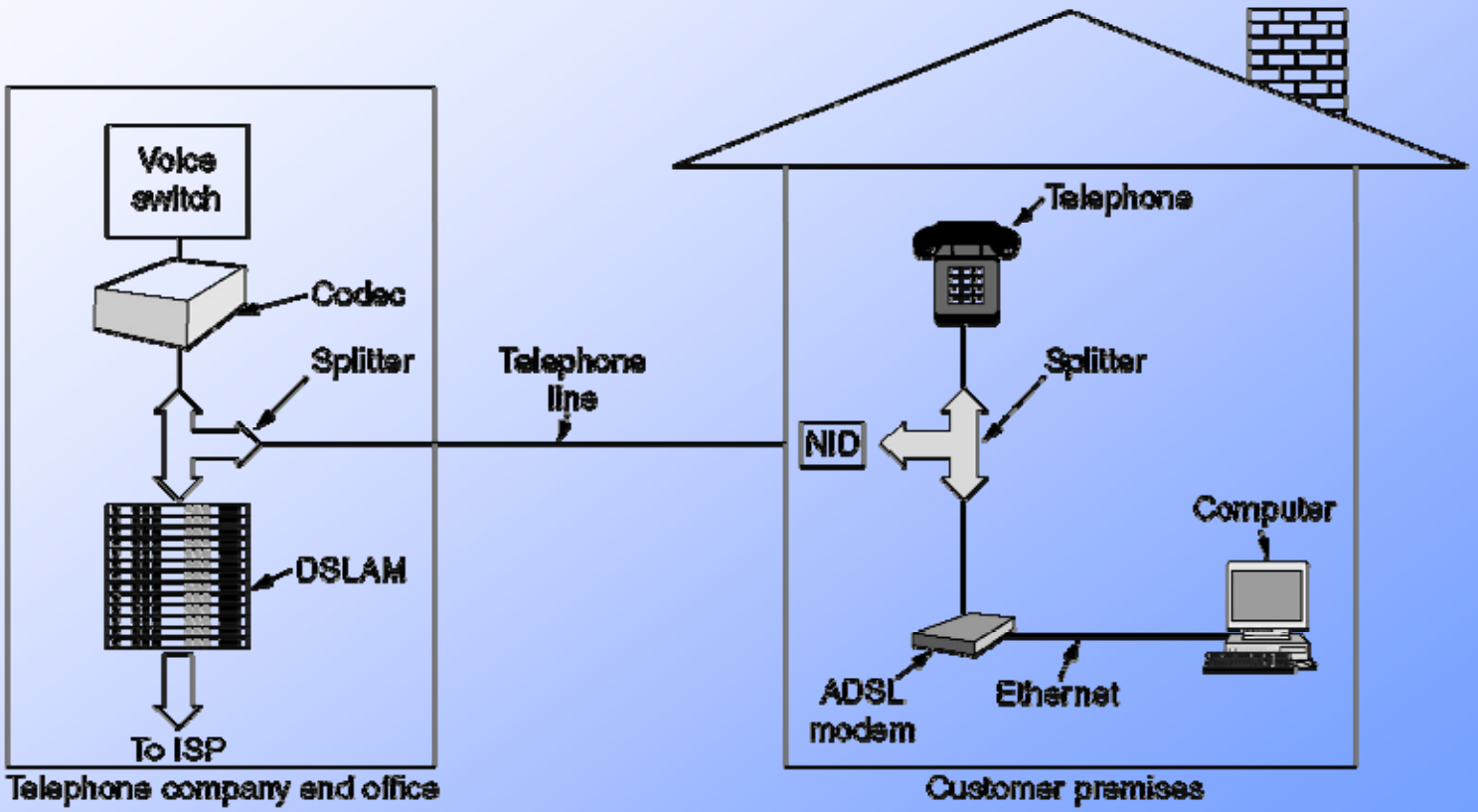
۱- باند POTS (سرویس تلفن معمولی)

۲- باند ارسال از کاربر به ایستگاه پایانی (Upstream)

۳- باند ارسال از ایستگاه پایانی به کاربر (Downstream)



یک طرح ساده ADSL



طرز کار ADSL

سیگنال POTS به یک دستگاه تلفن و سیگنال داده به یک مودم ADSL متصلند .

سیگنال ها پس از عبور از مدارهای پایانی به ایستگاه مرکزی شرکت تلفن می‌رسند که در آنجا نیز یک تقسیم کننده مشابه قبلی وجود دارد که سیگنالهای داده را به ISP ها و سیگنال های آنالوگ را به شبکه تلفن می‌فرستد.

برای تبدیل سیگنال های آنالوگ به دیجیتال در ایستگاه شرکت تلفن از دستگاهی به نام DSLAM که بسیار شبیه مودم ADSL است، استفاده می‌شود.

جداکننده (Splitter) باند POTS را از باند داده جدا می‌کند.

مالتی پلکسینگ(تسهیم سازی)

روش های تسهیم سازی :

۱) **FDM (تسهیم سازی تقسیم فرکانسی)**

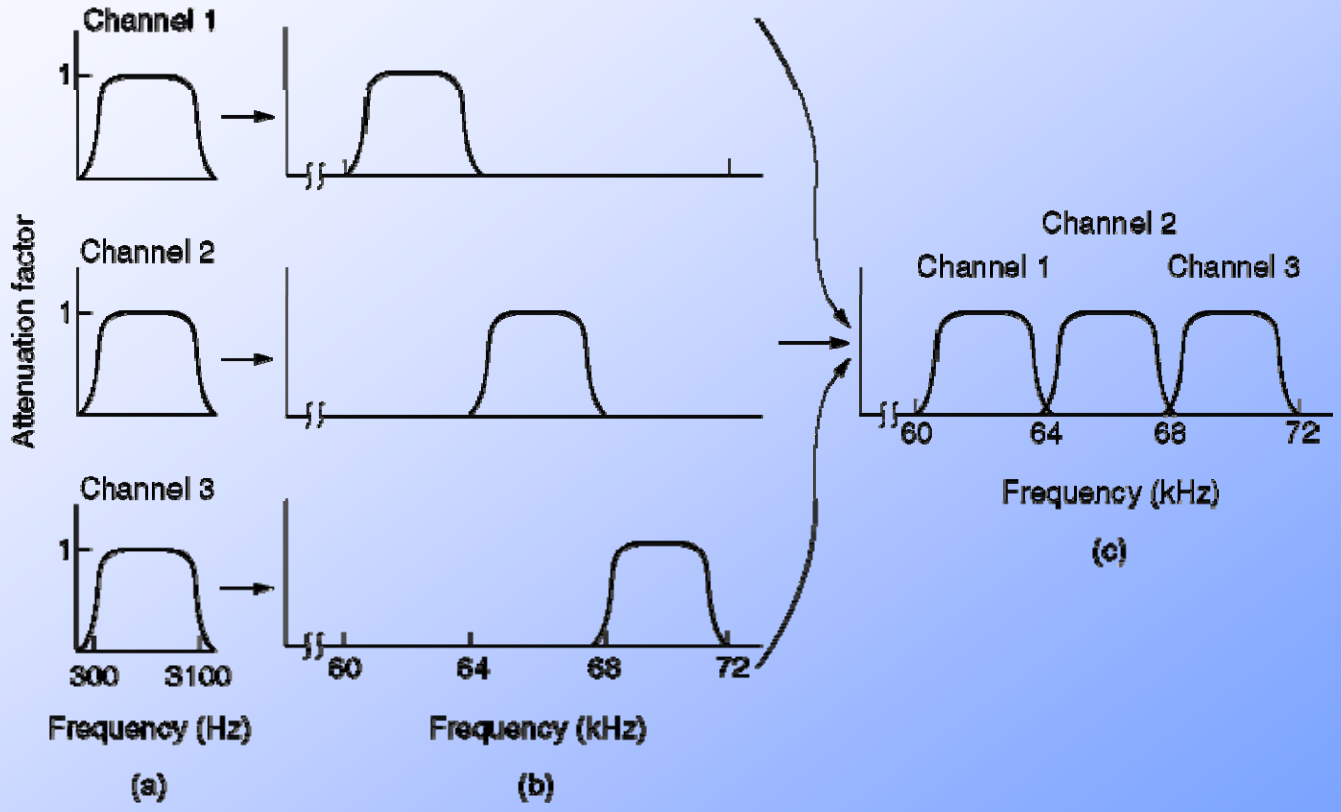
در FDM طیف فرکانسی به باندهای فرکانسی تقسیم می‌شود که در آن هر کاربر باند فرکانسی مخصوصی به خود را دارد.

۲) **TDM (تسهیم سازی تقسیم زمانی)**

در TDM کاربران هرکدام بصورت نوبتی برای مدت کوتاهی تمام پهنای باند را در اختیار می‌گیرند.

تسهیم سازی تقسیم فرکانسی

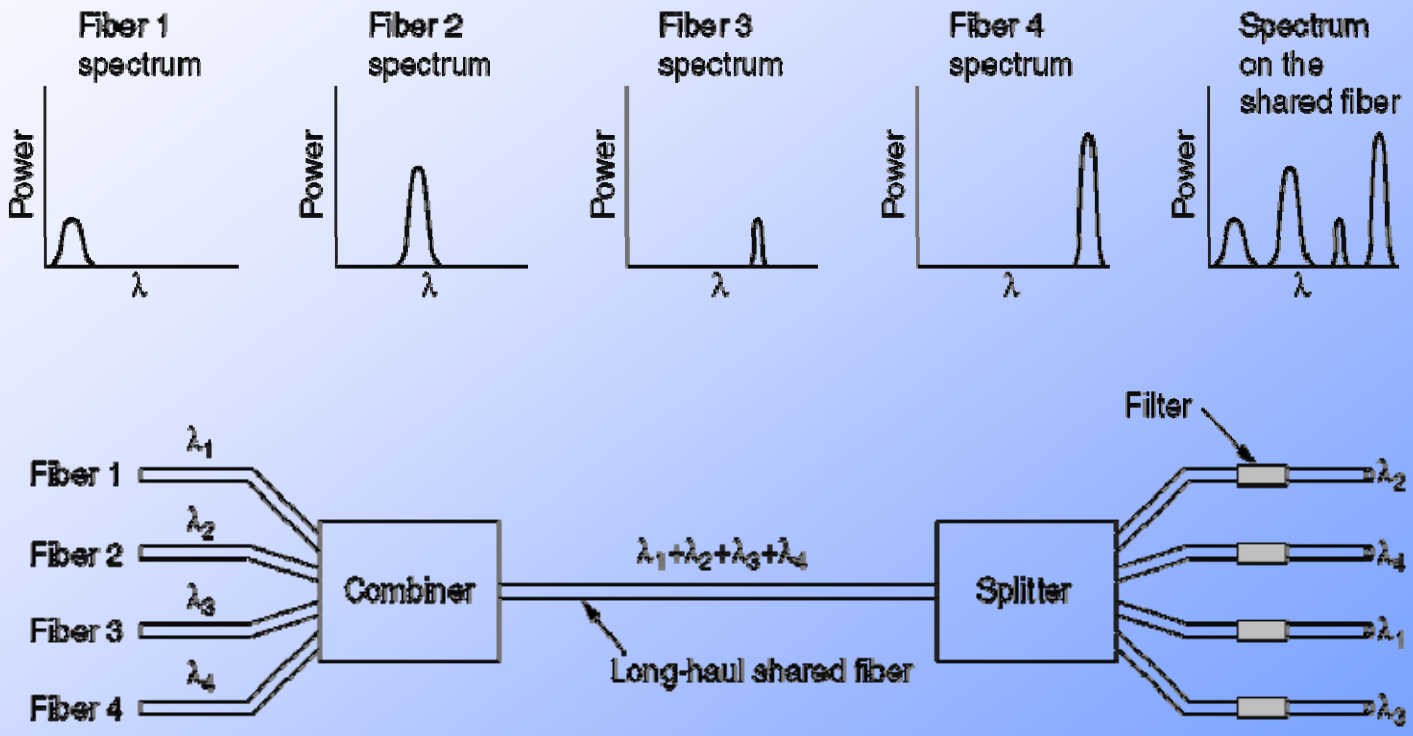
تسهیم سازی تقسیم فرکانسی در سیگنال های آنالوگ کاربرد دارد.



(a) The original bandwidths.
(b) The bandwidths raised in frequency.
(c) The multiplexed channel.

تسهیم سازی تقسیم طول موج

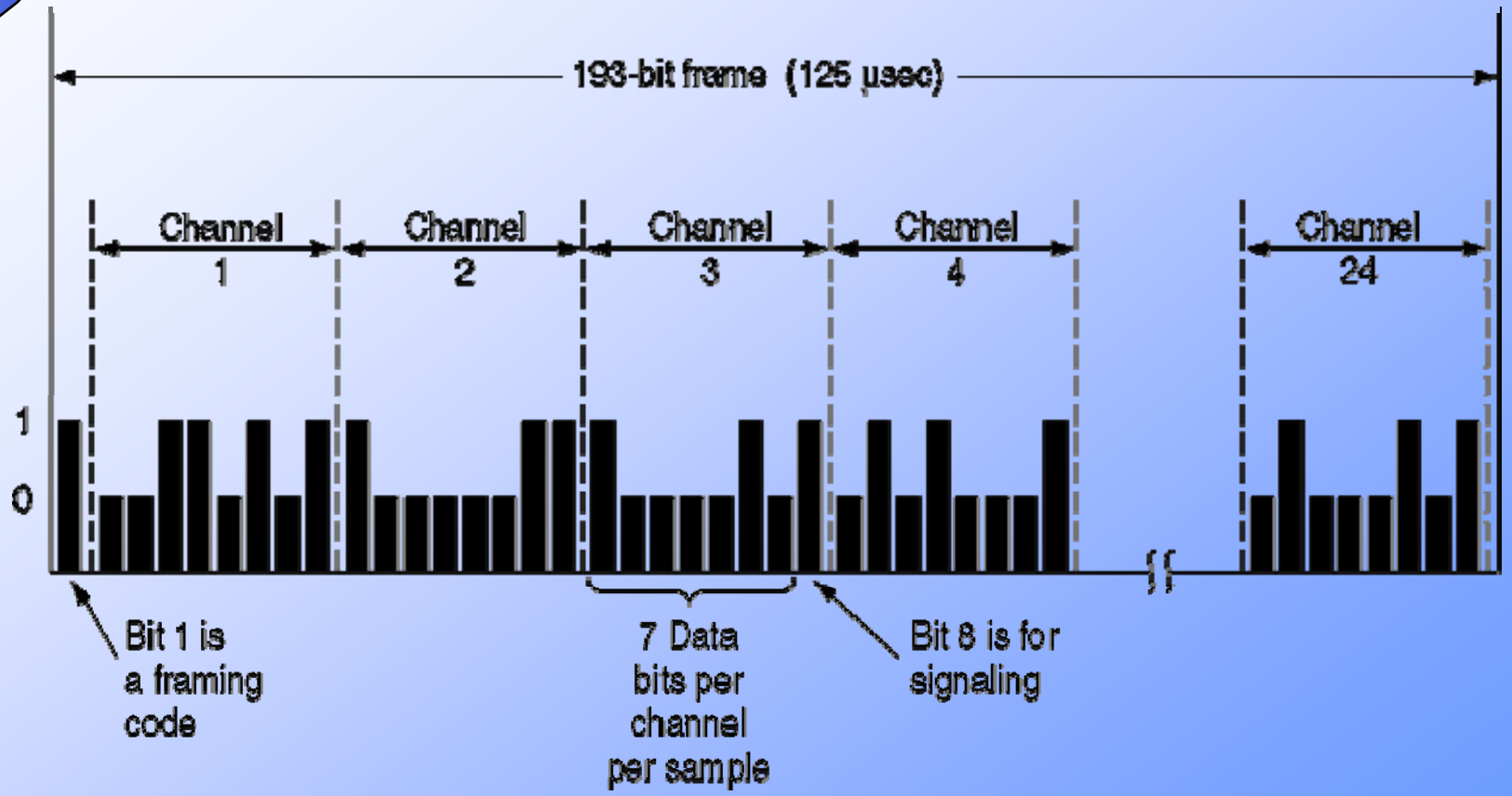
نوعی FDM است که برای کانال های فیبر نوری بکار می‌رود .



در این شکل ۴ فیبر با هم به یک ترکیب کننده و هر کدام با انرژی مخصوص به خود و طول موج مختلف وارد می‌شوند. این ۴ پرتو با هم ترکیب می شوند و تشکیل فیبر مشترکی را برای انتقال به مقصدی دور می‌دهند .

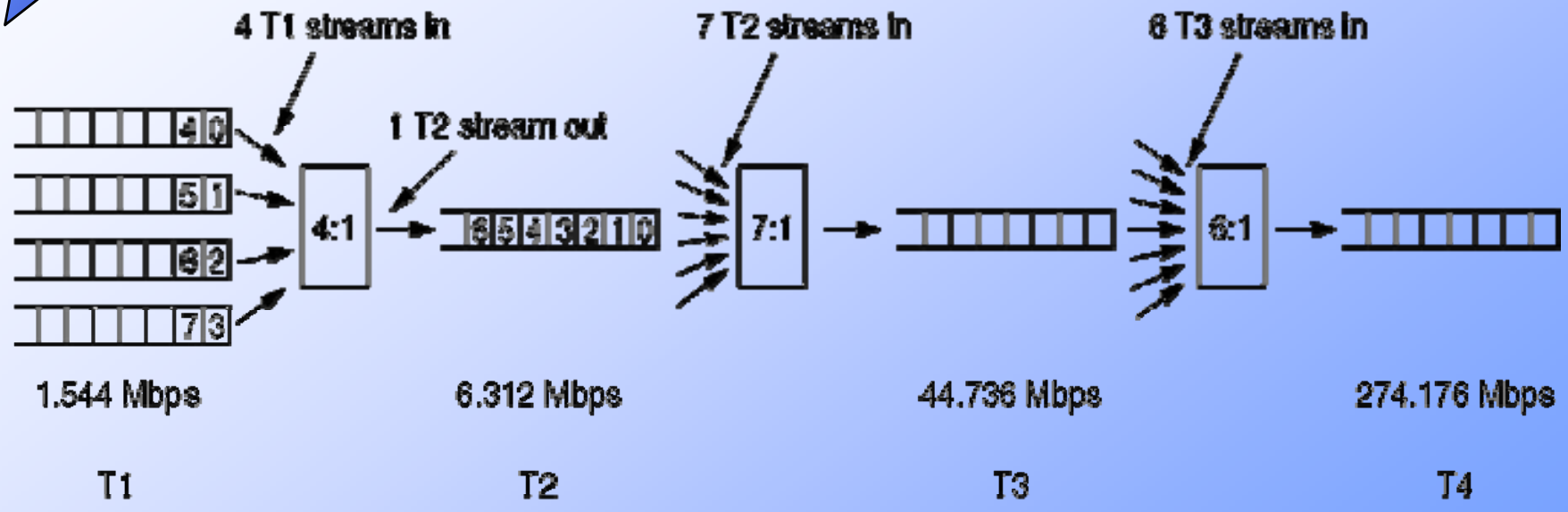
تسهیم سازی تقسیم زمانی

تسهیم سازی تقسیم زمانی در داده های دیجیتال کاربرد دارد.



The T1 carrier (1.544 Mbps).

مالتی پلکسینگ در حامل های دیجیتال



Multiplexing T1 streams into higher carriers

SONET/SDH

استاندارد سونت دارای چهار هدف اصلی است :

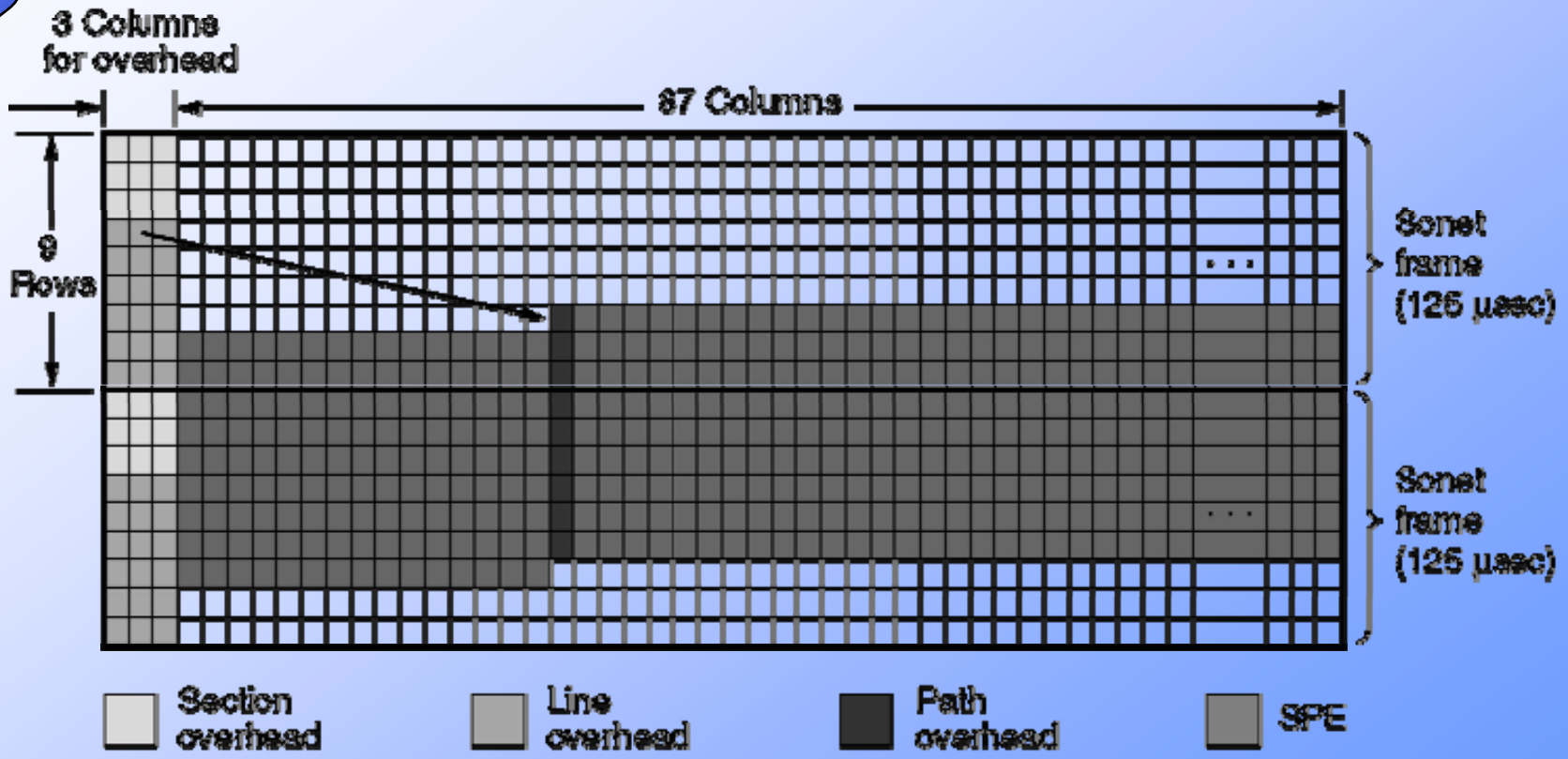
۱- همکاری حامل های مختلف را توسط تعریف استاندارد سیگنال دهی عمومی با در نظر گرفتن طول موج، زمان بندی و ... فراهم می کند.

۲- فراهم کردن وسایلی بود که برای سازگاری سیستم های دیجیتالی آمریکایی، ژاپنی و اروپایی.

۳- ارائه روشی برای تسهیم سازی چند کانال دیجیتال به یکدیگر.

۴- پشتیبانی از سیستم جامع عملیات ، مدیریت و نگهداری (OAM)

دو فریم متوالی SONET



نرخ های مالتی پلکس SONET و SDH

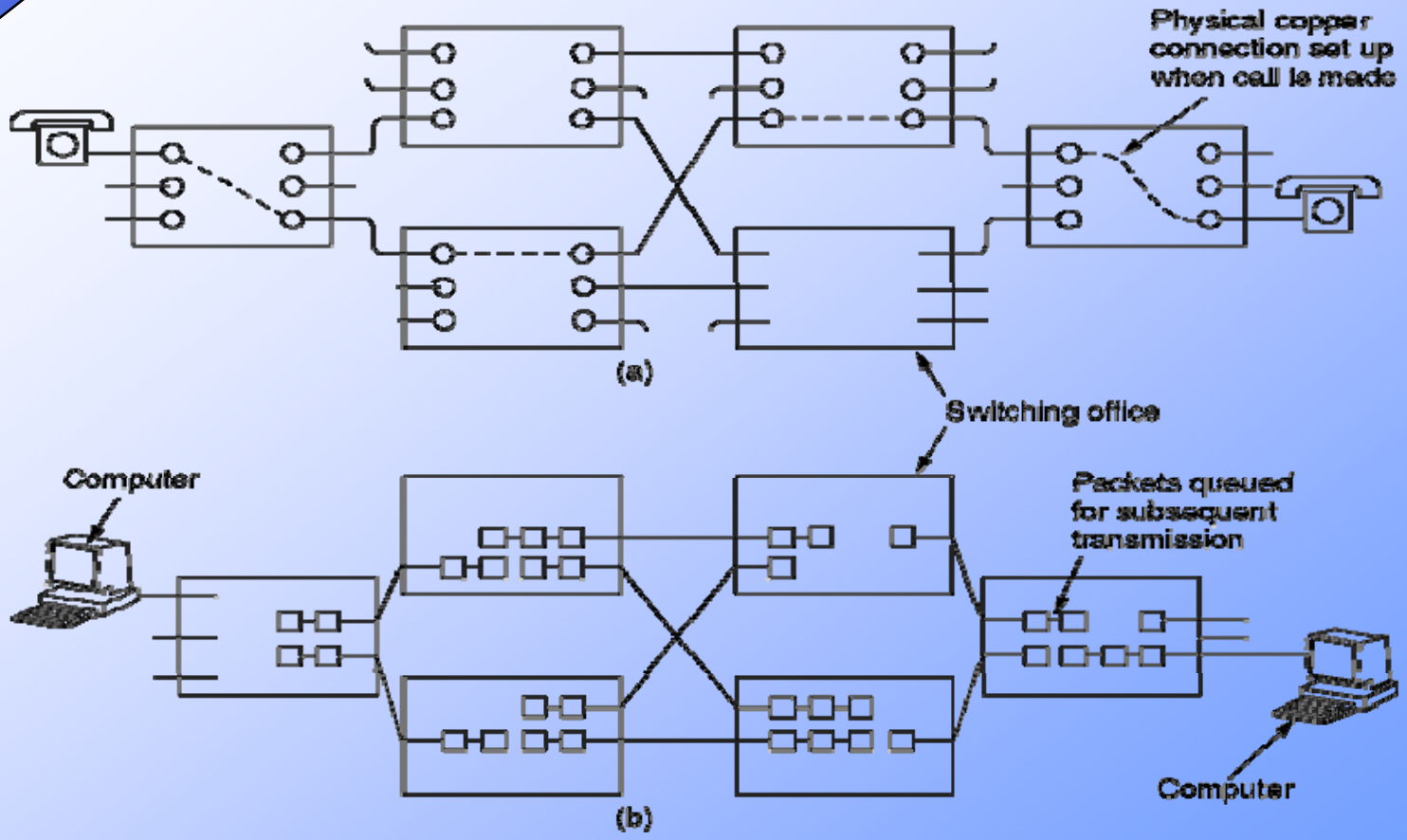
SONET		SDH	Data rate (Mbps)		
Electrical	Optical	Optical	Gross	SPE	User
STS-1	OC-1		51.84	50.112	49.536
STS-3	OC-3	STM-1	155.52	150.336	148.608
STS-9	OC-9	STM-3	466.56	451.008	445.824
STS-12	OC-12	STM-4	622.08	601.344	594.432
STS-18	OC-18	STM-6	933.12	902.016	891.648
STS-24	OC-24	STM-8	1244.16	1202.688	1188.864
STS-36	OC-36	STM-12	1866.24	1804.032	1783.296
STS-48	OC-48	STM-16	2488.32	2405.376	2377.728
STS-192	OC-192	STM-64	9953.28	9621.504	9510.912

راه گزینی (SWITCHING)

۱- راه گزینی مداری

۲- راه گزینی بسته‌ای

۳- راه گزینی پیام

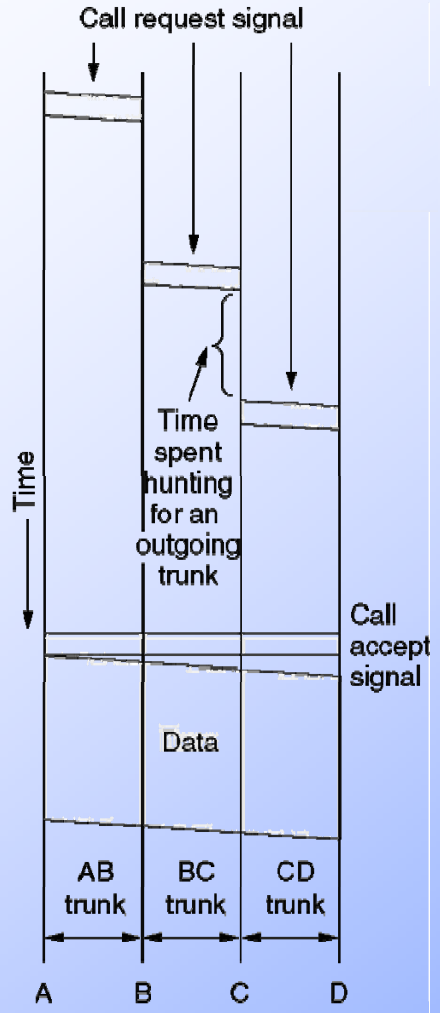


(a) Circuit switching. (b) Packet switching.

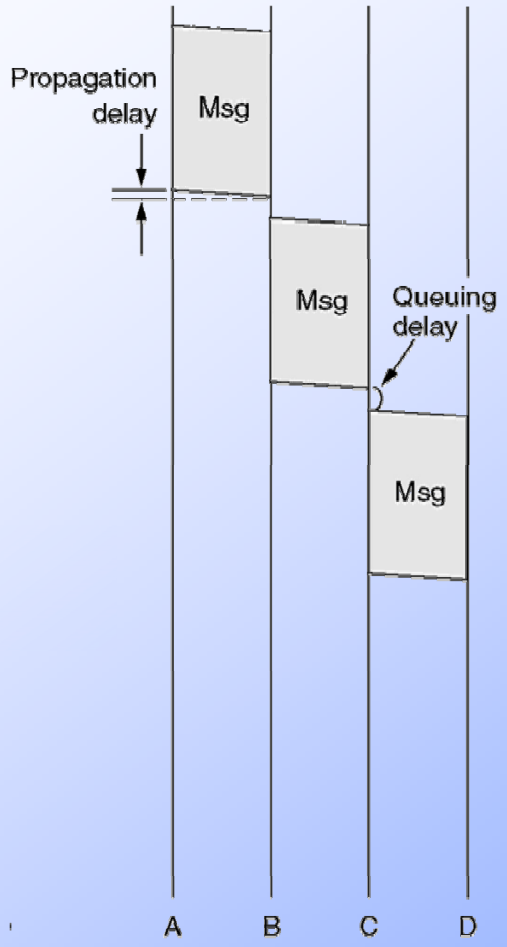
راه گزینی مداری

پس از برقراری تماس، مسیری بین دو انتها بوجود می‌اید و تا پایان تماس وجود خواهد داشت.

هنگامی که شما یا کامپیوترتان تماس برقرار می‌کند، تجهیزات راه گزینی درون سیستم تلفن، مسیر فیزیکی بین تلفن شما و تلفن گیرنده را جستجو می‌کند.



راه گزینی پیام

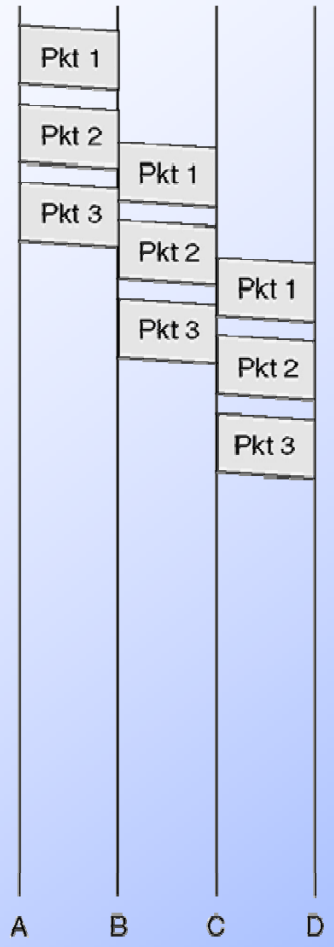


در این نوع راه گزینی از قبل هیچ مسیر فیزیکی بین فرستنده و گیرنده برقرار نمی‌شود.

وقتی فرستنده بلوکی از داده‌ها را منتقل می‌کند در اولین دفتر راه گزینی ذخیره می‌شود و سپس ارسال می گردد.

هر بلوک بطور کامل دریافت می‌شود، از نظر خطا کنترل می‌شود و سپس انتقال می یابد.

راه گزینی بسته‌ای



دراین تکنولوژی بسته‌های مخصوصی که مورد نیاز است بدون‌اینکه مسیر خاصی برای آنها در نظر گرفته شود فرستاده می‌شوند. این کار بر عهده هر بسته است که راه مخصوص به خود را برای رسیدن به مقصد پیدا کند

مقایسه سوئیچینگ مداری و بسته ای

Item	Circuit-switched	Packet-switched
Call setup	Required	Not needed
Dedicated physical path	Yes	No
Each packet follows the same route	Yes	No
Packets arrive in order	Yes	No
Is a switch crash fatal	Yes	No
Bandwidth available	Fixed	Dynamic
When can congestion occur	At setup time	On every packet
Potentially wasted bandwidth	Yes	No
Store-and-forward transmission	No	Yes
Transparency	Yes	No
Charging	Per minute	Per packet

شبکه تلفن همراه

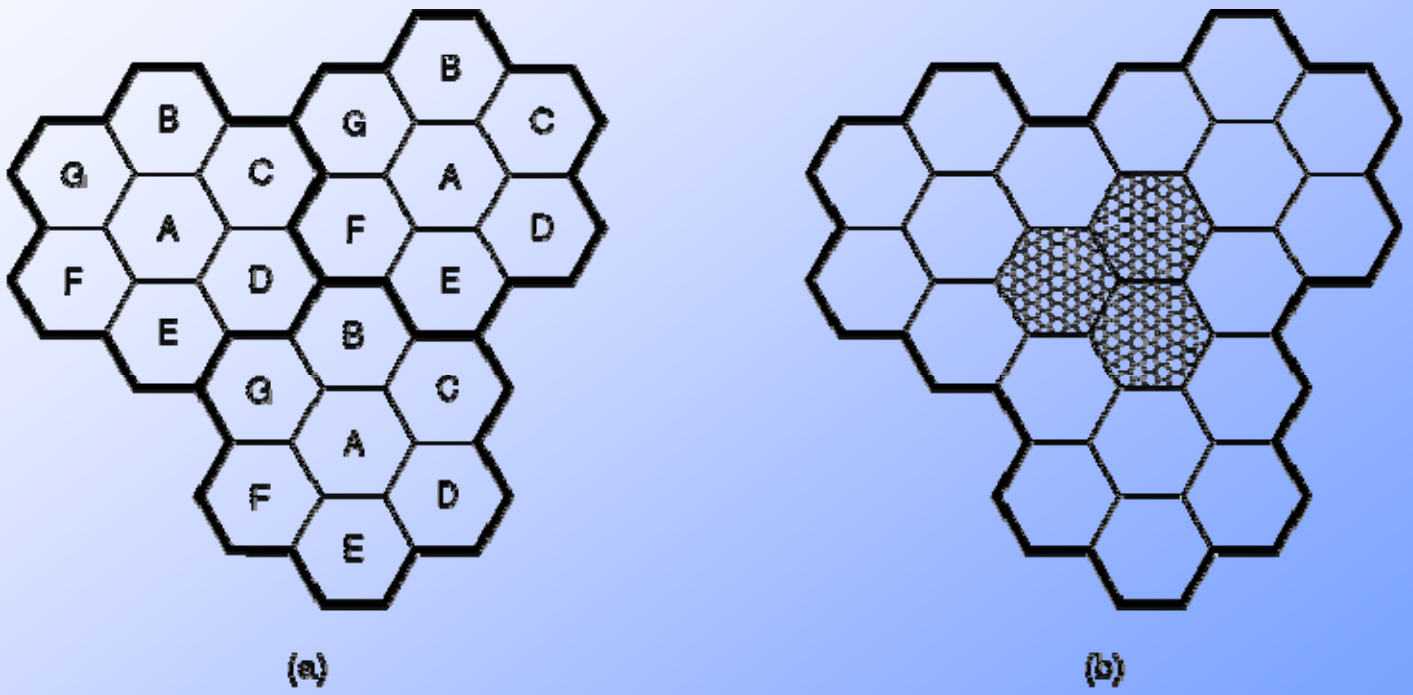
تلفن های همراه در مسیر تکامل خود سه نسل را به خود دیده‌اند:

۱- صدای آنالوگ

۲- صدای دیجیتال

۳- صدای دیجیتال و داده

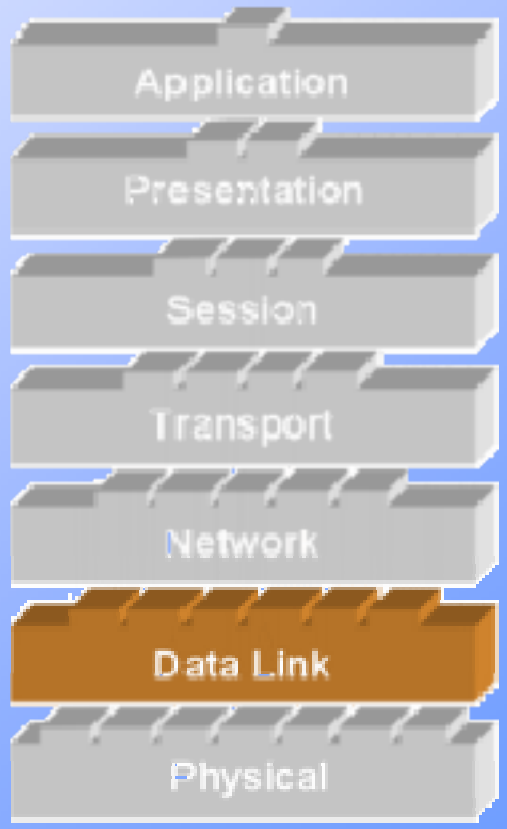
در تمام سیستم های تلفن همراه، یک منطقه جغرافیایی به تعدادی سلول تقسیم می‌شود.



(a) Frequencies are not reused in adjacent cells.
(b) To add more users, smaller cells can be used.

فصل سوم :

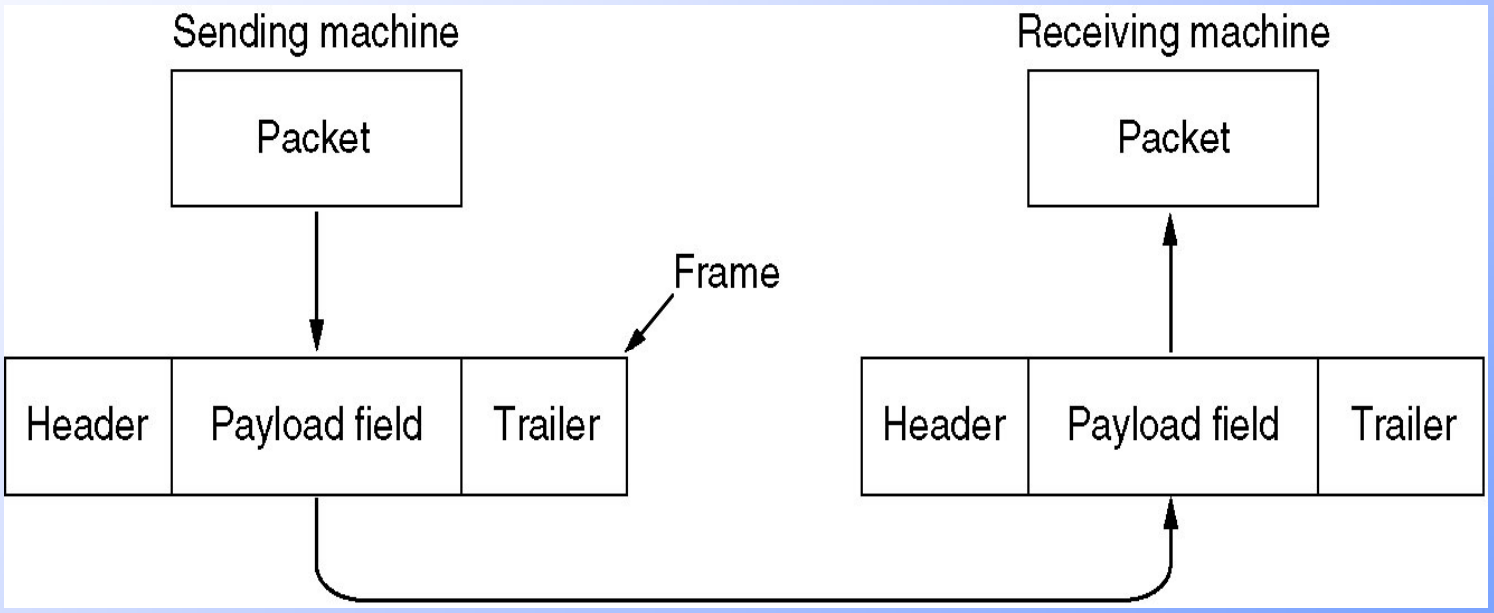
لايه پيوند داده‌ها



وظایف لایه پیوند داده‌ها

- ارائه سرویس های مشخص به لایه شبکه
- مدیریت خطاهای انتقال
- کنترل جریان داده ها

تشکیل فریم



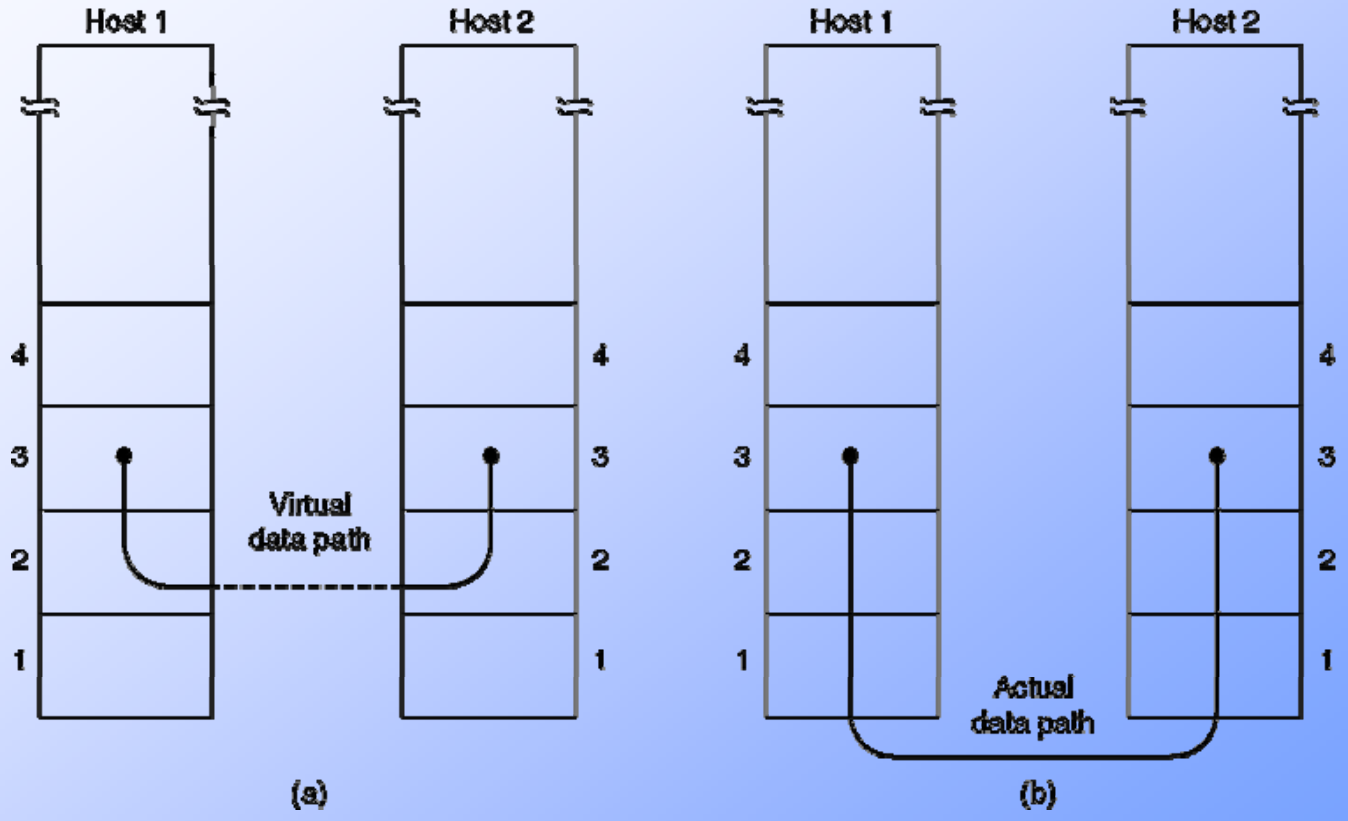
مدیریت فریم ها کلیدی ترین وظیفه لایه پیوند داده‌ها است.

۱) ارائه خدمات به لایه شبکه

خدمت اصلی، انتقال داده‌ها از لایه شبکه ماشین منبع به لایه شبکه ماشین مقصد است.

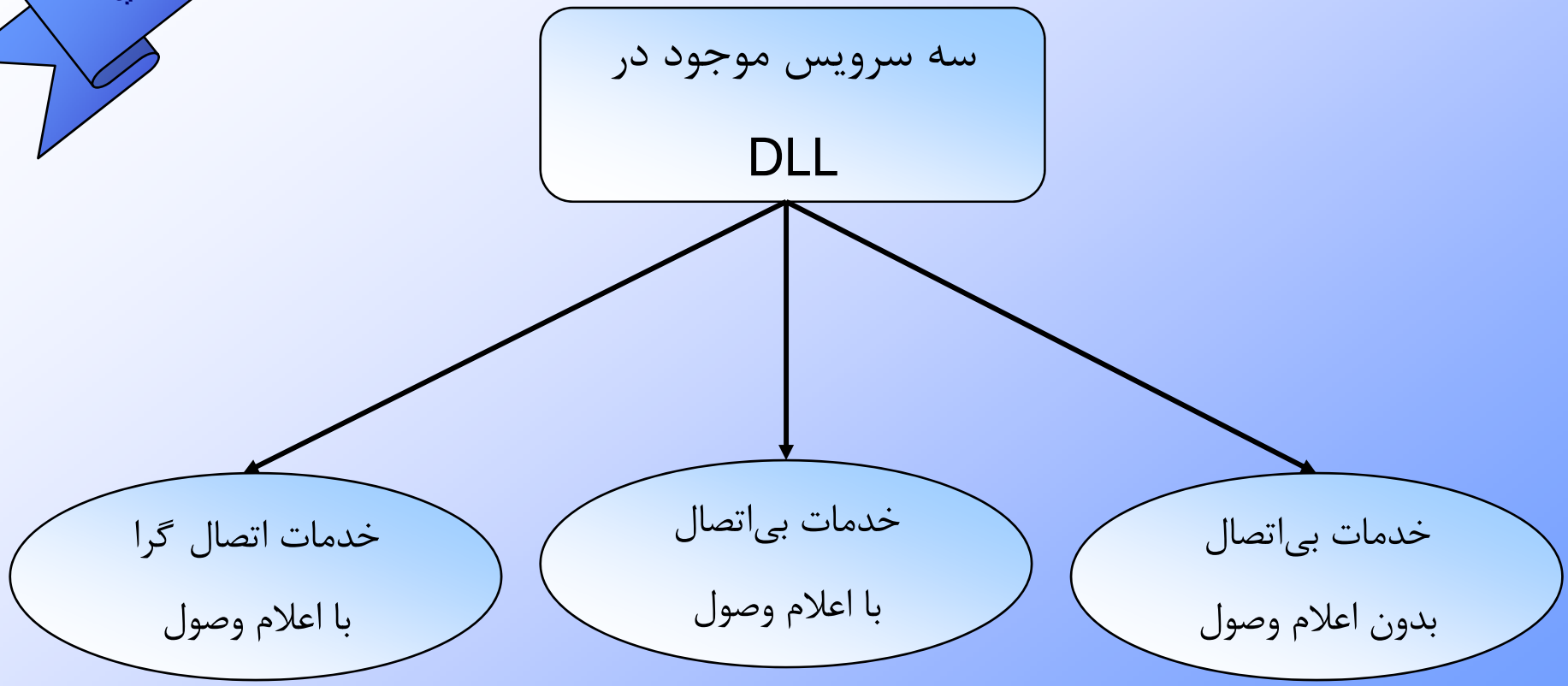
در واقع لایه پیوند داده‌ها وظیفه انتقال بیت هایی را بر عهده دارد که لایه شبکه به منظور انتقال به مقصد به لایه پیوند داده‌ها واگذار می‌کند.

خدمات DLL به لایه شبکه



(a) ارتباط مجازی

(b) ارتباط واقعی


سه سرویس موجود در
DLL
خدمات اتصال گرا
با اعلام وصول
خدمات بی‌اتصال
با اعلام وصول
خدمات بی‌اتصال
بدون اعلام وصول

الف) خدمات بی اتصال بدون اعلام وصول

ماشین منبع قاب های مستقلی را به ماشین مقصد می‌فرستد در حالیکه ماشین مقصد وصول آن ها را اعلام نمی‌کند.

قبل از انتقال ، اتصال منطقی وجود ندارد یا پس از آن نیز هیچ ارتباطی آزاد نمی‌شود.

این نوع خدمات برای ترافیک بلادرنگ نظیر مکالمات که در آن تاخیر داده‌ها بدتر از داده‌های بد است ، مناسب است.

ب) خدمات بی اتصال با اعلام وصول

هیچ اتصالی بین مبدا و مقصد وجود ندارد اما هر قاب ارسال شده مستقلاً اعلام وصول می شود. در این روش فرستنده می‌داند که قاب به سلامت رسید یا خیر.

Time out ⟵ ارسال مجدد

این خدمات برای کانال های غیر قابل اعتماد (نویزدار) مثل سیستم‌های بی‌سیم مناسب است.

ج) خدمات اتصال گرا با اعلام وصول

با این خدمات ماشین های منبع و مقصد قبل از ارسال داده‌ها، ارتباطی برقرار می‌کنند.

هر قاب ارسال شده از این طریق، شماره‌گذاری می‌شود و به همین علت :

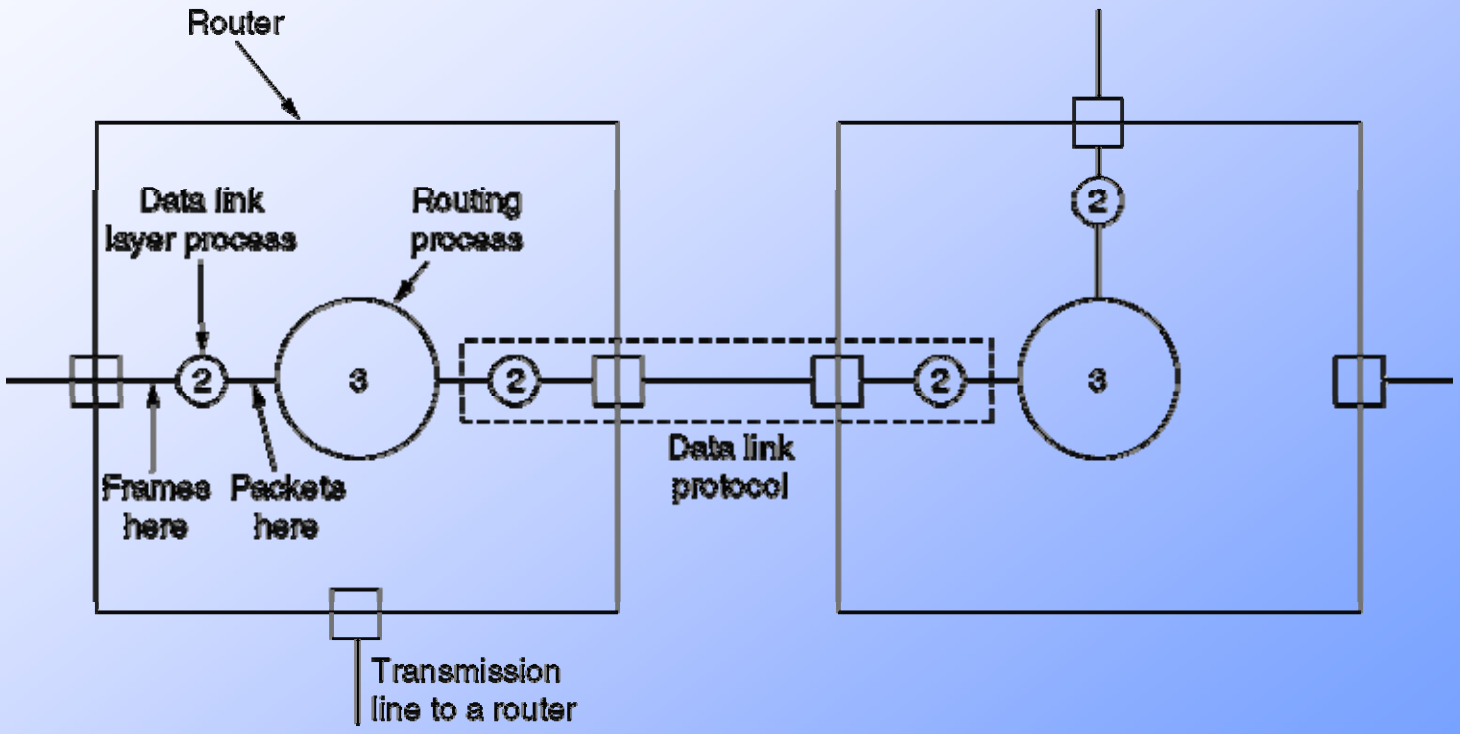
۱) لایه پیوند داده‌ها دریافت مرتب تمام قاب های ارسالی را تضمین می‌کند.

۲) هر فریم فقط یکبار دریافت می شود.

سه فاز انتقال در خدمات اتصال‌گرا

- ✓ اتصال برقرار می‌شود به این طریق که هر دو طرف متغیرها و شمارنده‌های مورد نیاز را برای اینکه مشخص شود چه قاب هایی دریافت شده‌اند و چه قاب هایی نرسیده‌اند را تایید اولیه می‌کنند .
- ✓ یک یا چند قاب بطور واقعی انتقال می‌یابند .
- ✓ اتصال قطع شده و متغیرها، بافرها و سایر منابع مورد استفاده در این اتصال آزاد می گردند .

محل پروتکل لایه پیوند داده ها



۲) کنترل جریان

مشکل دیگری که در مورد لایه پیوند داده‌ها و لایه‌های بالایی آن رخ می‌دهد مشکل فرستنده سریع و گیرنده کند و یا به عبارت دیگر عدم هماهنگی بین گیرنده و فرستنده است که برای آن، دو راه حل زیر پیشنهاد می‌شود:

- کنترل جریان مبتنی بر بازخورد (FeedBack-Based Flow control)
- کنترل جریان مبتنی بر سرعت (Rate-Based Flow control)

- **کنترل جریان بر مبنای بازخورد**

گیرنده اطلاعات مربوط به شرایط فرستادن داده‌های بیشتر را به فرستنده اعلام می‌کند.

- **کنترل جریان بر مبنای سرعت**

پروتکل در درون خود دارای مکانیسمی می باشد که میزان داده‌هایی که هر فرستنده ممکن است بفرستد را بدون دریافت بازخورد از گیرنده ، محدود می‌کند.

۳) قاب بندی و کنترل خطا

تشخیص‌خطا : روش معمول برای لایه پیوند داده‌ها، شکستن رشته بیت ها به قاب های مجزا و محاسبه جمع کنترلی (checksum) برای هر قاب در مبدأ و ضمیمه کردن آن به انتهای قاب و ارسال آن است. چنانچه در مقصد جمع کنترلی محاسبه شده با جمع کنترلی موجود در قاب متفاوت باشد لایه پیوند داده‌ها تشخیص می‌دهد که خطایی رخ داده است و تلاش می‌کند آن را رفع کند.

قاب بندی : شکستن رشته بیت ها به قاب ها

یک روش قاب بندی درج فواصل زمانی در نقاطی از رشته بیت ها است.

مشکل زمان بندی در شبکه ها ⟵ وجود مشکل در تعیین ابتدا و انتهای قاب ها

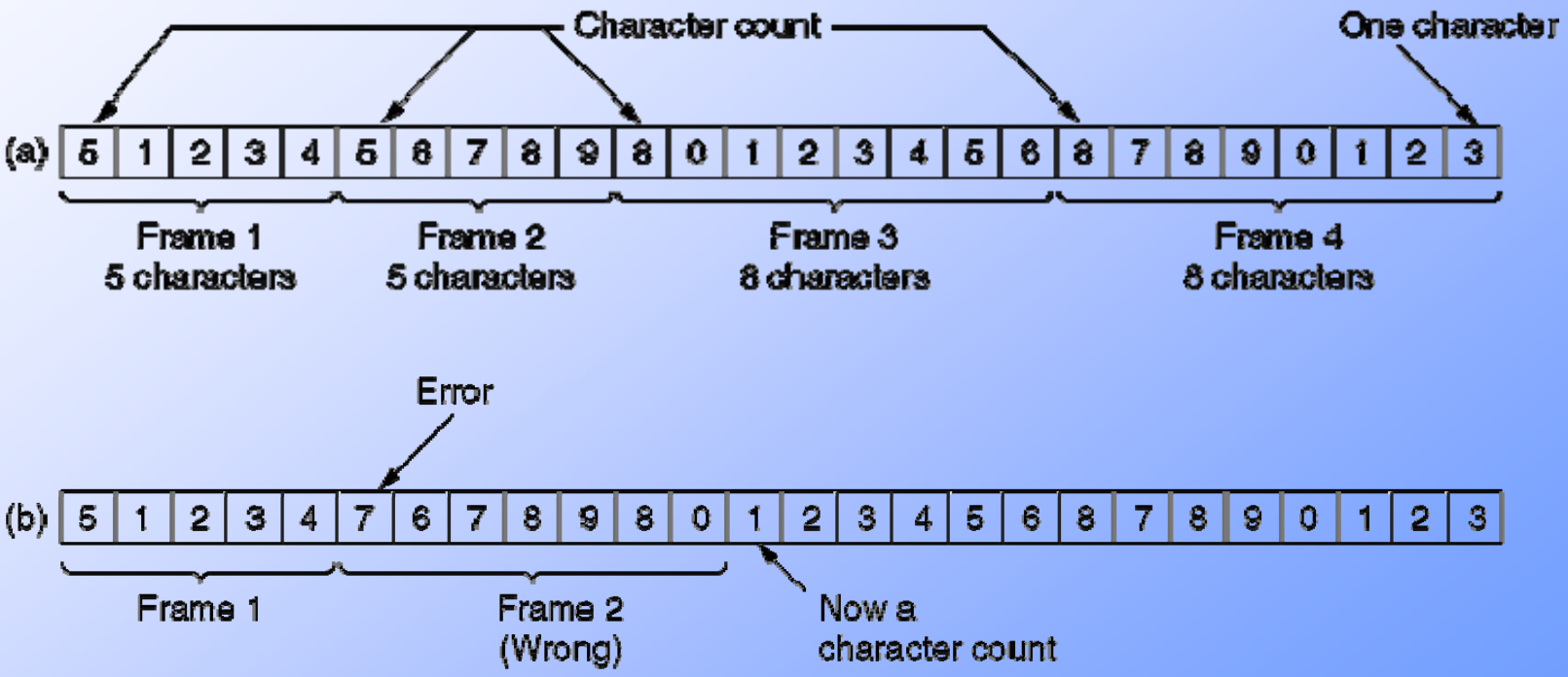
الف) فریم بندی

چهار روش برای مشخص نمودن ابتدا و انتهای هر قاب عبارتند از :

- شمارش کارکترها
- بایت های نشانگر با درج بایت
- نشانگرهای ابتدایی و انتهایی با درج بیت
- تخطی از رمزگذاری لایه فیزیکی

۱) شمارش کارکترها

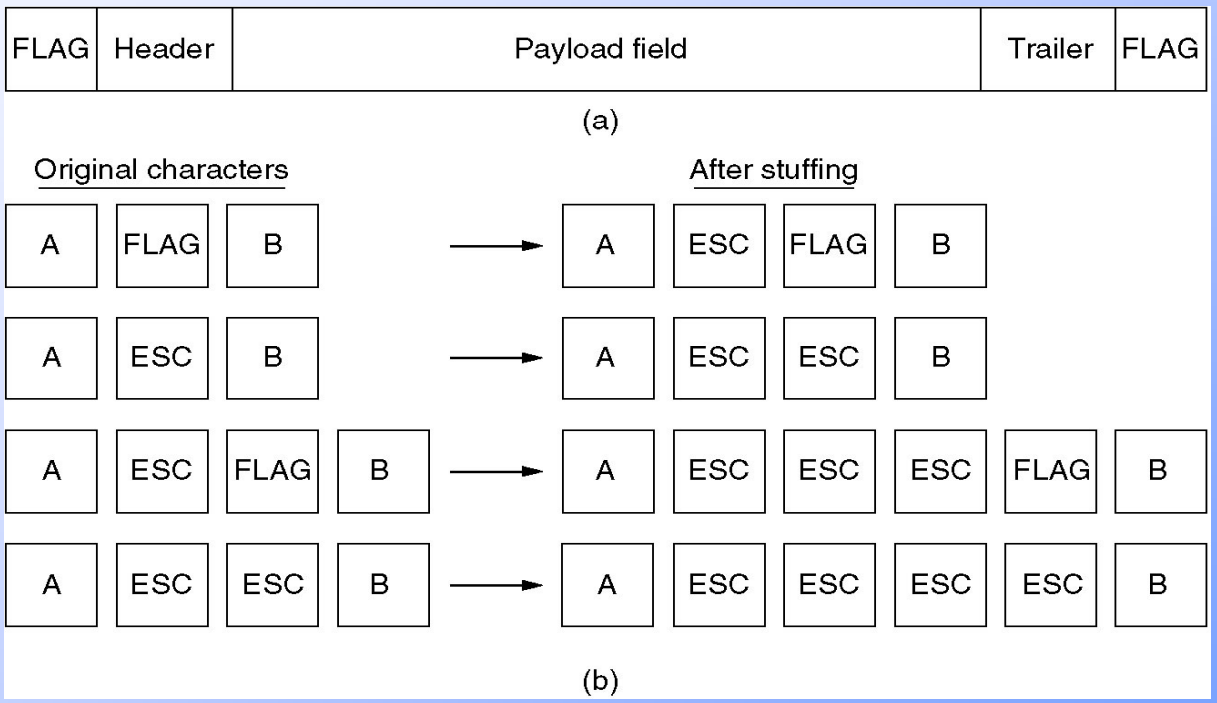
فیلدی در سرآیند قاب برای نگهداری تعداد کارکترهای قاب بکار می‌رود.



جریان کاراکترها : (a) بدون خطا (b) با خطا

۲) بایت های نشانگر با درج بایت

با این روش مشکل همزمان سازی مجدد که پس از بروز خطا رخ می‌داد با گذاشتن بایت های ویژه‌ای در ابتدا و انتهای هر قاب حل می‌گردد.

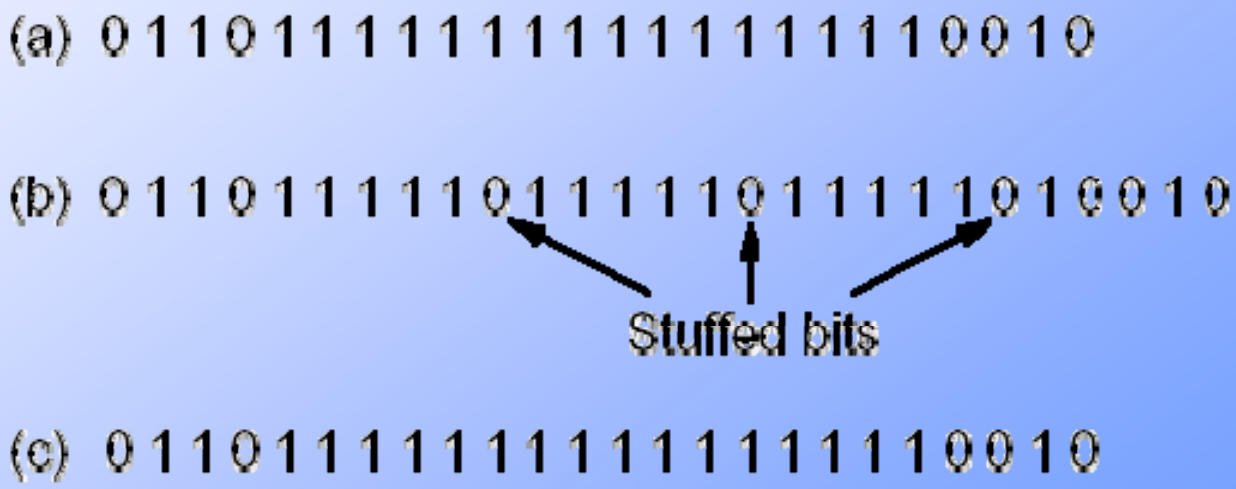


(a) نمایش یک فریم داده به همراه بایت نشانگر

(b) مثالی از یک بایت قبل و بعد از درج بایت گریز ویژه (ESC)

۳) نشانگرهای ابتدایی و انتهایی با درج بیت (Bit stuffing)

در این روش شروع و پایان هر قاب با الگوی بیتی(بایت نشانگر) ۰۱۱۱۱۱۱۰ مشخص می‌شود. وقتی لایه پیوند داده‌های فرستنده با پنج بیت متوالی ۱ مواجه شد بطور خودکار یک بیت ۰در رشته بیت خروجی قرار می‌دهد.



(a) داده اولیه **(b) جریان بیت ارسالی** **(c) جریان بیت دریافتی**

۴) تخطی از رمزگذاری لایه فیزیکی

این روش فقط در شبکه‌هایی قابل استفاده است که رمزگذاری در لایه فیزیکی شامل افزونگی (Redundancy) باشد.

ب) کنترل خطا

روش معمول برای تضمین تحویل مطمئن آن است که فرستنده به نحوی از آنچه که در انتهای دیگر خط رخ می‌دهد آگاه گردد. به طور متداول در این پروتکل لازم است گیرنده، قاب های کنترلی ویژه‌ای (Ack) را ارسال کند که دریافت قاب ورودی را به صورت مثبت یا منفی اعلام نماید.

اگر در اثر نقص سخت‌افزاری یک قاب Ack از بین برود فرستنده قفل می‌کند، که این حالت با اضافه کردن تایمری در لایه پیوند داده‌ها حل می‌شود.

مشکل ارسال چند کپی از یک فریم به لایه شبکه ⟵ شماره دار کردن فریم ها

تشخیص و تصحیح خطا

خطا :

- تک بیتی
- دسته ای (Burst)

کد واژه (code word)

هر فریم n بیتی شامل m بیت داده و r بیت کنترلی است.

فاصله همینگ :

- d+1 ⟵ d بیت خطا قابل تشخیص
- 2d+1 ⟵ d بیت خطا قابل تصحیح

روش های کشف و تصحیح خطا در کانال

دو راهبرد برطرف کردن خطاها در شبکه :

تشخیص خطا ⟵ افزودن اطلاعاتی به اطلاعات ارسالی جهت آگاه کردن گیرنده از وقوع یا عدم وقوع خطا .

تصحیح خطا ⟵ افزودن اطلاعاتی به اطلاعات ارسالی به گونه ای که گیرنده قادر به استنباط اطلاعات اصلی باشد.

- ✓ کدهای تشخیص خطا
  - بیت توازن
  - جمع کنترلی
  - کد افرونگی چرخشی
- ✓ کدهای تصحیح خطا ⟵ روش همینگ

بیت توازن (parity bit)

- انواع توازن
  - توازن زوج (even)
  - توازن فرد (odd)

- فرستنده و گیرنده بر سر نوع توازن توافق دارند.

روش کار :

در فرستنده بیت توازن فریم ارسالی محاسبه شده و همراه با فریم ، ارسال می شود.

در گیرنده اطلاعات دریافتی (بیت توازن + فریم) چک می شود و در صورتی که بیت توازن محاسبه شده برای فریم دریافتی با بیت توازن دریافتی برابر باشد، خطا نداریم.

جمع کنترلی (checksum)

در این روش در فرستنده بلوک های ارسالی را با هم جمع کرده و از حاصل جمع مکمل دو می گیرند و آنرا به عنوان checksum همراه داده ها ارسال می کنند.

در گیرنده اطلاعات دریافتی اعم از بلوک های داده و بایت checksum را با هم جمع کرده و اگر حاصل جمع برابر صفر شود به معنی عدم وجود خطا است.

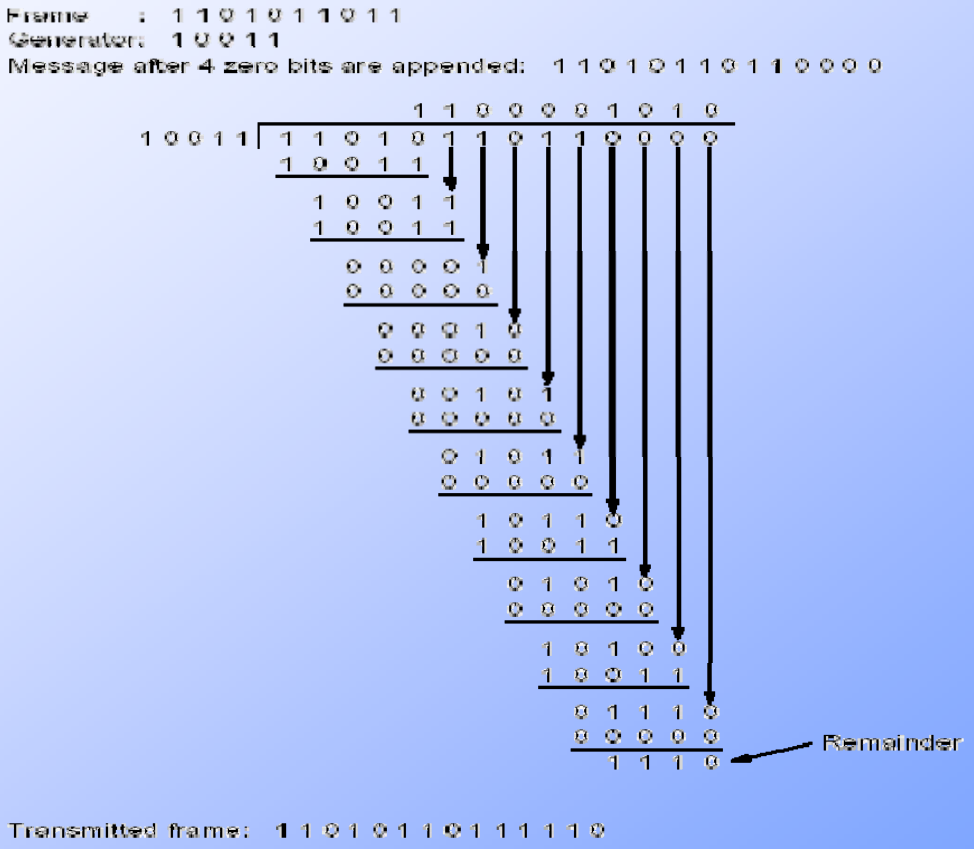
الگوریتم کد افرونگی چرخشی (CRC)

- فرض کنید $G(x)$ از درجه r باشد. r بیت صفر به طرف مرتبه پایین قاب بیفزاید. اکنون حاوی $m+r$ بیت بوده و متناظر با چند جمله ای $X^r M(X)$ است.

- رشته بیتی متناظر با $G(x)$ را با استفاده از تقسیم به پیمانه ۲ بر $X^r M(X)$ تقسیم کنید.

- باقیمانده را (که همواره دارای تعداد بیتهای کوچکتر یا مساوی r است) با استفاده از تفریق پیمانه ۲ از رشته بیتی متناظر با $X^r M(X)$ کم کنید. نتیجه، قابی با جمع کنترلی است که باید ارسال شود. چند جمله ای مربوط به آن را $T(x)$ بنامید. بدیهی است که $T(X)$ بر $G(x)$ بخشپذیر به پیمانه ۲ است. در هر مساله تقسیم، اگر باقیمانده را از مقسوم کم کنیم آنچه که باقی می‌ماند بر مقسوم علیه بخشپذیر است.

مثال برای CRC :



کدهای تصحیح خطا

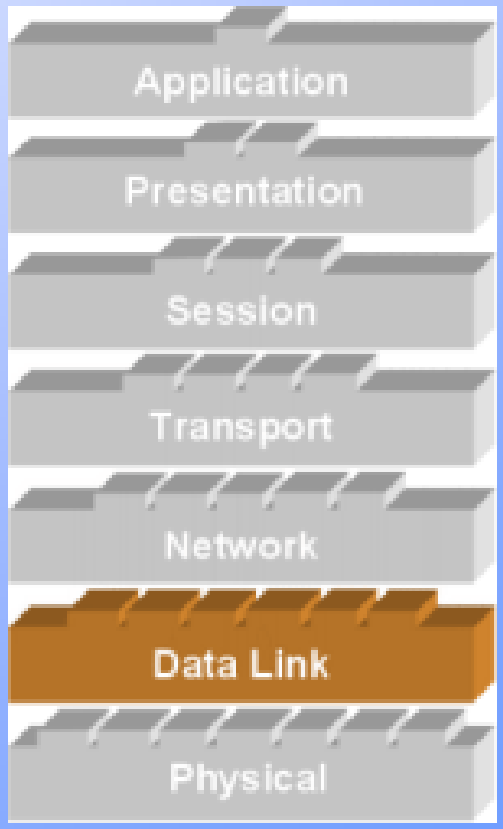
Char.	ASCII	Check bits
H	1001000	00110010000
a	1100001	10111001001
m	1101101	11101010101
m	1101101	11101010101
i	1101001	01101011001
n	1101110	01101010110
g	1100111	01111001111
	0100000	10011000000
c	1100011	11111000011
o	1101111	10101011111
d	1100100	11111001100
e	1100101	00111000101

Order of bit transmission

استفاده از کد همینگ جهت کشف و تصحیح خطا

فصل چهارم :

زير لايه دسترسی به رسانه



زیر لایه دسترسی به رسانه انتقال

نکته اصلی و مهم در شبکه پخشی تعیین چگونگی استفاده از کانالی است که برای آن رقابت وجود دارد. پروتکل هایی که برای تعیین نفر بعدی در کانال های دستیابی چندگانه استفاده می‌شود متعلق به یک زیر لایه از لایه پیوند داده‌ها می‌باشد که زیر لایه MAC (کنترل دستیابی به رسانه) نامیده می‌شود.

تخصیص کانال

- تخصیص کانال به شکل ایستا در شبکه های محلی و شهری
- تخصیص کانال به شکل پویا در شبکه های محلی و شهری

تخصیص کانال به شکل ایستا

FDM (تسهیم‌سازی فرکانسی):

یکی از روش های مرسوم برای تخصیص یک کانال است که در آن ها 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 می‌کند، بنابراین بین کاربران برخوردی صورت نمی‌گیرد .

TDM (تسهیم سازی زمانی) :

در این روش زمان مالکیت کانال ، به N قسمت مساوی تقسیم و به هر کاربر یکی از N برش زمانی اختصاص داده می شود.

دامنه فعالیت FDM

- **تعداد کاربران ثابت و کم**

درصورتی که هر کدام از آن ها بار ترافیکی ثابت و سنگینی را ایجاد کنند، مکانیسم تخصیص تسهیم‌سازی فرکانسی مؤثر و ساده می‌باشد.

- **تعداد فرستنده‌ها زیاد و متغیر**

اگر طیف به N ناحیه تقسیم گردد و کمتر از N کاربر مایل به برقراری ارتباط همزمان باشد، یک بخش بزرگی از طیف های در دسترس از بین خواهند رفت و یا اگر کاربران بیشتر از N مایل به برقراری ارتباط باشند ، به علت پهنای باند کم موفق نخواهند شد.

اثبات کارآیی‌ضعیف FDM (تخصیص ایستا)

- زمان تأخیر میانگین : T (ثانیه)
- ظرفیت کانال : C (bps)
- نرخ دریافت قاب : λ (قاب بر ثانیه)

هر قاب دارای یک طول است که از یک تابع چگالی احتمال تصاعدی با میانگین $1/\mu$ بیت بر قاب بدست آمده است، بنابراین با این پارامترها سرعت خدمات μC قاب بر ثانیه می باشد.

بوسیله نظریه صف‌بندی می‌توان نشان داد که :

$$T=1/(\mu C - \lambda)$$

پس از تقسیم کانال ها به N زیر کانال غیر وابسته ، داریم:

$$T_{FDM}=1/[\ \mu(C/N)-(\ \lambda/N)]=N/(\ \mu C-\ \lambda)=NT$$

تخصیص کانال به شکل پویا

- ✓ مدل ایستگاه
- ✓ فرض کانال منفرد
- ✓ فرض برخورد
- ✓ زمان ها
  - زمان پیوسته
  - زمان برهه‌ای (گسسته)
- ✓ وضعیت حامل
  - تشخیص وضعیت های حامل
  - عدم تشخیص وضعیت حامل

مدل ایستگاه

این مدل شامل N ایستگاه مستقل است که هر کدام شامل یک برنامه یا کاربری است که فریم هایی را برای انتقال ایجاد می کند.

وقتی یک فریم تولید شود، ایستگاه تا زمان ارسال موفقیت آمیز آن فریم قفل می شود.

فرض کانال منفرد

یک کانال منفرد و مشترک برای تمام ارتباطات در دسترس ایستگاه ها می‌باشد به این معنا که تمام ایستگاه ها از طریق آن می‌توانند پیامی را دریافت و یا ارسال کنند.

ایستگاه ها از نظر سخت‌افزار یکسان ولی ممکن است بوسیله نرم‌افزار پروتکل، اولویت هایی را برای آن ها ایجاد کنند.

فرض برخورد

- اگر دو فریم بطور همزمان با هم فرستاده شوند، از نظر زمانی با یکدیگر تداخل کرده و سیگنال حاصل نامفهوم خواهد بود، به این اتفاق برخورد (تصادم) گویند.
- اگر فریمی دچار برخورد شود، باید دوباره ارسال شود.
- همه ایستگاه ها از برخورد مطلع می شوند.

زمان پیوسته

انتقال فریم 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 و انتقال فریم همواره از ابتدای یک مقطع زمانی شروع می‌شود.

تشخیص وضعیت حامل

ایستگاه ها 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 از آن استفاده نمی کند تا آزاد شود.

مثال : شبکه های LAN

عدم تشخیص وضعیت حامل

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

مثال : شبکه های بی سیم

- منظور از حامل ، سیگنال الکتریکی در کابل است.

پروتکل های دستیابی چندگانه

- ALOHA ✓
  - Pure ALOHA •
  - Slotted ALOHA •
- CSMA ✓
  - Persistent and Non Persistent CSMA •
  - CSMA/CD •
- پروتکل های بدون برخورد ✓
  - Bitmap •
  - Binary Count Down •
- پروتکل های شبکه‌های محلی بی‌سیم ✓
  - MACA •
  - MACAW •

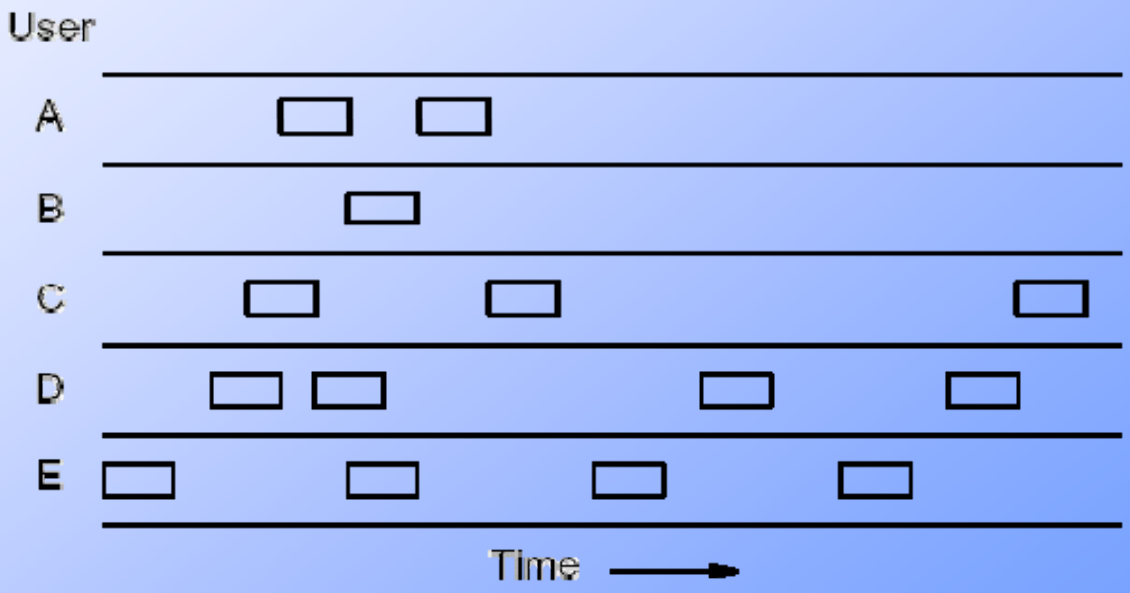
ALOHA (۱

- ایده اصلی آن متعلق به هر سیستمی می‌باشد که در آن کاربران به شکل هماهنگ نشده‌ای بخواهند برای استفاده از یک کانال مشترک در دسترس ، رقابت کنند.
- شامل دو نوع الوهای برهه‌ای و الوهای محض می‌باشد.
- کانال پخشی خاصیت بازخوردی دارد.
- سیستم های رقابتی :

سیستم هائی که در آن ها چندین کاربر از یک کانال مشترک به نحوی استفاده کنند که احتمال برخورد وجود دارد.

الف) Pure ALOHA

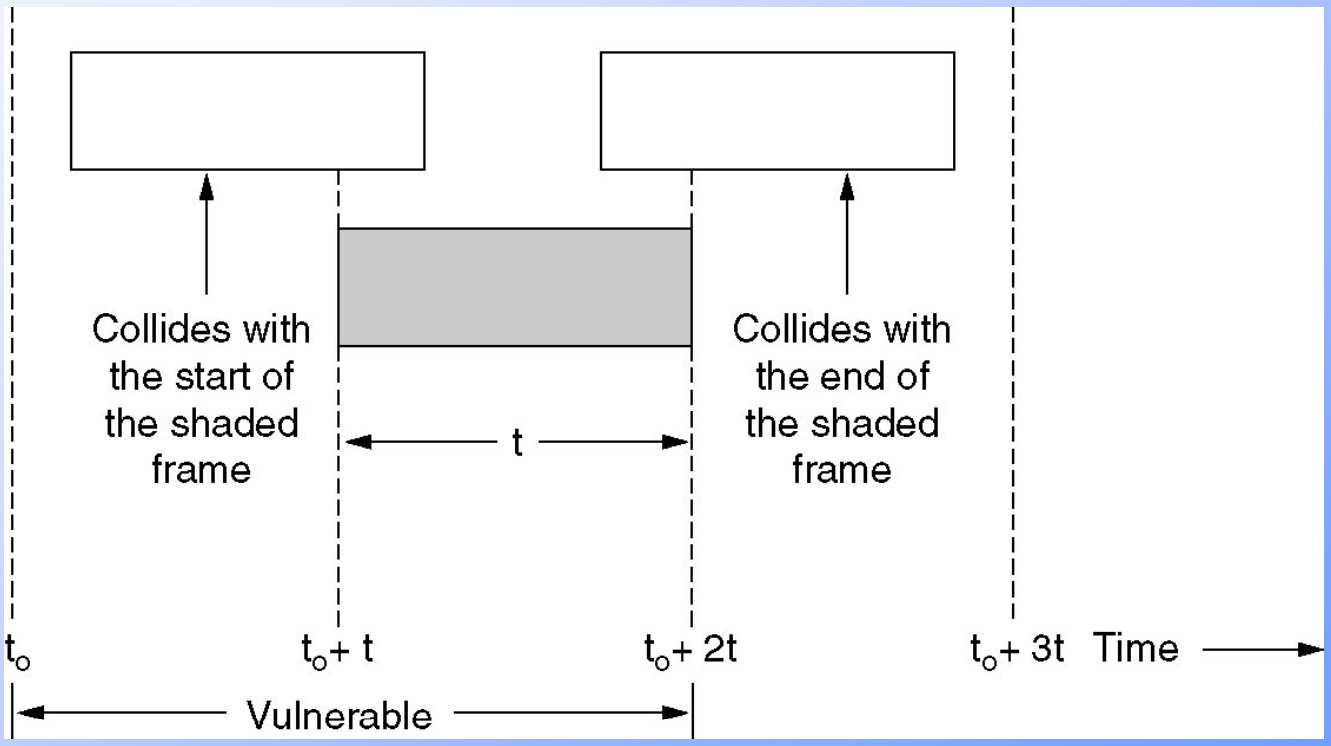
ایده اصلی در الوهای محض، سیستم ساده‌ای است که کاربران اجازه دارند در هر زمان که بخواهند داده‌ها را ارسال کنند البته با این کار برخوردهایی صورت می‌گیرد و قاب هایی نیز از بین می‌روند.



زمان آسیب پذیری

زمان فریم (Frame Time) :

مدت زمانی که طول می کشد تا یک فریم با طول ثابت و استاندارد ارسال شود.

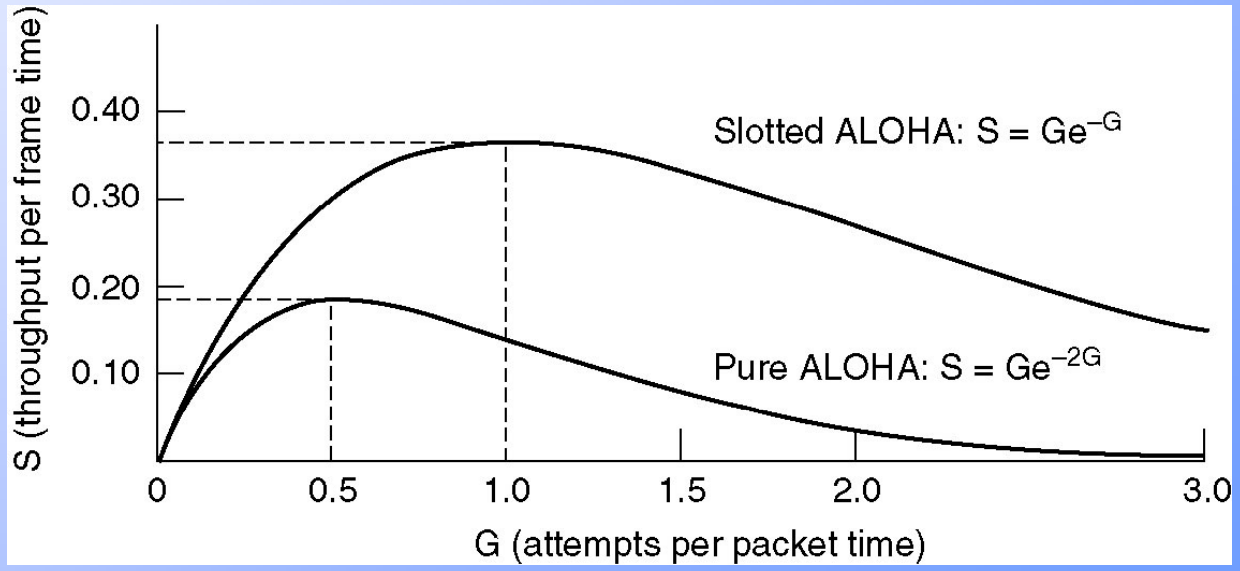


ب) Slotted ALOHA

این سیستم با الوهای برهه‌ای شناخته می‌شود درحقیقت نقطه مقابل الوهای محض می‌باشد به این معنا که اجازه ارسال به یک کامپیوتر در هر زمان داده نمی‌شود و لازم است که منتظر شروع برهه بعدی باشد.

مقایسه الوهای محض و برهه ای :

- ✓ الوهای محض نیازی به همزمان‌سازی زمانی ندارند در صورتیکه الوهای برهه‌ای نیازمند همزمان‌سازی زمانی است.
- ✓ احتمال برخورد در الوهای محض در هر زمانی از ارسال فریم وجود دارد، در حالیکه در الوهای برهه ای فقط در ابتدای ارسال فریم احتمال برخورد وجود دارد.
- ✓ کارآئی کانال در الوهای برهه ای تقریبا" دو برابر الوهای محض است.



۲) پروتکل های دسترسی چندگانه با قابلیت شنود سیگنال حامل (CSMA)

این پروتکل ها نوعی پروتکل شنود حامل اند یعنی در آن ها ابتدا به کانال گوش داده می‌شود و سپس بر طبق وضعیت کانال عمل می‌کنند.

برتری آن بر ALOHA از آن جهت است که در صورت اشغال بودن کانال هیچگونه انتقالی صورت نمی‌گیرد.

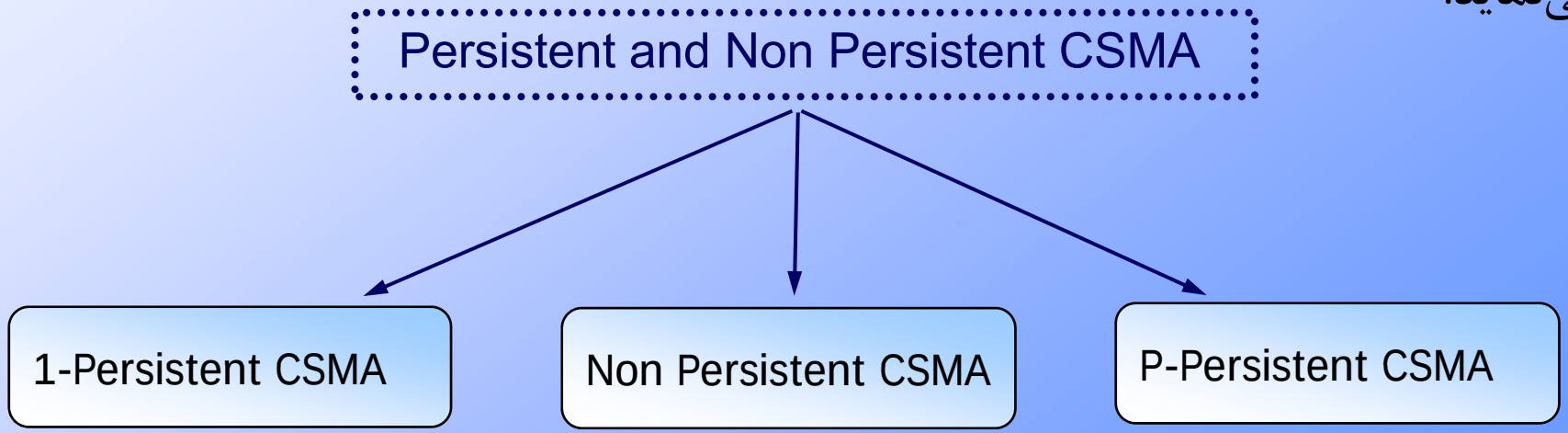
انواع CSMA:

- Persistent and Non Persistent CSMA
- CSMA/CD

هر چه تاخیر انتشار بیشتر باشد ، اثر آن بر کارآئی پروتکل بیشتر بوده و کارآئی را بدتر می کند.

الف) Persistent and Non Persistent CSMA

این نوع پروتکل به این صورت عمل می‌نماید که هر ایستگاه به هنگام ارسال داده به کانال گوش داده و در صورتی که کانال مشغول باشد، منتظر آزاد شدن کانال می‌ماند و زمانی که کانال را آزاد یافت، قاب را ارسال می‌کند و در صورت بروز تصادم، ایستگاه برای مدت زمانی که مقدار آن تصادفی است منتظر می‌ماند و مجدد قاب را ارسال می‌نماید.



1-Persistent CSMA

- در این پروتکل دستگاه فرستنده مرتبا" به کانال گوش می دهد و به محض آزاد یافتن کانال داده خود را ارسال می کند.
- در این روش، برخورد زیاد اتفاق می افتد.

Non Persistent CSMA

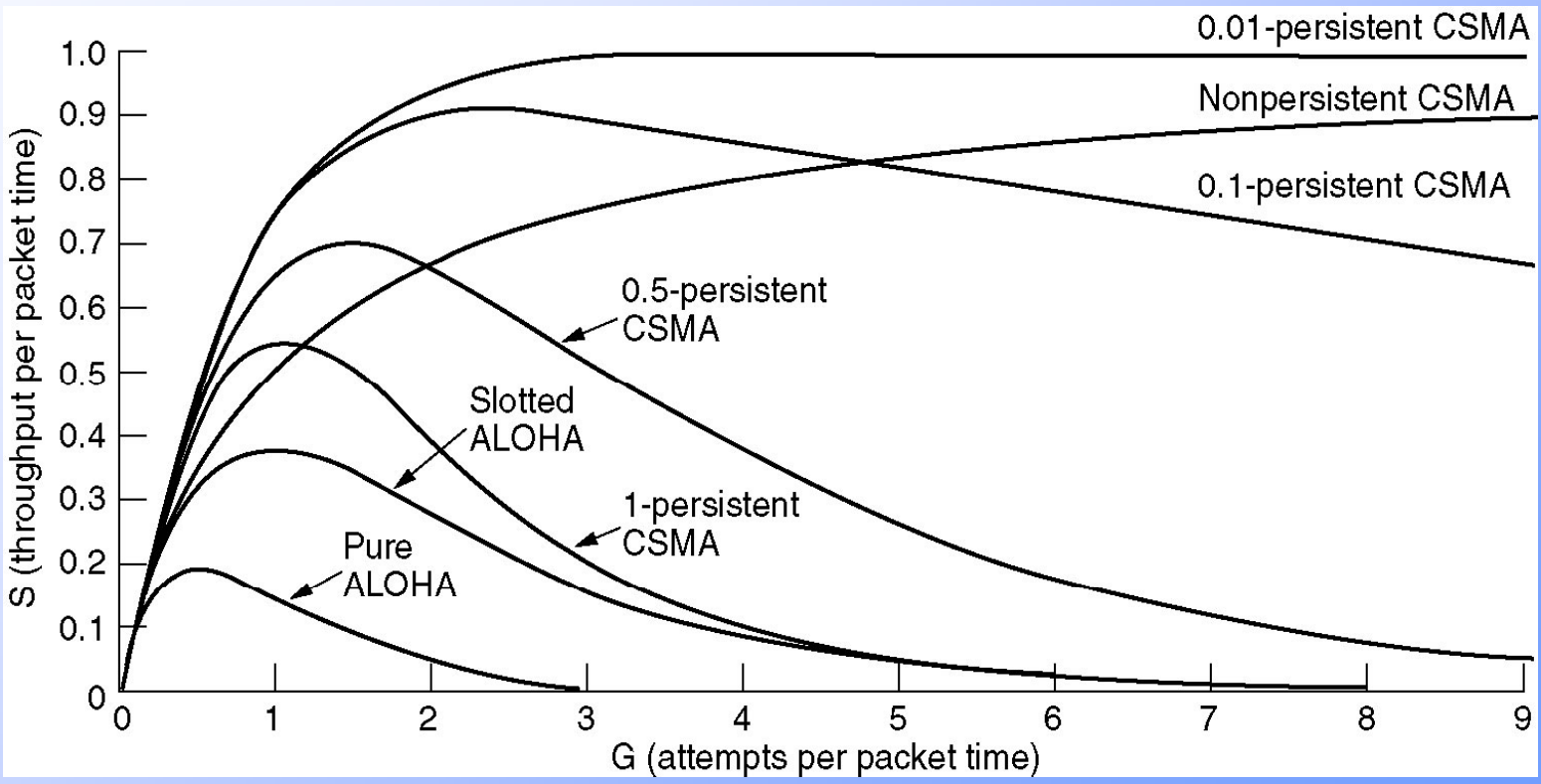
در این پروتکل ایستگاه فرستنده قبل از ارسال به کانال گوش می دهد و در صورتی که کانال را مشغول ببیند، یک مدت تصادفی صبر کرده و سپس کانال را چک می کند.

بهره وری این پروتکل از پروتکل 1-Persistent CSMA بهتر است، اما تاخیر بیشتری نسبت به آن دارد.

P-Persistent CSMA

- این پروتکل فقط برای کانال های زمان بندی شده (برهه ای) قابل استفاده است.
- در این پروتکل ایستگاه کانال را تست کرده و در صورت آزاد بودن با احتمال p داده را ارسال و با احتمال q (q=1-p) صبر می کند تا برش زمانی بعدی و در آن زمان دوباره کانال را تست می کند. ایستگاه این روند را ادامه می دهد تا اینکه قابی ارسال شود و یا این که ایستگاه دیگری داده خود را ارسال کند.
- ایستگاه در صورتی که کانال را مشغول بیابد تا برهه بعدی صبر می کند.

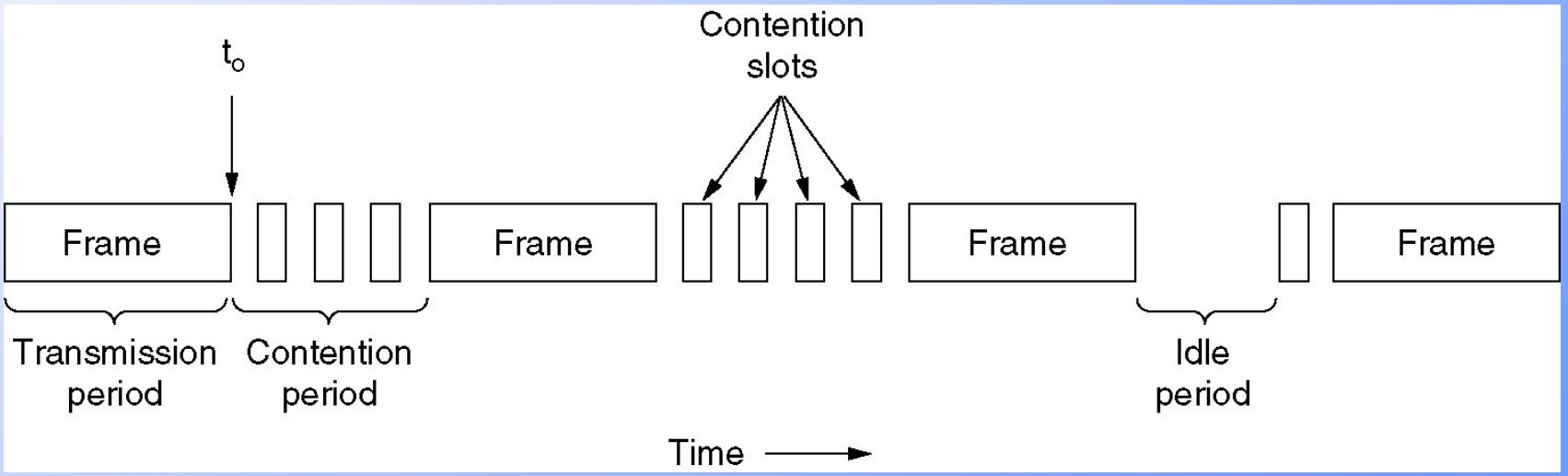
مقایسه انواع پروتکل ها از نظر بهره وری کانال



ب) CSMA/CD

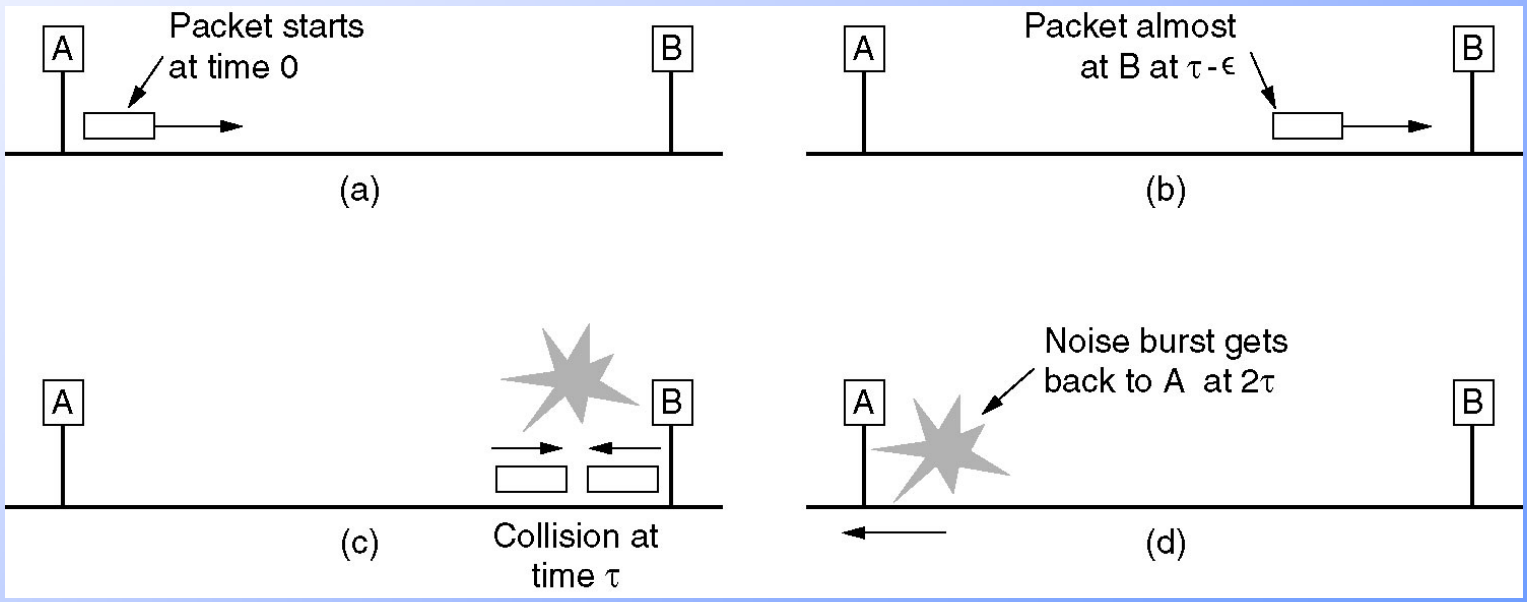
برتری آن بر Persistent and Non Persistent CSMA از آن جهت است که در صورت بروز تصادم عمل انتقال متوقف می‌شود. این عمل باعث صرفه‌جویی در زمان و پهنای باند نیز می‌شود.

این نوع پروتکل در شبکه های LAN کاربرد وسیعی دارد.



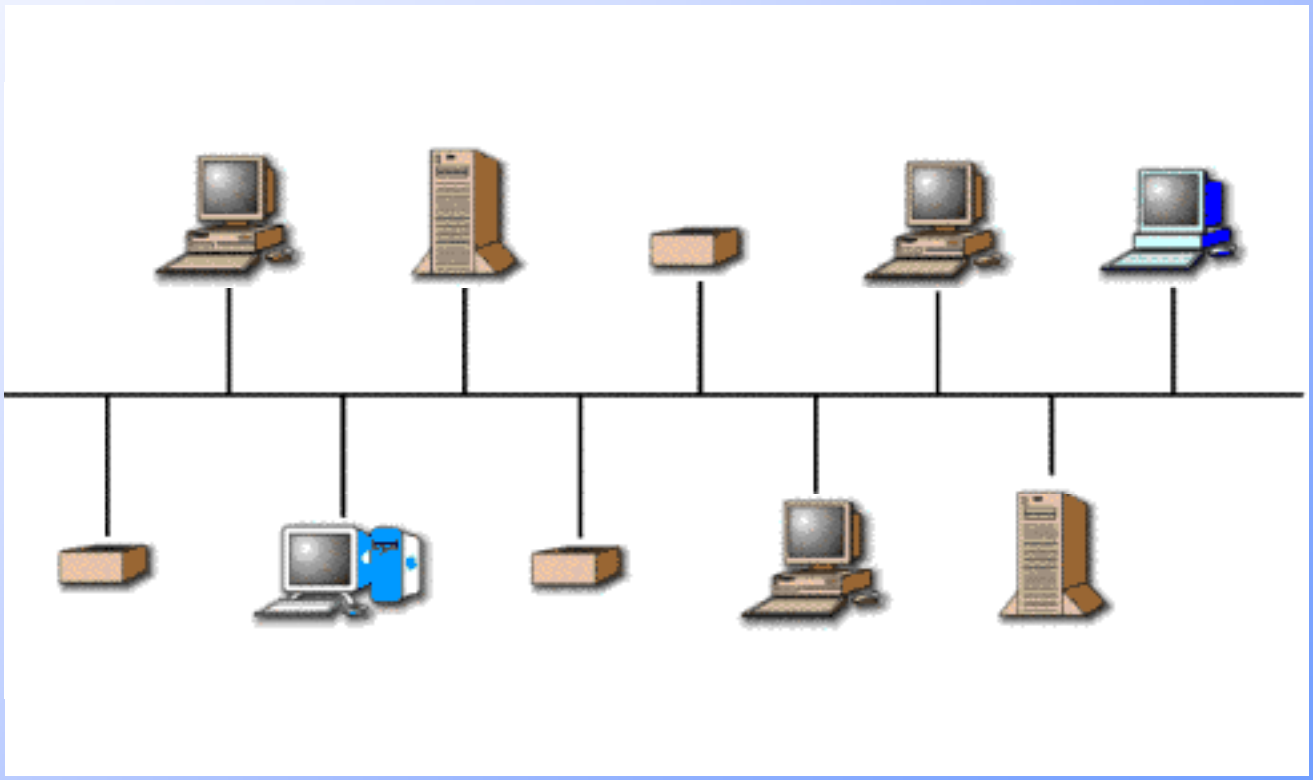
زمان لازم برای تشخیص برخورد

ایستگاه فرستنده پس از گذشت 2t می تواند برخورد را تشخیص دهد. به همین علت برهه های دوره رقابت برابر 2t در نظر گرفته می شود.



نمایش طرز کار CSMA/CD

CSMA/CD با یک کانال ذاتا" سیستمی نیمه دو طرفه (Half Duplex) است.



۳) پروتکل های بدون برخورد

حتی با وجود CSMA/CD امکان بروز تصادم در زمان رقابت وجود دارد. این برخوردها بویژه در زمانی که طول کابل زیاد و قاب کوتاه باشد باعث بروز آثار زیان باری بر کارآیی سیستم می‌شود.

پروتکل های بدون برخورد، پروتکل هائی هستند که رقابت برای تصاحب کانال را بدون برخورد ، مدیریت می کنند.

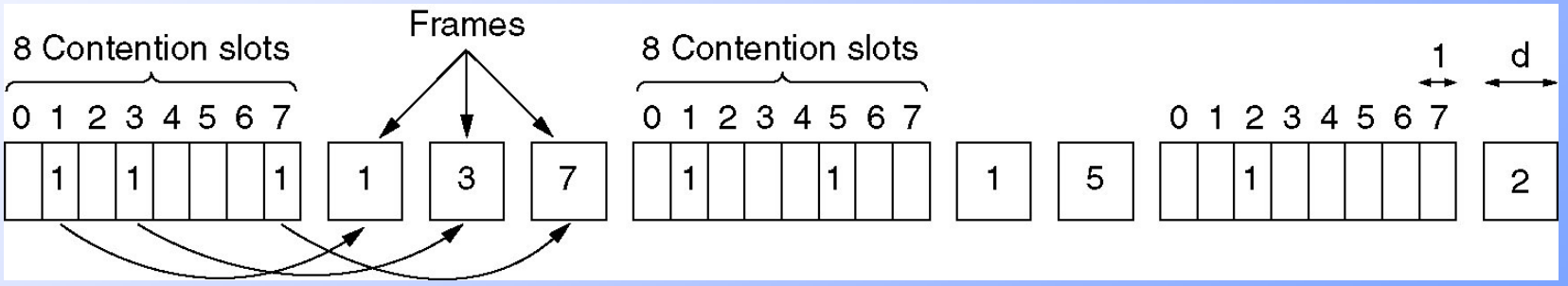
در تمام این پروتکل ها فرض بر این است که N ایستگاه وجود دارد و هر ایستگاهی آدرس منحصر به فرد از 0 تا N-1 را دارا می‌باشد.

دو نوع از پروتکل های بدون برخورد عبارتند از :

- Bitmap
- Binary Count Down

الف) Bitmap

پروتکل بدون برخورد Bitmap یا بیت نگاشت می‌باشد که هر دوره رقابت در آن دقیقاً شامل N برهه یا مقطع زمانی است. که در طی این مقطع زمانی هیچ ایستگاهی اجازه انتقال ندارد.



کارایی کانال :

در بار کم ⟵ $\frac{d}{d+N}$

در بار زیاد ⟵ $\frac{d}{d+1}$

ب) Binary Count Down

حل مشکل پروتکل بیت نگاشت (وجود بار اضافی در هر ایستگاه) با استفاده از آدرس دستگاه :

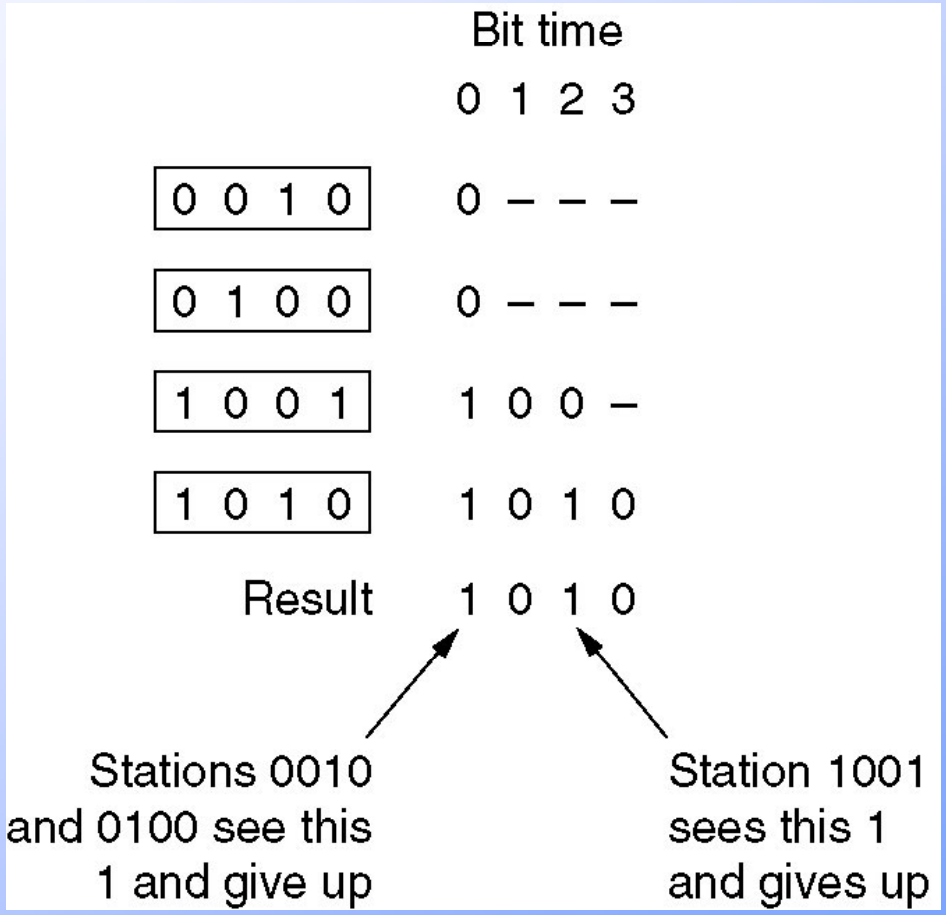
یک ایستگاه برای استفاده از کانال آدرس خود را به شکل یک رشته بیت دودویی با شروع از بیت پر ارزش پخش می‌کند بیت ها در هر آدرس و موقعیت ایستگاه های متفاوت با هم OR منطقی می‌شوند این پروتکل را شمارش معکوس دودویی می نامیم.

- در این پروتکل ایستگاه های با آدرس یزرگتر اولویت بالاتری دارند.

- کارایی کانال :

$$\frac{d}{d+\log_2 N}$$

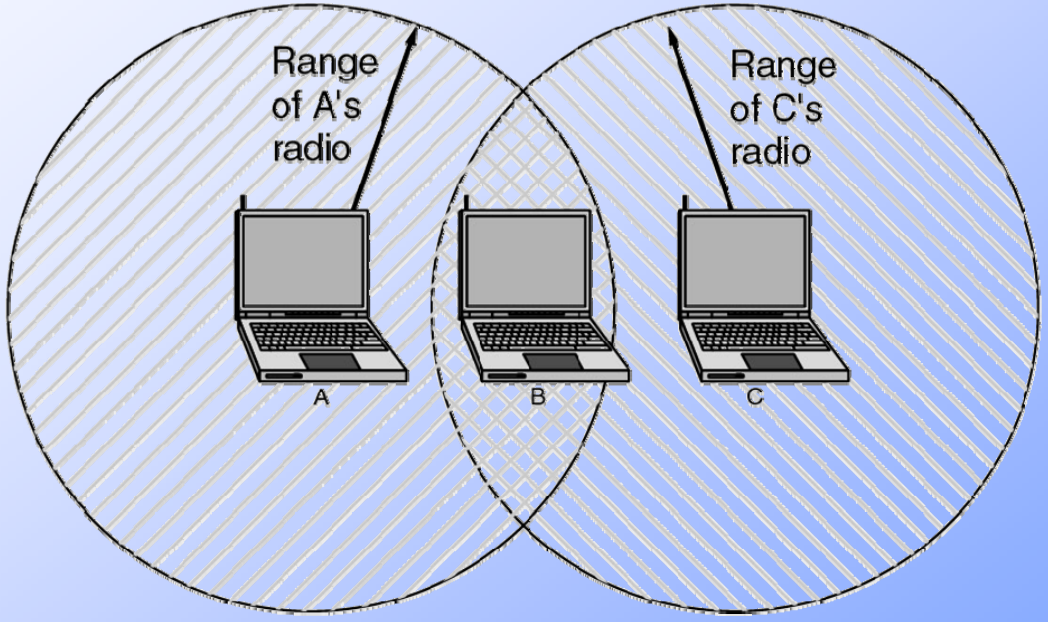
پروتکل شمارش معکوس دودوئی :



۴) پروتکل های شبکه‌های محلی بی‌سیم

این نوع از شبکه‌های محلی نیاز به زیر لایه MAC خاصی دارند.

یک نظریه برای استفاده از شبکهٔ محلی بی‌سیم استفاده از CSMA می‌باشد که البته مشکلاتی نیز دارد ، از جمله این که این پروتکل کاملاً مناسب نیست زیرا آنچه که مهم است تداخل درگیرنده است نه در فرستنده !

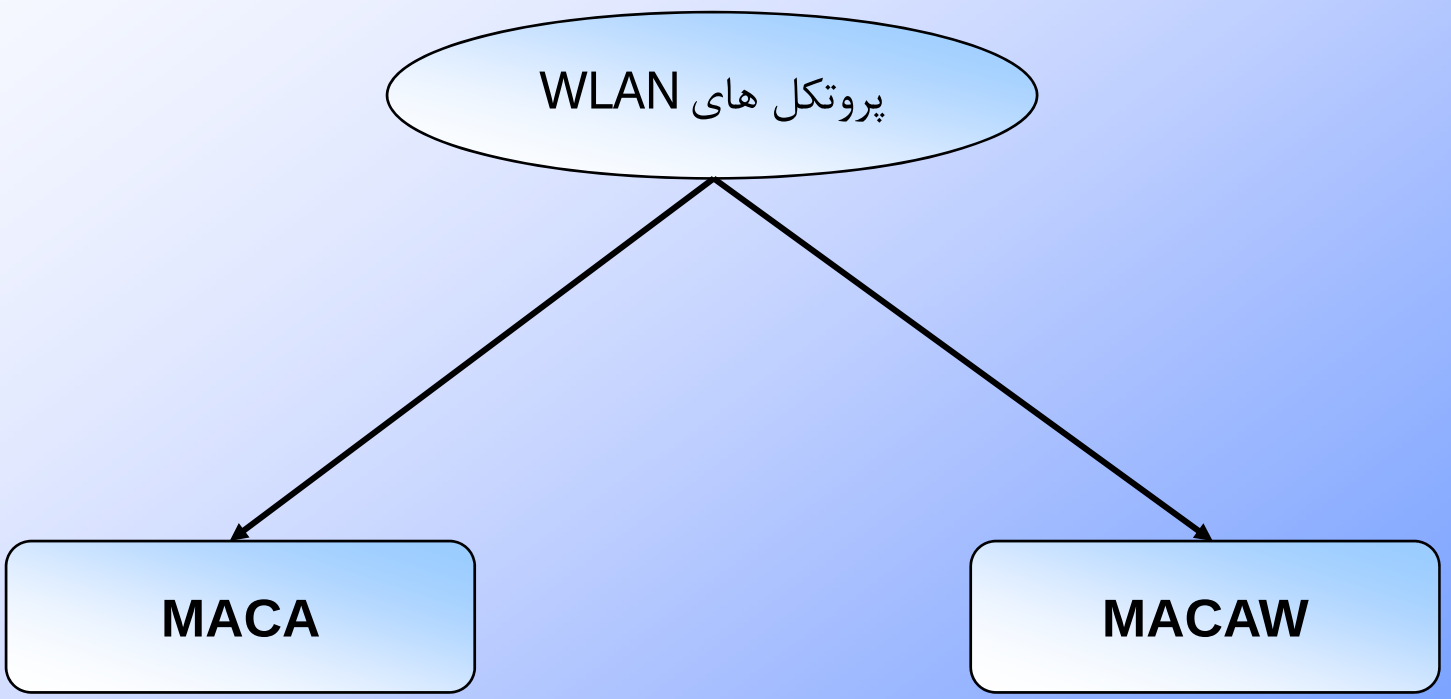


برد هیچ یک از ایستگاه‌ها کل سیستم را پوشش نمی‌دهد.

مشکلات LANهای بی‌سیم مبتنی بر CSMA

a) مشکل ایستگاه مخفی (Hidden station problem)

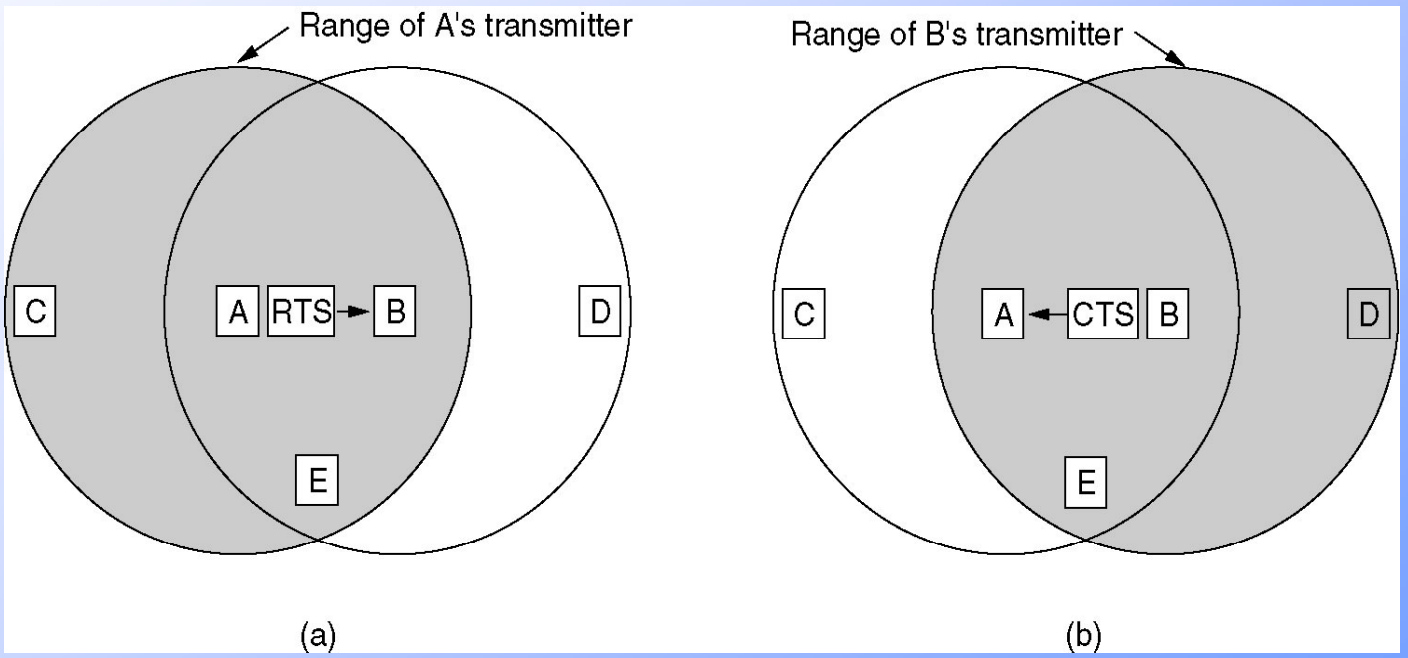
b) مشکل ایستگاه آشکار (Exposed station problem)


پروتکل های WLAN
MACA
MACAW

دستیابی چندگانه با پرهیز از برخورد (MACA)

شامل قراداد اولیه‌ای است که برای شبکه‌های محلی بی‌سیم طراحی شد.

ایده اصلی آن این است که فرستنده, گیرنده را به خروج قاب کوچک وادار کند تا ایستگاه های مجاور از انتقال داده در حین ارسال قاب داده بزرگ خودداری کنند.



قاب RTS : درخواست ارسال

قاب CTS : آمادگی ارسال

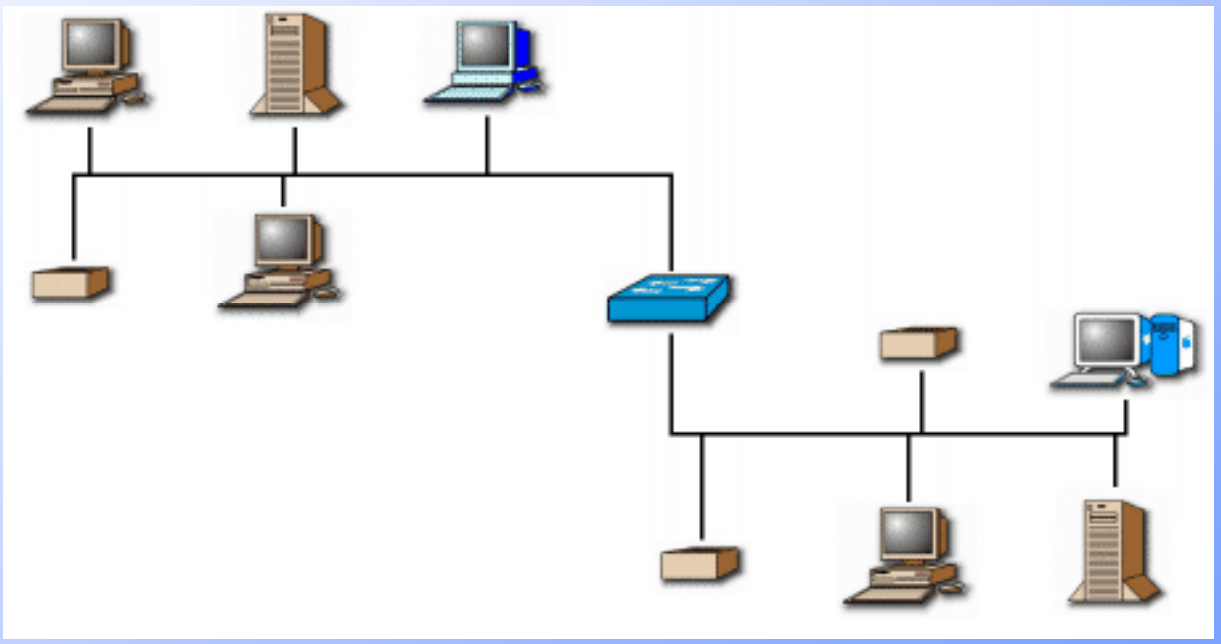
MACAW

- ✓ شامل پروتکل توسعه یافته‌ای از نظر کارآیی نسبت به MACA می‌باشد.
- ✓ بدون اعلام وصول لایه پیوند داده ، قاب ها از بین رفته و ارسال نمی‌شوند تا لایه انتقال به عدم حضور آنها پی ببرد و یعنی تاخیر طولانی و در نتیجه کاهش کارآئی پروتکل. آن ها این مشکل را با معرفی قاب ACK بعد از قاب داده موفق حل کردند.
- ✓ استفاده از خاصیت CSMA یعنی تشخیص وضعیت حامل جهت جلوگیری از ارسال همزمان دو RST به یک مقصد.
- ✓ افزودن مکانیزم هائی به پروتکل تا ایستگاه ها با یکدیگر اطلاعاتی در خصوص ازدحام رد و بدل کنند.

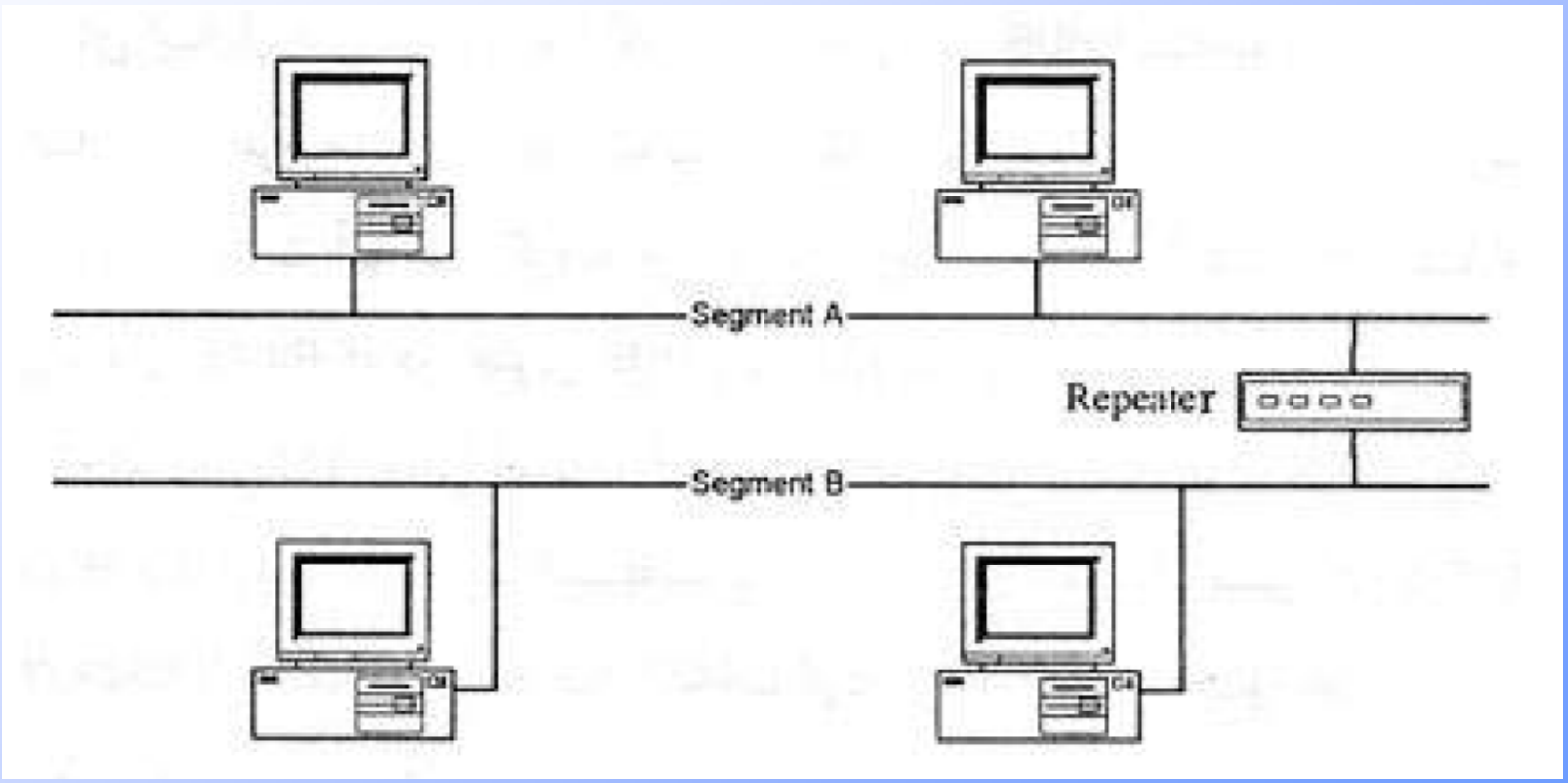
اترنت

اولین شبکه محلی که توسط دو دانشجوی MIT طراحی و پیاده‌سازی شد و از یک رشته کابل هم محور(coaxial) ضخیم بطول حداکثر ۲.۵ کیلومتر با سرعت 2.94 Mbps تشکیل شده بود.

این شبکه به مرور به استانداردهایی مثل DIX و IEEE 802.3 دست پیدا کرد.



اتصال دو سگمنت با استفاده از یک تکرار کننده (Repeater)



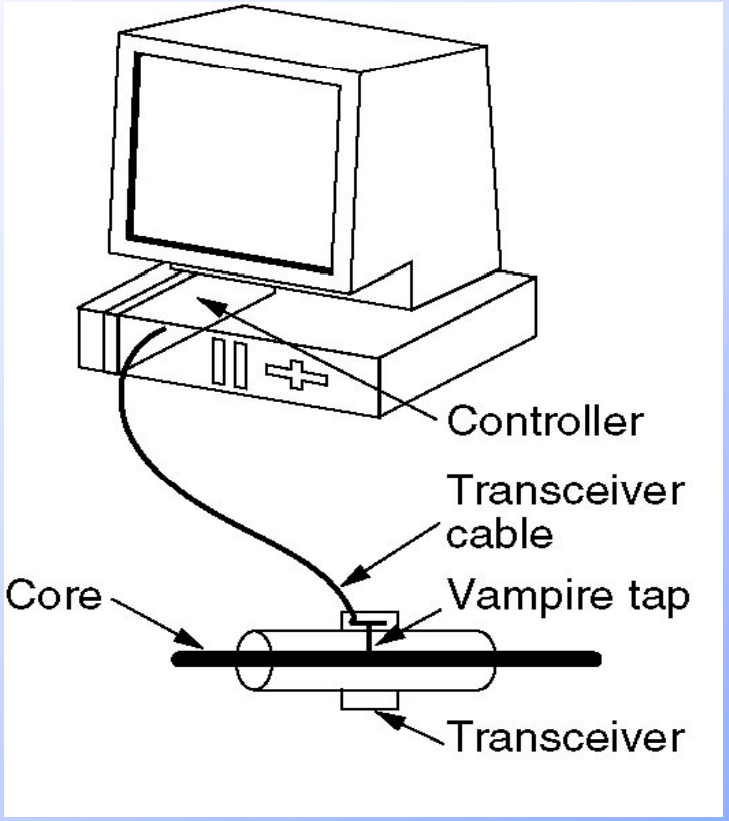
کابل کشی اترنت

نام کابل	نوع کابل	حداکثر طول قطعه	تعداد گره در هر قطعه	مزایا
10Base5	**Thick coax**	**500 m**	**100**	کابل اصلی و اولیه (از رده خارج)
10Base2	**Thin coax**	**185 m**	**30**	به هاب نیازی نیست
10Base-T	**Twised pair**	**100 m**	**1024**	ارزانترین سیستم
10Base-F	**Fiber optics**	**2000 m**	**1024**	بهترین انتخاب برای مابین ساختمانها

جدول انواع کابل‌کشی در اترنت

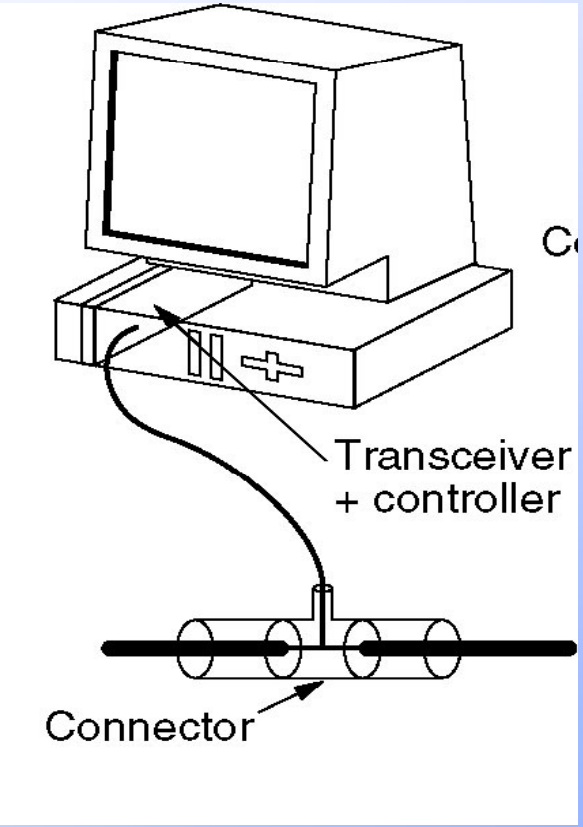
10Base5

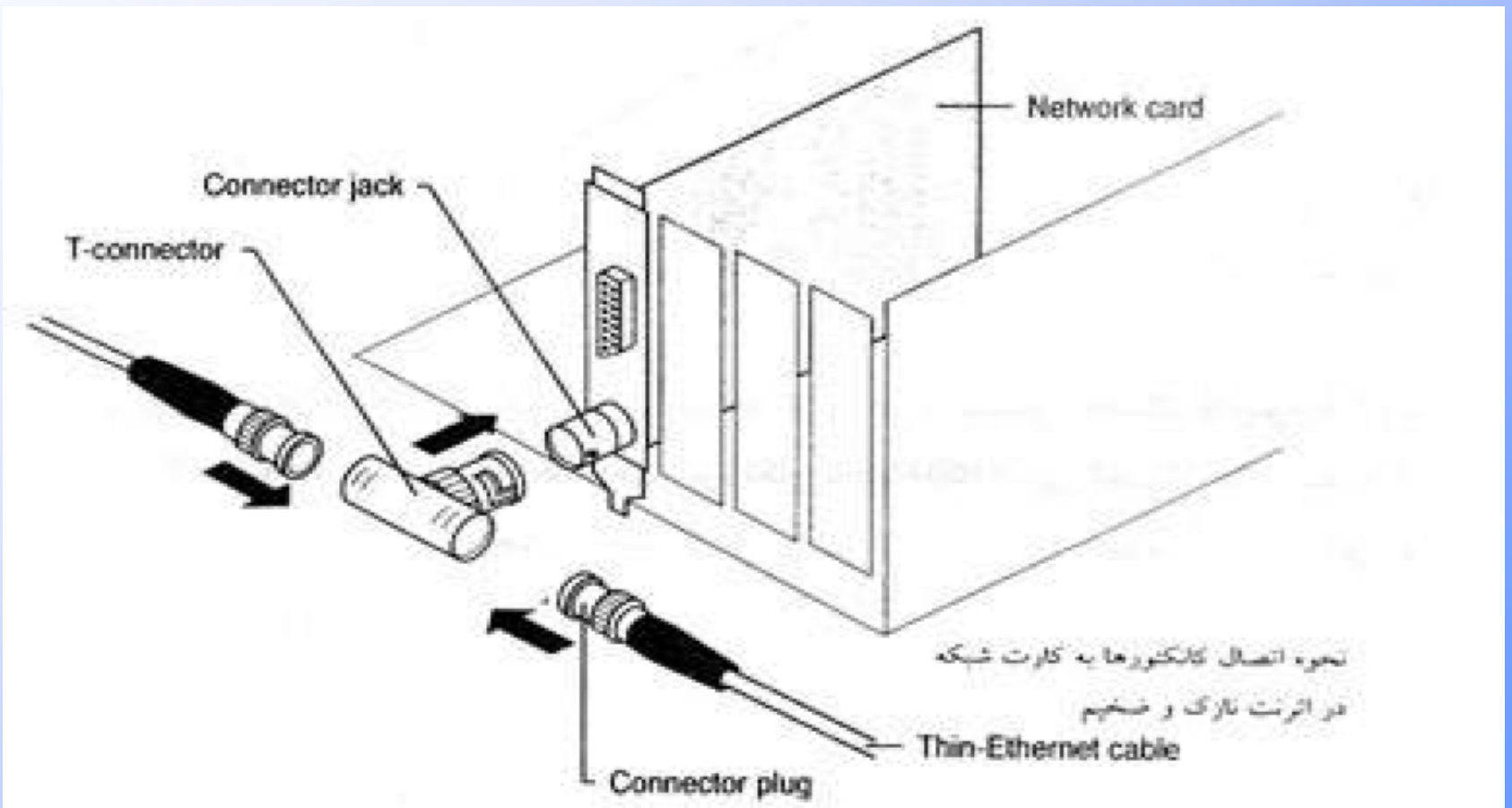
این کابل به اترنت ضخیم شهرت دارد و اتصال به کابل از طریق انشعاب تزریقی (Vampire Tap) انجام می‌شود که در آن یک سوزن به دقت در مرکز کابل کواکسیال فرو می‌رود.



10Base2

این نوع از کابل کشی، اترنت نازک نامیده می‌شود و برای اتصال به این نوع کابل به جای انشعاب تزریقی از کانکتورهای BNC معمولی و ایجاد یک اتصال بشکل T استفاده می کنند.





نحوه اتصال کانکتورها به کارت شبکه
در اترنت نازک و ضخیم

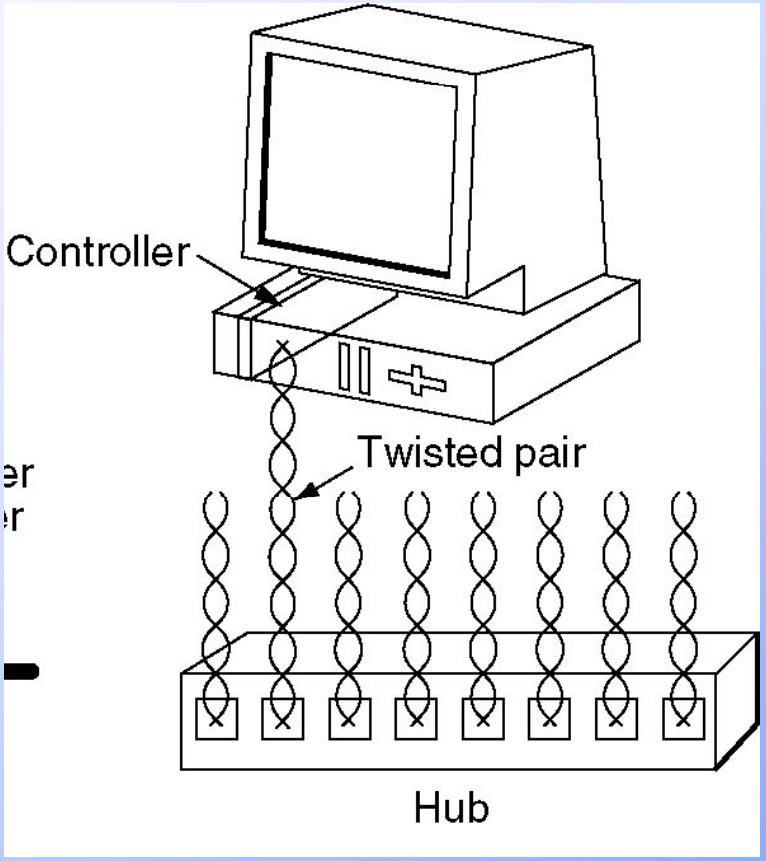
مشکلات کابل کشی 10Base2 & 10Base5

- ✓ طول بیش از اندازه کابل
- ✓ انشعابات نامناسب و بد
- ✓ شل شدن اتصالات
- ✓ بروز هرگونه پارگی در کابل

برای تشخیص معایب فوق تکنیک هائی ابداع شد ⟵ تکنیک بازتاب سنجی در حوزه زمان
(Time Domain Reflectometry)

10Base-T

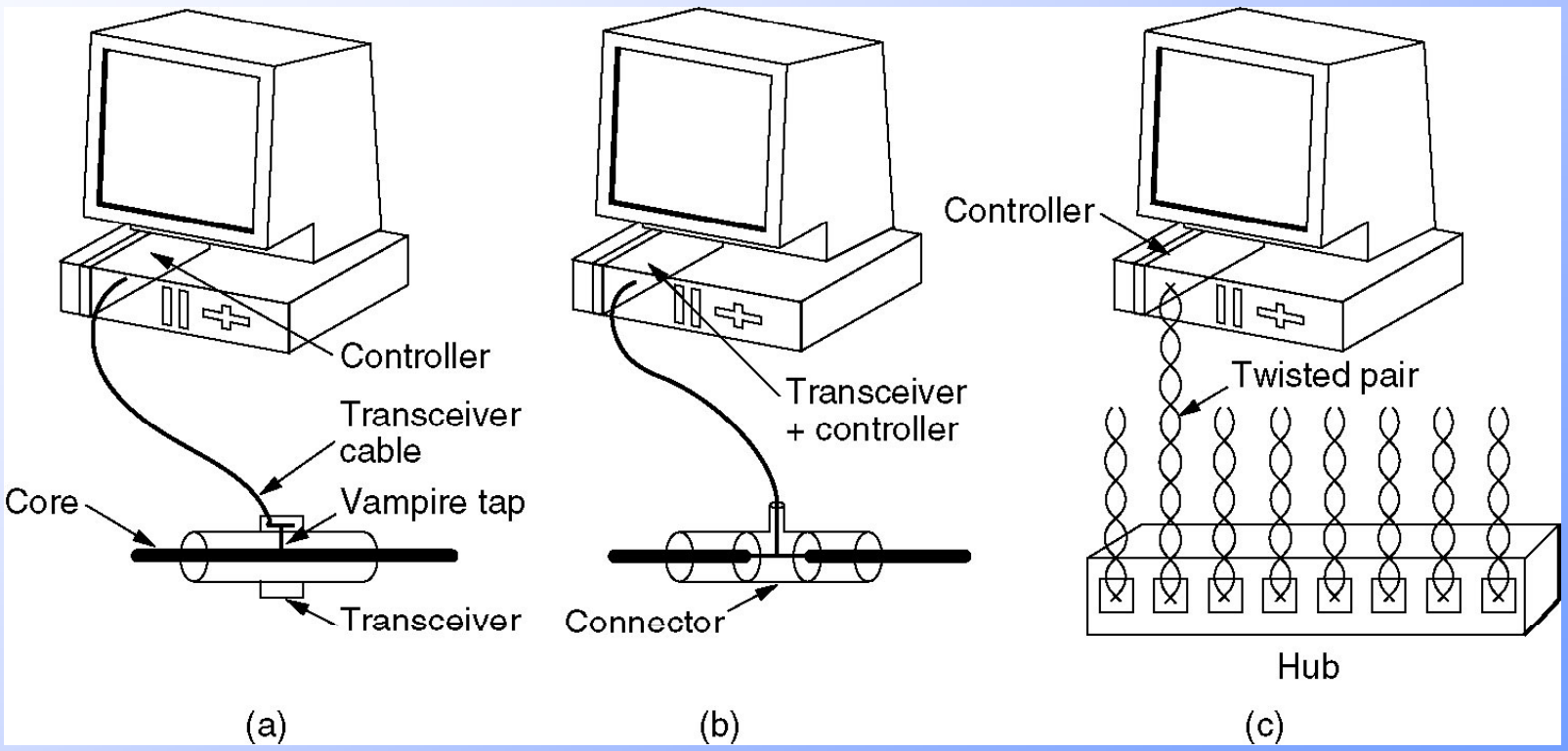
در ساختار آن هیچ کابل مشترکی وجود ندارد بلکه فقط یک Hub(جعبه‌ای پر از مدارات الکترونیک) وجود دارد که تمام ایستگاه ها با یک کابل اختصاصی (غیر مشترک) بدان متصل می‌شود.



10Base-F

در آن از فیبرهای نوری استفاده شده است ولی به دلیل هزینه بالای اتصالات و پایانه‌های مورد نیاز بسیار گران است اما به دلیل ایمنی بسیار بالائی که در مقابل نویز دارد ،گزینه مناسبی برای کابل‌کشی بین ساختمان ها و یا هاب های دور از هم محسوب می‌شود.

مقایسه انواع کابل کشی های اترنت



سه روش کابل کشی اترنت : **10 Base5 (a)** **10Base2 (b)** **10Base-T (c)**

کدینگ منچستر

روشی که در آن گیرنده قادر خواهد بود تا شروع و پایان یا وسط هر بیت را بدون نیاز به یک سیگنال ساعت خارجی تشخیص دهد. (همزمانی بین فرستنده و گیرنده)

در این روش هر بیت به لحاظ زمانی به دو نیم بیت تقسیم می‌شود: برای ارسال بیت ۱، در نیم بیت اول ولتاژ بالا و در نیم بیت دوم ولتاژ پایین قرار داده می‌شود و در مورد بیت ۰ به صورت عکس عمل می‌کند.

در اترنت از کدینگ منچستر استفاده می شود.

اشکال این روش :

چون طول هر پالس نصف طول یک بیت است به همین دلیل به پهنای باند دو برابر نیاز خواهد بود. (یعنی برای هر بیت دو پالس ارسال می شود.)

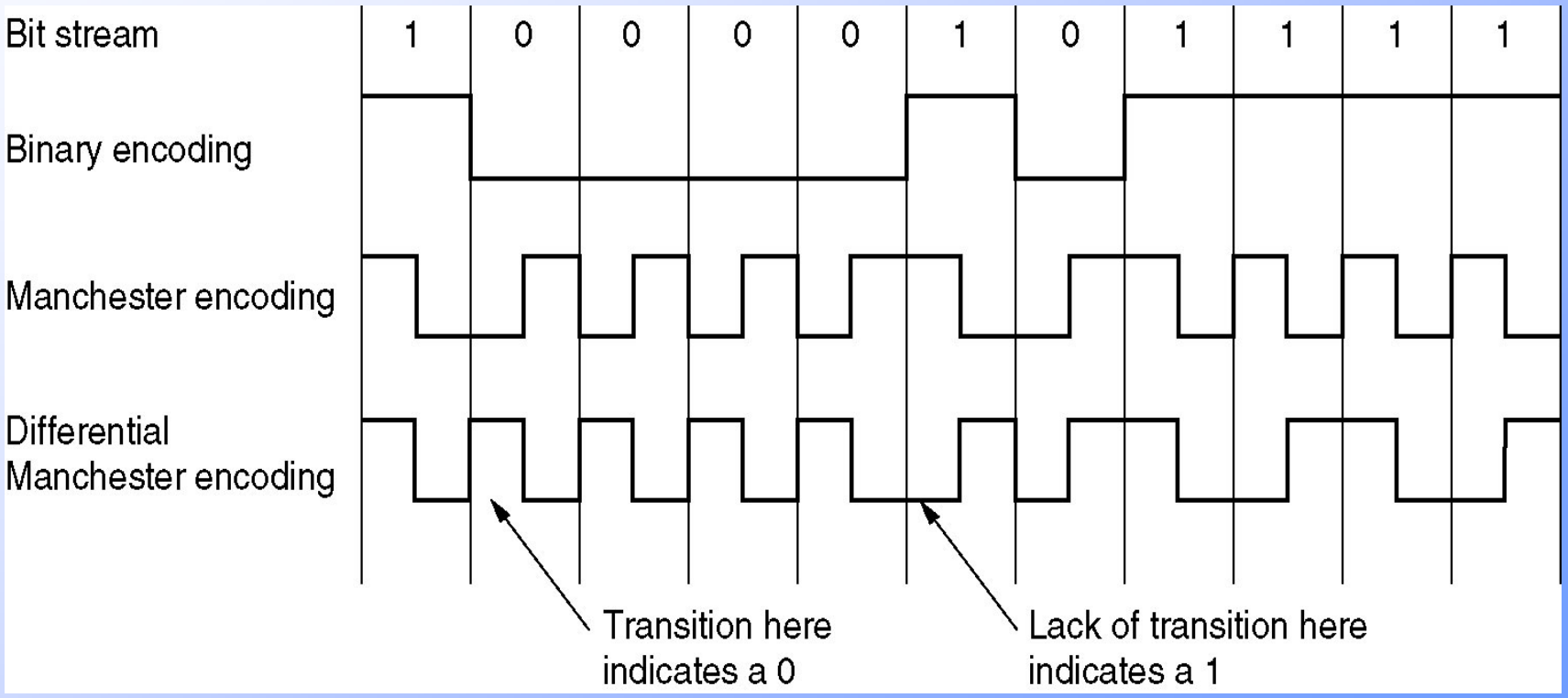
کدینگ منچستر تفاضلی

در این روش عدم وجود لبه در ابتدای هر بیت نشان دهنده بیت ۱ و وجود لبه در ابتدای هر بیت نشان دهنده بیت ۰ می باشد.

روش منچستر تفاضلی به ابزارهای پیچیده‌تری نسبت به کدینگ منچستر نیازمند است ولی در عوض ایمنی بیشتری در مقابل نویز از خود نشان می‌دهد.

این روش در شبکه اترنت استفاده نمی شود و در شبکه های محلی دیگر همچون Token Ring (IEEE 802.5) کاربرد دارد.

مقایسه انواع روش های کدینگ



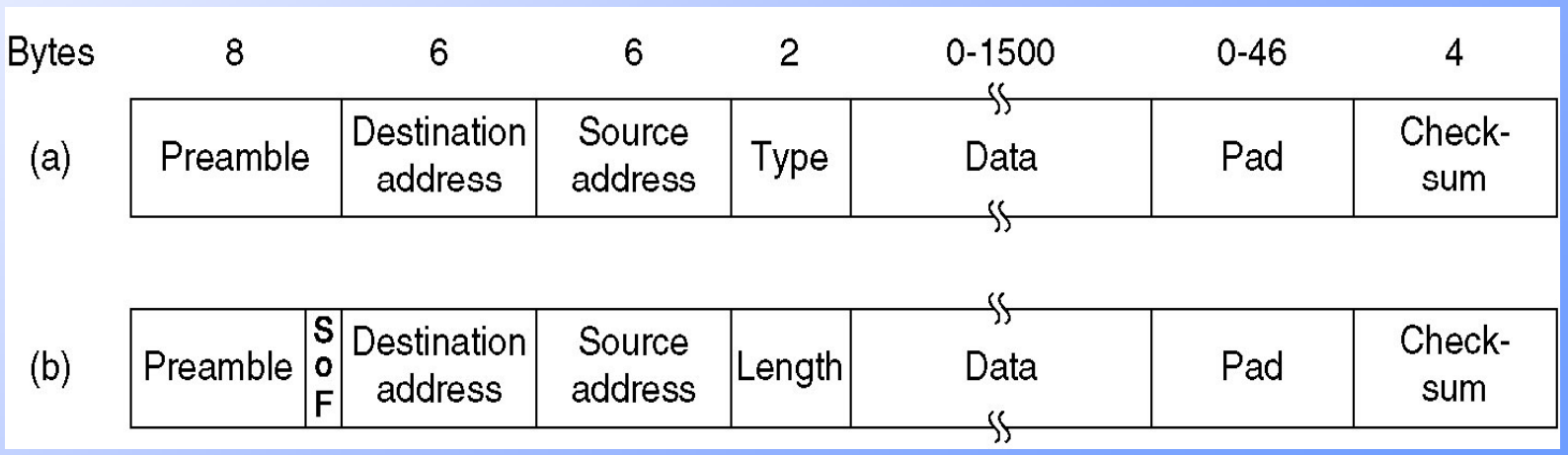
کدینگ باینری معمولی، کدینگ منچستر و کدینگ منچستر تفاضلی

قالب فریم اترنت

دو تفاوت قالب استاندارد IEEE 802.3 و DIX عبارتند از :

1) در قالب فریم استاندارد IEEE 802.3 بایت هشتم Preamble به عنوان بایت مشخص‌کننده ابتدای فریم درنظر گرفته می‌شود.

2) در قالب فریم استاندارد IEEE 802.3 به جای تخصیص دو بایت برای فیلد نوع، دو بایت برای فیلد طول در نظر گرفته شده است.



Frame formats : (a) DIX Ethernet (b) IEEE 802.3

اترنت سریع و اترنت گیگابیت

دلایل سرعت بخشیدن به شبکه 802.3 بدون تغییر در ساختار آن:

1. نیاز به سازگاری شبکه جدید با شبکه‌های اترنت موجود.
2. نگرانی از آنکه پروتکل جدید مشکلات پیش‌بینی نشده داشته باشد.
3. تمایل به آنکه قبل از تغییر تکنولوژی بتوانند کار را به اتمام رسانده و مشمول زمان نشود.

اترنت سریع

ایده اصلی اترنت سریع ← حفظ تمام ویژگی های اترنت اولیه

کاهش زمان بیتی از 100 ns به 10 ns (۱۰ برابر کردن سرعت)

این استاندارد جدید که به اترنت سریع معروف شد 802.3u نام گرفت.

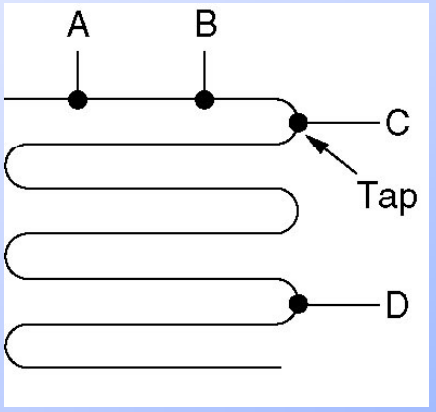
انواع کابل کشی اترنت سریع

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

اترنت گیگابیت

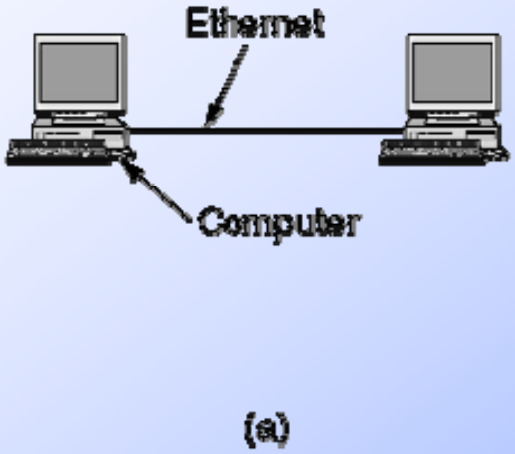
پس از مدت کوتاهی ، اترنت گیگابیت با همان اهداف اترنت سریع و افزایش ۱۰ برابری سرعت با عنوان استاندارد 802.3z عرضه شد.

کل پیکربندی اترنت گیگابیت نقطه به نقطه است یعنی برخلاف اترنت معمولی که براساس ساختار باس چند اتصالی است.

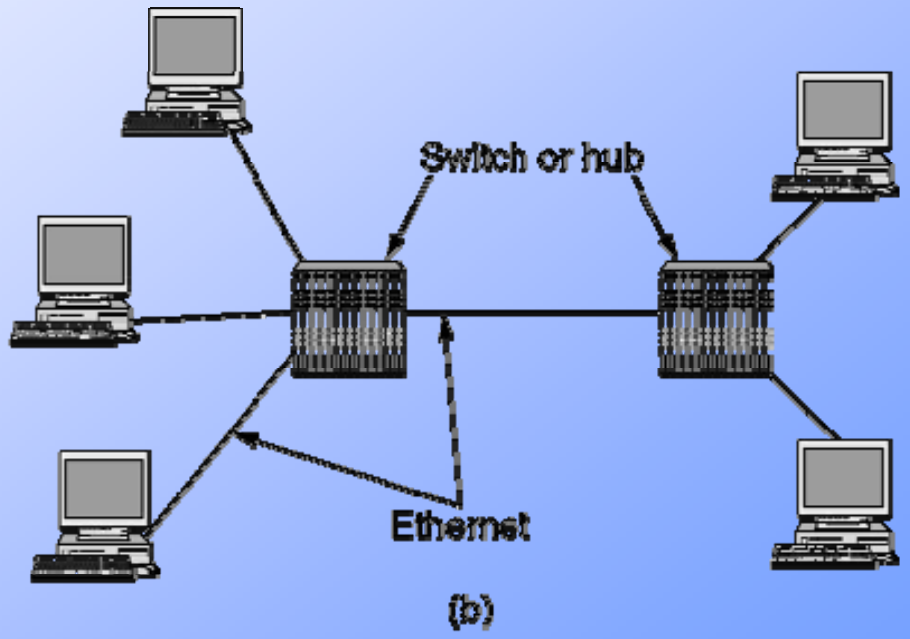


ساختار باس چند اتصالی

انواع پیکربندی اترنت گیگابیت



(a) اترنت گیگابیت با دو دستگاه



(b) اترنت گیگابیت با چند دستگاه

انواع کابل کشی اترنت گیگابیت

Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 μ) or multimode (50, 62.5 μ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

شبکه های بی سیم (Wireless Networking)

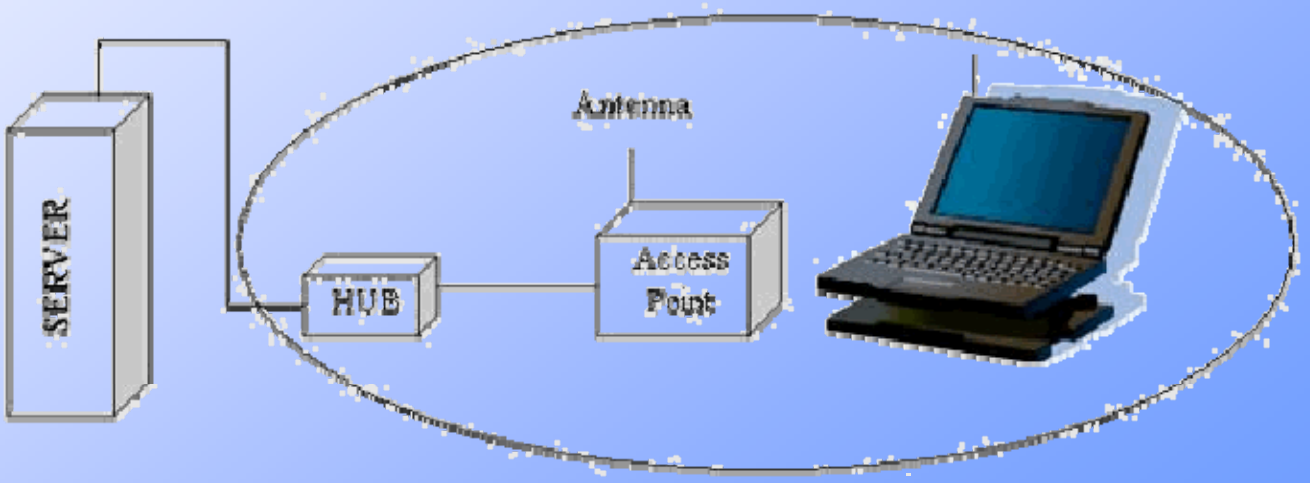
WLANها (شبکه های محلی بی‌سیم) که از امواج الکترومغناطیسی(رادیویی یا مادون قرمز) برای انتقال اطلاعات از یک نقطه به نقطه دیگر استفاده می‌کنند.

مفاهیم

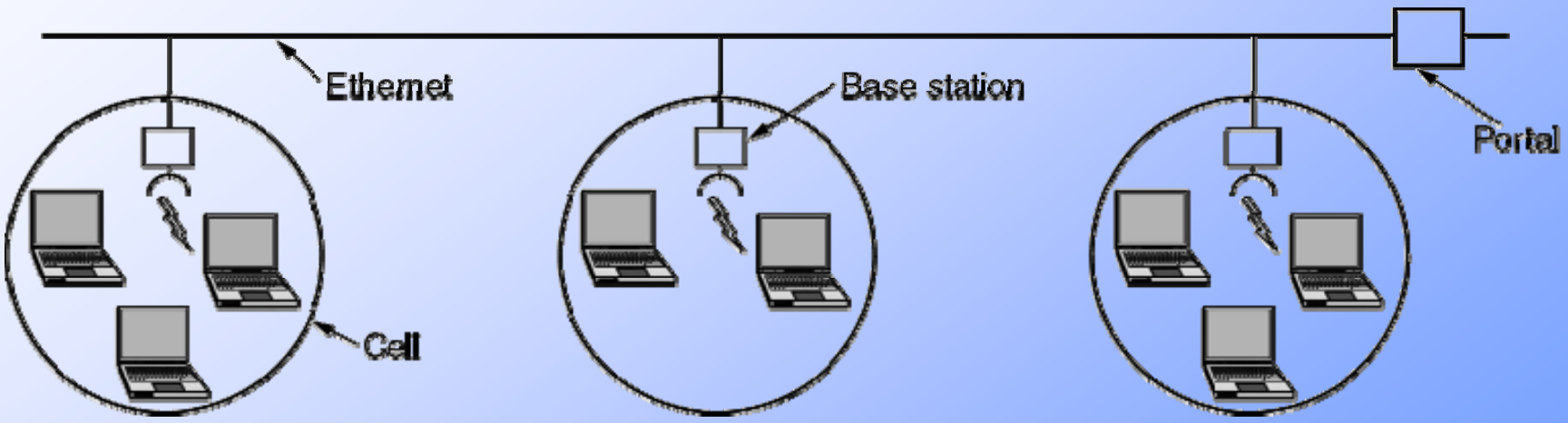
- Access Point(AP): دستگاه فرستنده و گیرنده مرکزی

گیرنده AP وظیفه دریافت، ذخیره و ارسال داده را بین شبکه محلی سیمی وWLAN بعهده دارد.

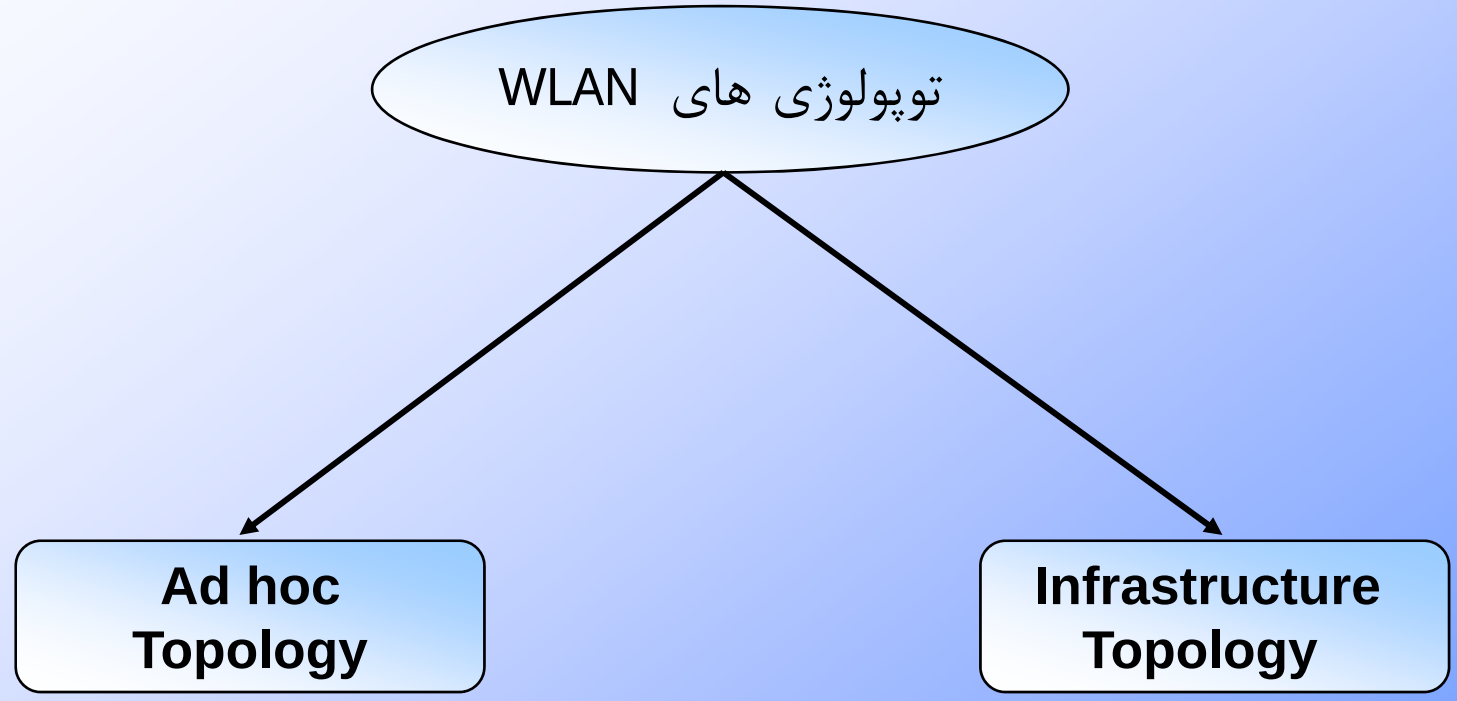
- استاندارد غالب در این شبکه‌ها IEEE 802.11 می‌باشد .



LANهای بی‌سیم



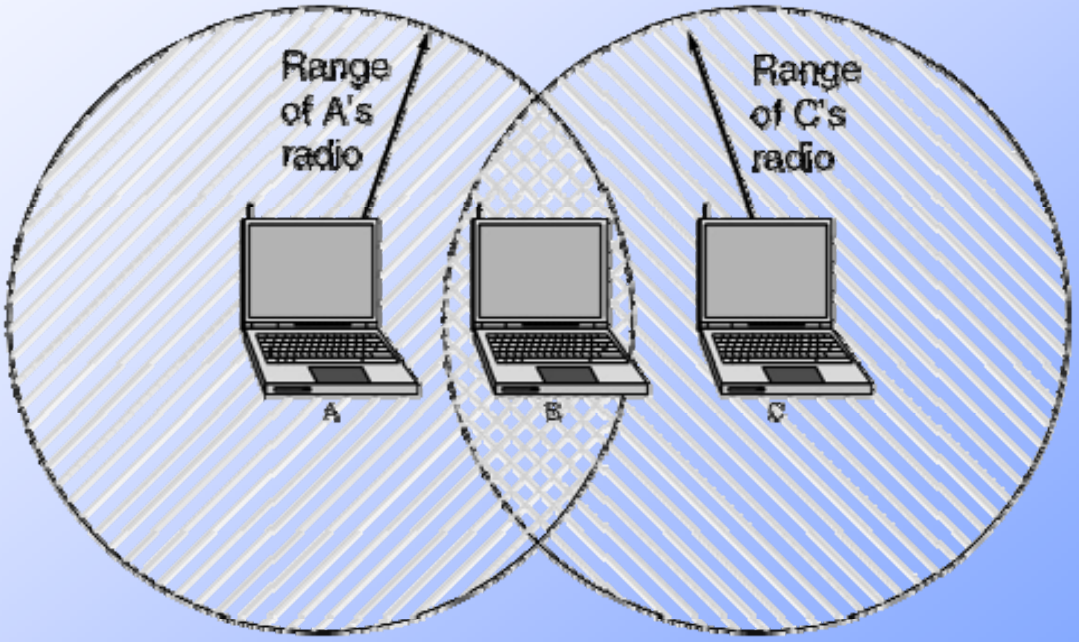
A multicell 802.11 network.


توپولوژی های WLAN
Ad hoc Topology
Infrastructure Topology

۱) Ad hoc Topology

در این توپولوژی کامپیوترها به واسط شبکه بی‌سیم مجهز بوده و مستقیماً با یکدیگر به شکل peer- to- peer ارتباط برقرار می‌کنند.

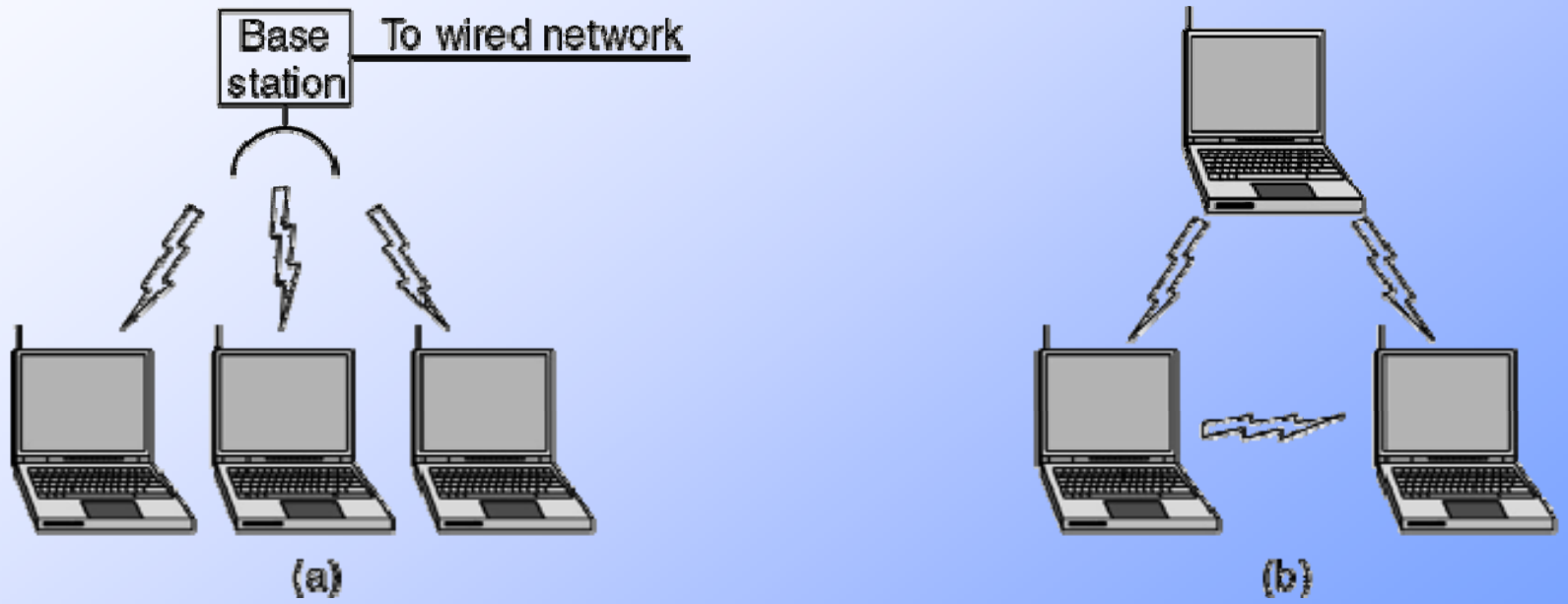
یعنی کامپیوترها برای برقراری ارتباط باید در محدوده یکدیگر قرار داشته باشند.



برد هیچیک از ایستگاه‌ها کل سیستم را پوشش نمی‌دهد.

۲) Infrastructure Topology

این توپولوژی برای گسترش و افزایش انعطاف‌پذیری شبکه‌های کابلی معمولی از طریق اتصال کامپیوترهای مجهز به تکنولوژی بی‌سیم با استفاده از Access Point به آن بکار می‌رود.



(a) Wireless networking with a base station.

(b) Ad hoc networking.

انواع سیگنال هایی که توسط استاندارد IEEE 802.11 در لایه فیزیکی پشتیبانی می‌شود:

- ✓ DSSS (Direct Sequence Spread Spectrum)
- ✓ FHSS (Frequency Hopping Spread Spectr)
- ✓ infrared (مادون قرمز)

DSSS (Direct Sequence Spread Spectrum)

یک روش انتقال رادیویی که در آن سیگنال‌های خروجی با استفاده از یک کد دیجیتال مدوله شده و استفاده از DSSS باعث افزایش سرعت انتقال سیستم تا ۱۱ مگابیت در ثانیه می‌شود.

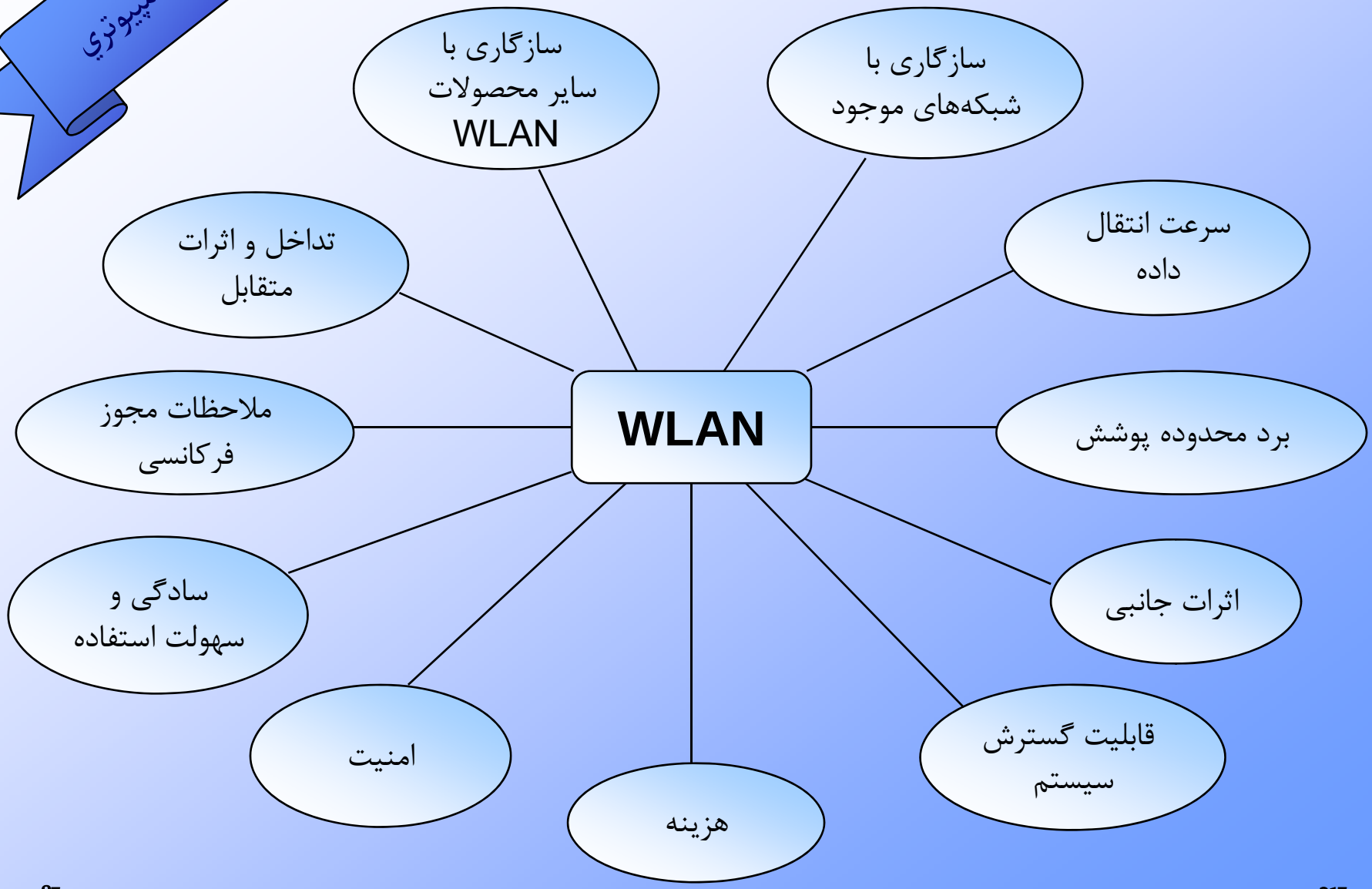
FHSS (Frequency Hopping Spread Spectrum)

روش دیگری که در آن انتقال دهنده به طور مداوم تغییرات سریعی را در فرکانس انجام می‌دهد. دریافت کننده برای خواندن سیگنال‌های دریافتی، دقیقاً همان تغییرات را اعمال می‌کند. این روش تنها استاندارد IEEE802.11a را پوشش می‌دهد.

infrared (مادون قرمز)

در ارتباطات infrared از فرکانس های بالا استفاده می‌شود. در فناوری مادون قرمز ارسال کننده و دریافت کننده باید همانند یک کنترل کننده راه دور، در خط دید یکدیگر باشند.

پارامترهای مؤثر در انتخاب یک سیستم WLAN



تاریخچه بلوتوث

• فکر اولیه بلوتوث در شرکت موبایل اریکسون در سال ۱۹۹۴ شکل گرفت.

• کار مهندسی در سال ۱۹۹۵ شروع شد و فکر اولیه به فراتر از تلفن های همراه و گوشی‌های آنها توسعه یافت تا شامل همه انواع وسایل همراه شود.

• نام "بلوتوث" از نام یک پادشاه دانمارکی گرفته شده است که بین سال های ۹۴۰ و ۹۸۱ میلادی می‌زیست. به طور صلح‌آمیز، دانمارک، سوئد جنوبی و نروژ شمالی را متحد کرد. از آنجایی که این کار به او شهرت یک پادشاه ماهر در ارتباط و مذاکره را در تاریخ داد ، اریکسون نیز امیدوار بود بتواند به طور صلح آمیز وسایل مختلف را متحد کند.

• اریکسون یک موافقت نامه با IBM، Intel، Nokia، Toshiba امضا کرد و گروه Bluetooth SIG را به وجود آورد.

بلوتوث چیست؟

بلوتوث یک رشتـه خصوصیت بی‌سیم است که ارتباطات کوتاه برد بین وسایل مجهز به تراشه‌های کوچک و اختصاصی بلوتوث را تعریف می‌کند و با این امکان قادر به ایجاد شبکه‌های کوچک شخصی یا PAN می‌باشد.

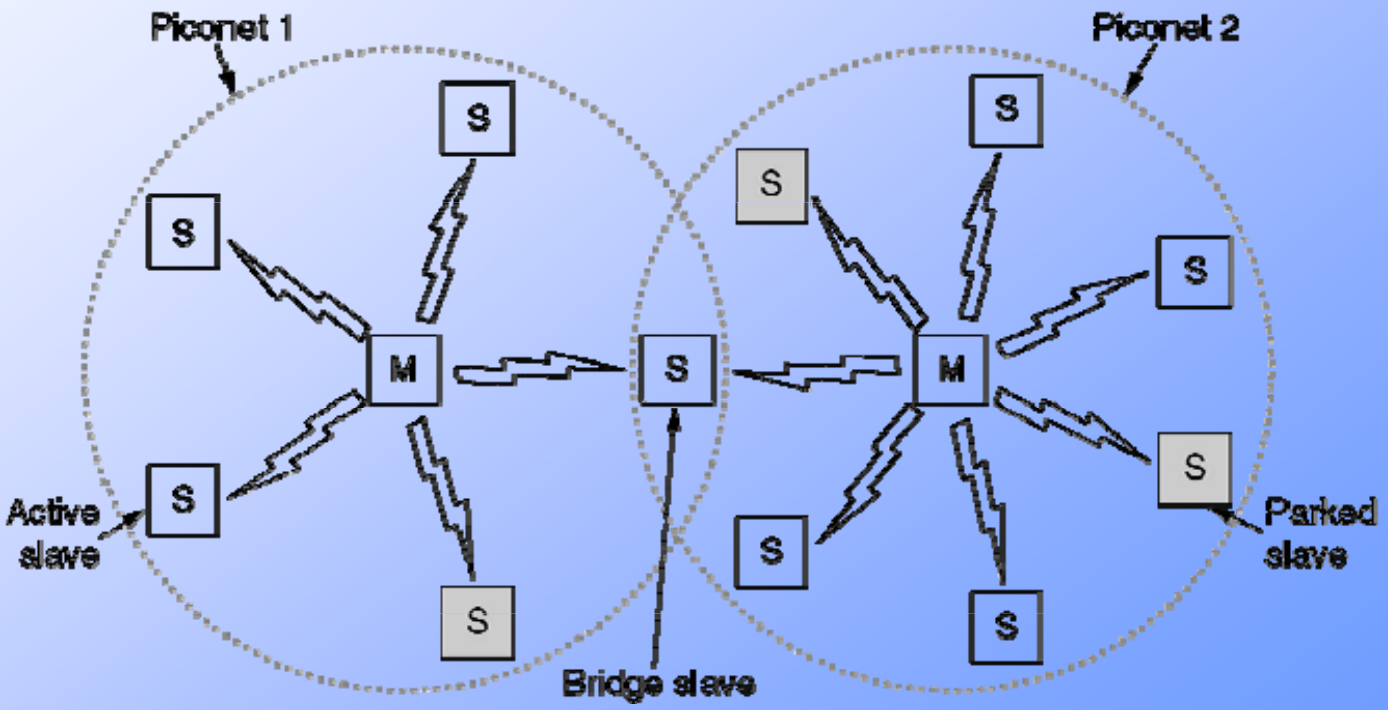
ساختار بلوتوث

- ✓ بلوتوث یک زبان مشترک بین وسایل مختلف بوجود می‌آورد.
- ✓ وسایل مجهز به تراشه‌های بلوتوث حدود ۱۰ متر برد دارند و می‌توانند داده‌ها در سرعت ۷۲۰ کیلوبیت در ثانیه از طریق دیوارها، کیف‌ها و پوشاک انتقال دهند.
- ✓ در بلوتوث از تکنیک FHSS استفاده می شود.(۱۶۰۰ جهش در ثانیه)
- ✓ در محدوده ۲.۴۰ GHZ تا ۲.۴۸ GHZ کار می کند. (باند فرکانسی 2.4 GHZ)
- ✓ پهنای باند آن به ۷۹ کانال ۱ MHZ تقسیم می شود.

معماری بلوتوث

Piconet : شامل یک master و حداکثر ۷ ایستگاه slave فعال است.

Scatternet : از اتصال چندین **Piconet** به هم ایجاد می‌شود.



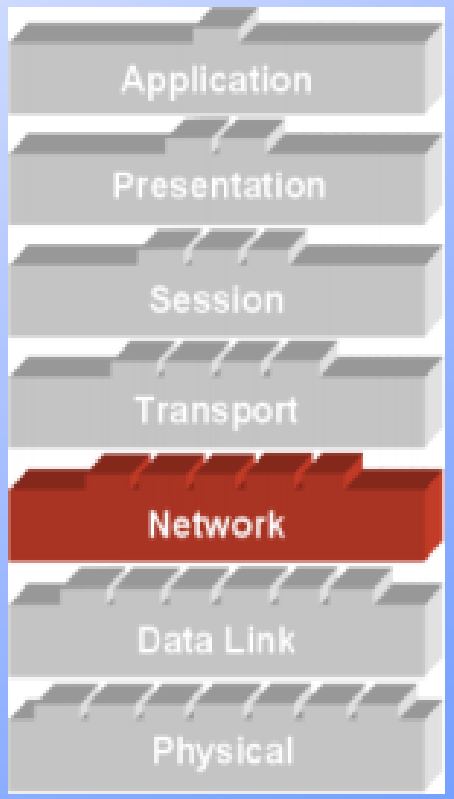
مزایای بلوتوث

دلایل استفاده ازبلوتوث :

- ✓ محدودیت انتقال Data از طریق سیم
- ✓ عدم وجود یک استاندارد مشخص و ثابت برای ارتباط دستگاه‌های مختلف با یکدیگر
- ✓جایگزین مناسب تکنولوژی مادون قرمز
- ✓ قیمت بسیار مناسب آن

فصل پنجم

لايه شبکه



لایه شبکه

هنگامی که بخواهیم بین LANهای مختلف ارتباط برقرار کنیم وظایف لایه شبکه شروع می‌شود.

هنگامیکه بسته‌های اطلاعاتی روی شبکه WAN 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 ، مسیریابی گفته می‌شود.

اصول طراحی لایه شبکه

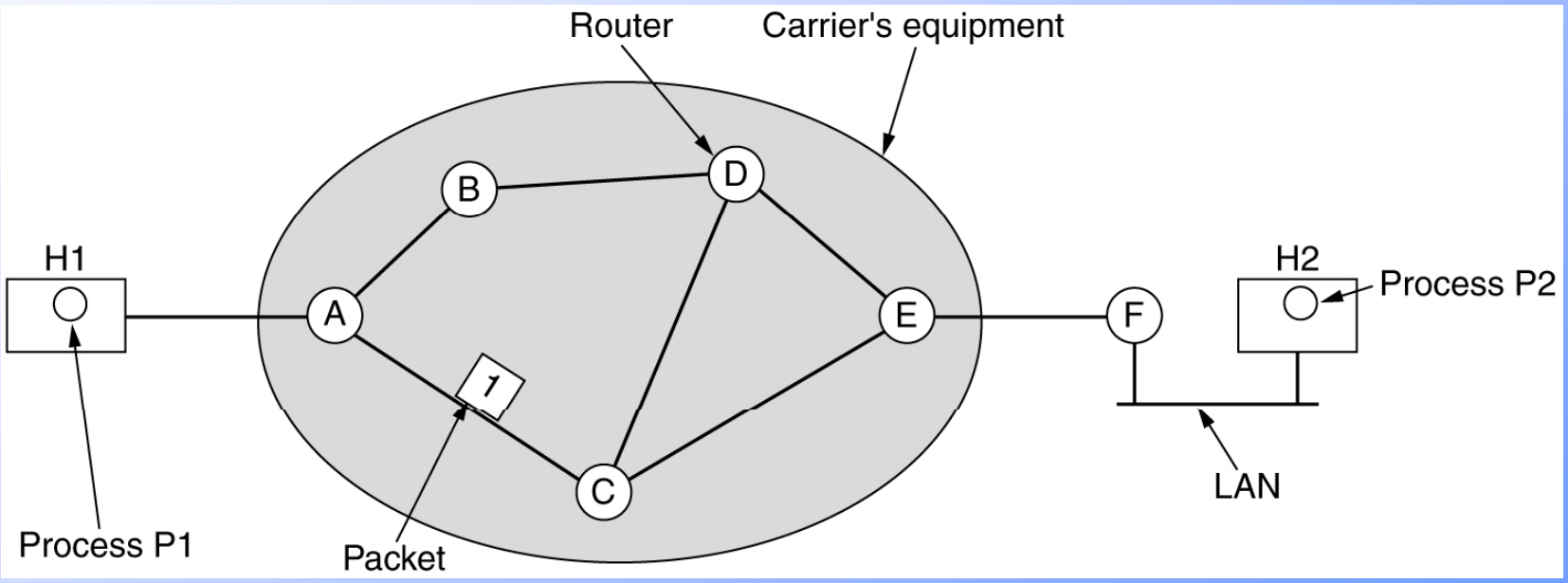
- سوئیچینگ بسته به روش store-and-forward
- خدمات تهیه شده برای لایه انتقال
- پیاده سازی خدمات اتصال گرا و غیراتصال گرا
- مقایسه زیرشبکه های داده گرام و مدارمجازی

الف) سوئیچینگ به روش ذخیره و ارسال

اجزاء اصلی این سیستم :

۱- تجهیزات حامل

۲- تجهیزات مشتریان



محیطی که پروتکل های لایه شبکه در آن عمل می کنند.

ب) خدمات تهیه شده برای لایه انتقال

اهدافی که این خدمات بر اساس آن ها تدارک دیده شده است :

۱- خدمات باید مستقل از تکنولوژی مسیریاب باشد .

۲- لایه انتقال باید از تعداد، نوع و توپولوژی مسیریاب های حاضر حمایت کند.

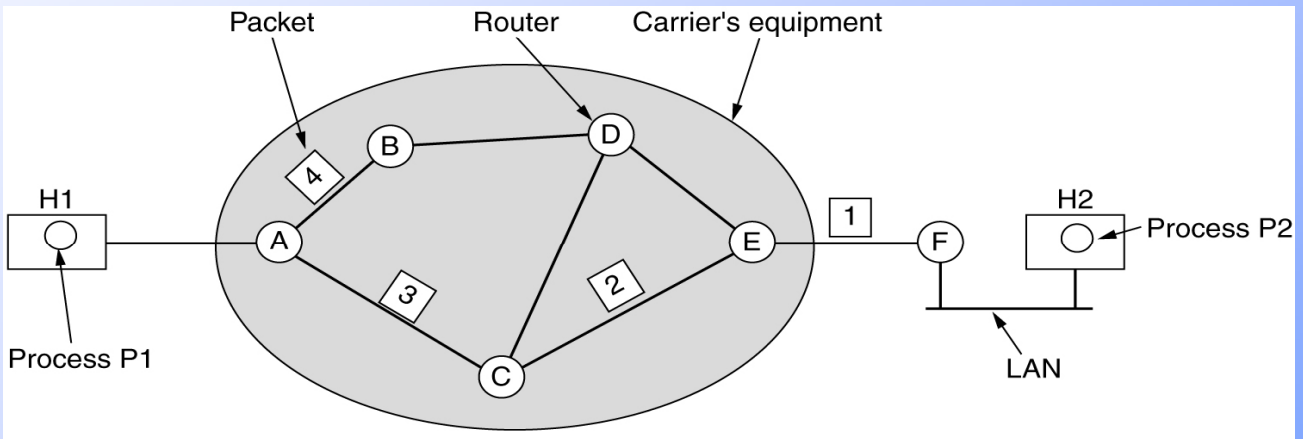
۳- آدرس های شبکه ای که برای لایه انتقال تهیه می شوند حتی در صورت وجود شبکه های محلی و گسترده باید از شماره گذاری یکنواختی استفاده کند.

ج) خدمات اتصال‌گرا و غیراتصال گرا

غیراتصال گرا :

اگر خدمات بدون اتصال باشد ، بسته ها جداگانه به شبکه وارد شده و جدا از یکدیگر و مستقلا" مسیریابی می شوند. بسته ها را داده گرام می نامند.

زیر شبکه مورد استفاده ، زیر شبکه داده گرام نامیده می شود.



A's table

Dest.	initially Line	later Line
A	–	–
B	B	B
C	C	C
D	B	B
E	C	B
F	C	B

C's table

Dest.	Line
A	A
B	A
C	–
D	D
E	E
F	E

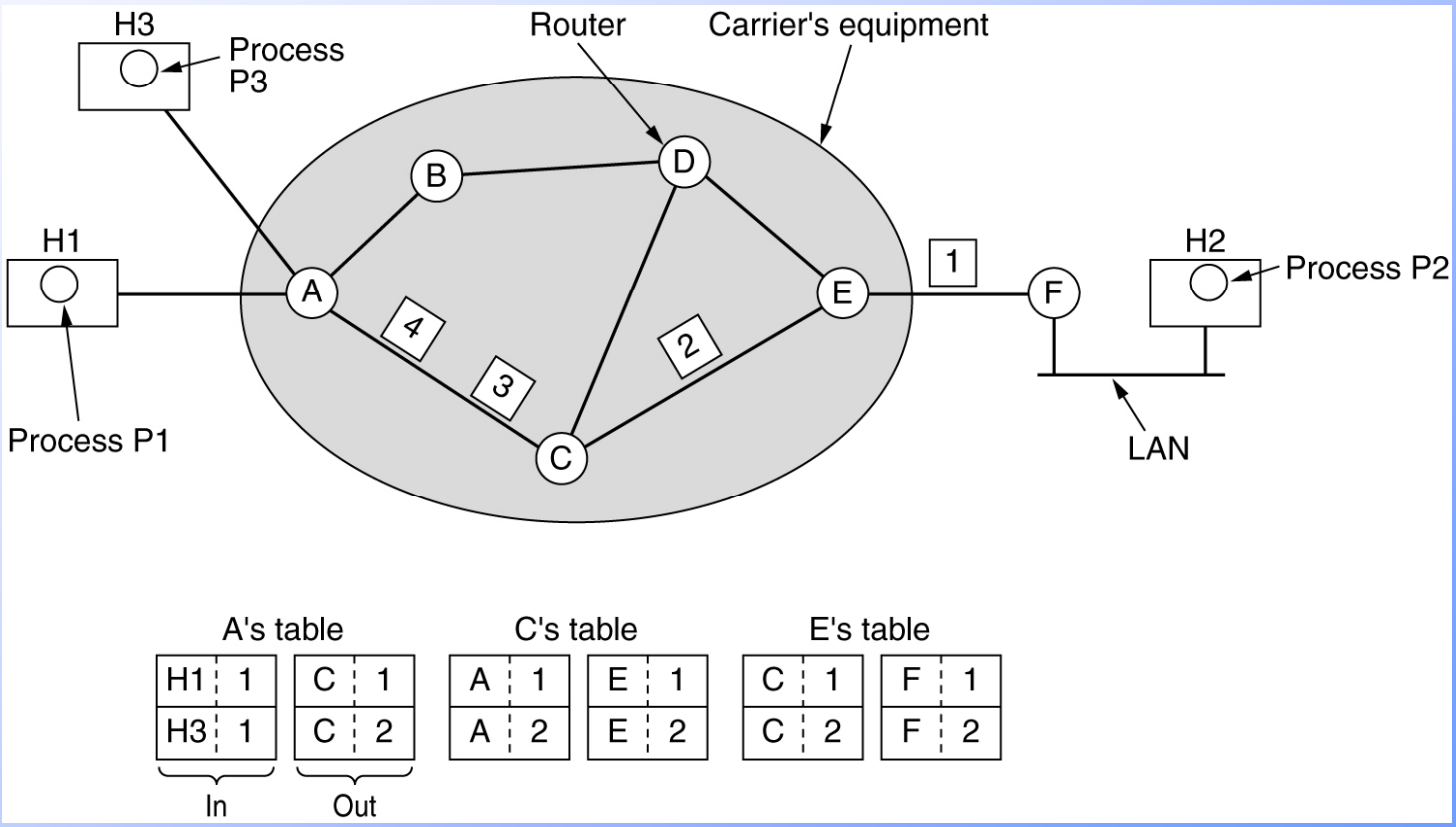
E's table

Dest.	Line
A	C
B	D
C	C
D	D
E	–
F	F

اتصال‌گرا :

یک مسیر از منبع به مقصد باید ایجاد شود قبل از آنکه بسته ها فرستاده شود. این اتصال مدار مجازی نامیده می شود.

زیر شبکه مورد استفاده ، زیر شبکه مدار مجازی نامیده می شود.



د) مقایسه زیرشبکه مدار مجازی و داده گرام

مورد	زیرشبکه داده گرام	زیر شبکه مدار مجازی
تنظیم مدار	نیازی نیست	نیاز است
آدرس دهی	هر بسته آدرس دقیق و کامل مبدا و مقصد را با خود حمل می‌کند	هر بسته فقط یک شماره کوتاه مدار مجازی(VC) با خود دارد
اطلاعات وضعیت	مسیریاب نیازی به نگهداری اطلاعاتی در خصوص وضعیت هر اتصال ندارد	به ازای هر مدار مجازی تمام مسیریاب ها باید اطلاعاتی در خصوص وضعیت آن نگاه دارند
مسیریابی	هر بسته بطور مستقل مسیریابی می‌شود	مسیر فقط یکبار و آنهم در هنگام تنظیم مدار مجازی انتخاب می‌شود و تمام بسته‌ها از همان مسیر حرکت می‌کنند
تاثیر خرابی مسیریاب	بی تاثیر، مگر در مورد بسته‌هایی که در حین خرابی از بین رفته‌اند	تمام مدارات مجازی که از مسیریاب خراب می‌گذشته‌اند قطع می‌شوند
تضمین کیفیت خدمات	دشوار	اگر برای هر مدار مجازی منابع لازم از قبل تخصیص یابد بسیار آسان است
کنترل ازدحام	دشوار	اگر برای هر مدار مجازی از قبل منابع لازم تخصیص یابد بسیار آسان است

مسیریابی

وظیفه اصلی لایه شبکه مسیریابی و هدایت بسته ها از منبع به مقصد مـی باشـد . در بیشتر زیر شبکه ها بسته ها برای آنکه به مقصد برسند نیاز دارند که چند پرش انجام دهند.

عبور یک بسته از یک مسیریاب را یک پرش (hop) گویند.

الگوریتم مسیریابی

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

فرآیندهای موجود در یک مسیریاب ← هدایت (Forwarding)

فرآیندهای موجود در یک مسیریاب ← الگوریتم مسیریابی

خواص یک الگوریتم مسیریابی

۱- صحت عملکرد

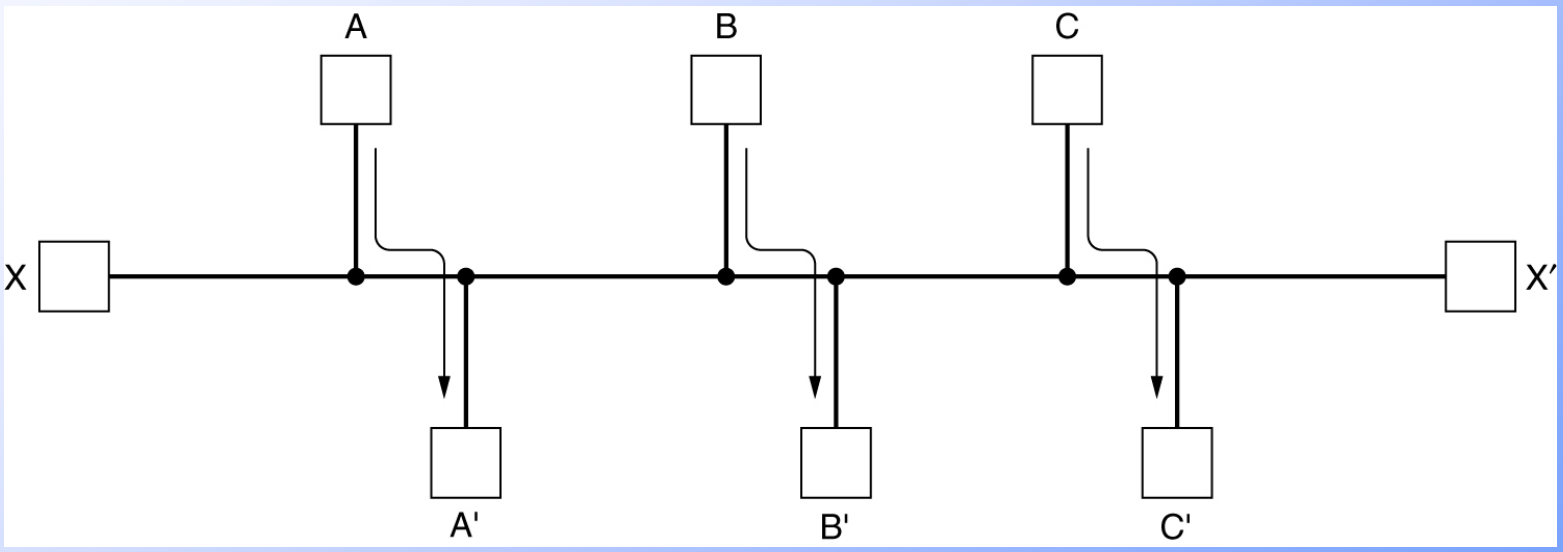
۲- سادگی یا سهولت

۳- تحمل عیب

۴- پایداری

۵- عدالت و بهینگی

تناقض بین عدالت و بهینگی



الگوریتم های مسیریابی به دو گروه کلی تقسیم می شوند :

الگوریتم های غیر وفقی:

تصمیمات مسیریابی خود را بر اندازه گیری یا تخمین توپولوژی و ترافیک فعلی بنا نمی نهند ، درعوض برای انتخاب یک مسیر مورد استفاده ، از قبل محاسبه و هنگامی که شبکه راه اندازی شد به شبکه بار می شود .

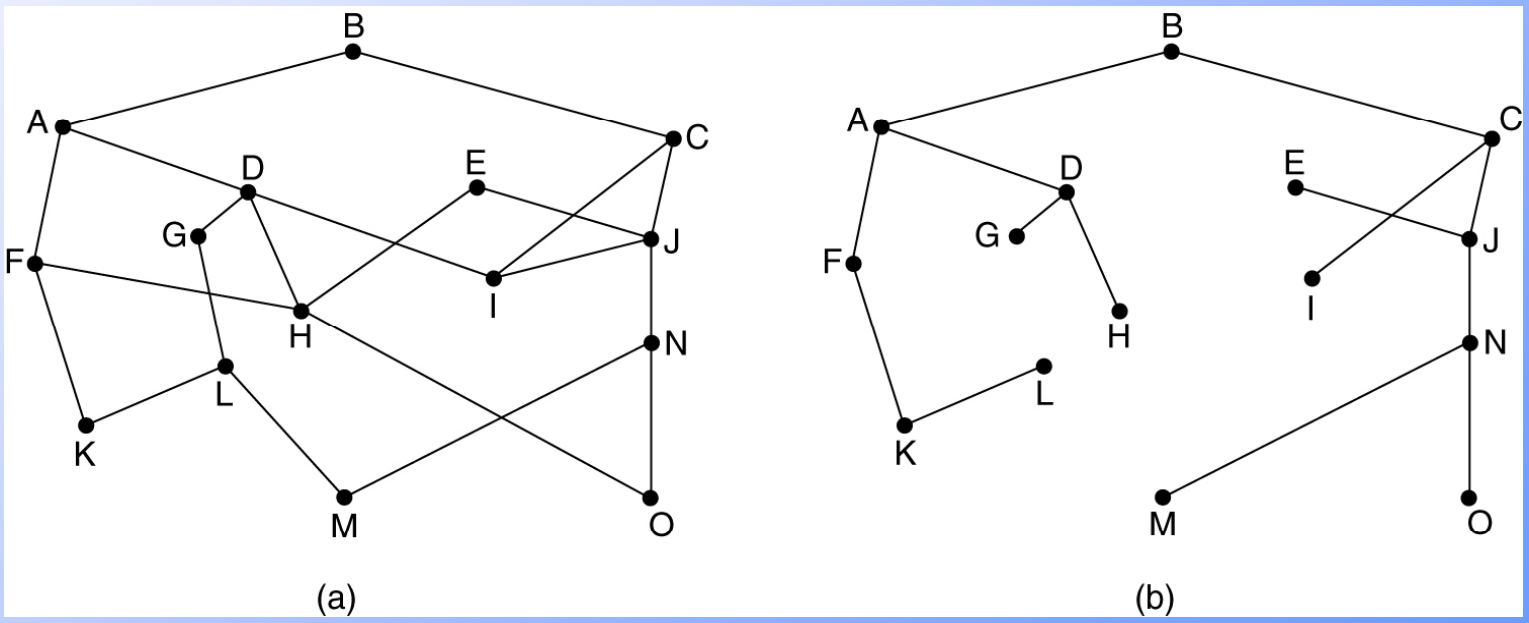
الگوریتم های وفقی:

الگوریتم وفقی تصمیمات مسیریابی خود را بر اساس تغییرات در توپولوژی و ترافیک تغییر می دهد .

اصل بهینگی

آن اصل بیان می کند که اگر مسیریاب J از مسیریاب I به مسیریاب K در مسیر بهینه ای قرارگیرد آنگاه مسیر بهینه ای از J به K نیز درهمان مسیر قرارمی 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 ، گره مقصد است. چنین درختی را sink tree می نامیم.



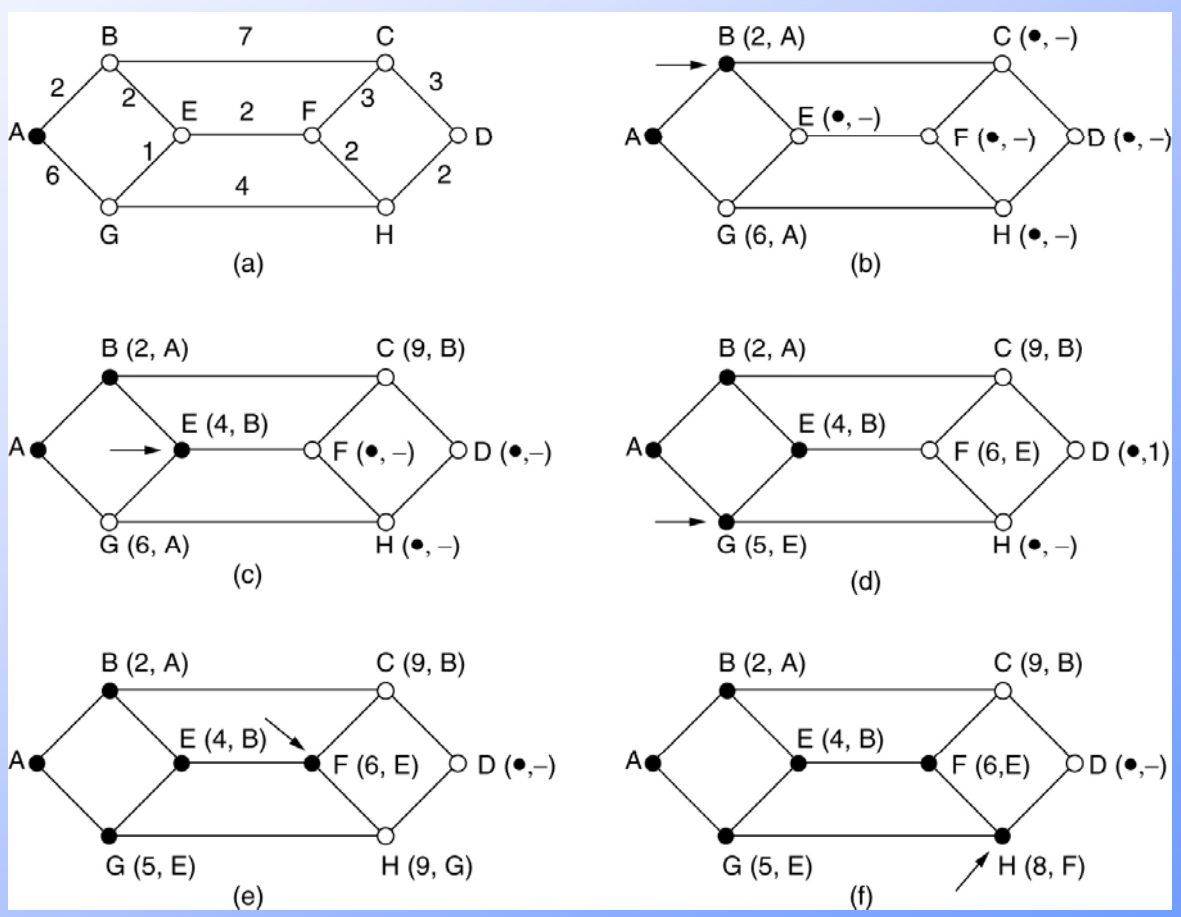
(a) یک زیر شبکه (b) درخت sink tree برای مسیریاب B

الگوریتم های مسیریابی

1) مسیریابی کوتاهترین مسیر
2) مسیریابی سیل‌آسا
3) مسیریابی بردار فاصله(DV)
4) مسیریابی حالت پیوند(LS)
5) مسیریابی سلسله مراتبی

۱) مسیریابی کوتاهترین مسیر

برای انتخاب مسیری بین دو مسیر یاب معین، الگوریتم فقط کوتاهترین مسیر بین آن ها را در گراف مشخص می کند.



۲) الگوریتم سیل‌آسا

در آن هر بسته ورودی بر روی خطوط خروجی بجز خطی که عمـل دریافـت از آن طریق صورت گرفته فرستاده می شود.

مزیت ⟵ انتخاب کوتاهترین مسیر(کمترین تاخیر)⟵ به عنوان الگو برای مقایسه

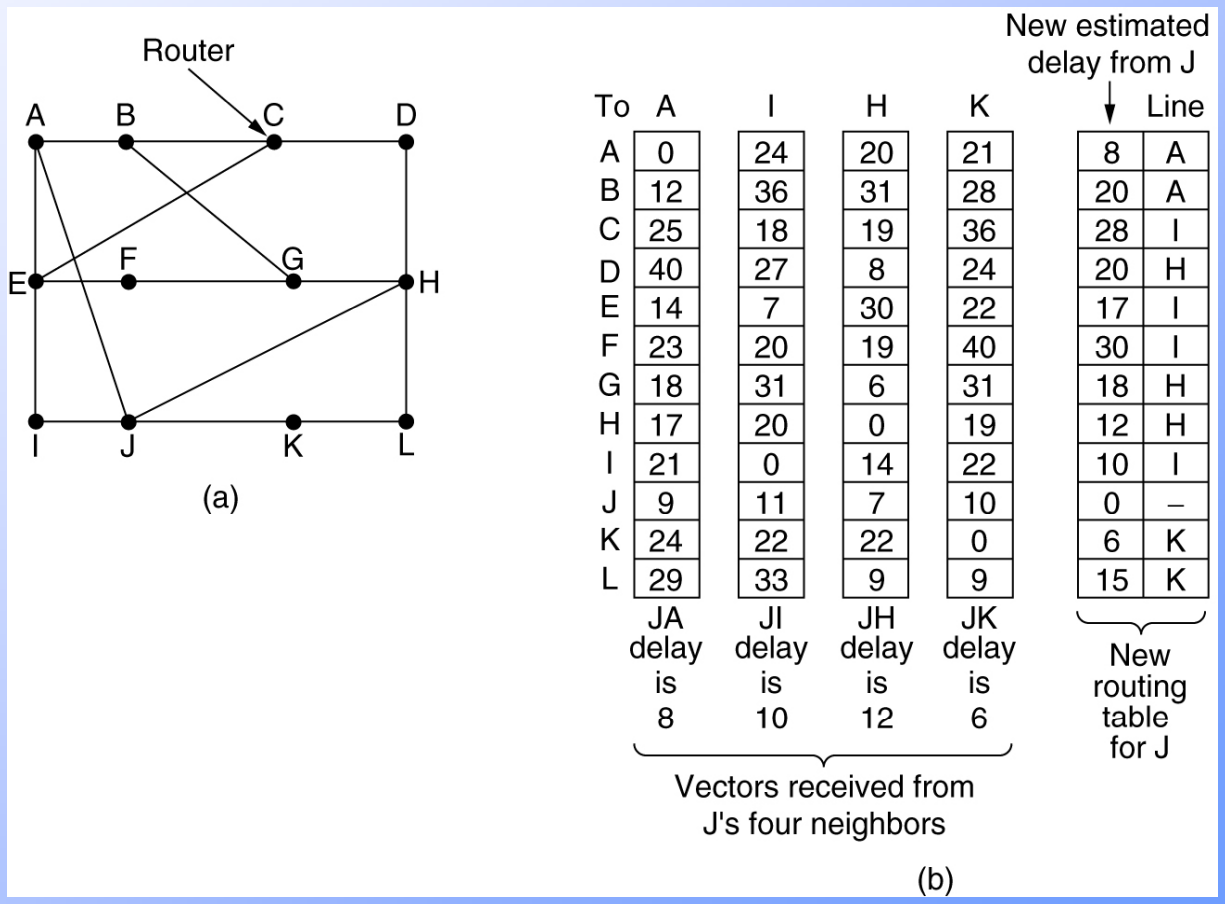
عیب ⟵ ترافیک بالا (بسته های تکراری زیاد)

راهکارهای جلوگیری از ترافیک زیاد :

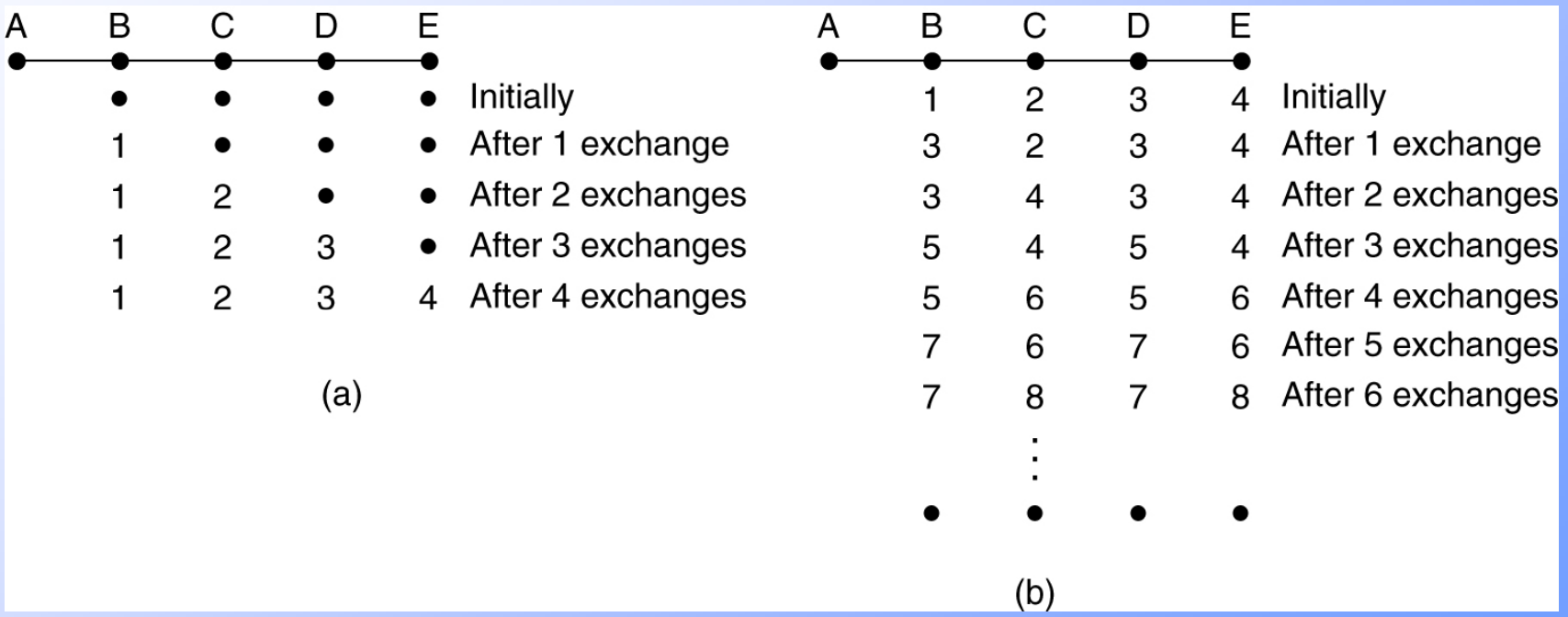
- قرار دادن شمارنده پرش در سرآیند هر بسته
- life time
- نگهداری اطلاعات هر بسته توسط مسیریاب

۳) الگوریتم مسیریابی بردار فاصله (DV)

نحوه عملکرد بدین ترتیب است که باعث می شود هر مسیریاب جدولی را که نشان دهنده بهترین فاصله به هر مقصد و خطی که برای رسیدن به آنجا نیاز است را به همراه داشته باشد . این جداول ، با تبادل اطلاعات با جداول همجوارشان نوسازی می شوند.



مشکل بینهایت گرائی(count-to-infinity problem):



۴) مسیریابی حالت پیوند (LS)

ایده مسیریابی حالت پیوند در پنج بخش بیان می شود . هر مسیریاب باید :

۱- همسایه هایش را تشخیص داده و آدرس های شبکه آن ها را بداند.

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

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

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

۵- کوتاهترین مسیر به هر مسیریاب دیگر را محاسبه کند.

الف) کسب اطلاعات همسایه ها :

- ارسال و دریافت بسته HELLO
- نام (آدرس) همسایه ها باید سراسری و منحصر به فرد باشد .

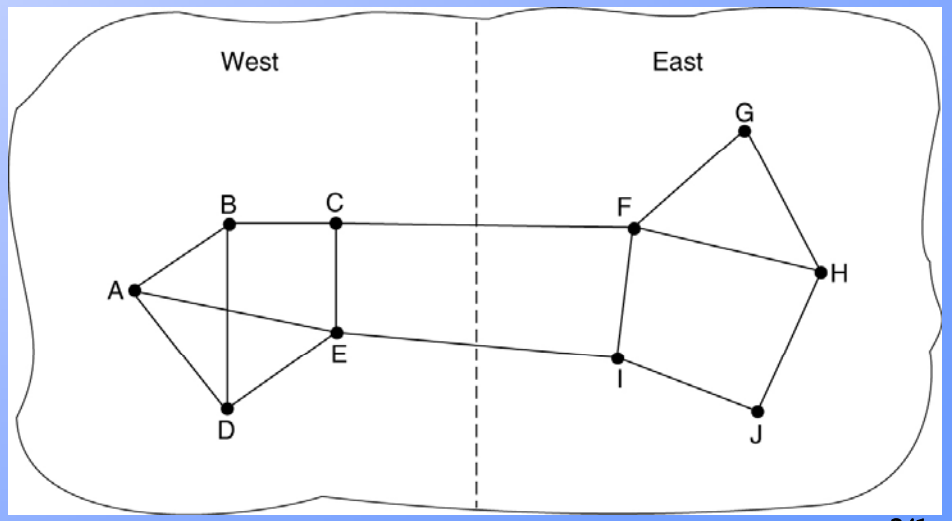
ب) اندازه گیری هزینه خط :

- ارسال و دریافت بسته ECHO
- در نظر گرفتن میزان بار در تاخیر به همراه پهنای باند خط ⟵ تغییرنوسانی جداول مسیریابی

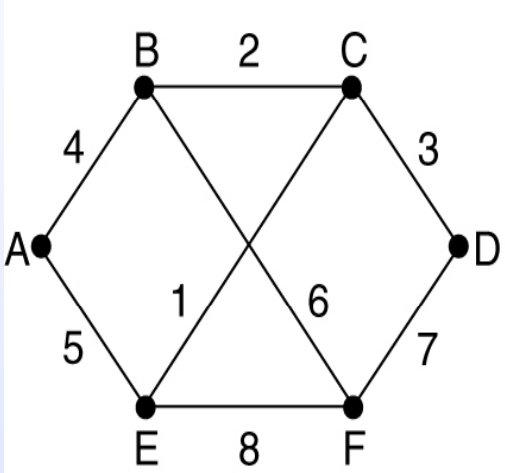
- جلوگیری از تغییرنوسانی جداول مسیریابی ⟵ فقط دخیل کردن پهنای باند
  توزیع بار بین خطوط علاوه بر در نظر گرفتن پهنای باند

↓

عدم استفاده مناسب از مسیر بهینه



ج) ساخت بسته های حالت پیوند :



(a)

	Link State Packets				
A	B	C	D	E	F
Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
Age	Age	Age	Age	Age	Age
B 4	A 4	B 2	C 3	A 5	B 6
E 5	C 2	D 3	F 7	C 1	D 7
	F 6	E 1		F 8	E 8

(b)

(a) A subnet. (b) The link state packets for this subnet.

د) توزیع بسته های حالت پیوند :

- استفاده از الگوریتم سیل آسا
- یک واحد افزایش شماره ترتیب بسته به ازای تولید هر بسته LS جدید.
- هر مسیریاب آدرس مسیریاب مبدا و شماره ترتیب بسته دریافتی را ذخیره می کند. وقتی یک بسته دریافت شد ، تکراری نبودن آن بوسیله مسیریاب چک شده و سپس ارسال می شود.

مشکلات این الگوریتم :

۱) صفر شدن شماره ترتیب در اثر چرخشی بودن آن ⟵ استفاده از شماره ترتیب ۳۲ بیتی

۲) صفر شدن شماره ترتیب در اثر از کار افتادن یک مسیریاب و راه اندازی مجدد آن

۳) خطادار شدن شماره ترتیب

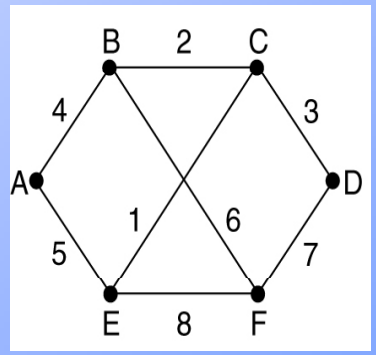
راه حل کلی ⟵ استفاده از طول عمر بسته (فیلد سن در بسته)

اصلاح الگوریتم جهت افزایش قدرت :

استفاده از فضای انتظار (بافر) ⟵ تشخیص بسته های تکراری

استفاده از بسته اعلام وصول (Ack) ⟵ پیشگیری از بروز خطا

			Send flags			ACK flags			
Source	Seq.	Age	A	C	F	A	C	F	Data
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	



The packet buffer for router B

ه) محاسبه مسیرهای جدید :

استفاده از الگوریتم دایکسترا

۵) مسیریابی سلسله مراتبی

✓با استفاده از مسیریابی سلسله مراتبی مسیریاب ها به قسمت هایی تقسیم می شوند که آن ها را منطقه (Region) می نامیم .

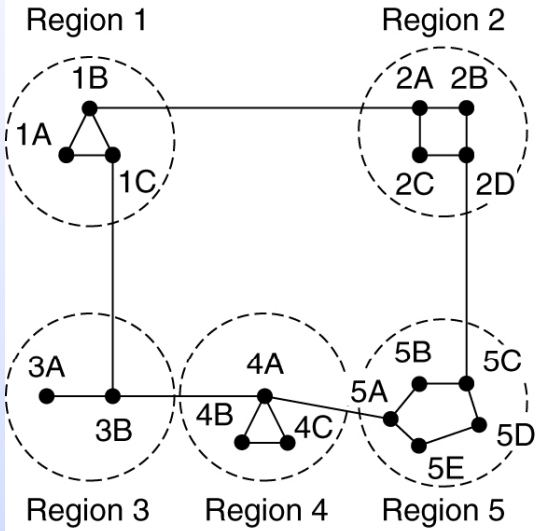
✓هر مسیریاب تمام جزئیات منطقه خود را درباره اینکه چطور بسته ها به مقصد ارسال می شود، می داند ولی از ساختار داخلی سایر مناطق خبر ندارد.

✓مهمترین هدف مسیریابی سلسله مراتبی ، صرفه جوئی در حافظه مورد نیاز برای جداول در مسیریاب است.

✓صرفه جوئی در حافظه ، موجب افزایش طول برخی مسیرها یعنی عدم بهینگی کامل مسیرها می شود ⟵ مسیر بهینه از 1A به 5C از منطقه ۲ می گذرد در حالیکه از منطقه ۳ عبور کرده است.

✓برای یک زیرشبکه با N مسیریاب ، بهترین تعداد سطوح سلسله مراتب برابر با Ln(N) است و هر مسیریاب جمعا" به e.Ln(N) درایه (Entry) نیاز خواهد داشت.

مسیریابی سلسله مراتبی دو سطحی با پنج منطقه



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

الگوریتم های کنترل ازدحام

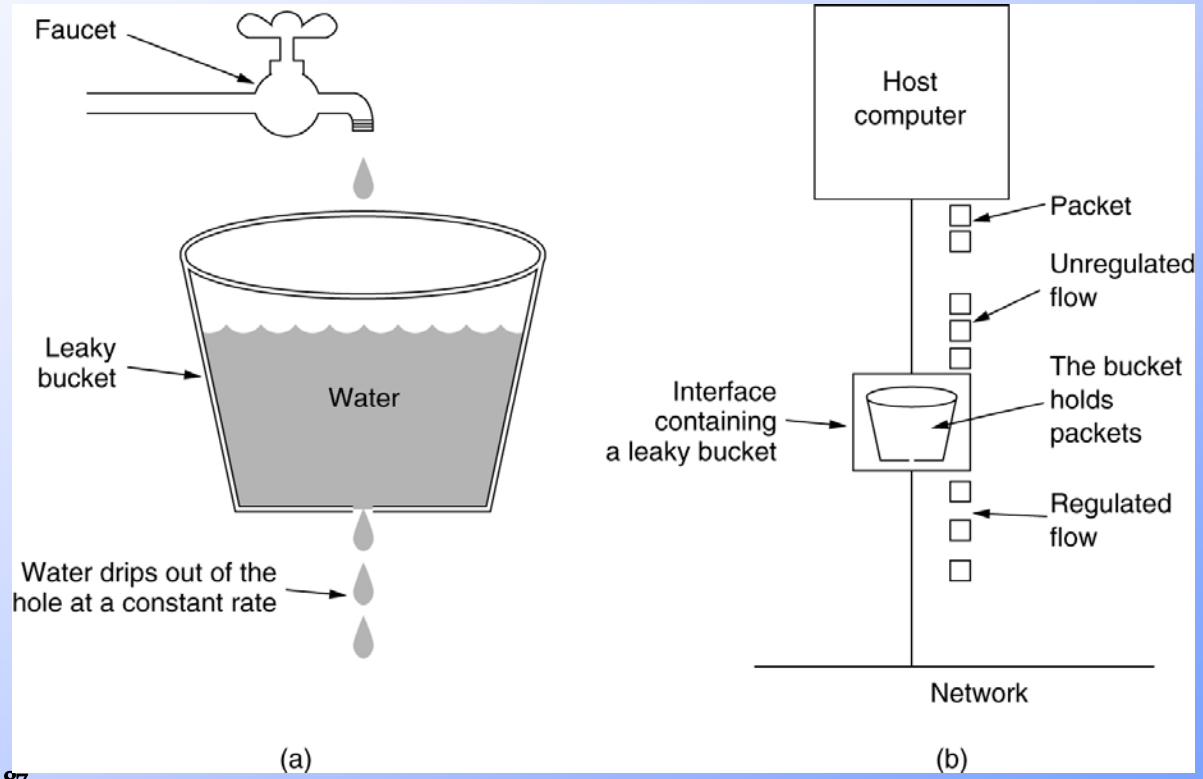
۱- الگوریتم سطل سوراخ دار

۲- الگوریتم سطل نشانه

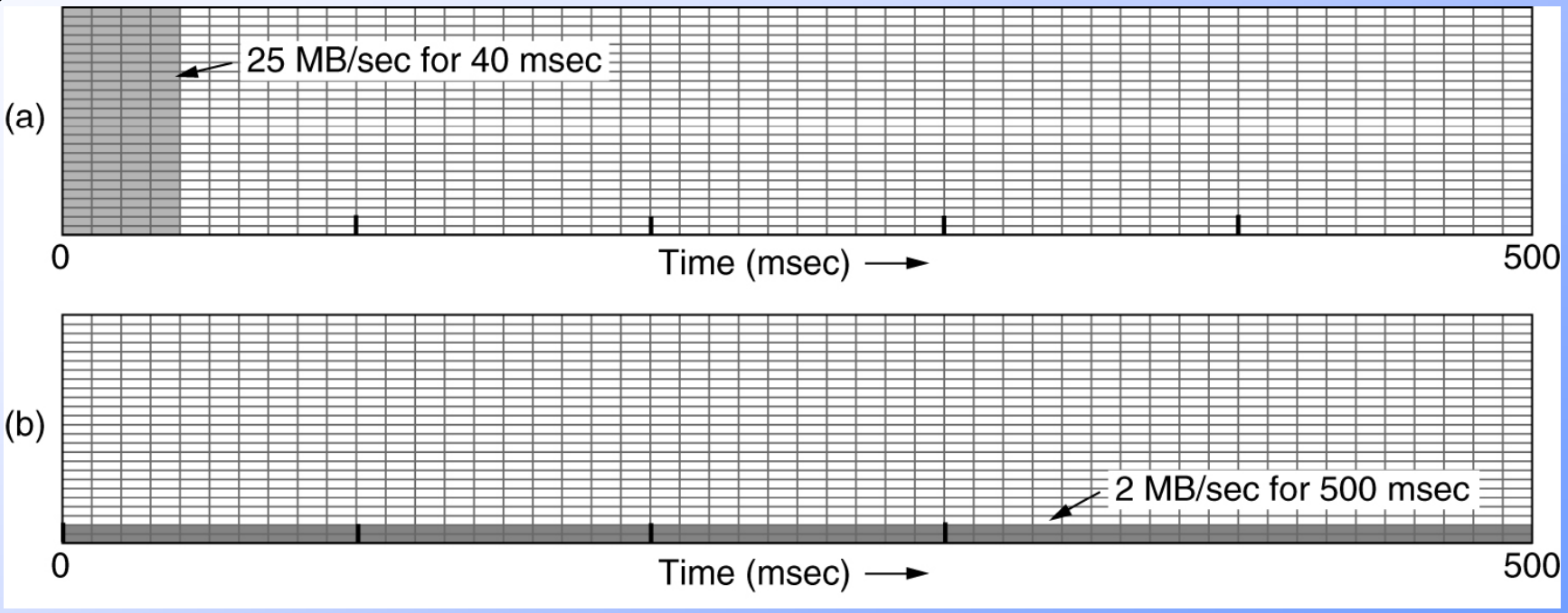
۱) الگوریتم سطل سوراخ دار

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

هر میزبان بوسیله رابطی که حاوی سطح سوراخ دار 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.



مثال برای حجم داده ۱ MB

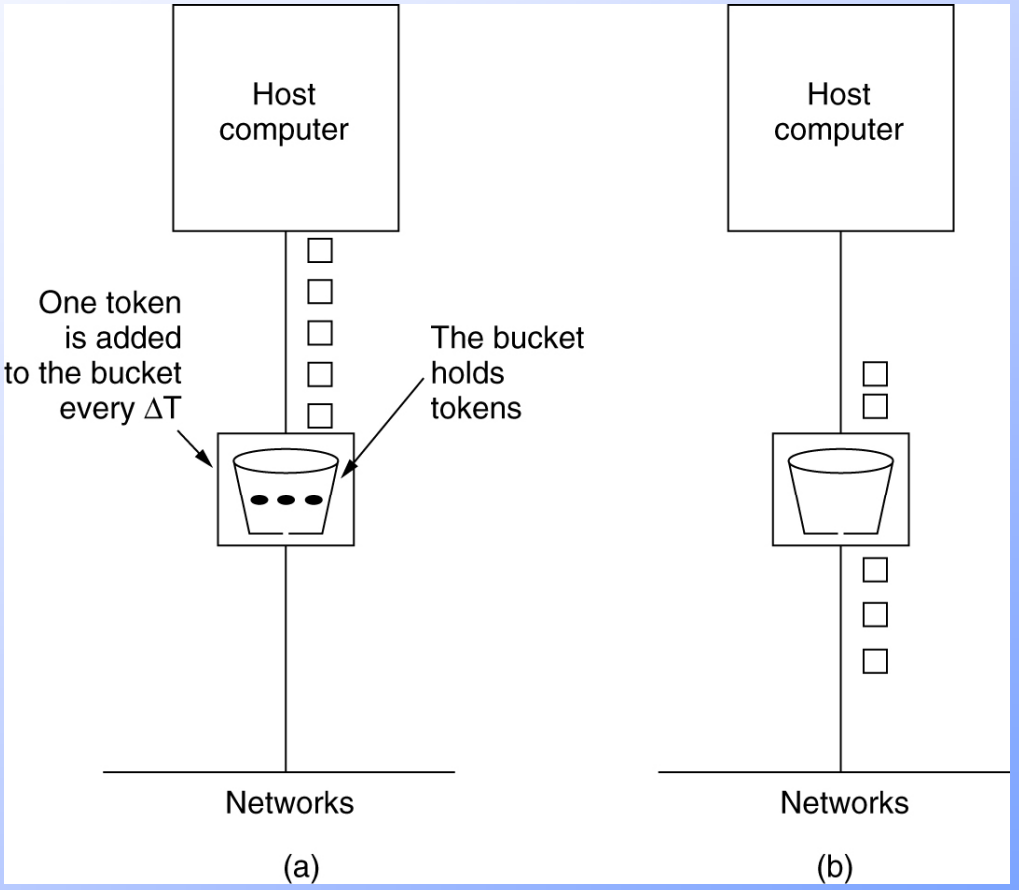


(a) ورودی سطل سوراخ دار
(b) خروجی سطل سوراخ دار

۲) الگوریتم سطل نشانه

در این الگوریتم ، سطل سوراخ دار ، نشانه ها را نگهداری می کند . این نشانه ها توسط یک ساعت با سرعت یک نشانه در هر ΔT ثانیه ایجاد می شود .

هر بسته ای که می خواهد منتقل شود یک نشانه را ذخیره و سپس از بین می برد .



(a) Before. (b) After.

محاسبه مدت زمان لازم برای ارسال داده انفجاری :

$$S = C/(M - \rho)$$

- S : ظرفیت سطل نشانه
- M : حداکثر سرعت خروجی
- ρ : نرخ تولید نشانه

مشکل سطل نشانه :

این است که اجازه تولید و ارسال انفجارگونه بسته ها را می دهد .

↓ راه حل

استفاده از سطل سوراخ دار پس از سطل نشانه به طوری که نرخ خروجی آن از سطل نشانه بیشتر و از حداکثر نرخ شبکه کمتر باشد .

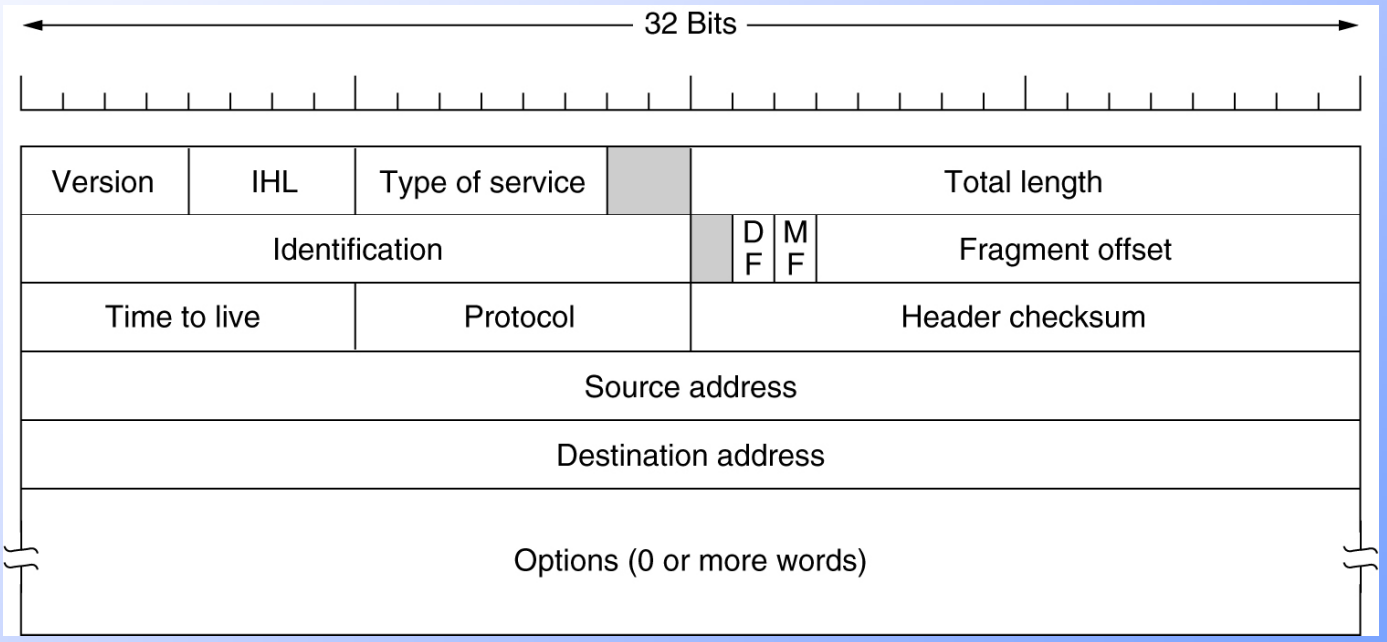
لایه شبکه در اینترنت

پروتکل IP

داده نگاشت (دیتاگرام/ بسته) IP شامل ۲ بخش می باشد :

۱- سرآیند

شامل یک بخش ثابت ۲۰ بایتی و یک بخش اختیاری با طول متغییر می باشد.



۲- متن

فیلد های بخش سرآیند

- 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 حالات 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 دستور می دهد که بسته را قطعه بندی نکند.
- MF : بیانگر قطعات بیشتر است . در تمام قطعات یک بسته به جزء آخری مقدار این بیت یک است.

- Fragment Offset : مشخص می کند که قطعه در کجای بسته قرار دارد.
- Time to live : شمارنده ای است که طول عمر بسته را محدود می کند .
- Protocol : تعیین می کند که بسته را به کدام فرآیند لایه انتقال تحویل دهد.
- Header chechsum : این جمع کنترلی برای تشخیص خطاهای حاصل از کلمات حافظه در یک مسیریاب مفید است.
- Source/Destination Adress : شماره شبکه و شماره میزبان را نشان می دهد.
- Options : اجازه می دهد نسخه های بعدی پروتکل حاوی اطلاعاتی باشند که در طراحی اولیه وجود ندارد.

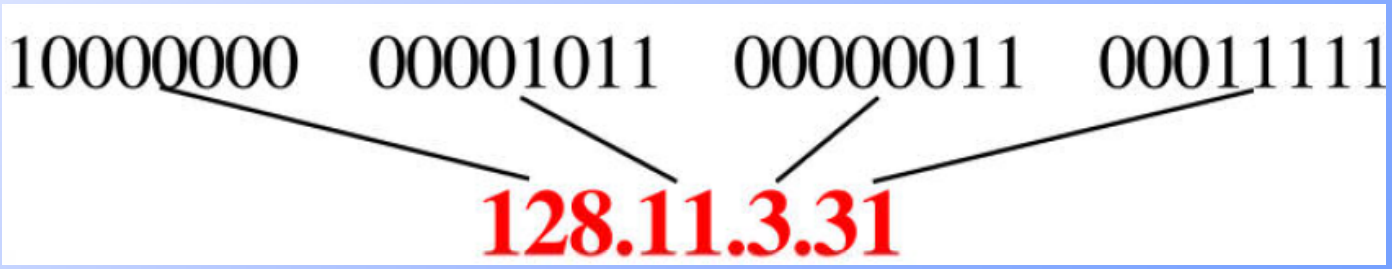
فیلد Options

Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

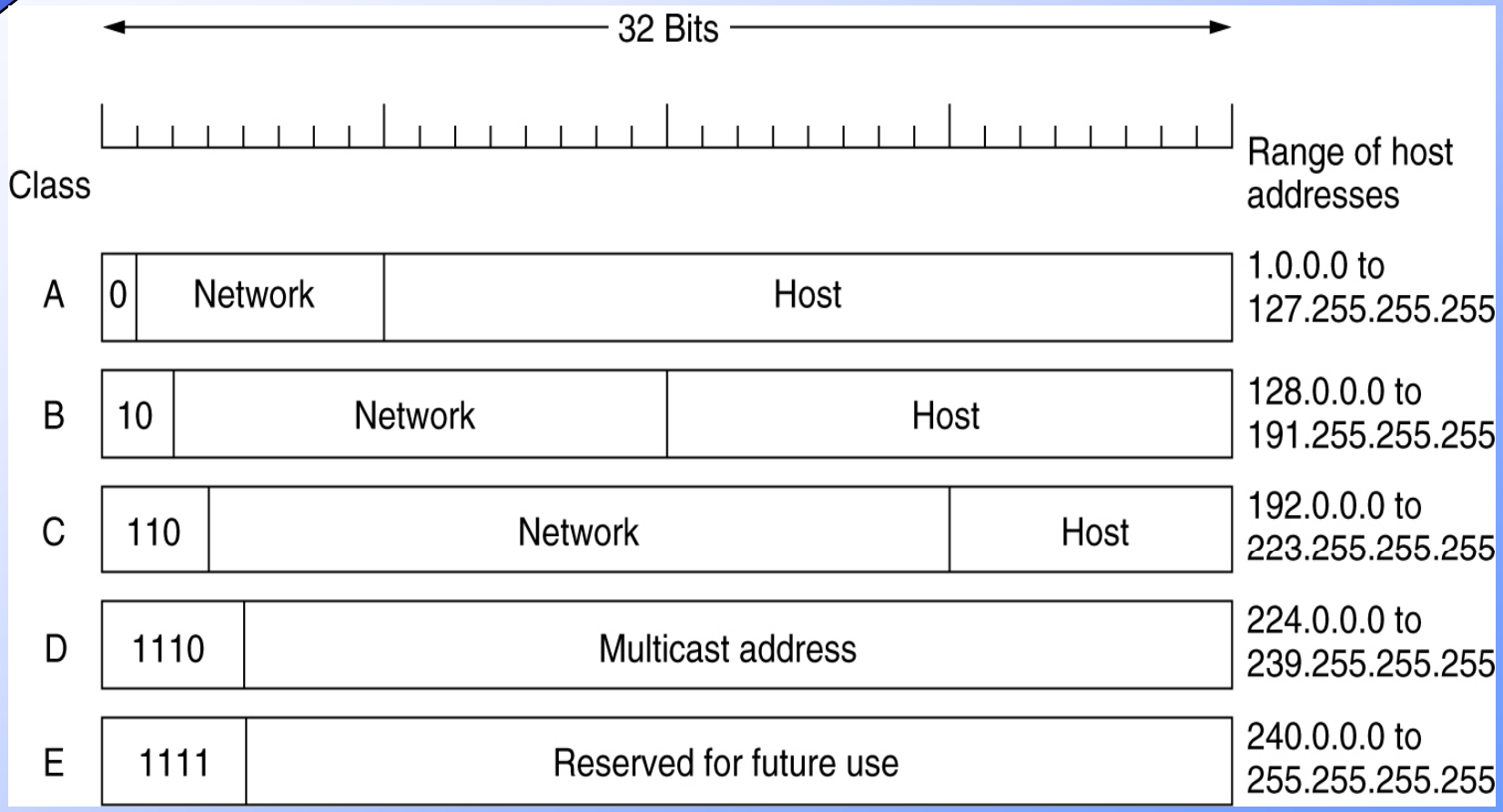
Some of the IP options.

آدرس های IP

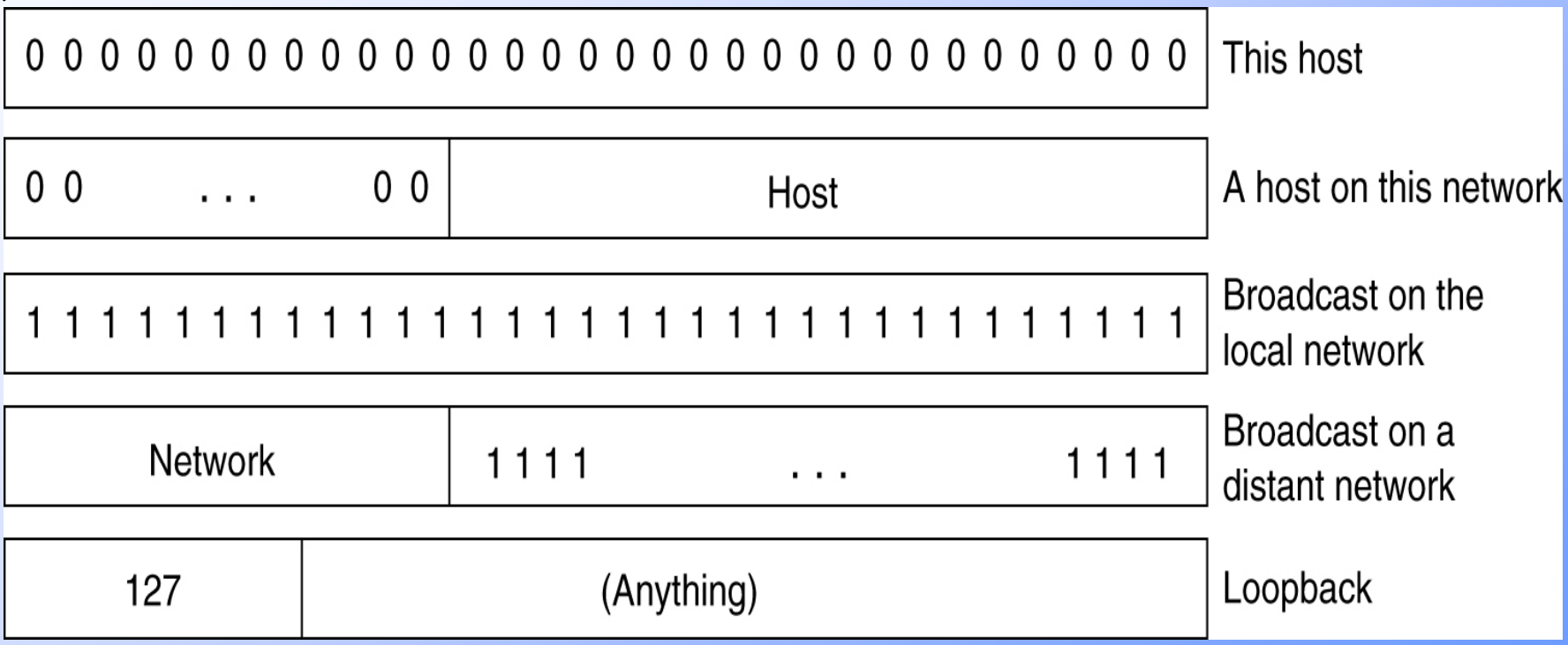
- هر میزبان و مسیریاب اینترنتی یک آدرس IP دارد که شماره شبکه و شماره میزبان خود را کدگذاری می کند . این ترکیب منحصر به فرد است .
- همه آدرس های IP به طول ۳۲ بیت هستند و در فیلد آدرس مبدأ و آدرس مقصد بسته های IP به کار می روند.
- آدرس های IP در واقع به رابط شبکه اشاره دارد و نه به میزبان ، بنابراین اگر یک میزبان بخواهد بر روی دو شبکه باشد ، باید دو آدرس IP داشته باشد .



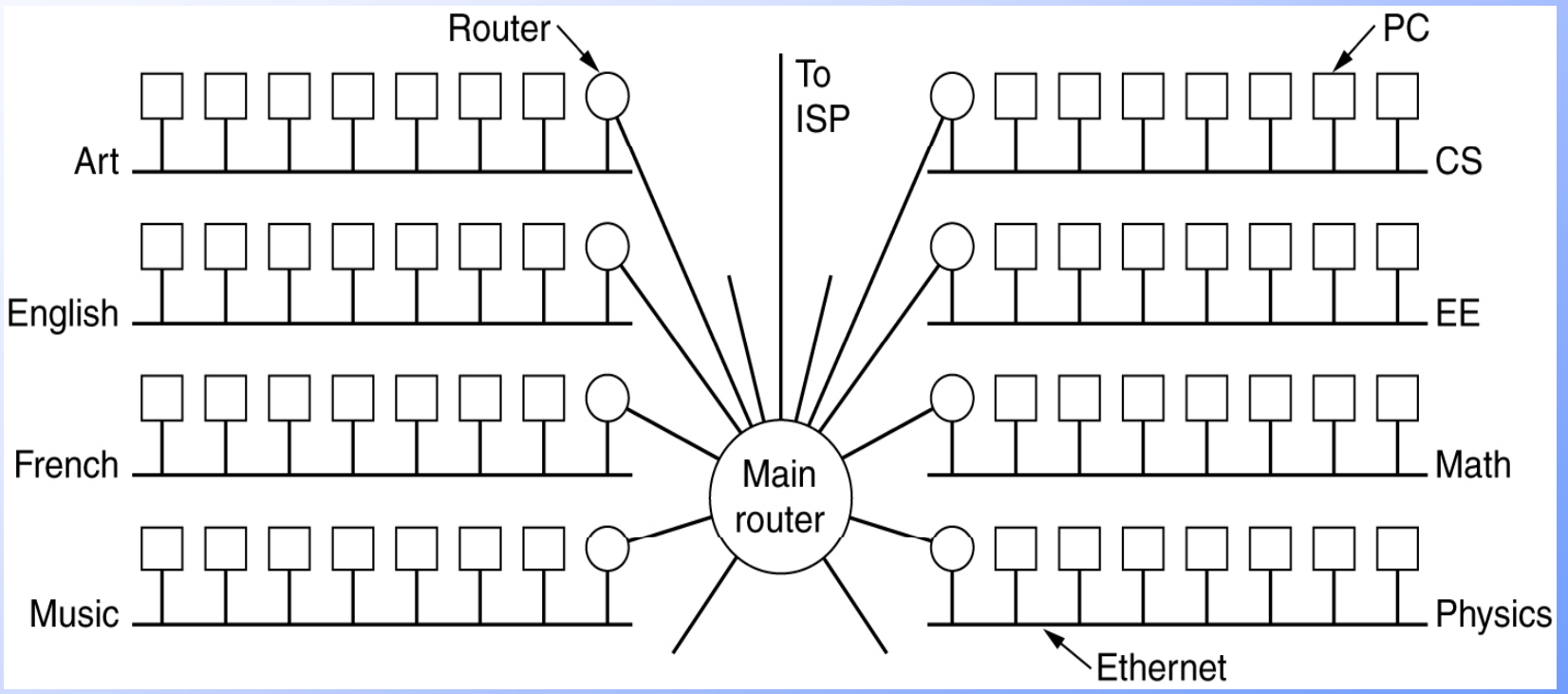
فرمت های آدرس IP



آدرس های IP ویژه

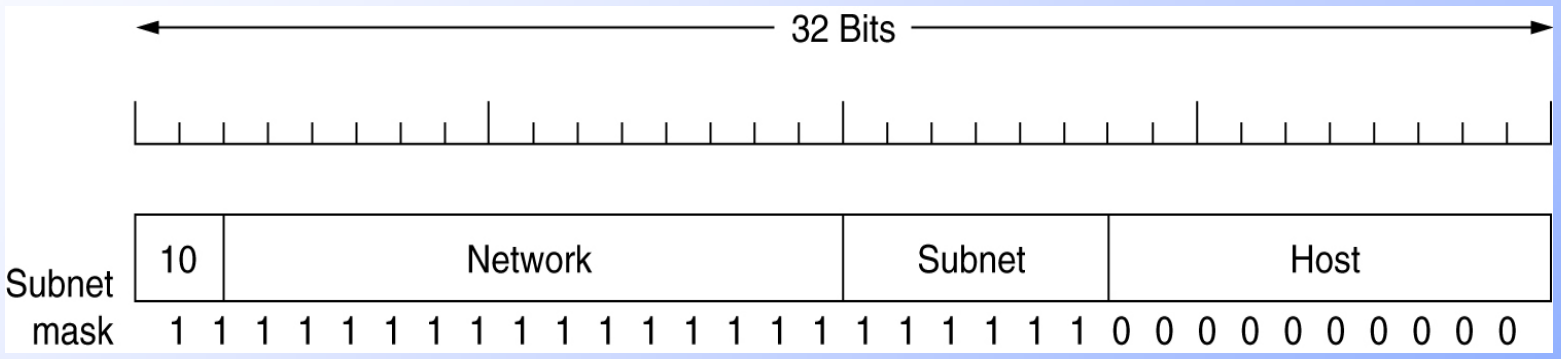


زیر شبکه ها

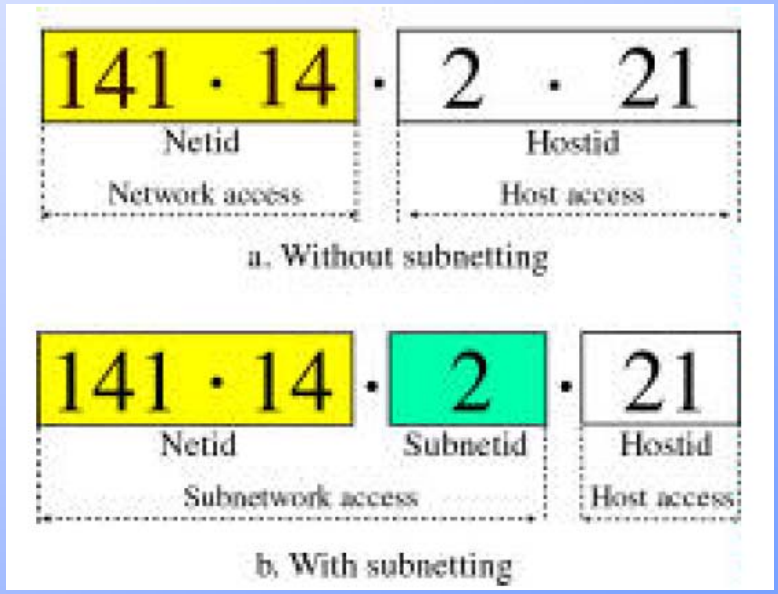


A campus network consisting of LANs for various departments.

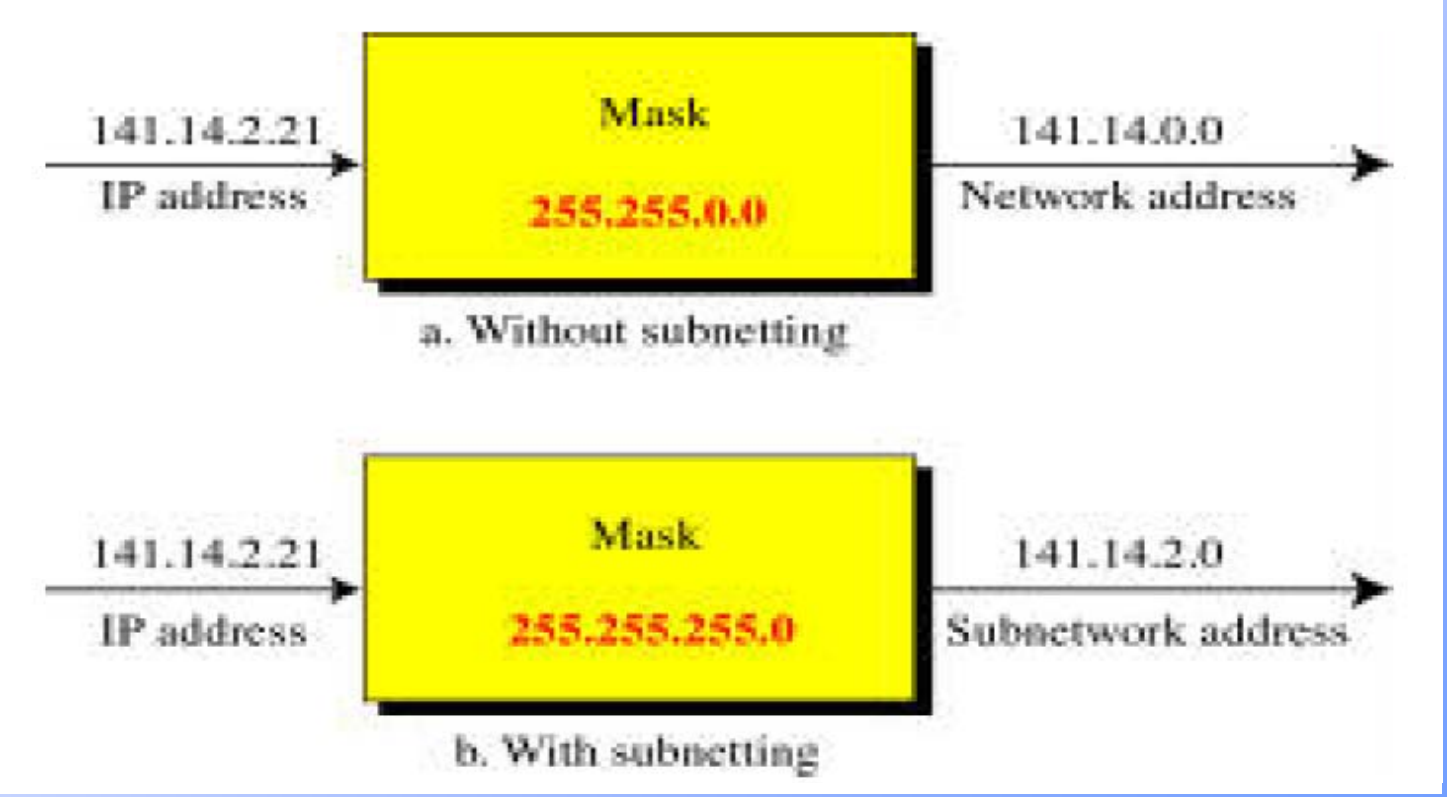
آدرس های زیر شبکه

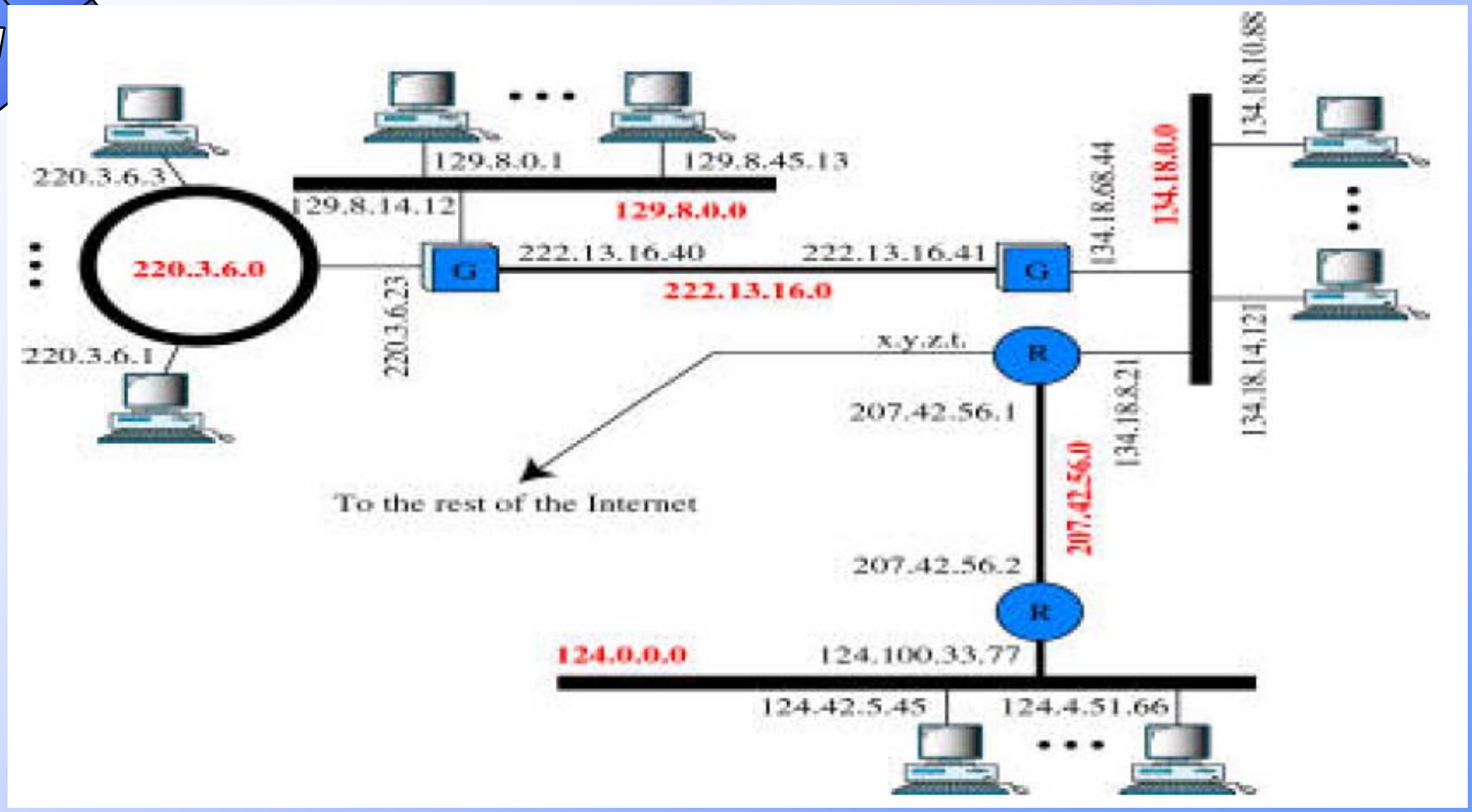


A class B network subnetted into 64 subnets.



ماسک زیر شبکه




220.3.6.3
220.3.6.0
220.3.6.1
129.8.0.1
129.8.45.13
129.8.14.12
129.8.0.0
G
220.3.6.23
222.13.16.40
222.13.16.41
G
222.13.16.0
134.18.68.44
134.18.0.0
134.18.10.88
134.18.14.121
x.y.z.t.
R
134.18.8.21
207.42.56.1
207.42.56.0
To the rest of the Internet
207.42.56.2
R
124.0.0.0
124.100.33.77
124.42.5.45
124.4.51.66

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 (۱

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

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
Source quench	بسته دعوت به آرامش
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 به منظور تایید فعالیت
Timestamp request	همانند پیام Echo به همراه مهر زمان
Timestamp reply	همانند پیام Echo Reply به همراه مهر زمان

پیام های ICMP

ARP (۲

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

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

۳) 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 آدرس های فیزیکی ماشین های مختلف را بصورت فراگیر روی شبکه پخش کرد یا آدرس IP یک ماشین در تصویر حافظه جاسازی شود.

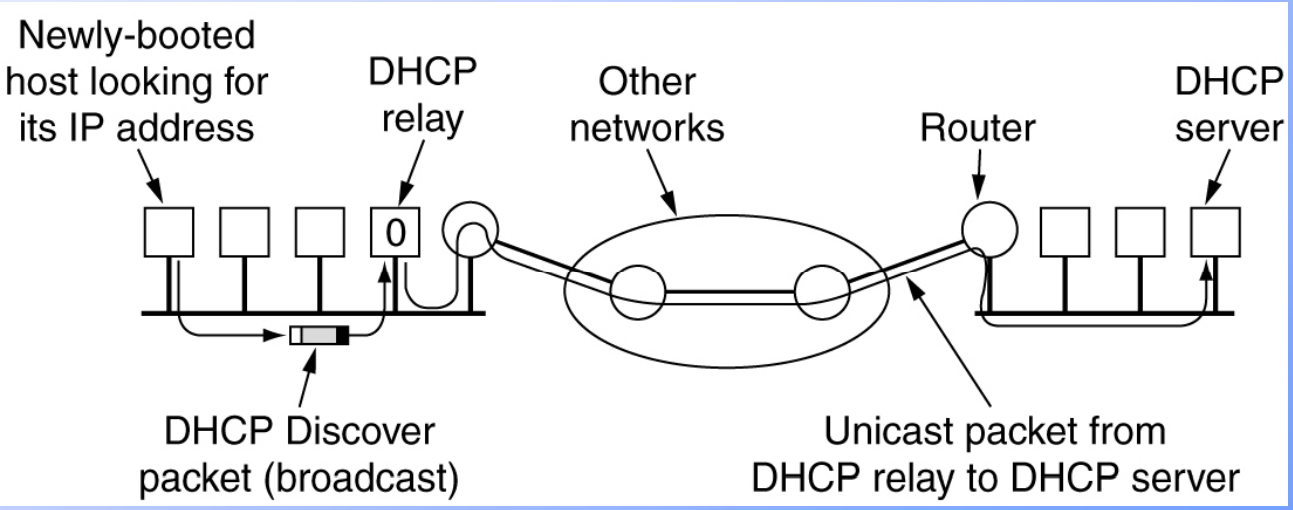
BootP (۴

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

از پروتکل BOOTP برای راه اندازی ایستگاه های 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 ایستگاه ها ارایه دهد.

DHCP (۵

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



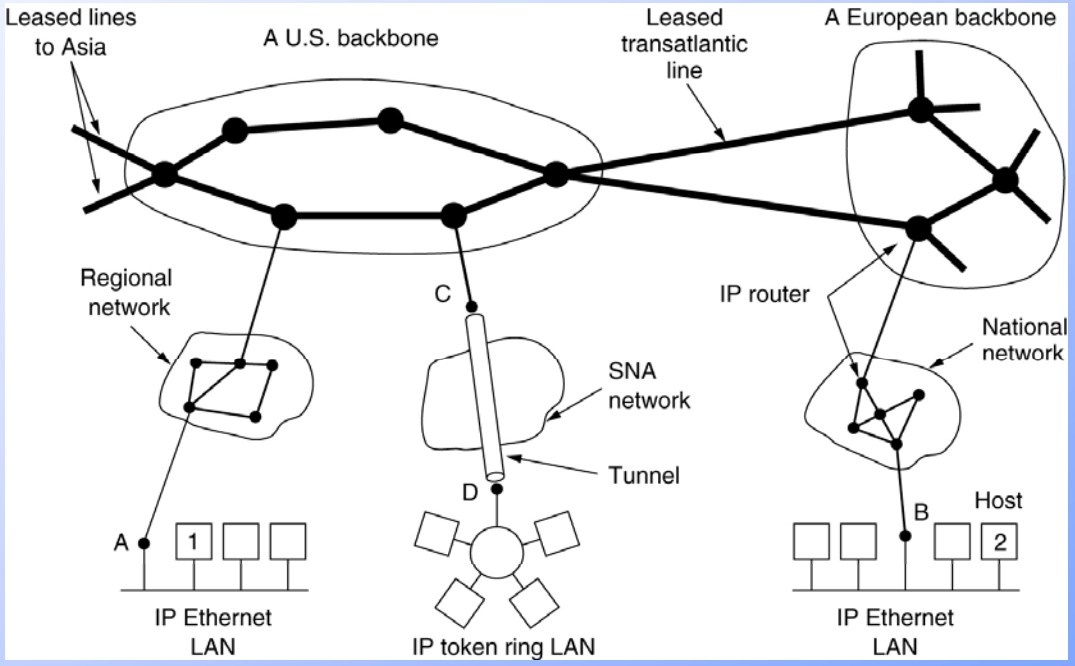
Operation of DHCP.

پروتکل های مسیریابی اینترنت

AS

شبکه اینترنت از تعداد بسیاری سیستم خودمختار(Autonomous System) یا اختصارا AS تشکیل شده است.

مسیریابی درون یک AS را مسیریابی دورنی و مسیریابی بین AS ها را مسیریابی خارجی یا بیرونی گویند.



الف) OSPF

OSPF پروتکل مسیریابی دورنی می باشد. بدین شکل عمل می‌کند :

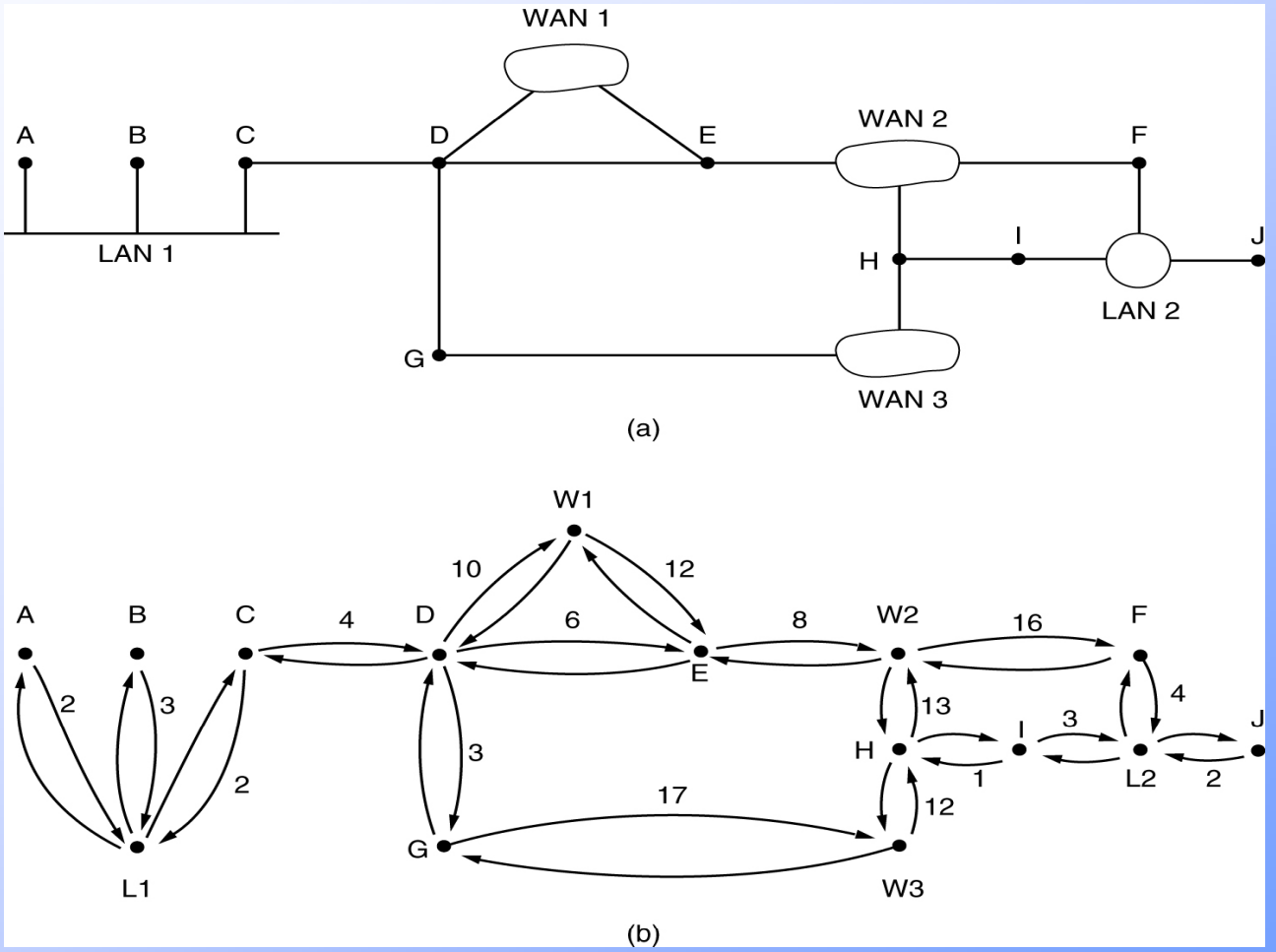
مجموعه شبکه‌ها ، مسیریاب ها و خطوط ارتباطی را در قالب یک گراف جهت دار مدل کرده و به هر کمان در گراف یک وزن می‌دهد که نشان دهنده پارامترهایی مانند تاخیر ، فاصله و امثال آن است. سپس براساس وزن کمان ها مسیر بهینه را پیدا می‌کند.

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)


WAN 1
A
B
C
D
E
WAN 2
F
LAN 1
H
I
J
LAN 2
G
WAN 3
(a)
W1
10
12
A
B
C
4
D
6
8
W2
16
F
E
2
3
13
4
I
3
J
H
3
2
1
L2
2
17
12
G
L1
W3
(b)

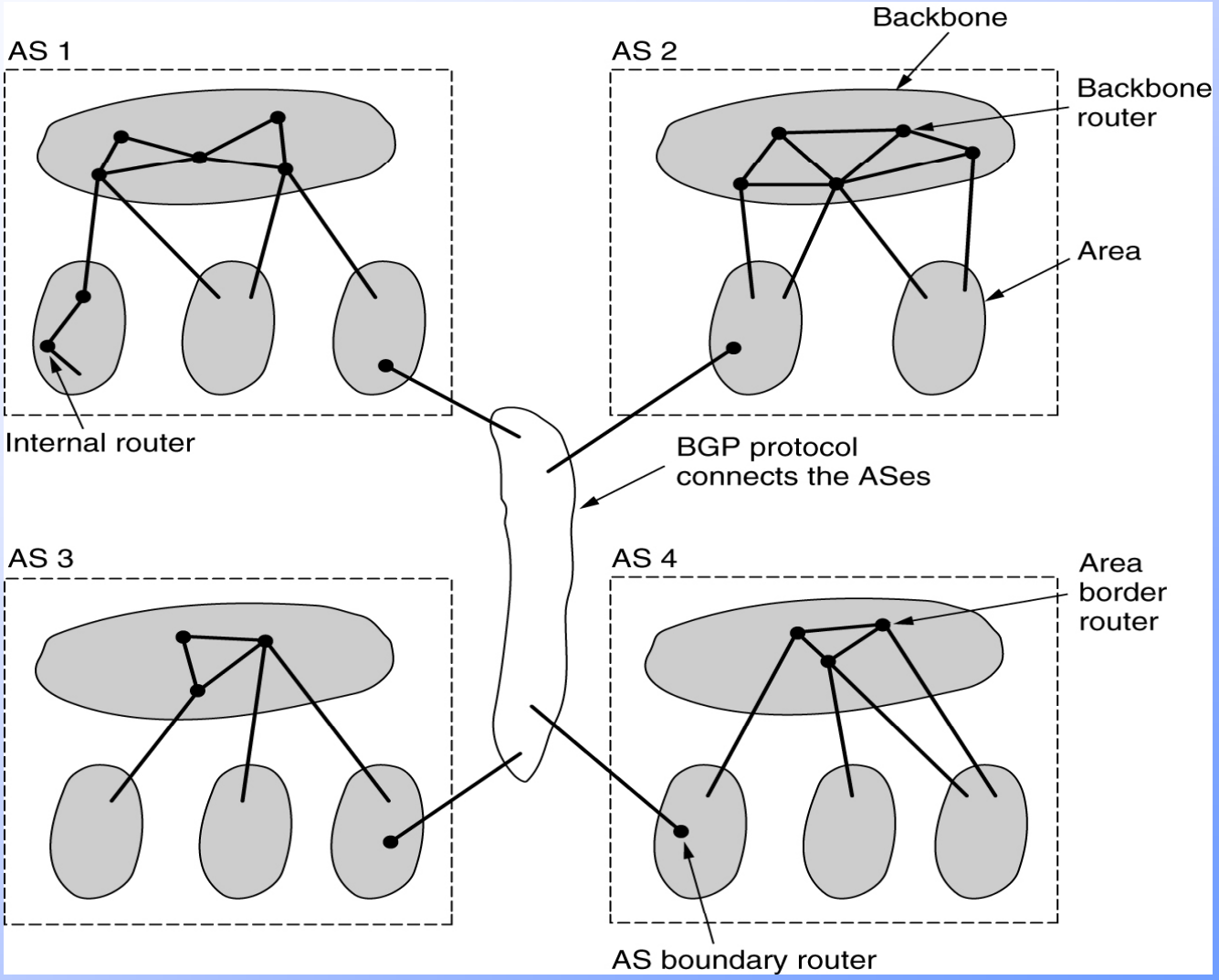
OSPF چهار کلاس مسیریاب را به رسمیت می‌شناسد :

۱- مسیریاب های درونی

۲- مسیریاب های واقع در مرز دو ناحیه

۳- مسیریاب های ستون فقرات

۴- مسیریاب های مرزی AS که می‌توانند با مسیریاب های دیگر محاوره کنند.


AS 1
AS 2
Backbone
Backbone router
Area
Internal router
BGP protocol connects the ASes
AS 3
AS 4
Area border router
AS boundary router

انواع پیام های 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
Dataebase descripotion	مسیریاب با این پیام فهرست درایه‌های بهنگام‌سازی خود را اعلام می‌کند
Link state request	از شریک خود اطلاعاتی را درخواست می‌کند

ب) BGP

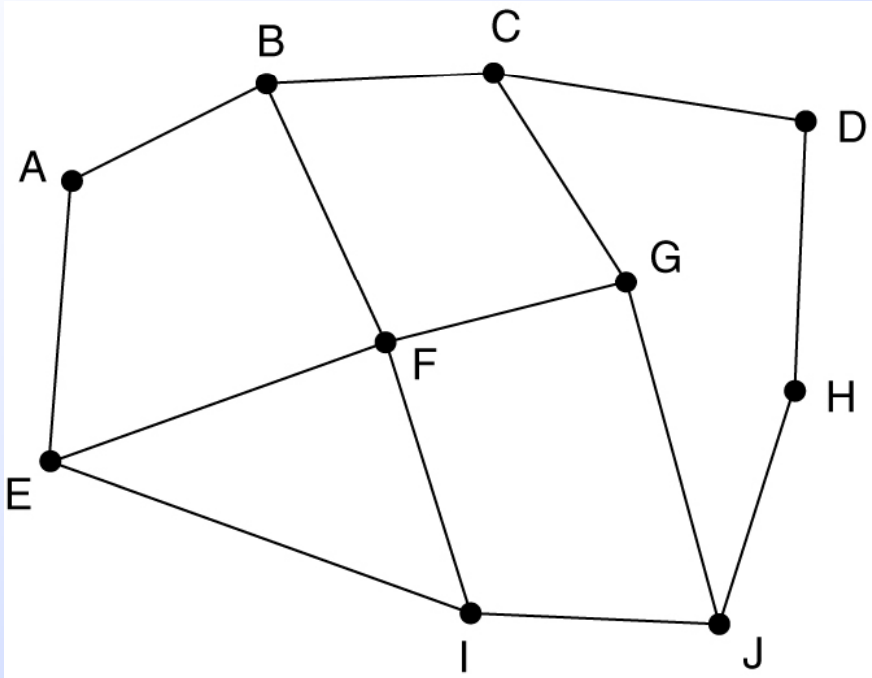
برای مسیریابی بین ASها از پروتکل BGP استفاده می‌شود. پروتکل BGP مبتنی بر الگوریتم بردار فاصله است.

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.



(a)

Information F receives from its neighbors about D

From B: "I use BCD"
From G: "I use GCD"
From I: "I use IFGCD"
From E: "I use EFGCD"

(b)

(a) A set of BGP routers. (b) Information sent to F.