

اسلایدهای درس شبکه‌های کامپیوتری

براساس کتاب «مهندسی اینترنت» تألیف دکتر احسان ملکیان

طرح اسلایدهای خلاصه درس: دکتر داود کریمزادگان مقدم
تکمیل و تلخیص: دکتر جواد راستی

آشنایی با شبکه

مفاهیم شبکه‌های کامپیووتری

• کاربردهای شبکه‌های کامپیووتری

- سخت افزار شبکه

- دسته‌بندی شبکه‌ها

- روش‌های برقراری ارتباط دو ماشین در شبکه

- مدل هفت‌لایه‌ای **OSI**

- مدل چهار‌لایه‌ای **TCP/IP**

مفاهیم شبکه‌های کامپیوتری

هدفهای آموزشی

- مفهوم شبکه و کاربردهای آن
- سخت افزار شبکه
- انواع سوئیچینگ
- طراحی شبکه و اصول لایه بندی
- مدل هفت لایه ای **OSI** از سازمان استاندارد جهانی
- مدل چهار لایه ای **TCP/IP**



چرا شبکه؟

پیشرفت و توسعهٔ مرزهای دانش امروزه به شبکه‌های کامپیوتری وابسته است.

هدف IT: گردآوری، سازماندهی و فرآوری دانش پراکنده در سطح دنیا

یاور *IT*: شبکه!

شبکه‌های کامپیوتو^{ری} مجموعه‌ای از کامپیوترهای **مستقل** است که به نحوی با یکدیگر اطلاعات و داده **مبادله** می‌نمایند.

تبادل داده

ردوبدل‌نmodن داده بدون توجه به نوع کانال انتقال

استقلال کامپیوترها

کار کردن هر ماشین به تنها بی در صورت نبودن در شبکه

یعنی از شبکه فقط برای تبادل اطلاعات استفاده می‌شود

با سیستم‌های توزیع شده متفاوت است.

یک رسانه‌ی مادی یا غیرمادی برای انتقال اطلاعات با چزییات مشخص و استاندارد

شبکه‌ی اینترنت ...؟

شبکه‌های مستقل از هم و مربوط به سازمان‌های مستقل: اینترانت

با ارزان شدن سخت‌افزار شبکه و ایجاد زیرساخت ارتباطی در شبکه‌ی داده، شبکه‌های اینترانت به هم متصل شدند و اینترنت را ایجاد کردند.

اینترنت: زیرساختی ۴۰ ساله برای حمل و جابجایی اطلاعات
وب: معماری ۲۰ ساله برای سازماندهی دسترسی به اطلاعات توزیع شده در جهان

کاربردهای شبکه‌های کامپیوتری

- ✓ اشتراک منابع (سخت‌افزار – نرم‌افزار – داده‌ها)
- ✓ حذف محدودیت‌های جغرافیایی در تبادل داده‌ها (درمان از راه دور)
- ✓ کاهش هزینه‌ها (email، خرید اینترنتی، استفاده از نتایج تحقیقات دیگران، اشتراک چاپگر)
- ✓ بالا رفتن قابلیت اعتماد سیستمها (حفظ اطلاعات در صورت خرابی یک دستگاه)
- ✓ افزایش کارایی سیستم (توزیع وظایف سازمانی مثلاً در یک سیستم بیمارستانی (HIS))



خدمات معمول در شبکه

دسترسی به بانکهای اطلاعاتی راه دور

پست الکترونیکی

خدمات انتقال فایل

ورود به سیستم از راه دور

گروههای خبری

جستجوی اطلاعات مورد نیاز

تبلیغات

تجارت الکترونیکی

بانکداری الکترونیکی

سرگرمی و محاوره

مجلات و روزنامه‌های الکترونیکی

محاوره مستقیم و چهره به چهره از راه دور

کنفرانس از راه دور

یافتن اشخاص مورد نظر در جهان

تلفن و دورنگار از طریق شبکه

رادیو از طریق شبکه

آموزش از راه دور

ارائه مدون اطلاعات فنی و علمی

اخبار مربوط به هنر ، ورزش ، سیاست ، تجارت و ...

کاریابی و اشتغال

درمان از راه دور

خرید و فروش روزمره با استفاده از کارت اعتباری

انجمن‌های خیریه

مشاوره از راه دور



اجزاء شبکه



نرم افزار



سخت افزار

پروتکل

برنامه

الگوریتم

NIC,
Hub,
Switch,
Router,
cable,
آنتن

دسته بندی سخت افزار شبکه های کامپیوتری

- مساحت جغرافیایی چند ایستگاه در شبکه
-

از دیدگاه
مقیاس بزرگی

1-شبکه های PAN

2-شبکه های LAN

3-شبکه های MAN

4-شبکه های RAN

5-شبکه های WAN

از دیدگاه
تکنولوژی
انتقال

شبکه های
 نقطه به نقطه
(point to point)

شبکه های پخش
فراگیر
(Broadcast)

دسترسی به نوع کanal

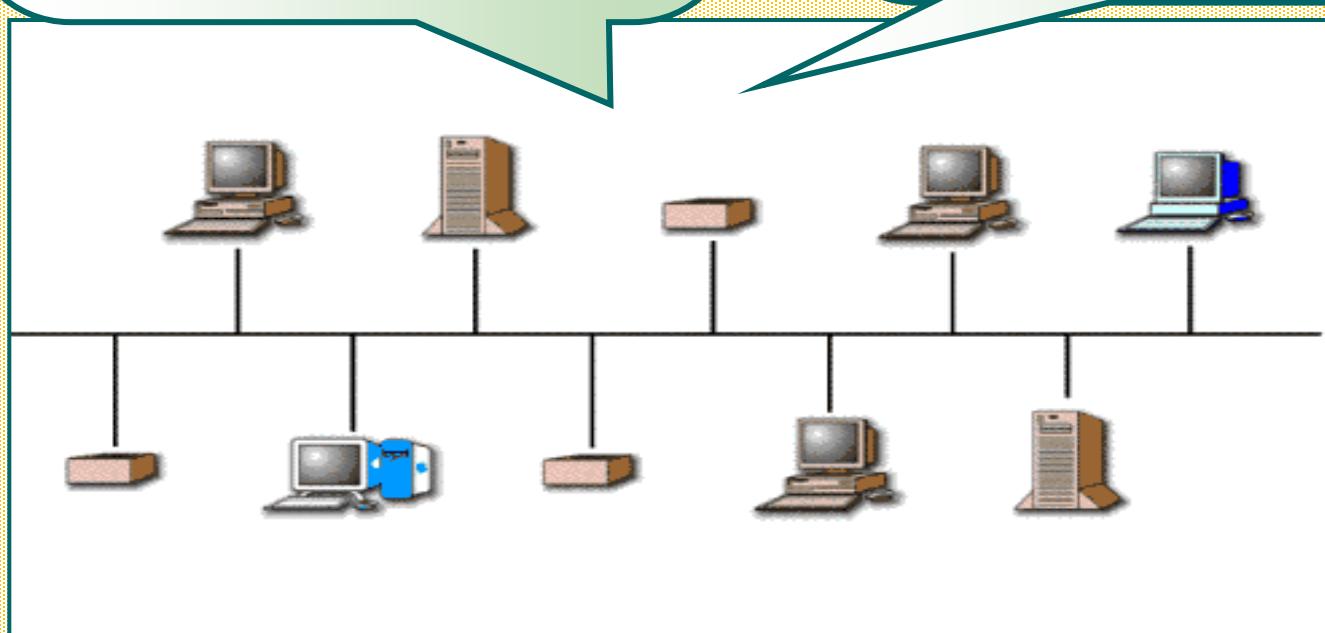
معایب شبکه‌های پخش فراگیر

- ۱- مدیریت پیچیده کانال (عدالت با/بدون حاکمیت - پروتکل (MAC)
- ۲- امنیت کم (رمزنگاری)
- ۳- کارآیی پایین (سهم کم هر ماشین از پهنای باند)

شبکه پخش فراگیر (Broadcast)

انتقال اطلاعات از طریق یک کانال فیزیکی مشترک توسط تمام ایستگاهها

- بسیار مقرون به صرفه
- ماهواره، اترنت (Ethernet)، WiFi، بلوتوث،

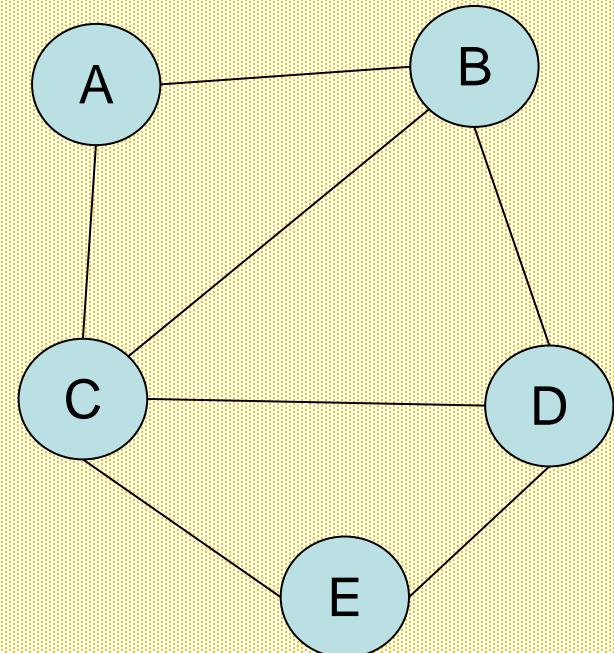
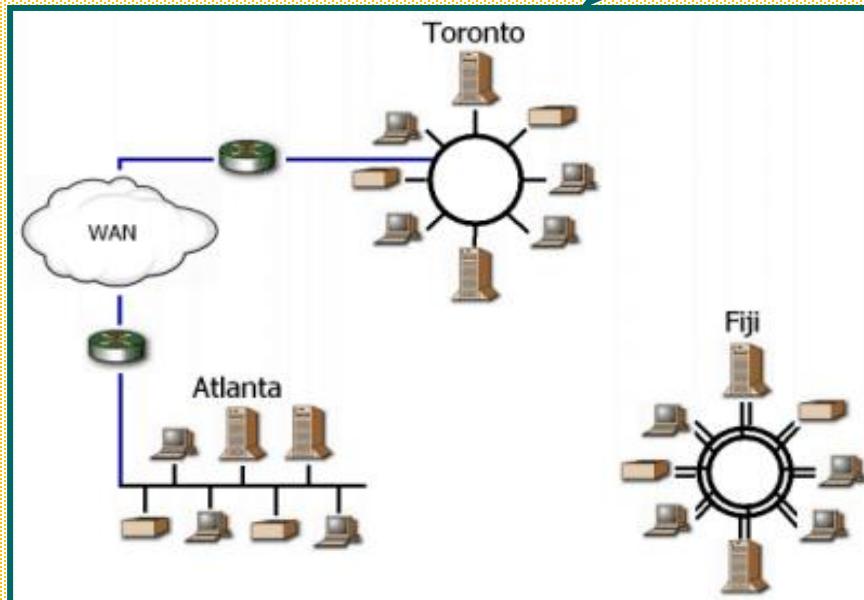


همه ایستگاه‌ها باید دائم به خط گوش بدهند و در صورت خالی بودن اطلاعات ارسال کنند

معمولًاً برای اتصال
شبکه‌ها به هم استفاده
می‌شود

شبکه‌های نقطه به نقطه (point to point)

وجود **فقط و فقط** یک کانال فیزیکی و مستقیم بین
دو ماشین در شبکه



شبکه شخصی Personal Area Network



زیر ۱۰ متر

مالکیت فردی

اتصال دستگاه‌های شخصی و خانگی (Bluetooth و USB و ...)

سادگی کاربری

ارزانی

Ethernet

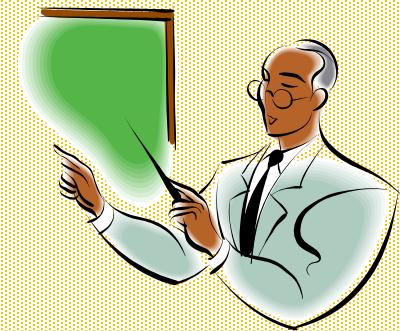
WiFi (IEEE 802.11)

Token Ring

شبکه محلی (Local) LAN

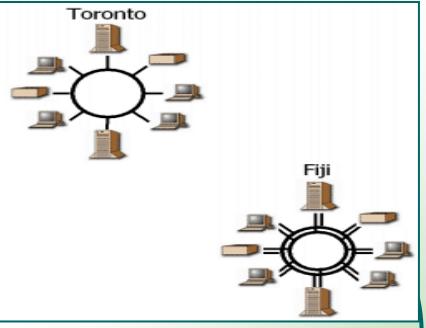
- 1- فواصل جغرافیایی محدود (حداکثر تا چند کیلومتر)
- 2- تعداد ایستگاهها کم
- 3- کوتاه بودن طول کanal انتقال

ادارات و سازمان‌های کوچک

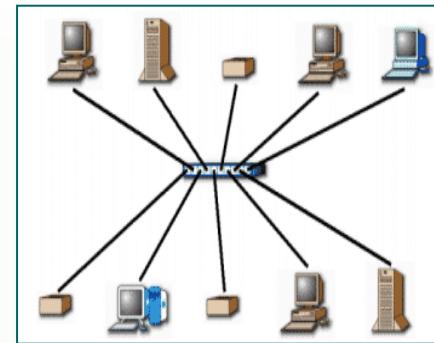


محاسن شبکه‌های LAN

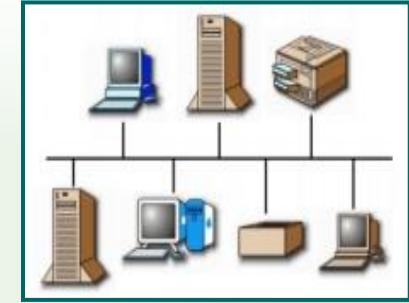
1. افت سیگنال کم، نرخ خطای پایین، نرخ ارسال بالا
2. تأخیر انتشار (مدت زمانی که یک سیگنال از ابتدا به انتهای کanal منتقل می‌شود – $\frac{3}{3}$ میکروثانیه برای هر کیلومتر فیبر نوری و ۵ میکروثانیه برای هر کیلومتر سیم مسی) بسیار ناچیز به دلیل کوتاه بودن طول کanal
3. مدیریت آسانتر شبکه به علت محدود بودن تعداد ایستگاهها
4. هزینه پایین نصب و راهاندازی این نوع شبکه.



RING



STAR



BUS

انواع توپولوژی‌های (به همبندی)
شبکه‌های محلی

چگونگی اتصال ماشین‌ها به کانال انتقال

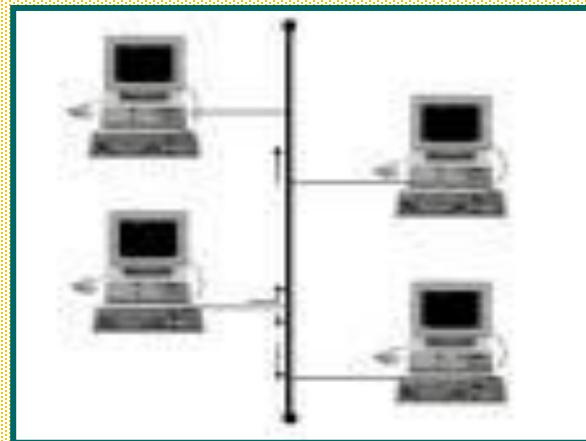
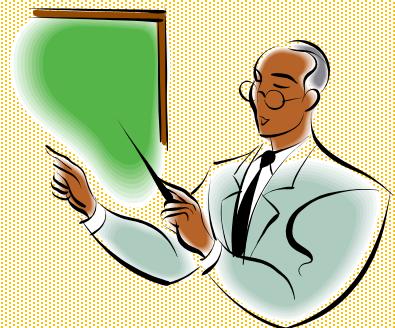


توبولوژی خطی – Bus

• اتصال تمام ایستگاهها از طریق یک کانال فیزیکی مشترک

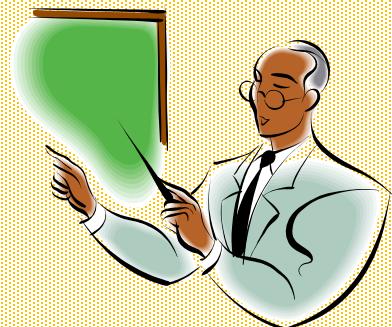
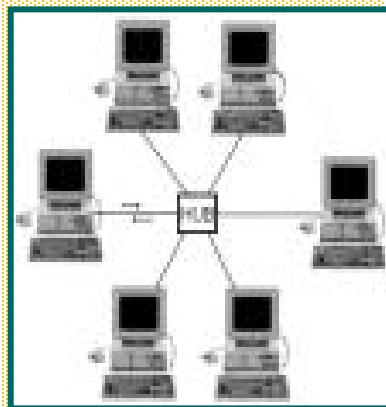
• سادگی در نصب و راه اندازی و ارزان بودن

• قبلًا پررونق بوده است...

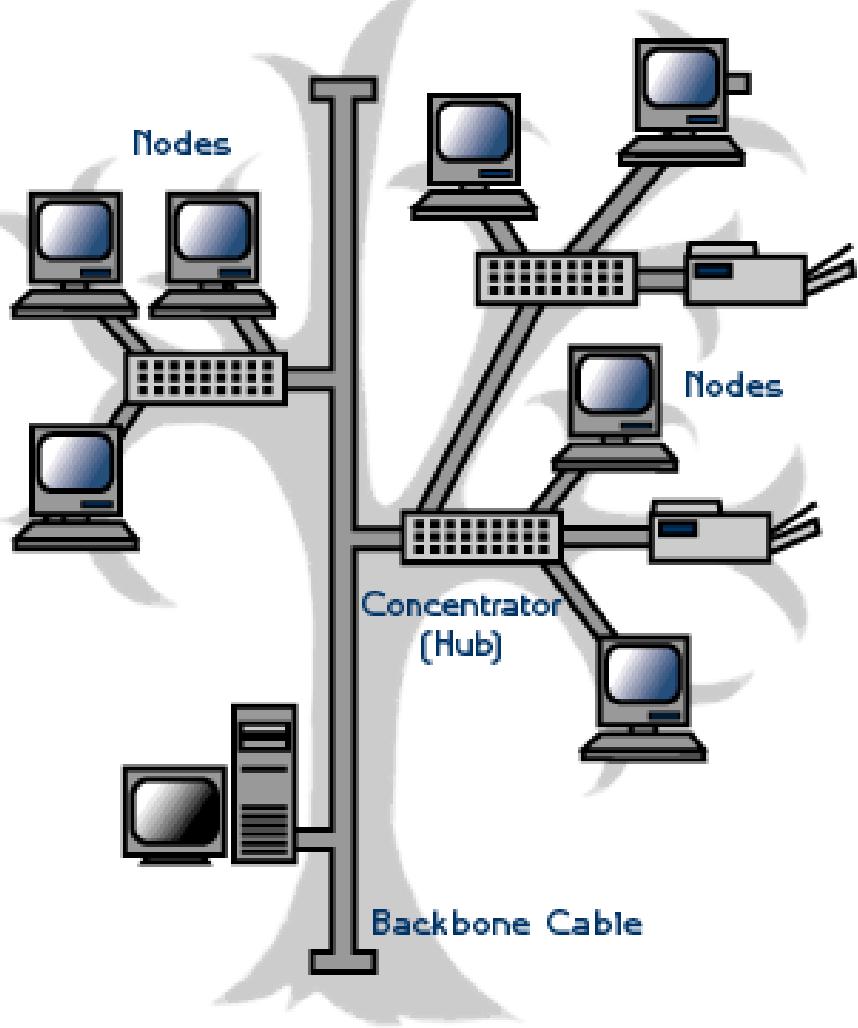


توپولوژی ستاره - (Star)

- اتصال تمام ماشینهای شبکه توسط یک گره مرکزی
- گره مرکزی میتواند سوئیچ سریع یا هاب (Hub) و یا کامپیوتر باشد.



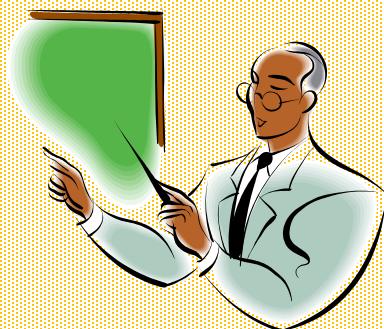
توبولوژی درختی - Tree



ماشین‌ها: برگ‌ها

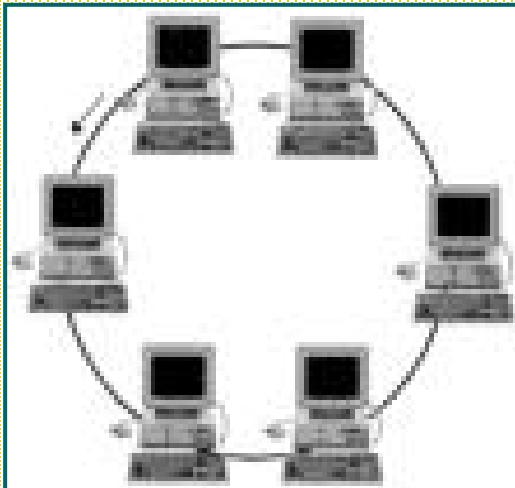
گره‌های میانی: سویچ

برای اتصال چند شبکه‌ی ستاره‌ای به کار می‌رود



توپولوژی حلقه – (Ring)

- اتصال ایستگاهها در یک ساختار حلقوی به یکدیگر
- یکطرفه بودن ارتباط هر ایستگاه با ایستگاه بعدی خود (برگشت به فقط یک ایستگاه حق ارسال دارد)
- دریافت پسته های اطلاعاتی توسط تمام ایستگاههای بین مسیر دو ایستگاه غیر مجاور و تکرار آنها جهت انتقال اطلاعات بین آن دو ایستگاه
- همه پخشی است

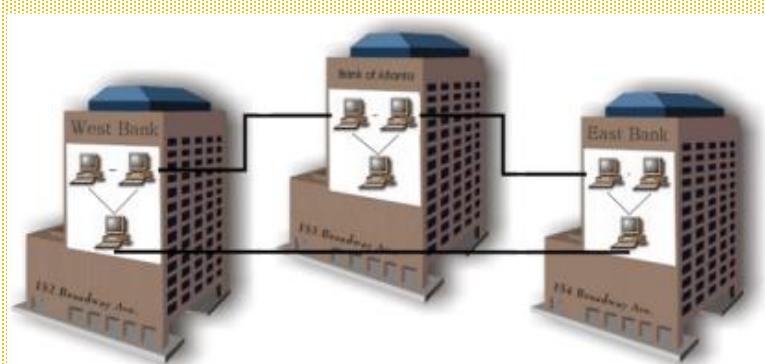


WiMax (IEEE 802.16)

شبکه های بین شهری (Metropolitan AN)

برای ایجاد شبکه در سطح یک منطقه وسیع در حد یک شهر یا اتصال چندین شبکه محلی ، از شبکه MAN استفاده می شود . این شبکه تکنولوژی و توپولوژی مشابه با شبکه های محلی دارد. بدلیل طول زیاد کanal معمولاً از فیبر نوری استفاده می شود.

• ۱۰۰ تا ۲۰۰ کیلومتر



شبکه های ایالتی (Regional AN)

با هدف ارائه خدمات خاص

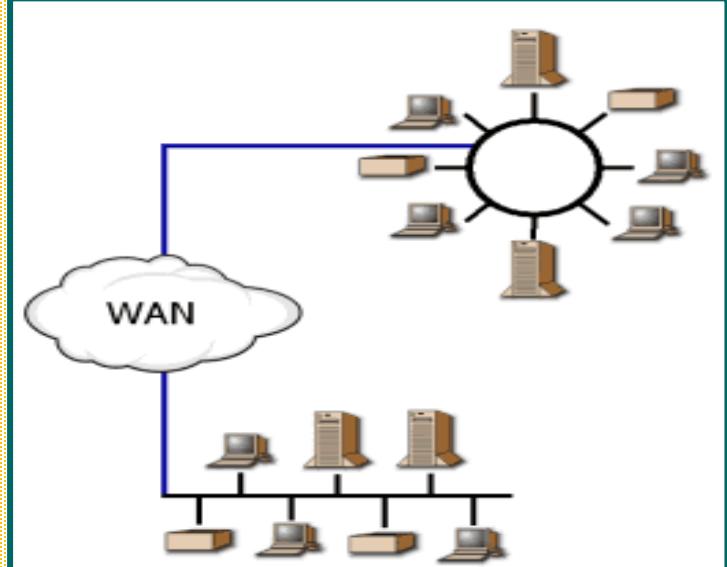
IEEE 802..2

شبکه های گسترده (Wide AN)

- یک زیرساخت ارتباطی یا ستون فقرات (Backbone) برای جابجایی داده ها
- پیاده سازی در گستره جغرافیایی یک کشور یا جهان
- اتصال شبکه های محلی و بین شهری
- ساختار ناهمگون



توپولوژیهای مختلف شبکه های محلی
تنوع در سخت افزار و نرم افزار ماشینهای موجود
در این شبکه ها



شبکه‌ی WAN: اتصال شبکه‌های LAN و MAN و RAN به یکدیگر

کامپیوترها: Host یا End System (مثل گوشی تلفن)

زیرساخت شبکه: بقیه‌ی عناصر ارتباطی (مثل شبکه‌ی تلفن)

بسته (Packet): یک قطعه اطلاعات دارای هویت که در یک میزبان سازماندهی شده و توسط

زیرساخت شبکه هدایت و تحویل مقصد می‌شود.

دو بخش زیرساخت ارتباطی در شبکه WAN

عناصر سویچ (مسیریاب)

خطوط ارتباطی یا کانالها
(Circuit, Channel)
(Trunc)

مسیریابها: کامپیوترهای ویژه‌ای که پس از دریافت بسته، با درنظرگرفتن مقصد آن، کانال خروجی مناسب برای انتقال بسته به مقصد را انتخاب می‌نمایند.

خطوط انتقال با پهنای باند بالا
برقرار کننده ارتباط عناصر سویچ

زیرساخت فرضی WAN در ایران



شبکه های بی سیم (Wireless LAN: WLAN)

WiMax و Wi-Fi شبکه های

موارد استفاده:

- 😊 ایجاد شبکه ای با وجود ایستگاه های متحرک
- 😊 استفاده در مکان هایی که کابل کشی در آن مقرر نبود به صرفه و یا عقلانی نیست.
- 😊 محدودیت های سخت افزاری (کمبود کابل یا پورت سخت افزاری)

مزایا

- 😊 ساده بودن نصب و راه اندازی این نوع شبکه

معایب

- 😊 نرخ ارسال و دریافت پایین
- 😊 نرخ خطا نسبتاً بالا
- 😊 امنیت اطلاعات کم

روش‌های برقراری ارتباط دو ماشین در زیرساخت شبکه

2- سوئیچینگ پیام

Message Switching

1- سوئیچینگ مداری

Circuit Switching

هدایت و انتقال اطلاعات بین
فرستنده و گیرنده

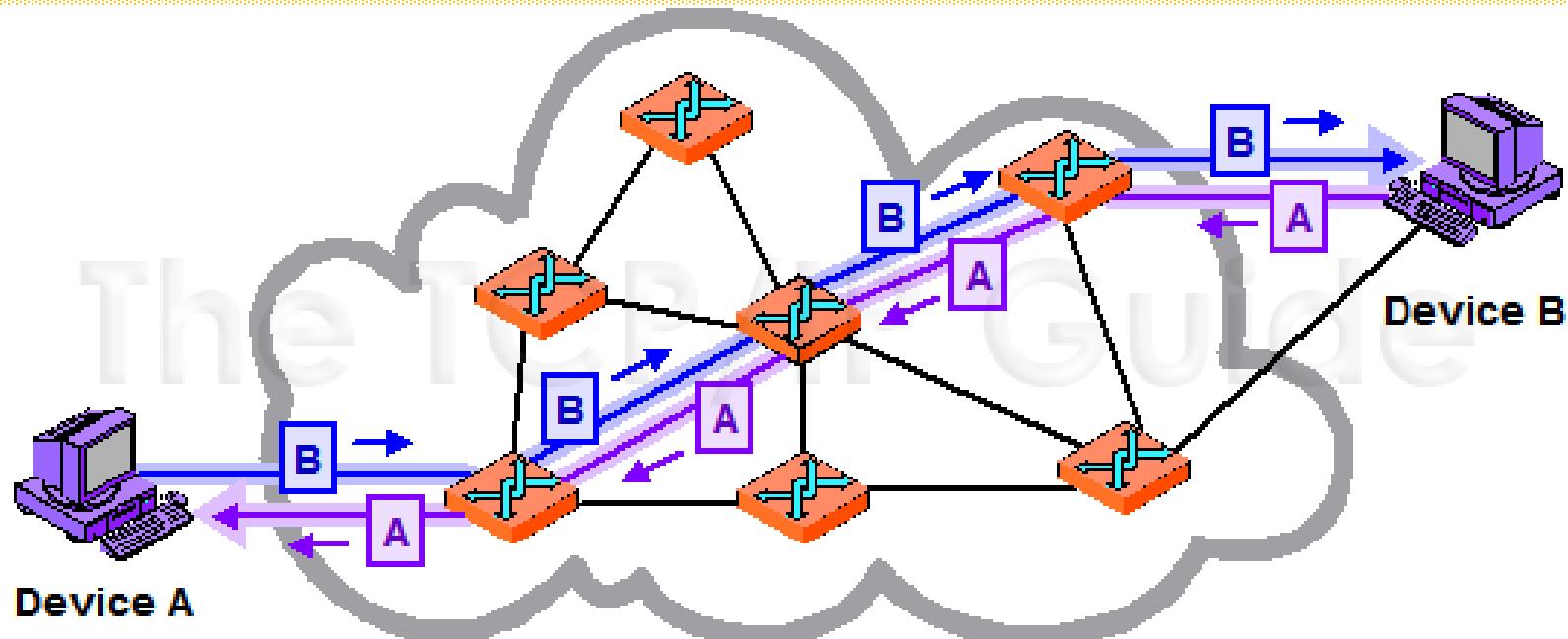
3- سوئیچینگ بسته و سلول

Packet Switching / Cell Switching

۱- سوئیچینگ مداری

Circuit Switching

لزوم برقراری اتصال فیزیکی (الکتریکی) بین مبدأ و مقصد جهت انتقال اطلاعات (مانند شبکه‌ی تلفن)



۱- سوئیچینگ مداری

Circuit Switching

لزوم برقراری اتصال فیزیکی (الکتریکی) بین مبدأ و مقصد جهت انتقال اطلاعات (مانند شبکه‌ی تلفن)

معایب

- ☺ نیاز به زمان قابل توجهی برای برقراری ارتباط بین فرستنده و گیرنده (مانند شماره‌گیری تلفن)
- ☺ عدم امکان برقراری ارتباط توسط ماشینهای دیگر با دو ماشین فرستنده و گیرنده هنگام اشغال بودن کanal توسط دو ماشین
- ☺ در دنیای شبکه طرفدار ندارد!
- ☺ در صورت قطع شدن یک عنصر میانی، ارتباط کلاً قطع می‌شود.

2- سوئیچینگ پیام

Messeage Switching

- مانند شبکه‌ی پست
- مختص انتقال داده‌ای دیجیتال
- اتصال دائمی هرایستگاه با مرکز سوئیچ خود
- اضافه نمودن اطلاعات لازم (مشخصات فرستنده و گیرنده) به داده‌ها قبل از ارسال آن به مرکز سوئیچ توسط ایستگاه فرستنده و تشکیل پیام
- دریافت کامل پیام توسط هر مرکز سوئیچ و انتخاب کanal خروجی مناسب به سوییچ بعدی بر اساس آدرس گیرنده موجود در داده (**Store & Forward**)

مشکل سوئیچینگ پیام

عدم محدودیت طول پیام

بالا بودن حافظه‌های موجود در هر مرکز سوئیچ

ارسال مجدد داده‌ها در صورت خرابی یک بیت در پیام

تأخیر زیاد در رسیدن پیام (چون کل پیام باید دریافت و سپس ارسال شود)

مزایا

سریع و کارآمد (از قبل نیاز به برقراری کانال نیست)

عدم اشغال کانال

۳- سوئیچینگ بسته و سلول

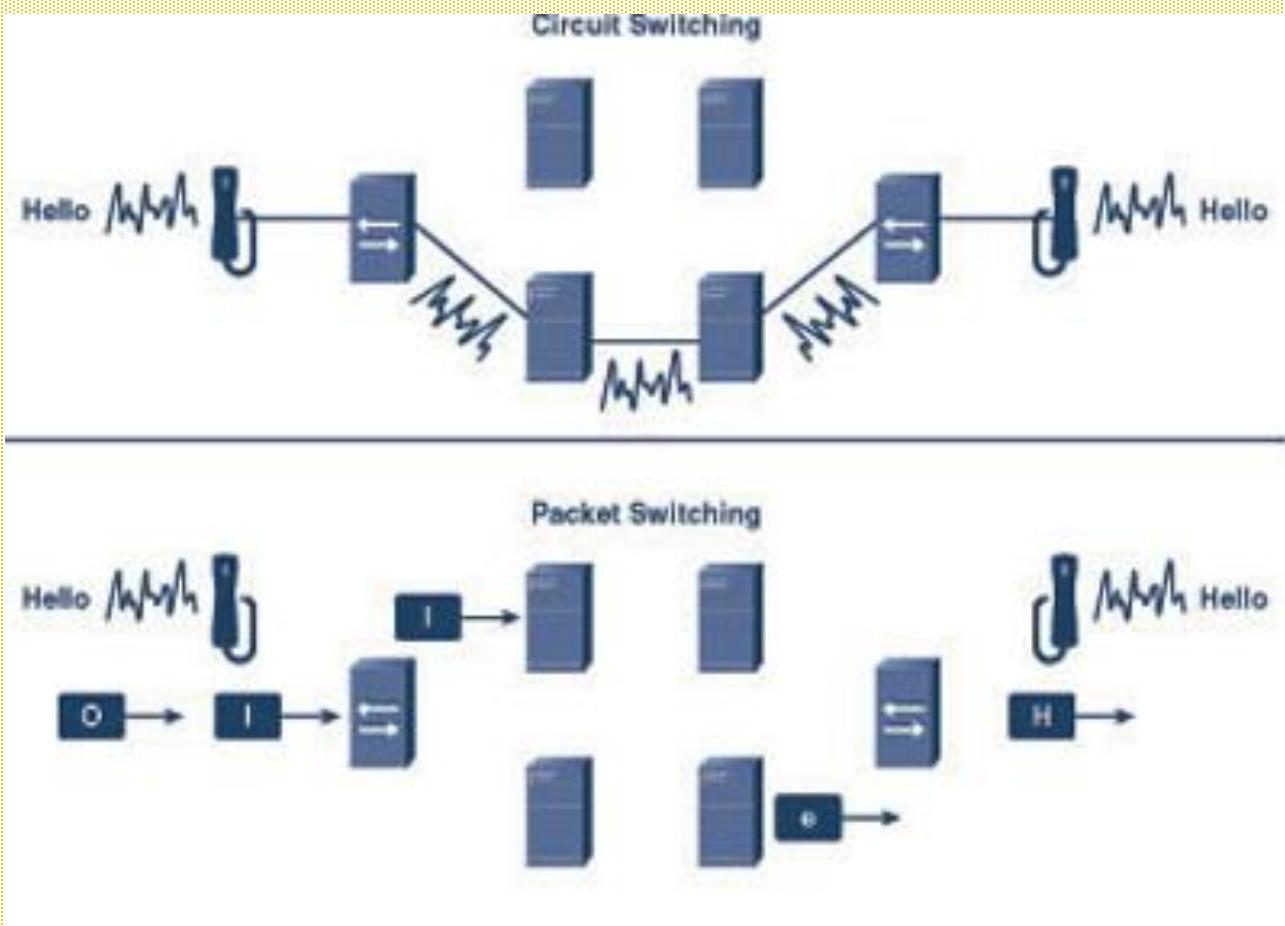
Packet / Cell Switching

حل مشکل سوئیچینگ پیام

شکستن پیام توسط ایستگاه فرستنده به قطعات کوچکتری به نام بسته (در سوییچ‌های مدرن طول آنها بسیار کم است مانند بسته‌های ۵۳ بایتی ATM) و ارسال هر بسته به همراه اطلاعات لازم برای بازسازی آن به طور جداگانه به مراکز سوئیچ

تأخیر آن از سوئیچینگ پیام کمتر است؛ چون بسته‌ها موازی یا هم توسط سوییچ‌های متنوع ارسال می‌شوند (لزوم شماره‌گذاری بسته‌ها)

مقایسه دو روش سوئیچینگ مداری و سوئیچینگ پیام/بسته



کاربران WLAN برای اتصال به ISP از سوئیچینگ مداری و ISP‌ها برای اتصال به زیرساخت از سوئیچینگ بسته/سلول استفاده می‌کنند.

مقایسه دو روش سوئیچینگ پیام وبسته / سلول

مجموع تأخیر کمتر در روش سوئیچینگ بسته نسبت به روش سوئیچینگ پیام

نیاز به فضای حافظه کمتر و قابل تأمین در هر مرکز سوئیچ در روش سوئیچینگ

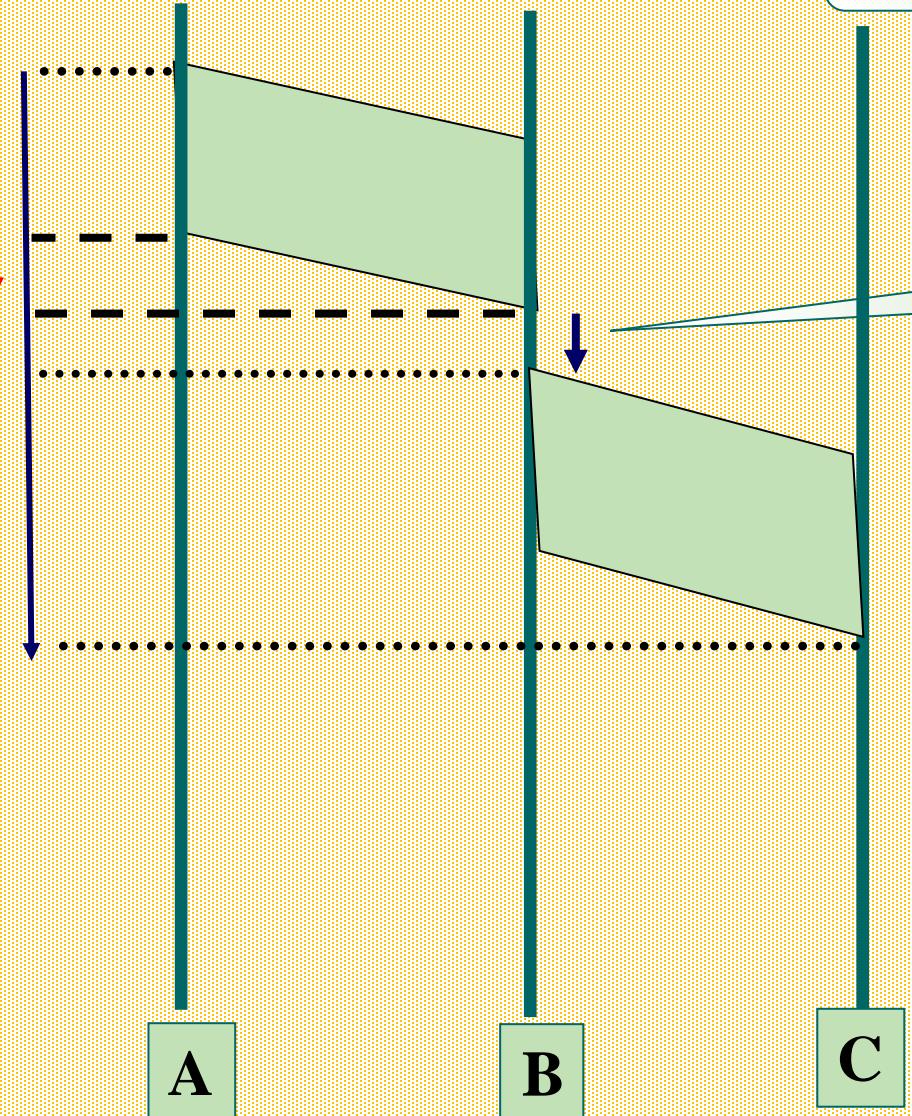
بسته

عدم تأثیر خرابی یک بسته در کل پیام ارسالی و نیاز به ارسال مجدد فقط همان بسته

سوئیچینگ پیام

تأخیر انتظار پردازش

تأخیر انتشار

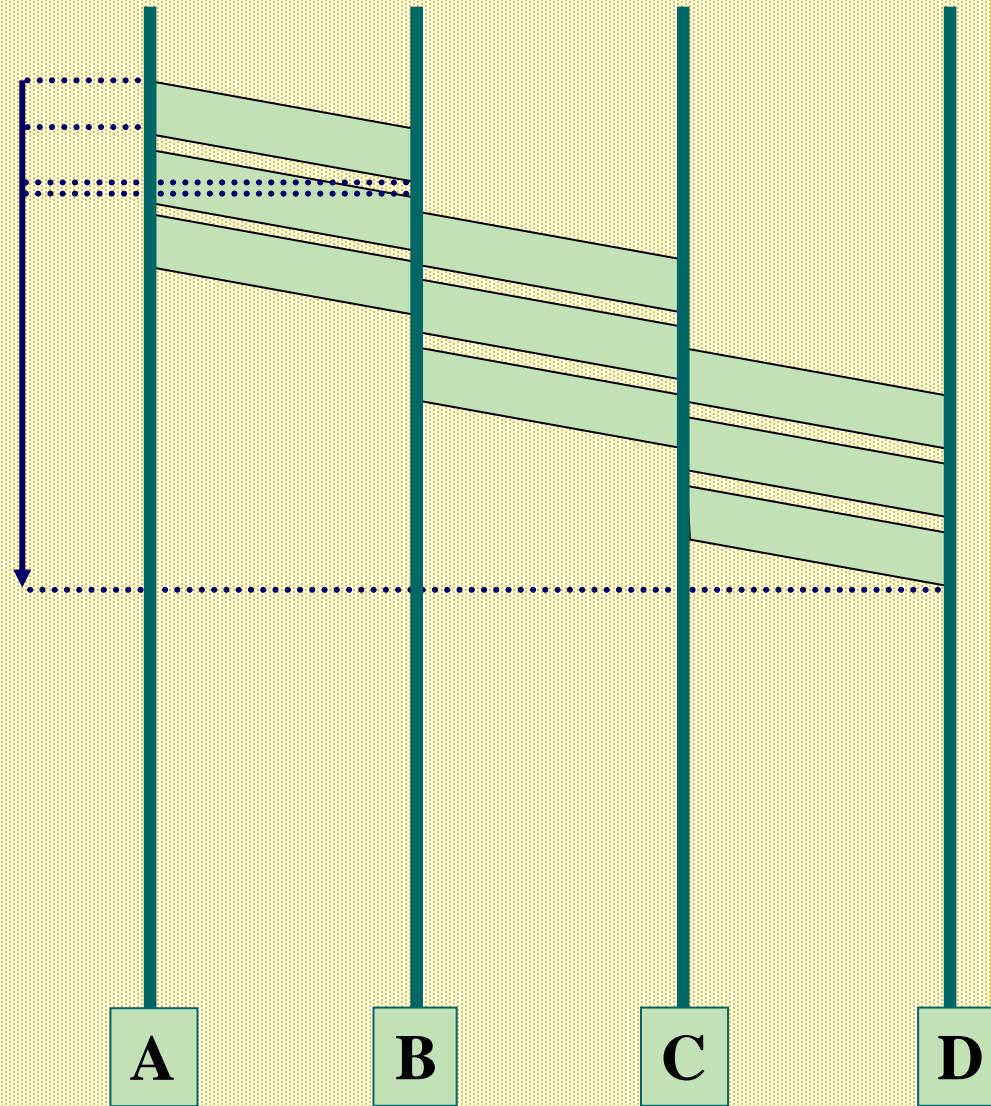


A

B

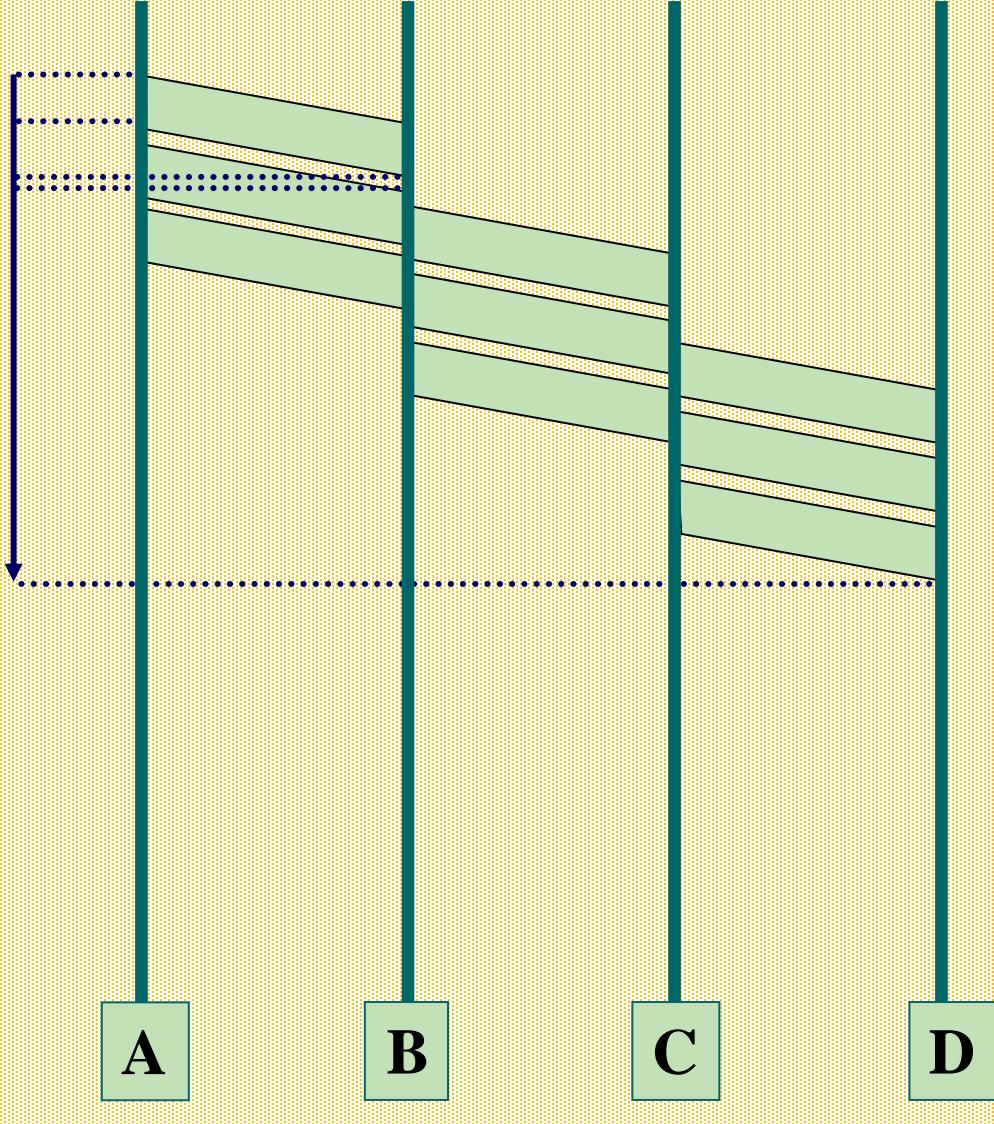
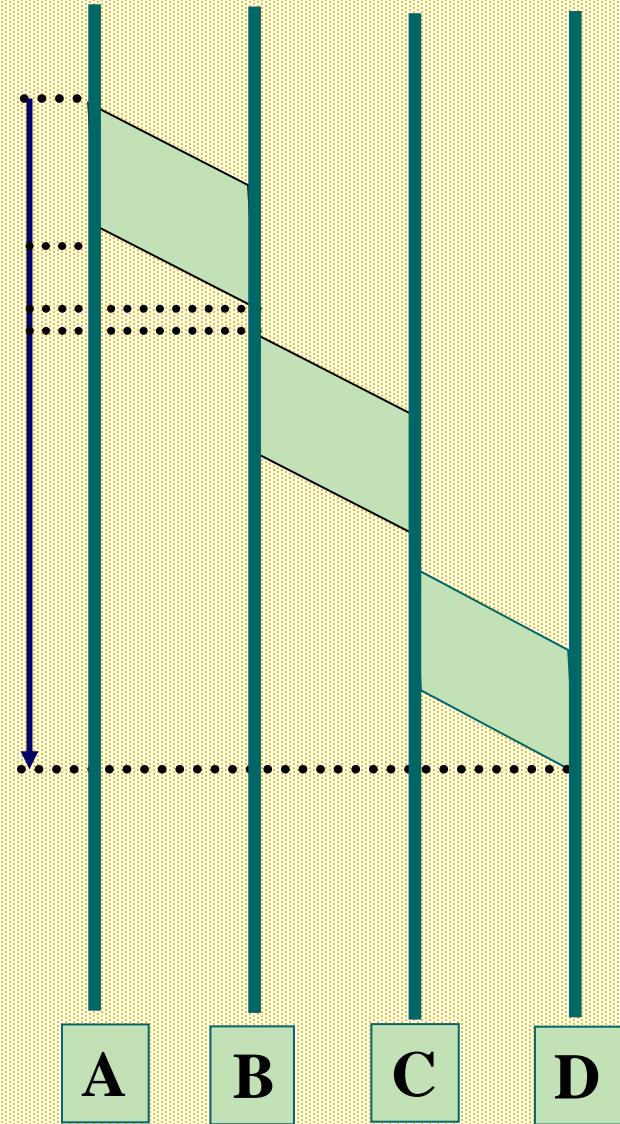
C

سوئیچینگ بسته



سوئیچینگ پیام

سوئیچینگ بسته



زمانبندی تأخیر در روش‌های سوئیچینگ پیام و بسته

انواع ارتباط میان دو ایستگاه

ارتباط یکطرفه – **Simplex** ☺

یکطرف همیشه گیرنده و یکطرف همیشه فرستنده

ارتباط دو طرفه غیرهمزمان – **Half duplex** ☺

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

ارتباط دو طرفه همزمان – **Full duplex** ☺

ارتباط دو طرفه همزمان مانند خطوط ماکروویو

طراحی شبکه ها و اصول لایه بندی

رسالت شبکه: برقراری کانال تبادل داده بین دو برنامه‌ی کاربردی روی دو سیستم میزبان

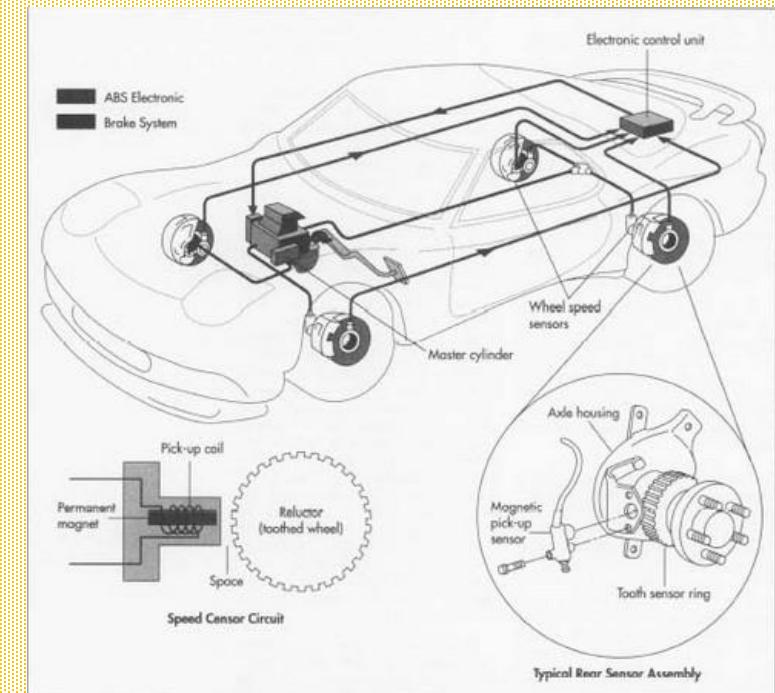
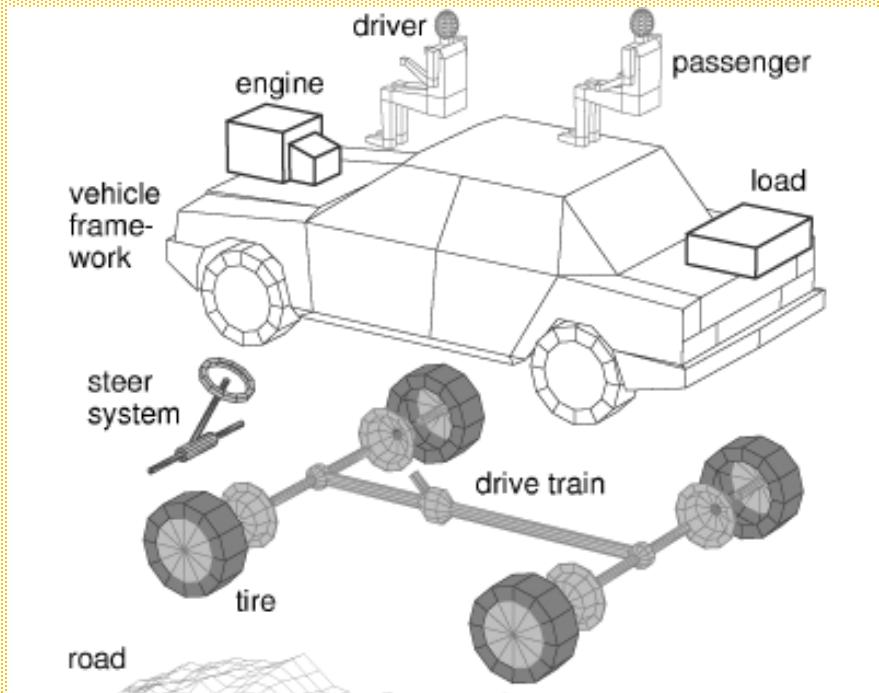
به دلیل پیچیدگی زیاد و گستره‌ی وسیع مؤلفه‌های شبکه، معماری را لایه‌ای در نظر می‌گیریم.

هر لایه به لایه‌ی بالاتر سرویس می‌دهد.

جزیيات پیاده‌سازی لایه‌های پایین از لایه‌های بالا مخفی است.

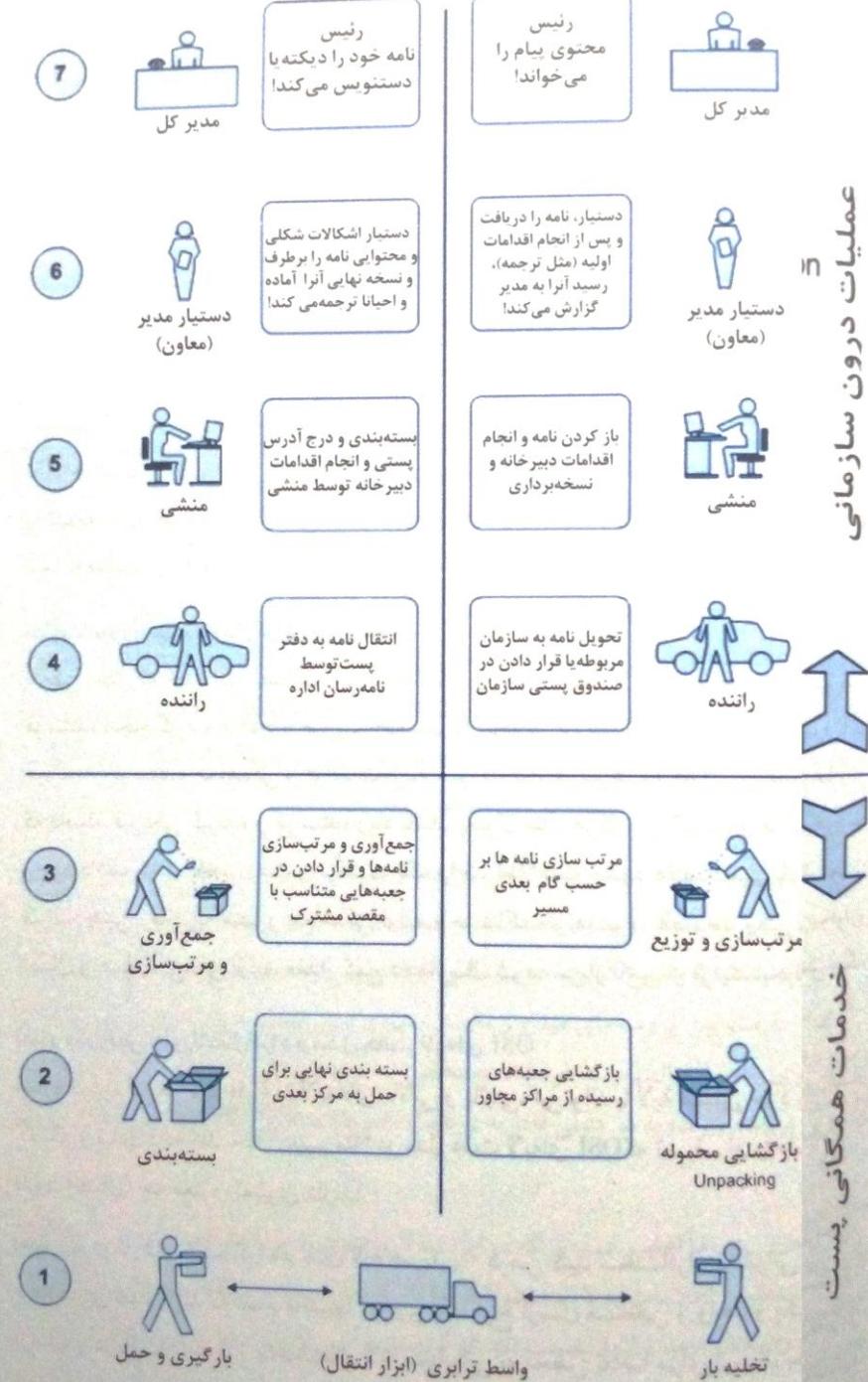
هر مسئله در یک یا چند لایه حل می‌شود.

طراحی شبکه ها و اصول لایه بندی



مدل آبادی ارائه دهنده

عملیات درون سازمانی



طراحی شبکه ها و اصول لایه بندی

برخی از مسائل قابل توجه در طراحی شبکه ها

☺ چگونگی ارسال و دریافت بیتهاي اطلاعات
(تبديل بيتها به يك سينال متناسب با کانال انتقال)

☺ ما هيّت انتقال

☺ خطأ و وجود نویز در کانالهای ارتباطی (کنترل خطأ)

☺ پیدا کردن بهترین مسیر و هدایت بسته ها

☺ تقسیم يك پیام بزرگ به واحدهای کوچکتر و بازسازی پیام

☺ طراحی مکانیزمهای حفظ هماهنگی بین مبدأ و مقصد (کنترل جریان داده)

☺ ازدحام ، تداخل و تصادم در شبکه ها

طراحی شبکه ها و اصول لایه بندی

بخشی از مسائل مهم در طراحی لایه ها

وظایف هر لایه به دقت تعریف شود.

تعداد لایه ها کافی باشد

جزییات لایه های زیرین مهم نباشد

خدمات به لایه های بالا طی یک روال ساده قابل انجام باشد.

مرزهای بین لایه ها طوری باشد که جریان اطلاعات بین لایه ها حداقل باشد.

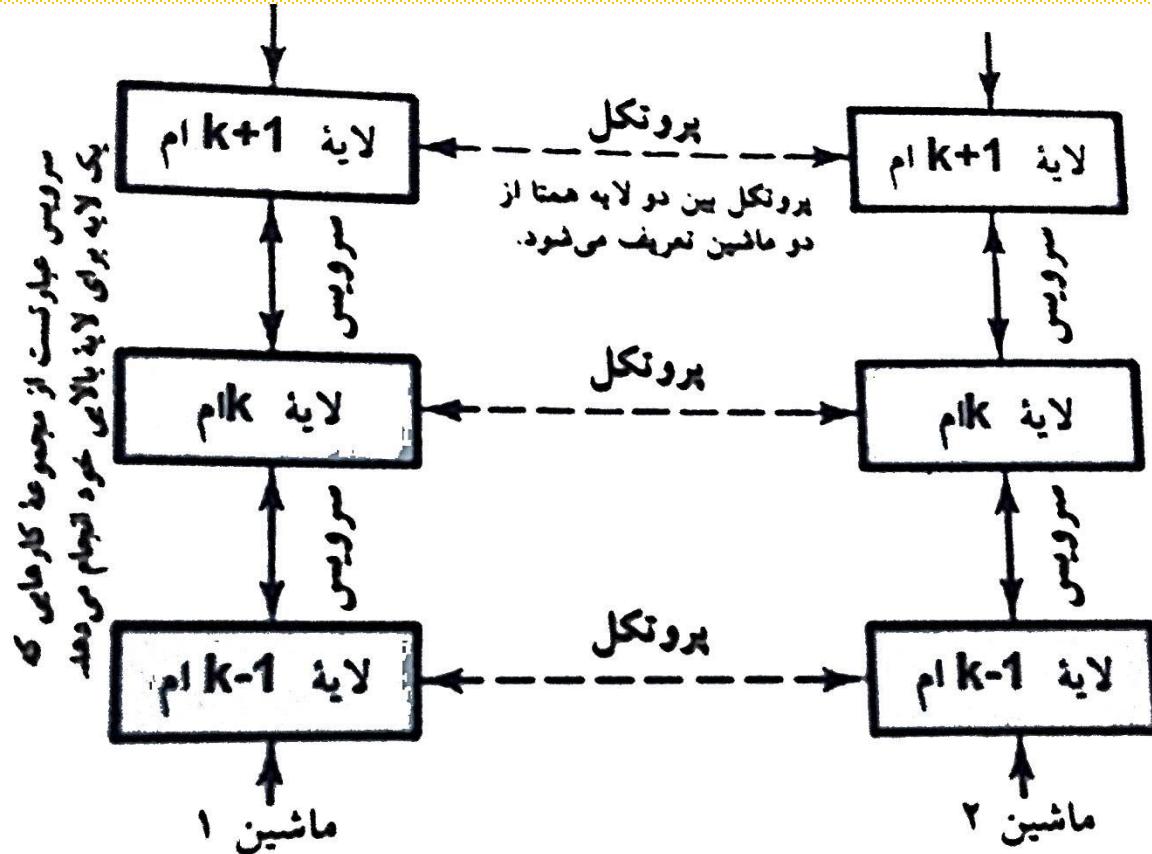
طراحی شبکه ها و اصول لایه بندی

چند اصطلاح

- لایه های همتا (Peer): لایه های مشابه دو ماشین که با هم تعامل دارند.
- واحد داده‌ی پروتکل (Protocol Data Unit: PDU): قطعه داده‌ای که در یک لایه سازماندهی و تحویل لایه‌ی زیرین می‌شود.
- کپسوله‌سازی: هر لایه قبل از تحویل PDU به لایه‌ی پایین‌تر به اول و آخر آن سرآیند و پی‌آیند اضافه می‌کند تا در لایه‌ی همتا قابل درک باشد. در لایه‌ی مقصد این اطلاعات سربار جدا می‌شوند.
- سرویس: مجموعه خدمات یک لایه به لایه‌ی بالاتر
- پروتکل: کلیه قراردادهای توافق شده بین لایه های همتا (قالب‌بندی، مفهوم و تعبیر پیام‌ها و ...)
- پشتی پروتکلی: مجموعه پروتکل‌های همه‌ی لایه‌ها
- معماری شبکه: مجموعه لایه‌ها و پروتکل‌های شبکه
- مدل مرجع: مدل انتزاعی معماری لایه‌ای شبکه بدون پرداختن به جزئیات پیاده‌سازی (SNA، Decnet، IPX، AppleTalk، TCP/IP، OSI).



محل تعریف سرویس و پروتکل در معماری لایه‌ای شبکه



محل تعریف سرویس و پروتکل در معماری لایه‌ای شبکه

مدل هفت لایه ای ISO از سازمان استاندارد جهانی Open System Interconnection:

Physical layer لایه فیزیکی ☺

Data link layer لایه پیوند داده ها ☺

Network layer لایه شبکه ☺

Transport layer لایه انتقال ☺

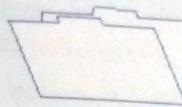
Session layer لایه جلسه ☺

Presentation layer لایه ارائه (نمایش) ☺

Application layer لایه کاربرد ☺

OSI MODEL

لایه کاربرد



انواع سرویس‌های کاربردی سطح بالا شامل:
پرونکل های انتقال نامه‌های الکترونیکی،
انتقال فایل، انتقال صدا و تصویر و صدها
سرویس کاربردی دیگر

۷

لایه نمایش (ارائه)



رمزگاری و رمزگشایی
فسرده‌سازی و بازگشایی
تبدیل کد (یونی‌کد، اسکی، ای‌سی‌دی‌ک و ...)

۶

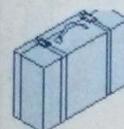
لایه نشست



شروع و ختم هماهنگ نشست
سنکرونیزاسیون و ایجاد رکوردهای حالت
ادامه نشستهای قطع شده

۵

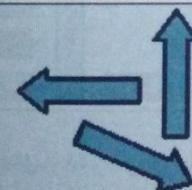
لایه انتقال



شکستن پیامهای بزرگ به قطعات دارای هویت
ایجاد اتصال‌های انتهایی به انتهای
حفظ ترتیب بسته‌ها و جریان بایت‌ها
هویت بخشیدن به پرسوهای و ...

۴

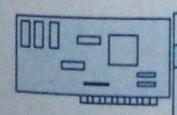
لایه شبکه



مسیریابی و هدایت بسته‌ها
بر اساس آدرس جهانی
پیشگیری از ازدحام و کنترل ترافیک

۳

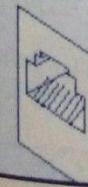
لایه پیوند داده



انتقال فرمهای اطلاعات بین دو
گره متصل به یک کانال فیزیکی
بر اساس آدرس محلی
کشف و کنترل خطأ، کنترل جریان

۲

لایه فیزیکی



انتقال بسته‌ها بر روی کانال فیزیکی
و حل مسائل مرتبط با کانال

۱

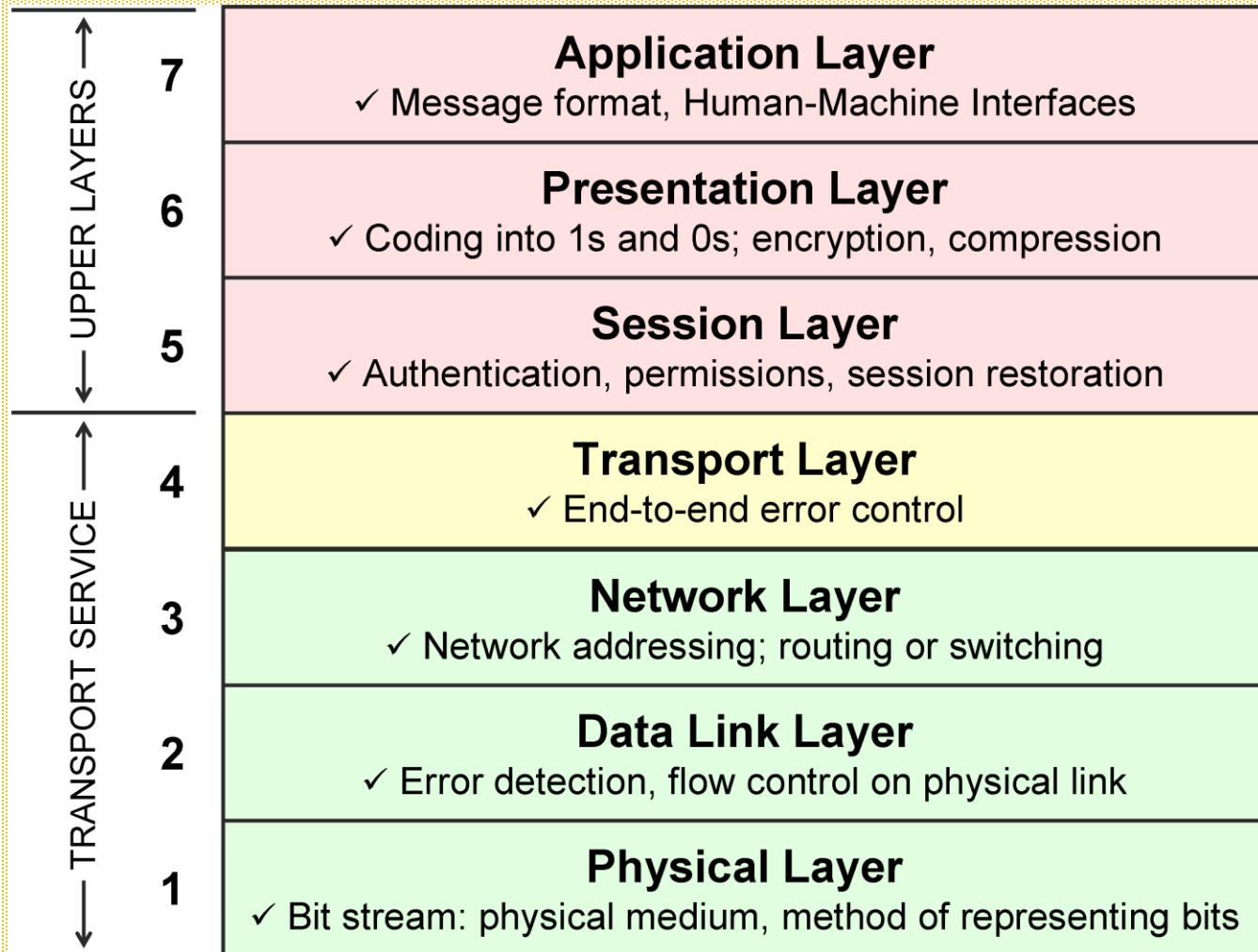
Segments

Packets

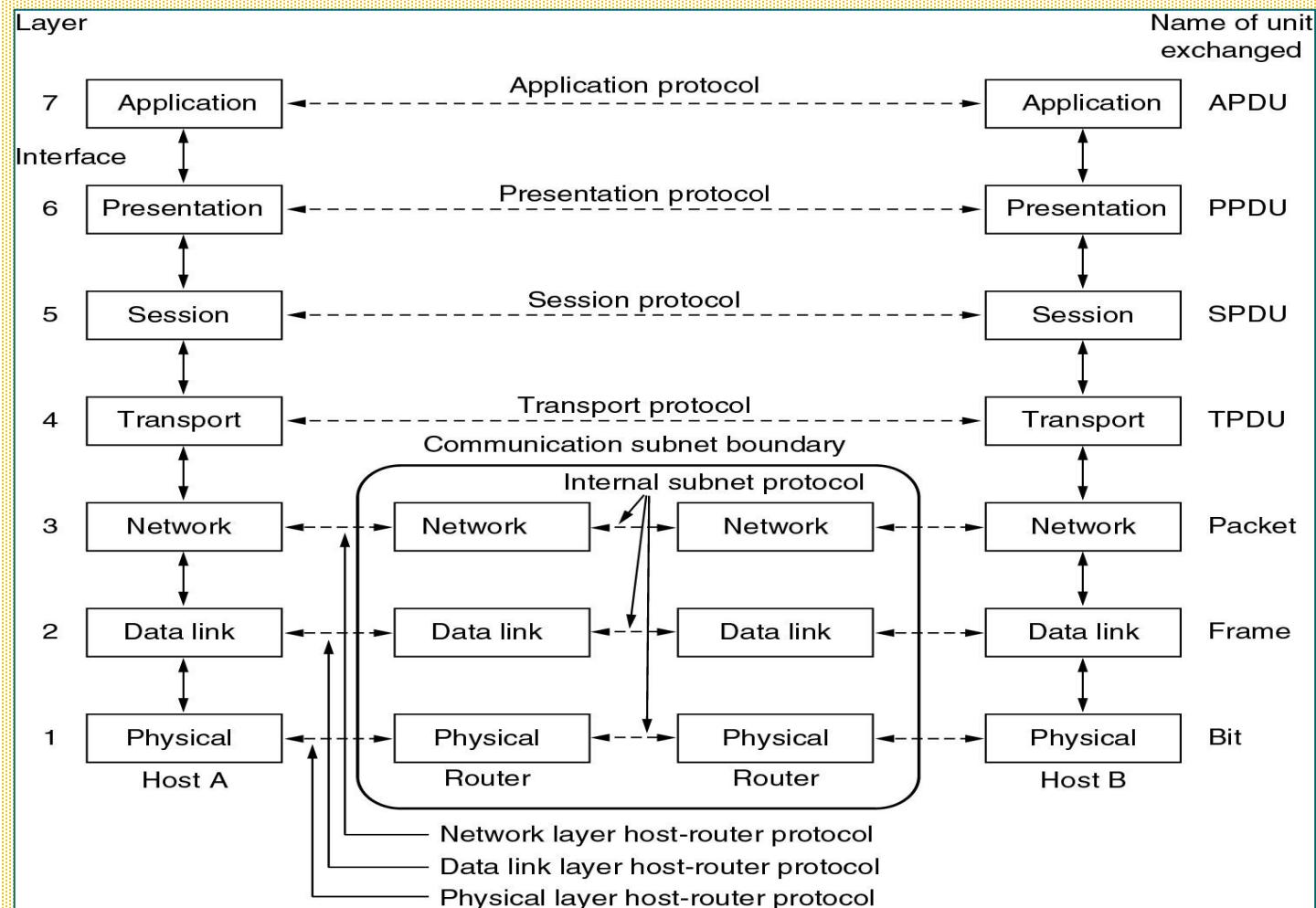
Frames

Bits

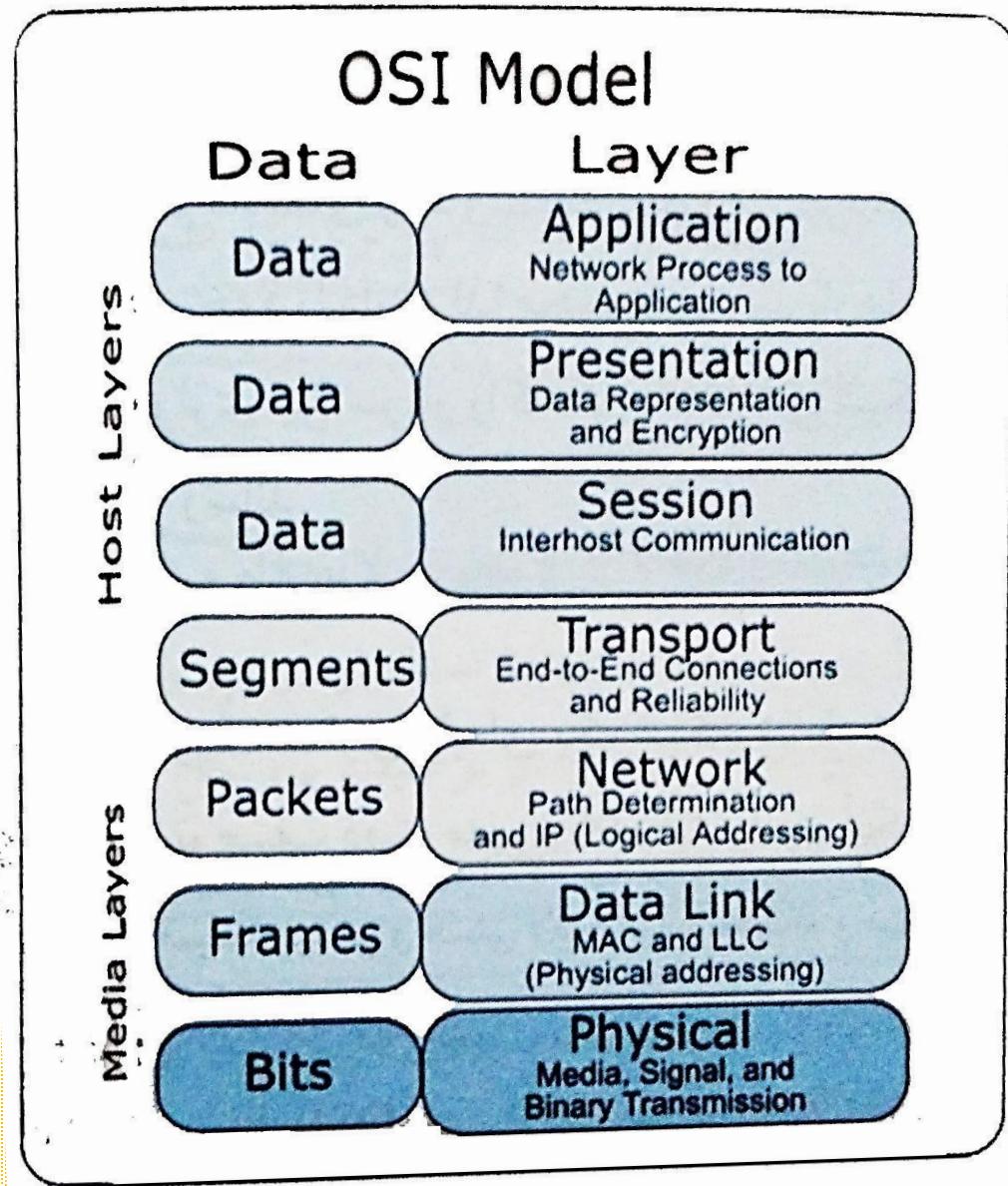
مدل هفت لایه‌ای ISO از سازمان استاندارد جهانی



مدل هفت لایه‌ای OSI

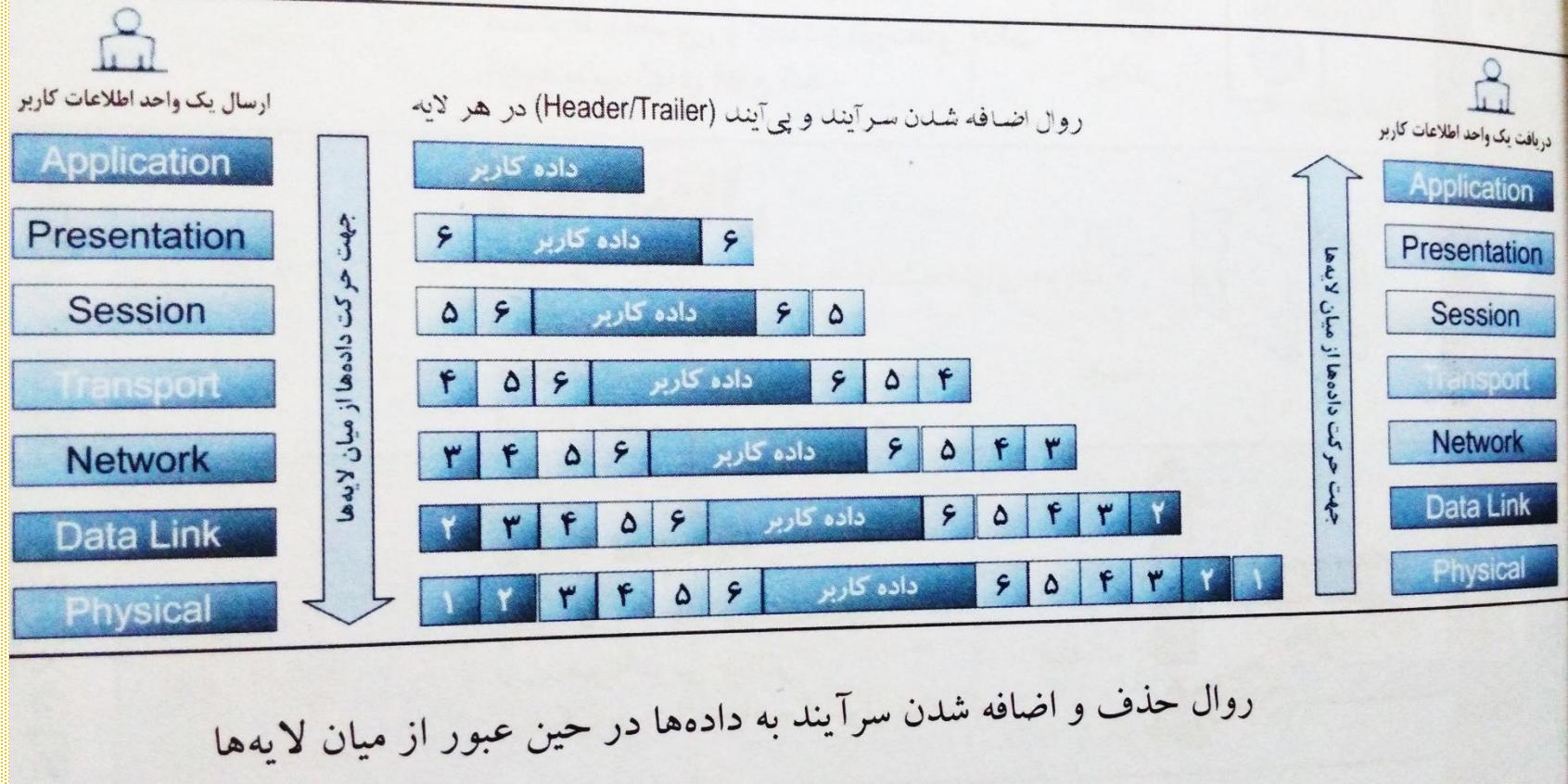


OSI Model



دorنمای مدل مرجع OSI

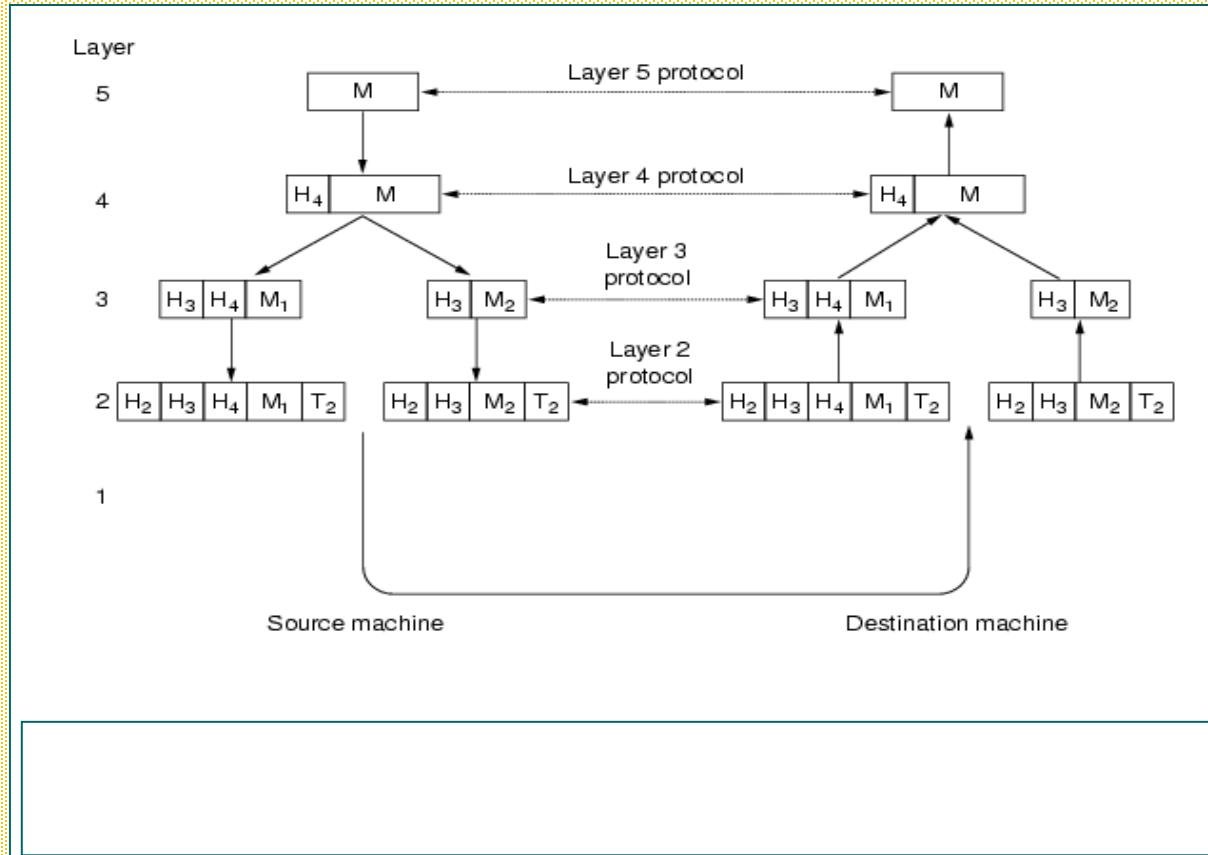
روند حذف و اضافه شدن سرآیند در هر لایه



روال حذف و اضافه شدن سرآیند به داده‌ها در حین عبور از میان لایه‌ها

ماشین مسیریاب فقط تا لایه‌ی شبکه را دارد

روند حذف و اضافه شدن سرآیند در هر لایه



لایه فیزیکی Physical Layer

(+ انتقال بیتها به صورت سیگنال الکتریکی و ارسال آن بر روی کانال

(+ واحد اطلاعات : بیت

(+ در کی از مفهوم پیام ندارد و تنها آن را منتقل می‌کند.

پارامترهای قابل توجه :

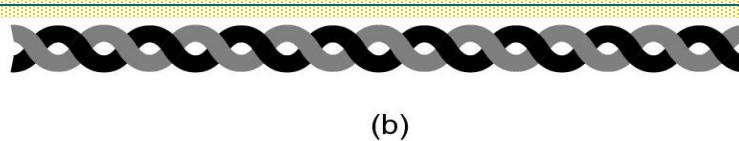
- ماهیت خط انتقال (سیم مسی، فیبر نوری، خلاء,...)
- ظرفیت کانال فیزیکی و نرخ ارسال (Bit Rate)
- نوع مدولاسیون
- سطح ولتاژ صفر و یک، مدت دوام یک بیت، جهت انتقال، اتصال اولیه، قطع اتصال، ...
- چگونگی کوپلر با خط انتقال
- مسائل مکانیکی و الکتریکی مانند نوع کابل، باند فرکانسی، نوع رابط (کانکتور) کابل

کانالهای انتقال

- خطوط تلفن
- فیبرهای نوری
- سیمهای به هم بافته شده زوجی
- کابلهای هم محور (کواکسیال)
- کانالهای ماهواره‌ای
- کانالهای رادیویی
- امواج طیف نوری



(a)



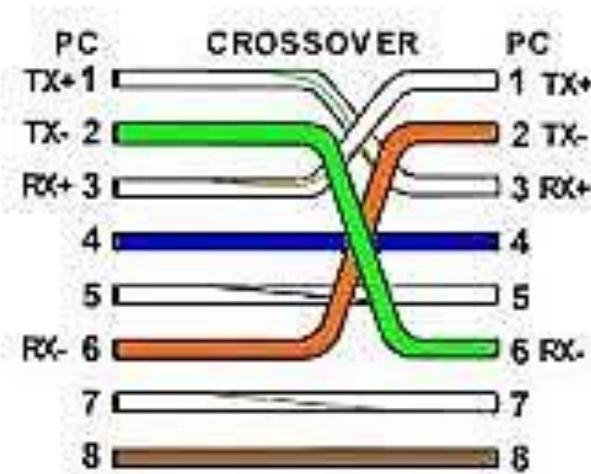
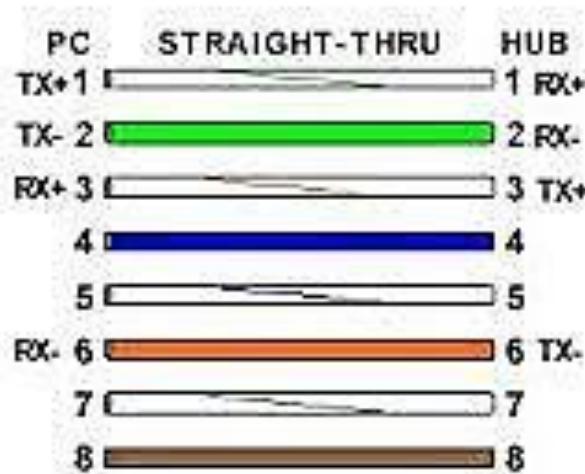
(b)

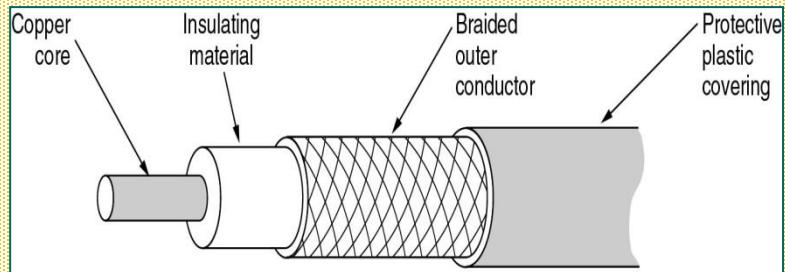
(a) Category 3 UTP.
 (b) Category 5 UTP.

سیمهای به هم بافته شده زوجی (Twisted Pair)

UTP : یک زوج سیم معمولی به هم بافته شده

STP : یک زوج سیم معمولی به هم بافته شده
 به همراه یک پوشش آلومینیمی بر روی آنها جهت
 کاهش اثر نویزهای محیطی بر روی سیم





کابل‌های هم محور (کواکسیال):
در انواع مختلف مانند:

Tick Coaxial Cable
Thin Coaxial Cable
کابل کواکس 50 اهم ضخیم
کابل کواکس 50 اهم نازک
کابل کواکس 75 اهم معمولی)



کانالهای ماهواره‌ای : در باندهای فرکانسی مختلف

مانند:

• باند C

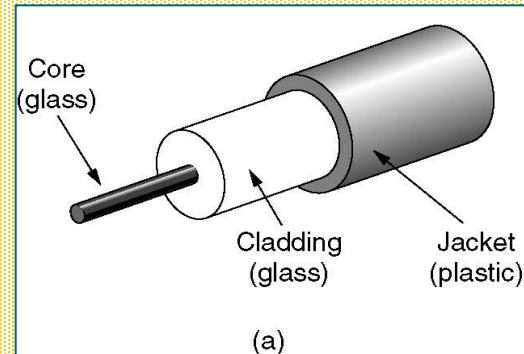
• باند Ku

• باند Ka

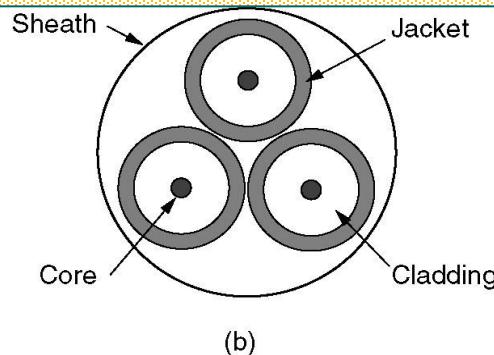
کانالهای رادیویی : شامل باندهای فرکانسی مختلف مثل VHF ، UHF

امواج طیف نوری: شامل نور مادون قرمز

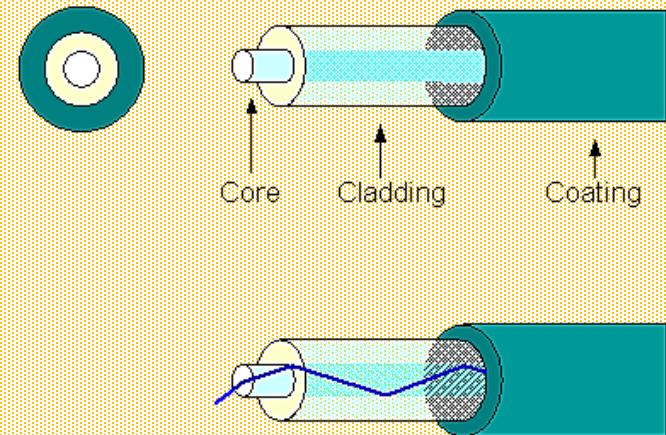
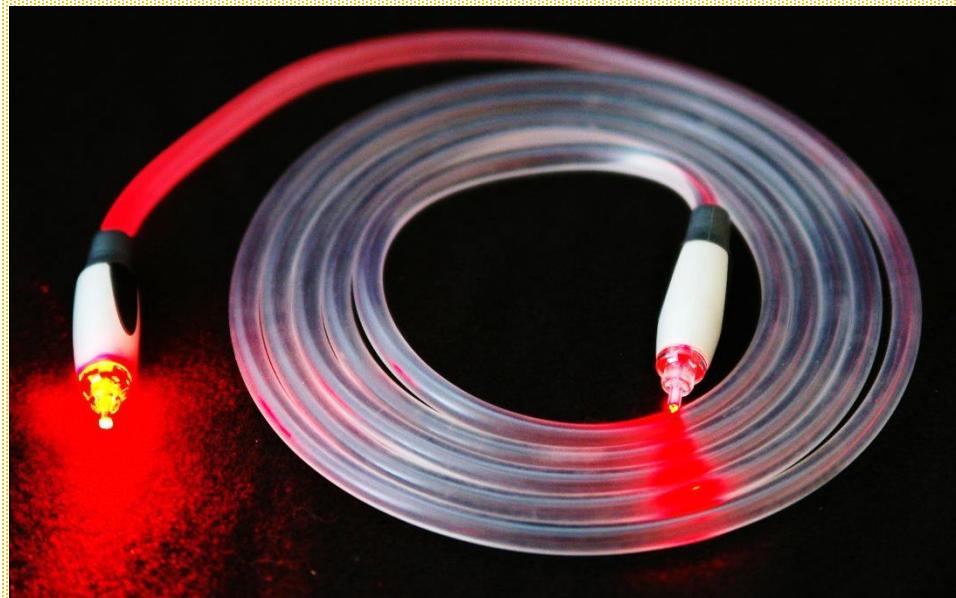
فیبرهای نوری : در انواع مختلف مثل فیبر تکموده و چندموده



(a)



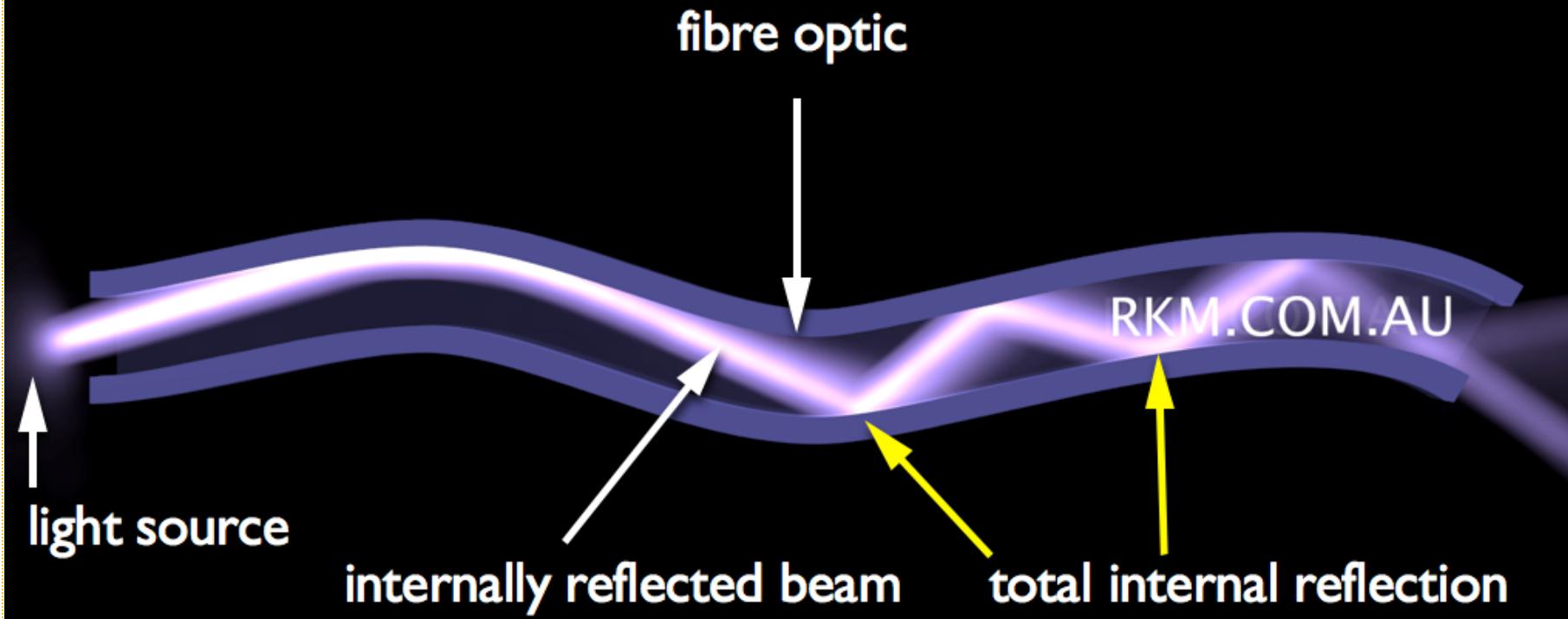
(b)



The Optical Fiber carries the light in its core, whose Refractive Index is greater than that of the cladding

فیبرهای نوری : در انواع مختلف مثل فیبر تکموده و چندموده

Fibre Optic: transmission of light

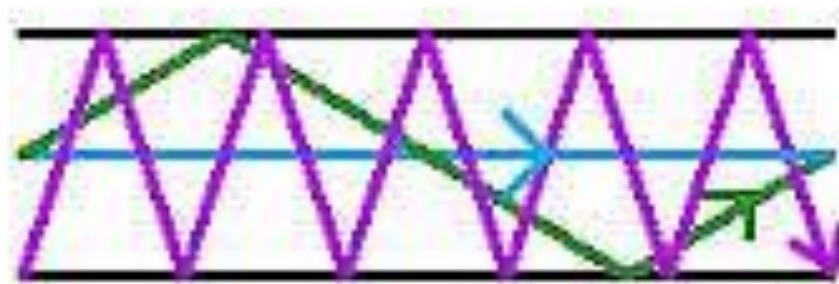


فیبرهای نوری : در انواع مختلف مثل فیبر تکموده و چندموده

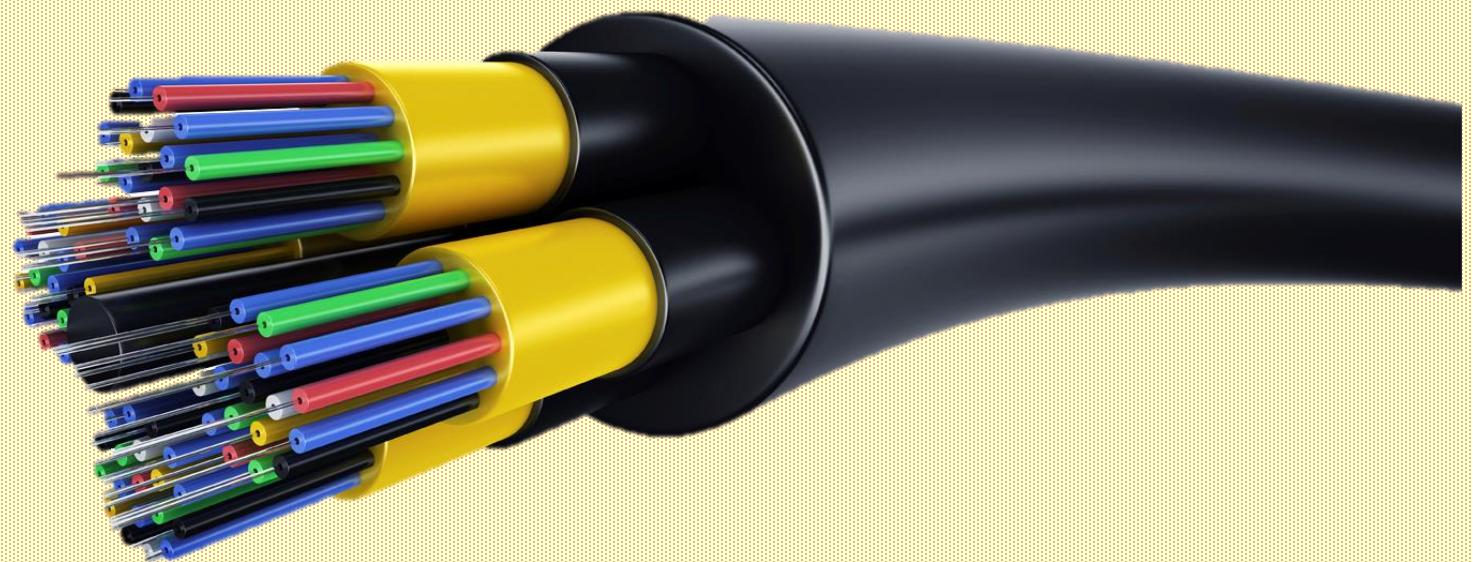
Single-mode fiber



Multi-mode fiber



فیبرهای نوری



توضیح	قیمت	پیاده سازی	خطا	پهنای باند	نوع کanal
از قبل وجود دارد	ارزان	ساده	زیاد	کم (حدود ۴ KHz)	خطوط تلفن معمولی
برای فواصل کوتاه مناسب است	ارزان	ساده	متوسط	متوسط (حدود چند ده تا صد مگاهرتز)	زوج سیم
	متوسط	متوسط	کم	حدود چند صد مگاهرتز	کابل‌های کواکس
بهترین کارایی در همه جا تحت پوشش	متوسط	پیچیده	بسیار کم	حدود چند گیگاهرتز	فیبر‌های نوری
در جایی که کابل کشی عقلایی نیست مناسب می‌باشد.	گران	بسیار پیچیده	متوسط	حدود چند صد مگاهرتز	کانال‌های ماهواره
	نسبتاً گران	نسبتاً پیچیده	زیاد	حدود چند مگاهرتز	کانال‌های رادیویی

مقایسه مشخصات برخی از کانال‌های انتقال

پهناى باند:

توانایی و ظرفیت کanal در ارسال اطلاعات با نرخ **B** بیت در هر ثانیه

رابطه شanon:

$$C=B \cdot \log_2(1+S/N)$$

C : ظرفیت کanal بر حسب بیت بر ثانیه

S : متوسط توان سیگنال

N : متوسط توان نویز

B : پهناى باند کanal بر حسب هرتز

لایه پیوند داده - Data Link Layer

بیمه‌ی اطلاعات: کنترل خطأ و جریان داده و مدیریت دسترسی به کانال ☺

واحد اطلاعات : فریم (Frame) ☺

داده‌های لایه‌های بالاتر در این لایه به فریم شکسته و با حفظ ترتیب ارسال می‌شود. ☺

وظایف:

- به مقصد رساندن داده‌ها روی یک کانال انتقال بدون خطأ (ذاتاً در کانال‌های فیزیکی خطأ وجود دارد) و مطمئن با استفاده از مکانیزم‌های کشف و کنترل خطأ.
- شکستن اطلاعات ارسالی از لایه بالاتر به واحدهای استاندارد و کوچکتر و مشخص نمودن ابتدا و انتهای آن از طریق نشانه‌های خاصی بنام **Delimiter**.
- کنترل جریان یا تنظیم جریان ارسال فریمها (مکانیزم‌های هماهنگی بین مبدأ و مقصد)
- اعلام وصول یا عدم رسیدن داده‌ها به فرستنده
- وضع قراردادهایی برای جلوگیری از تصادم سیگنال‌های ارسالی در شبکه‌های چندپیخشی (این قراردادها در زیرلایه‌ای بنام **MAS** (Medium Access Sub layer: 2.5) تعریف شده است)
- کنترل سخت‌افزار لایه فیزیکی

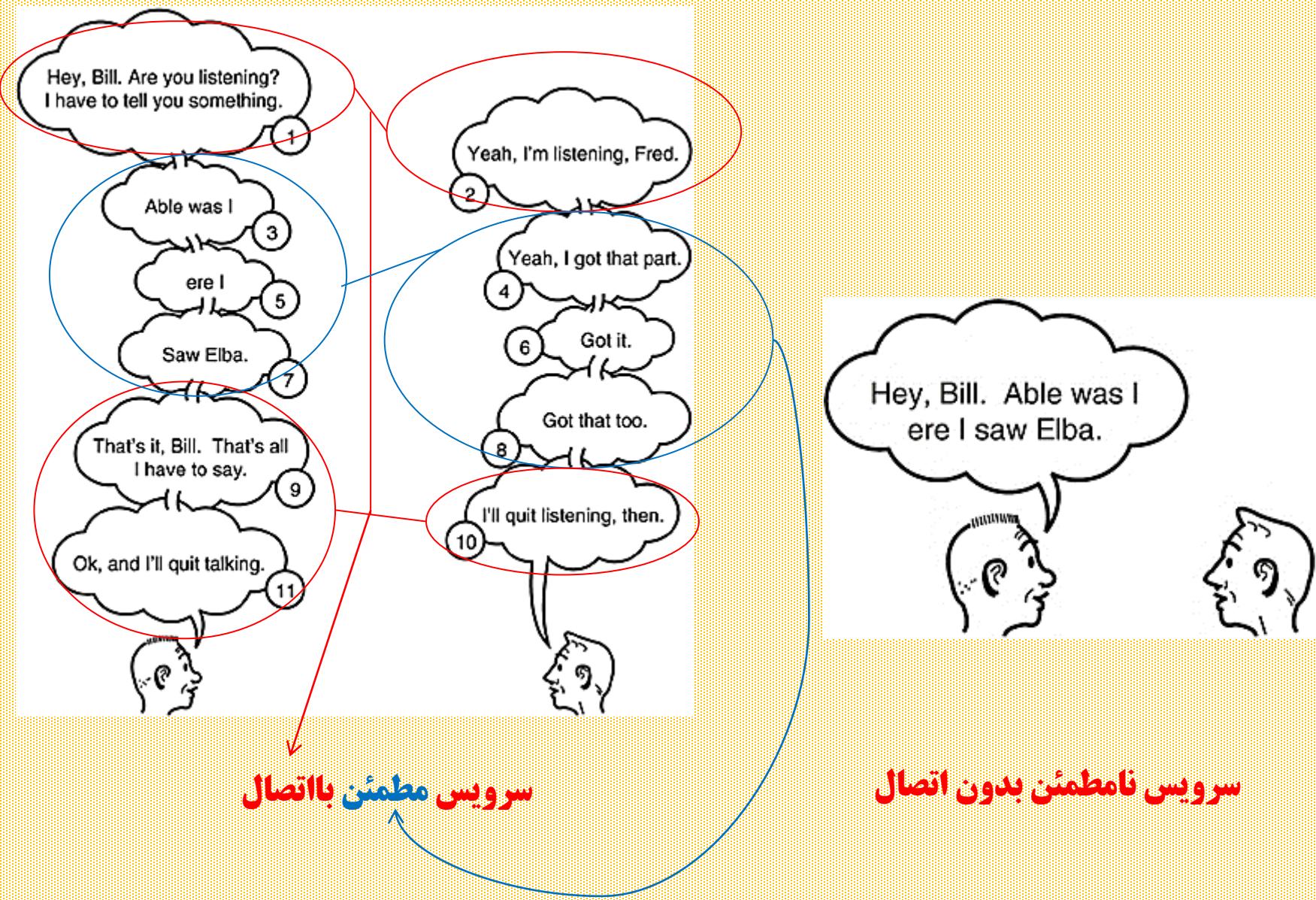
چند تعریف

• سرویس مطمئن (Reliable - Acknowledged): اگر یک لایه به لایه بالاترش این اطمینان را بدهد که داده‌های او را حتماً ارسال می‌کند (از طریق ACK).

• سرویس نامطمئن (Unreliable): یک لایه بیشترین تلاش را می‌کند تا داده‌های لایه بالا را ارسال کند. اما تضمین نمی‌دهد. اگر نیاز به اطمینان داشته باشیم باید در لایه بالاتر ایجاد کنیم.

- سرویس اتصال‌گرا (Connection Oriented): اگر قبل از برقراری ارتباط بین دو لایه همتا هماهنگی صورت گیرد.
- ترتیب بسته‌های حفظ می‌شود.
- ضریب اطمینان بالا
- اتلاف زمانی زیاد برای برقراری هماهنگی
- مانند ایجاد یک کانال مجازی بین دو طرف ارتباط است.

• سرویس بدون اتصال (Connectionless): اگر ارسال اطلاعات بدون اطلاع و هماهنگی بین دو لایه همتا صورت گیرد. هیچ تضمینی برای رسیدن اطلاعات، اطلاع فرستنده از نرسیدن اطلاعات، صحت و ترتیب داده‌ها وجود ندارد. در عوض سریع و ارزان است.



مثال	اطمینان	اتصال
Remote Login	✓	✓
Online Multimedia	✗	✓
File Transfer	✓	✗
Email	✗	✗

QoS: مجموعه قراردادهای (SLA) تضمین کیفیت خدمات (Loss, Jitter, Delay و ...)
 مثلاً پخش آفلاین صوت و تصویر به D و L حساس نیست، اما به L حساس است.

زیرلایه‌های لایه‌ی پیوند داده

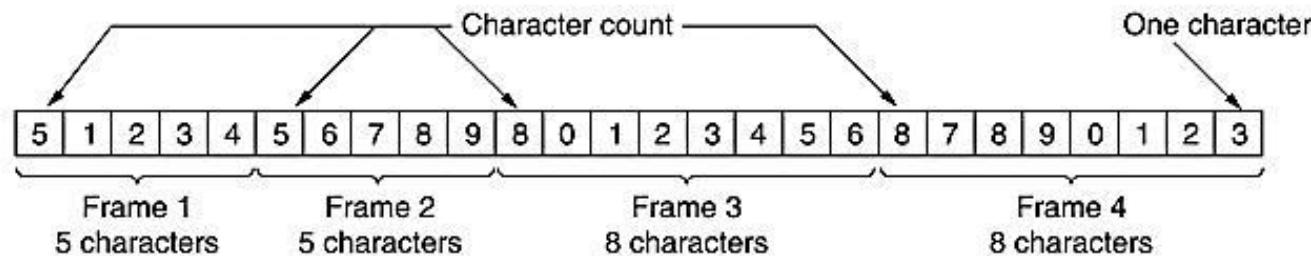
زیرلایه‌ی (Logic Line Control) LLC: ارتباط با لایه‌ی شبکه - کنترل جریان داده - ارائه‌ی سرویس مطمئن + حفظ ترتیب پسته‌ها) اگر در استاندارد مورد استفاده تعریف شده باشد (مثلاً اترنت ندارد)، کنترل خط، قاب‌بندی.

زیرلایه‌ی (Medium Access Control) MAC: ارتباط با لایه‌ی فیزیکی - کنترل دسترسی به کانال مشترک.

روش‌های قاب‌بندی

Character Count Framing

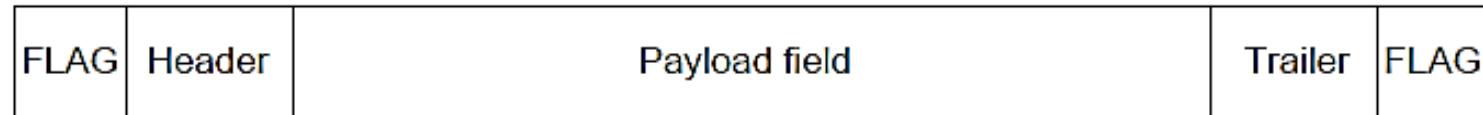
- Each frame contains a header with the number of characters in the frame



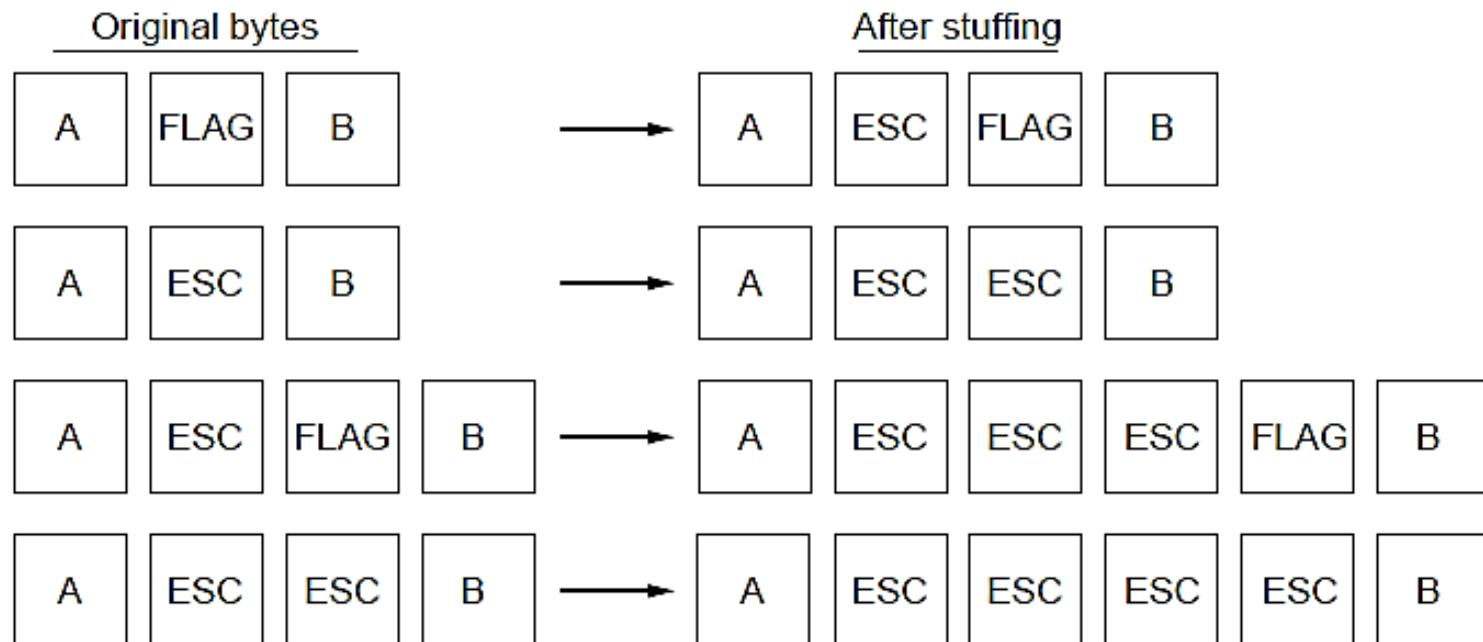
روش‌های قاب‌بندی

- Starting & Ending Characters with Character Stuffing

FLAG for delimitation, ESC for determining non-FLAG data



(a)



(b)

روش‌های قاب‌بندی

- **Starting & Ending Flags with bit Stuffing**
 - Each frames begins and ends with a special bit pattern (01111110 or 0x7E)
 - Whenever the sender's data link layer encounters five consecutive 1s in the data it automatically stuffs a 0 bit into the outgoing bit stream.
 - USB uses bit stuffing
 - When the receiver sees *five consecutive incoming ones followed by a 0 bit*, it automatically de-stuffs the 0 bit before sending the data to the network layer.

(a) 011011111111111111110010

(b) 01101111011111011111010010

(c) 0110111111111111111110010

Stuffed bits

- (a) The original data. (b) The data as they appear on the line. (c) The data as they are stored in the receiver's memory after destuffing.

روش‌های قاب‌بندی

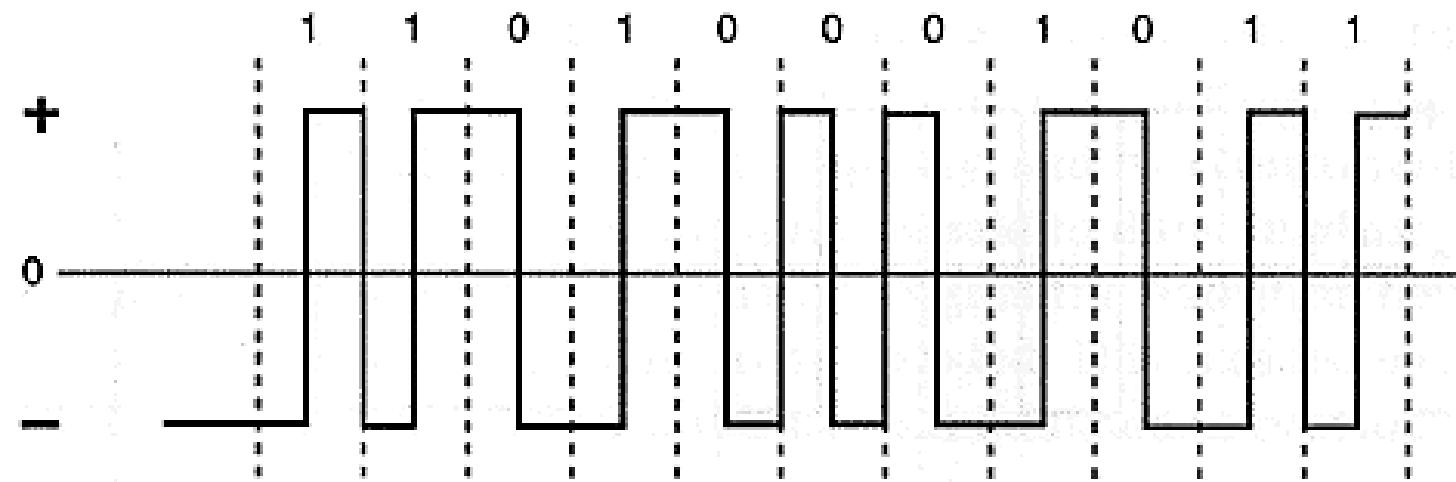
- **Starting & Ending Flags with bit Stuffing**
- Each frames begins and ends with a special bit pattern (01111110 or 0x7E)
- Whenever the sender's data link layer encounters five consecutive 1s in the data it automatically stuffs a 0 bit into the outgoing bit stream.
- USB uses bit stuffing
- When the receiver sees *five consecutive incoming ones followed by a 0 bit*, it automatically de-stuffs the 0 bit before sending the data to the network layer.

A bit string, 0111011110111110, needs to be transmitted at the data link layer. What is the string actually transmitted after bit stuffing?

The output is 011101111001111010

روش‌های قاب‌بندی

- Physical Coding Violation



Boundaries are determined by no change in the mid-clk-time

روش‌های قاب‌بندی

- Many data link protocols use a combination of presented methods for safety. For example in Ethernet and 802.11 each frame begin with a well-defined pattern called a preamble.
- Preamble is typically 72 bits long.
- It is then followed by a length field.

انواع خطا در شبکه‌های کامپیوتری

- نویز حرارتی
- شوک‌های الکتریکی
- نویز کیهانی

روشهای کشف خطا

- اضافه کردن بیت توازن به داده‌ها
- Checksum**
- کدهای کشف خطای **CRC**

بیت توازن

- ساده‌ترین روش کشف خطأ
- اضافه نمودن یک بیت توازن به ازای هر بایت از اطلاعات
- انتخاب بیت توازن به گونه‌ای که مجموع تعداد بیتهاي 1 همیشه زوج یا فرد باشد
- این روش در صورتی موثر است که تعداد خطاهای رخ داده زوج نباشد

Odd Parity 1
Even Parity 0

01101001
011010011
011010010

بایت اصلی:
بیت توان فرد
بیت توان زوج

بیت توازن

روش InterLeaving

1	2	...	k
1	2	...	k
1	2	...	k
1	2	...	k

در این روش از بیت توازن هم برای سطر ها یعنی (فریم ها) و هم برای ستون ها استفاده می شود.

Checksum روش

- جمع (XOR) تمام بایت‌های یک فریم ارسالی توسط فرستنده و **Checksum** ایجاد بایت

- این روش در صورتی قادر به کشف خطا است که تعداد خطاهای رخ داده در بیت‌های هم ارزش زوج نباشد

CRC کدهای کشف خطای

- محاسبه تعدادی بیت کنترلی به نام **(Cyclic Redundancy Check) CRC** به ازای مجموعه‌ای از بیتها و اضافه شدن به انتهای فریم
- مبنای کار : تقسیم چند جمله‌ای

$$\text{CRC12 : } G = X^{12} + X^{11} + X^3 + X^2 + X^1 + 1$$

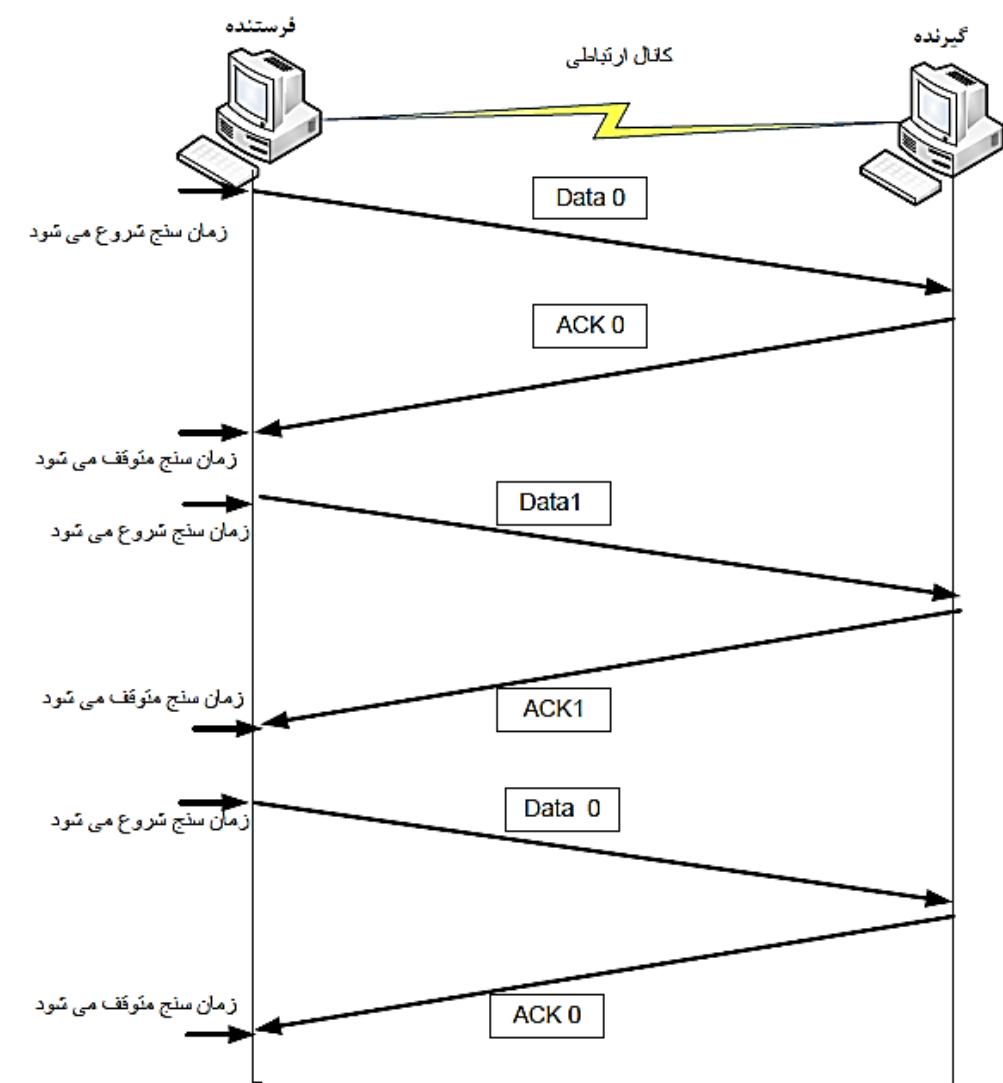
$$\text{CRC - CCIT : } G = X^{16} + X^{12} + X^5 + 1$$

$$\text{CRC16 : } G = X^{16} + X^{15} + X^2 + 1$$

روش‌های کنترل جریان داده و ارائه‌ی سرویس مطمئن (ARQ)

• Stop & Wait Protocol

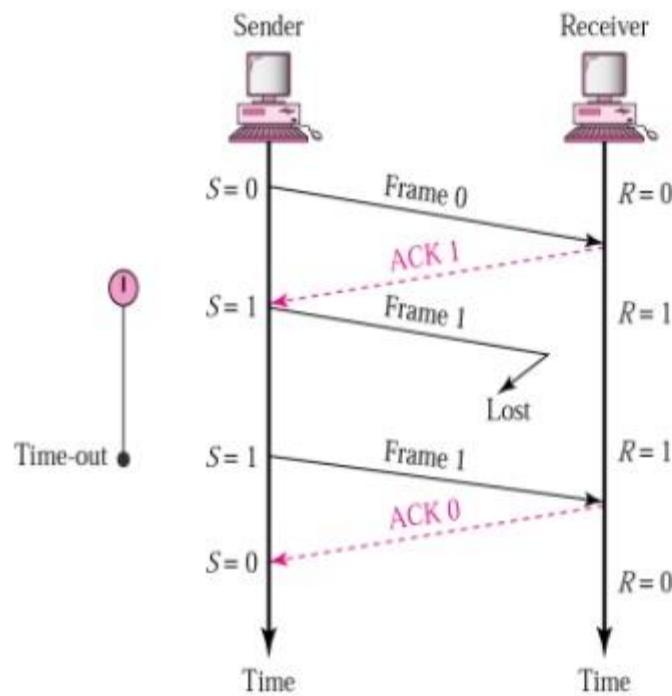
All packets and ACKs are numbered 0 or 1



روش‌های کنترل جریان داده و ارائه‌ی سرویس مطمئن

- Stop & Wait Protocol

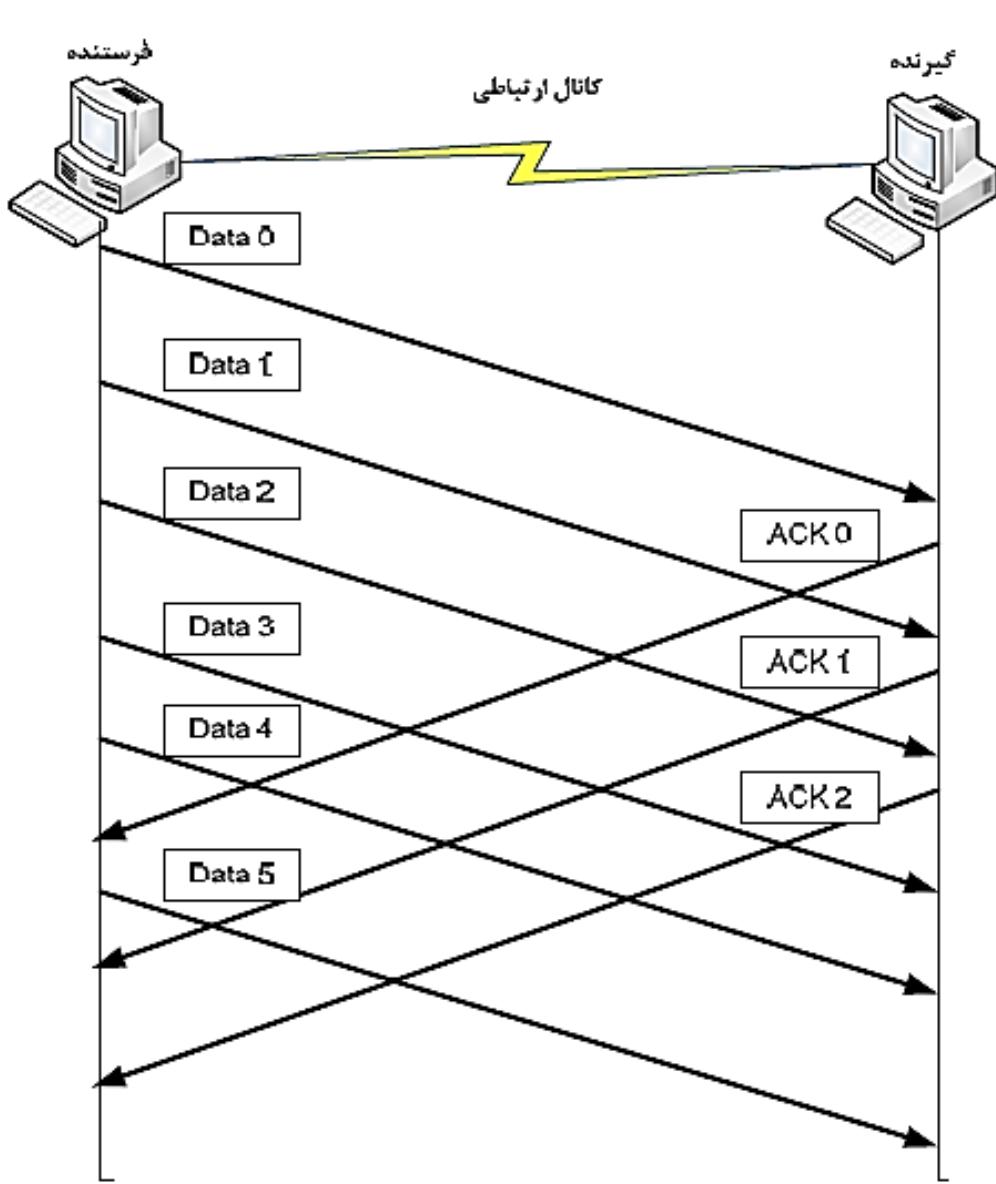
Stop-and-Wait ARQ, lost ACK frame



- When a receiver receives a damaged frame, it discards it and keeps its value of R .
- After the timer at the sender expires, another copy of frame 1 is sent.

برای کنترل جریان داده و ارائه سرویس مطمئن باید تکمیل کرد: **Stop-and-Wait ARQ**, **Go-back-N** و **Selective Repeat**.

روش‌های کنترل جریان داده و ارائه‌ی سرویس مطمئن (ARQ)



مشکل روش توقف و انتظار، در فواصل طولانی خود را نشان می‌دهد.

روش پنجره‌ی لغزان (Sliding Window)

فرستنده بدون منتظر ماندن برای ACK تک تک قاب‌ها، یک پنجره قاب را ارسال می‌کند و گیرنده نیز به صورت جمعی ACK صادر می‌کند.

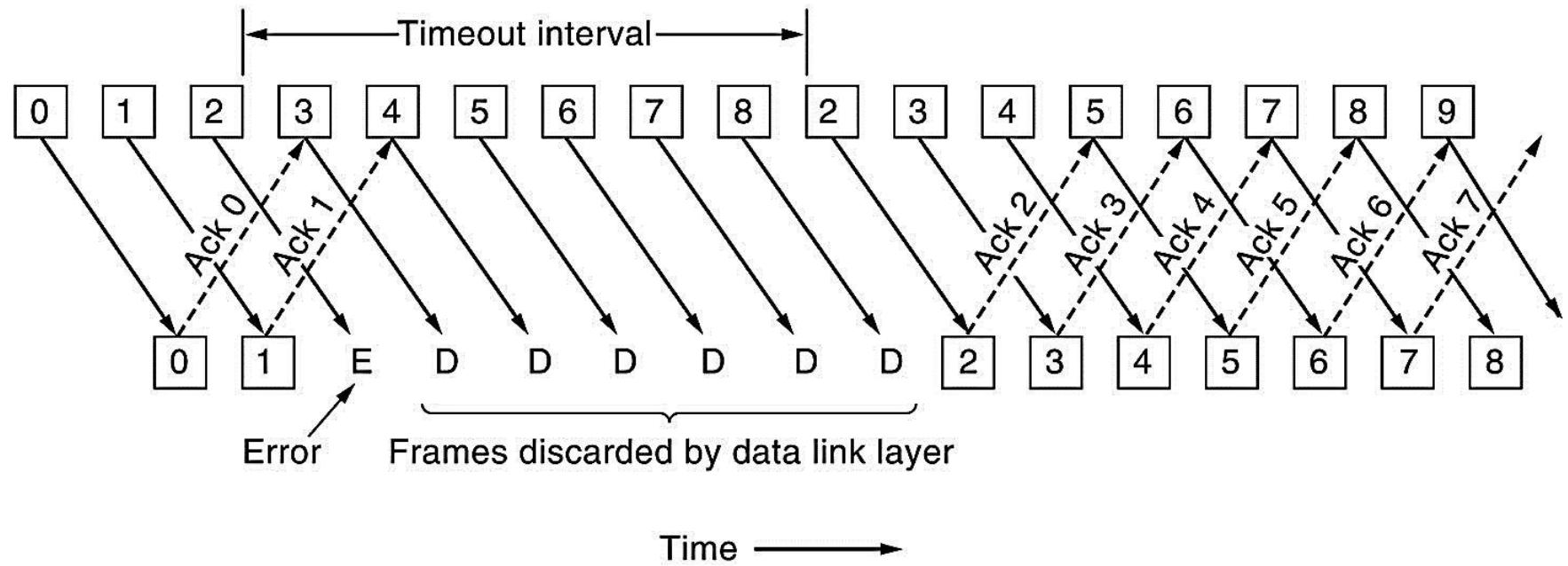
روش‌های کنترل جریان داده و ارائه‌ی سرویس مطمئن (ARQ)

روش پنجره‌ی لغزان (Sliding Window)

- قاب‌ها برای یک پنجره‌ی N تایی از صفر تا $N-1$ شماره‌گذاری می‌شوند. ACK‌ها نیز به همین ترتیب شماره‌گذاری می‌شوند.
- گیرنده هنگام ACK کردن، شماره‌ی قاب بعدی که در انتظار آن است را ارسال می‌کند.
- فرستنده با دریافت هر ACK و بررسی شماره‌ی آن، لبه‌ی پایانی پنجره را جلو می‌آورد.
- فرستنده با دریافت هر بسته از لایه‌ی شبکه خودش، اگر پنجره به حد اکثر اندازه‌ی خود نرسیده باشد، لبه‌ی ابتدایی پنجره را عقب می‌برد.

روش‌های کنترل جریان داده و ارائه‌ی سرویس مطمئن در پروتکل پنجره‌ی لغزان

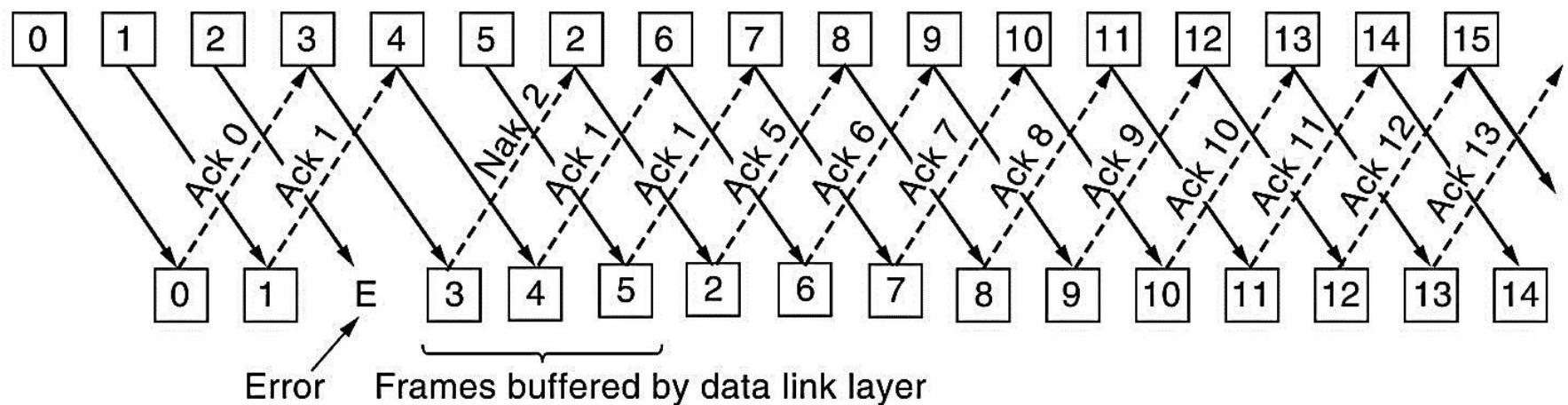
mekanizm baazgشت n tايی به عقب (Go Back n)



- Bufferless
- Simple
- Non-Efficient

روش‌های کنترل جریان داده و ارائه‌ی سرویس مطمئن در پروتکل پنجره‌ی لغزان

mekanizm tkarad antxabi (Selective Repeat)



- Buffering
- Complex
- Efficient

زیرلایه‌ی دسترسی به رسانه (MAC) در شبکه‌های محلی (چندپخشی)

• کنترل مرکزی (Centralized Control)

- نیاز به اخذ مجوز از ایستگاه مرکزی
- بدون تداخل
- پروتکل‌های سوییچینگ مداری، TDMA و Polling

زیرلایهی دسترسی به رسانه (MAC) در شبکه‌های محلی (چندپخشی)

کنترل توزیع شده (Distributed Control)

- مبتنی بر نشانه (Token)
- پروتکل‌های Token Bus و Token Ring

زیرلایهی دسترسی به رسانه (MAC) در شبکه‌های محلی (چندپوشی)

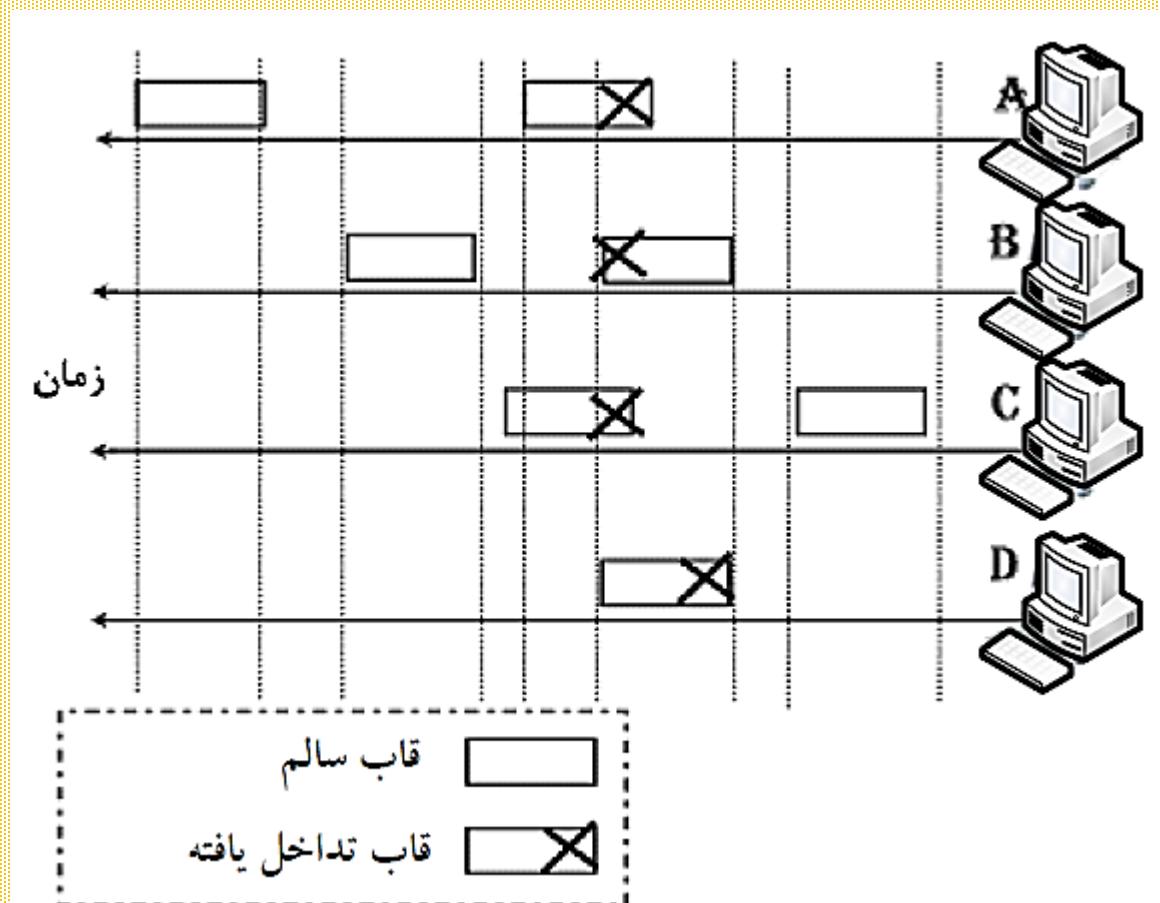
• کنترل تصادفی (Random Control)

- بدون کنترل
- رعایت عدالت جمعی
- پروتکل‌های CSMA/CD، ALOHA و Slotted Ring
- Register Insertion

زیرلایه‌ی دسترسی به رسانه (MAC) در شبکه‌های محلی (چندپخشی)

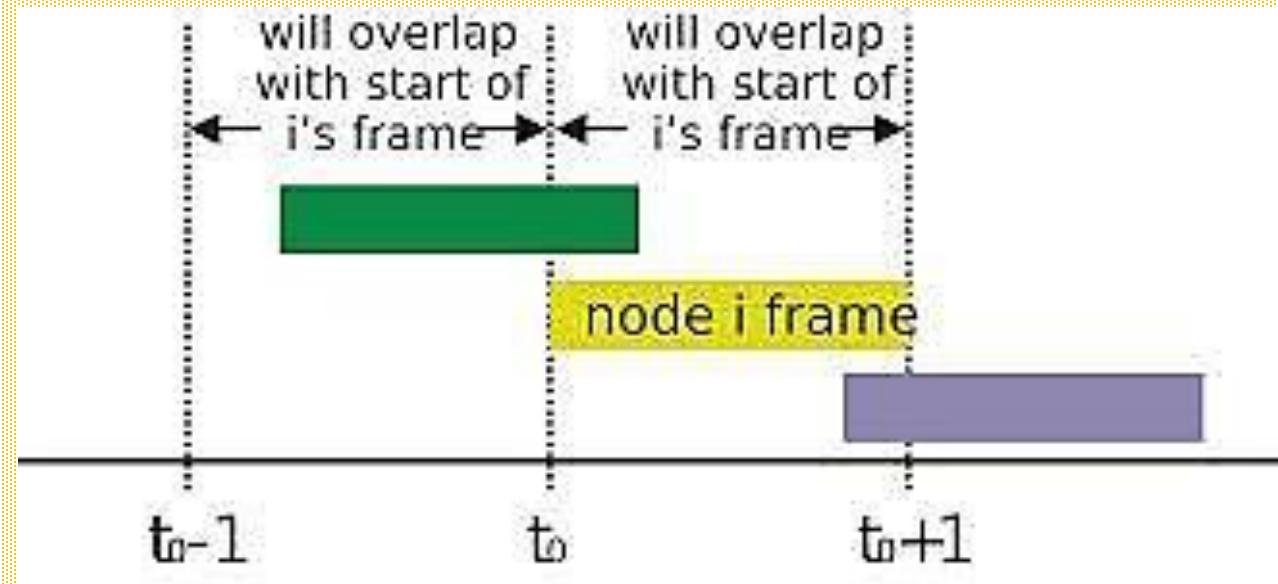
پروتکل Pure ALOHA

- ارسال در لحظه‌ی دلخواه و بررسی خط بعد از ارسال (یا انتظار برای ACK)
- ارسال بعد از مدت تصادفی در صورت تداخل



زیرلایه‌ی دسترسی به رسانه (MAC) در شبکه‌های محلی (چندپخشی)

مشکل پروتکل Pure ALOHA

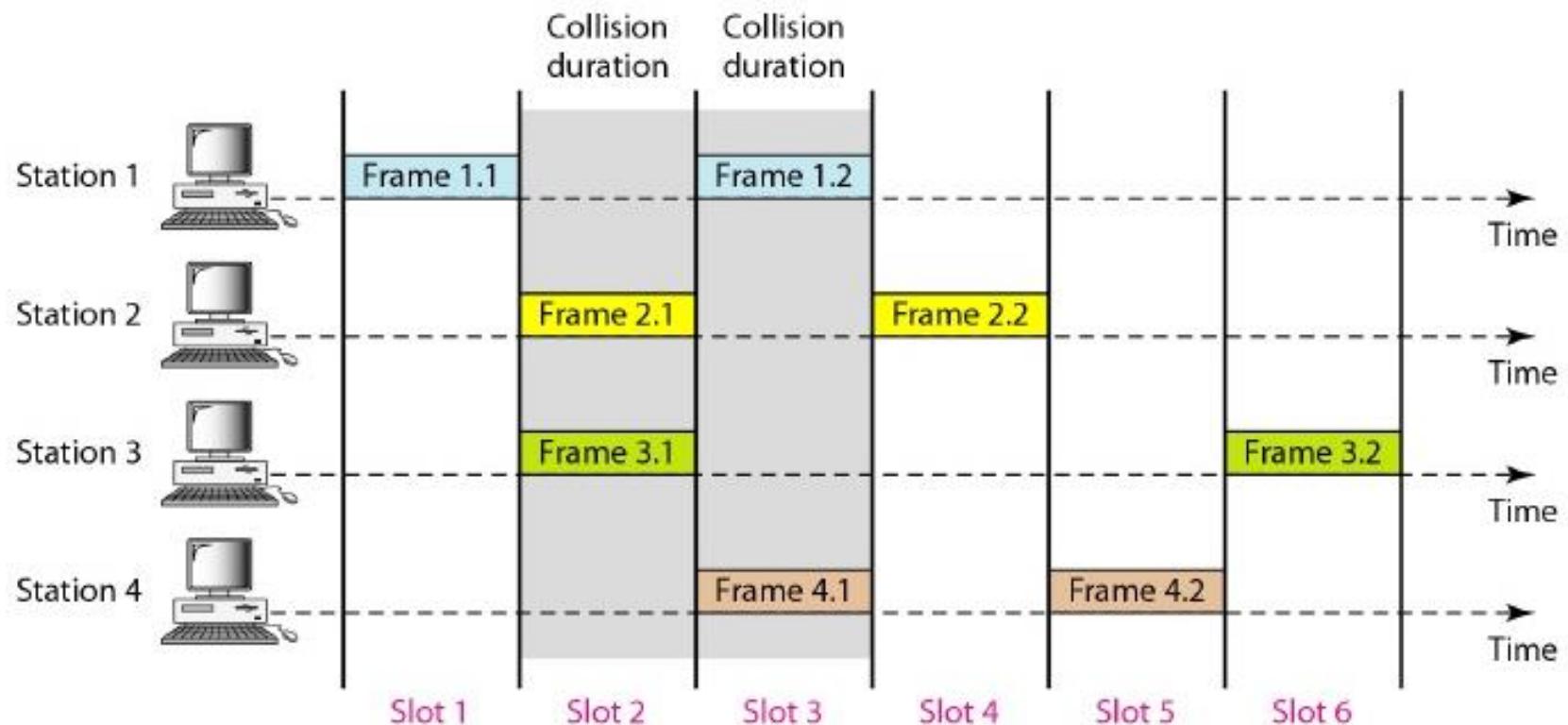


زیرلایهی دسترسی به رسانه (MAC) در شبکه‌های محلی (چندپخشی)

پروتکل Slotted ALOHA

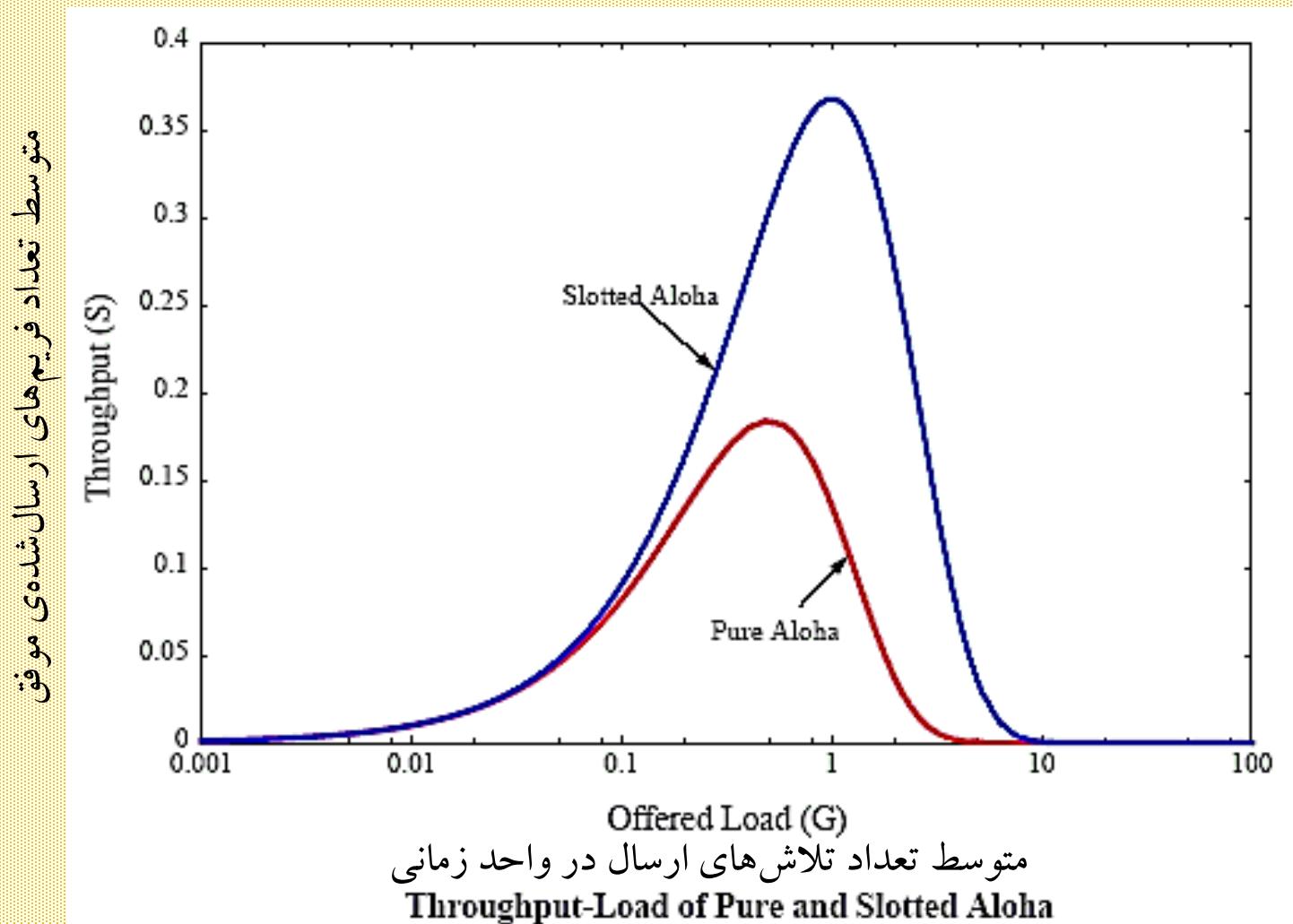
- ارسال در لحظات زمانی خاص (لبهی برش زمانی) امکان‌پذیر است

سنکرون



زیرلایه‌ی دسترسی به رسانه (MAC) در شبکه‌های محلی (چندپخشی)

مقایسه پروتکل‌های ALOHA

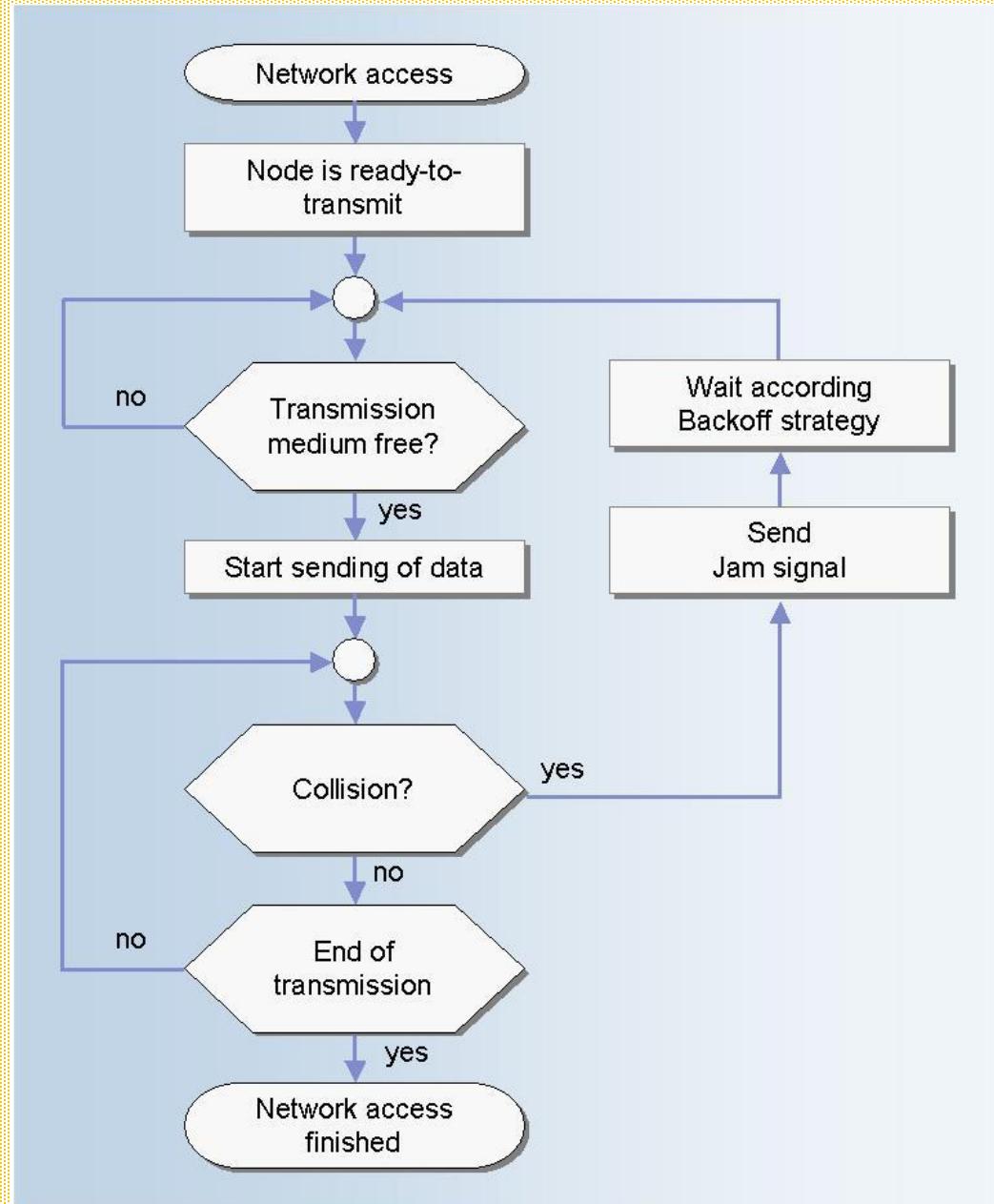


زیر لایه‌ی دسترسی به رسانه (MAC) در شبکه‌های محلی (چندپنجه)

روش :CSMA/CD

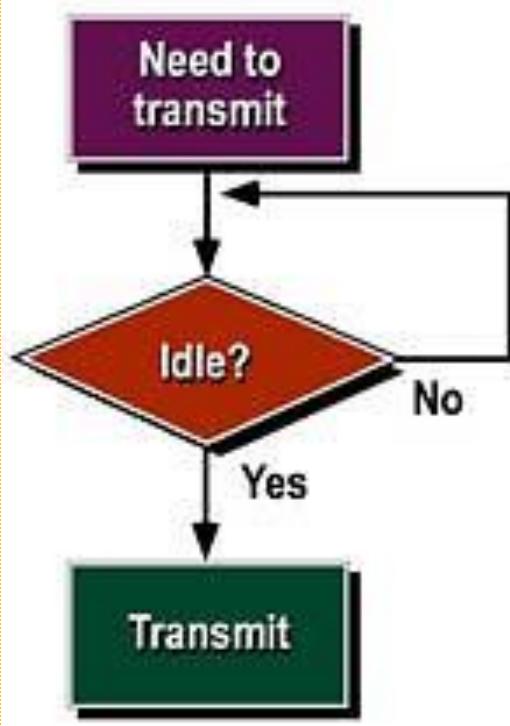
- گوش دادن ایستگاه متقاضی ارسال فریم به کانال
- در صورت آزاد بودن کانال آغاز ارسال فریم
- اشغال بودن کانال توسط ایستگاه دیگر ← متظر شدن تا اتمام ارسال و در صورت آزاد شدن کانال شروع ارسال فریم ← احتمال تصادم سیگнал به دلیل متظر بودن ایستگاههای دیگر جهت ارسال فریم
- جهت کشف سریع تصادم: گوش دادن به کانال هنگام ارسال فریم تا در صورت بروز تصادم ارسال فریم متوقف گردد
- مواجه شدن ایستگاه آغازکننده ارسال با تصادم ← تولید عدد تصادفی توسط ایستگاه و توقف ارسال فریم به مدت عدد تصادفی و گوش دادن به خط
- تولید سیگнал نویز (Jam) روی کانال هنگام آگاهی هر ایستگاه از تصادم جهت اطلاع ایستگاههای دیگر

زیر لایهی دسترسی به رسانه (MAC) در شبکه های محلی (چند پی خشی)



زیر لایه‌ی دسترسی به رسانه (MAC) در شبکه‌های محلی (چندپخشی)

پروتکل CSMA کاملاً مصراً (1-Persistent)



- اصرار بر حسّ خط در صورت مشغول بودن

- ارسال آنی هنگام آزاد شدن خط

- در صورت تداخل مدت زمان تصادفی صبر کرده و مجددًا تلاش می‌کند.

- بالا بودن احتمال تداخل در فواصل طولانی ایستگاه‌ها

- شبکه‌ی Ethernet

-

-

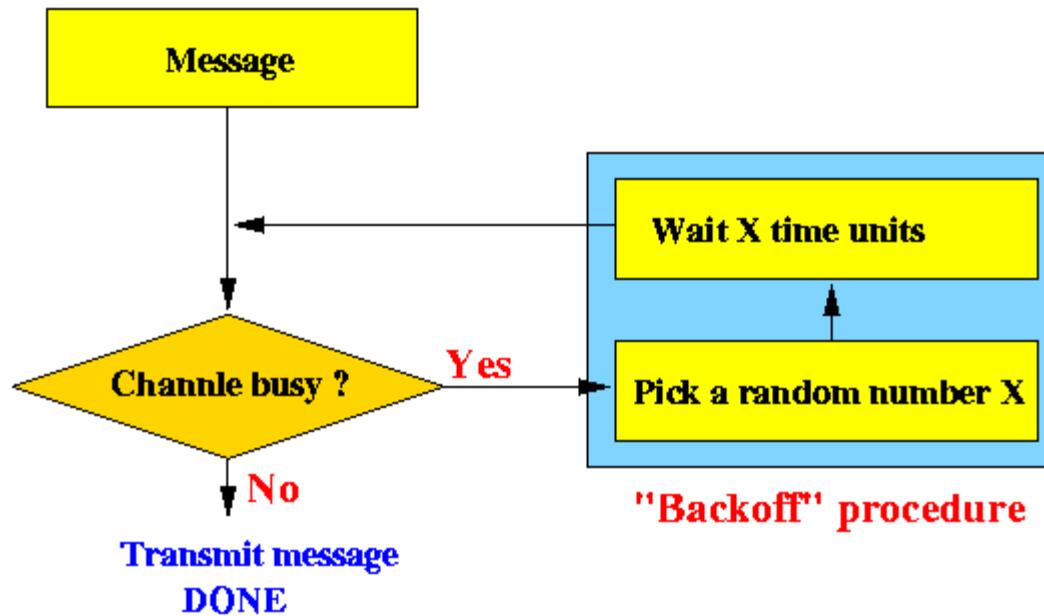
-

-

-

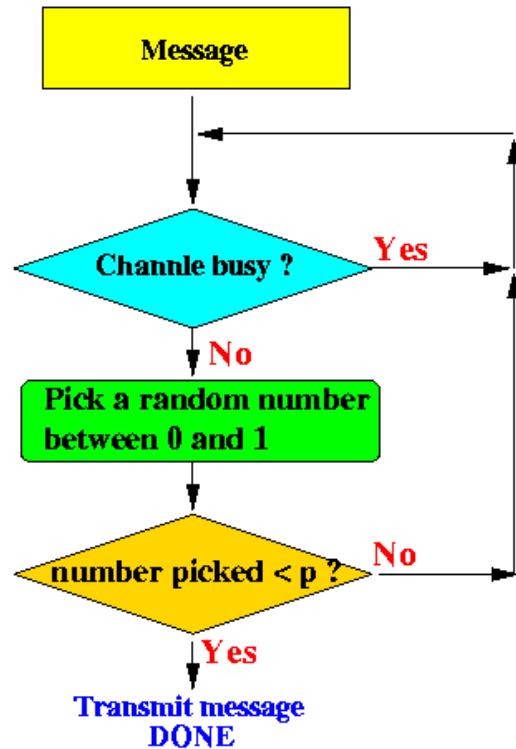
زیر لایهی دسترسی به رسانه (MAC) در شبکه های محلی (چند پخشی)

پروتکل CSMA غیر مصروف (Non Persistent)



- اصراری بر حسّ خط در صورت مشغول بودن نیست.
- بعد از مدت زمان تصادفی مجدداً حسّ خط انجام می شود.
- در صورت تداخل مدت زمان تصادفی صبر کرده و مجدداً تلاش می کند.
- تداخل کمتر و تأخیر بیشتر نسبت به کاملاً مصروف

زیرلایهی دسترسی به رسانه (MAC) در شبکه‌های محلی (چندپخشی)

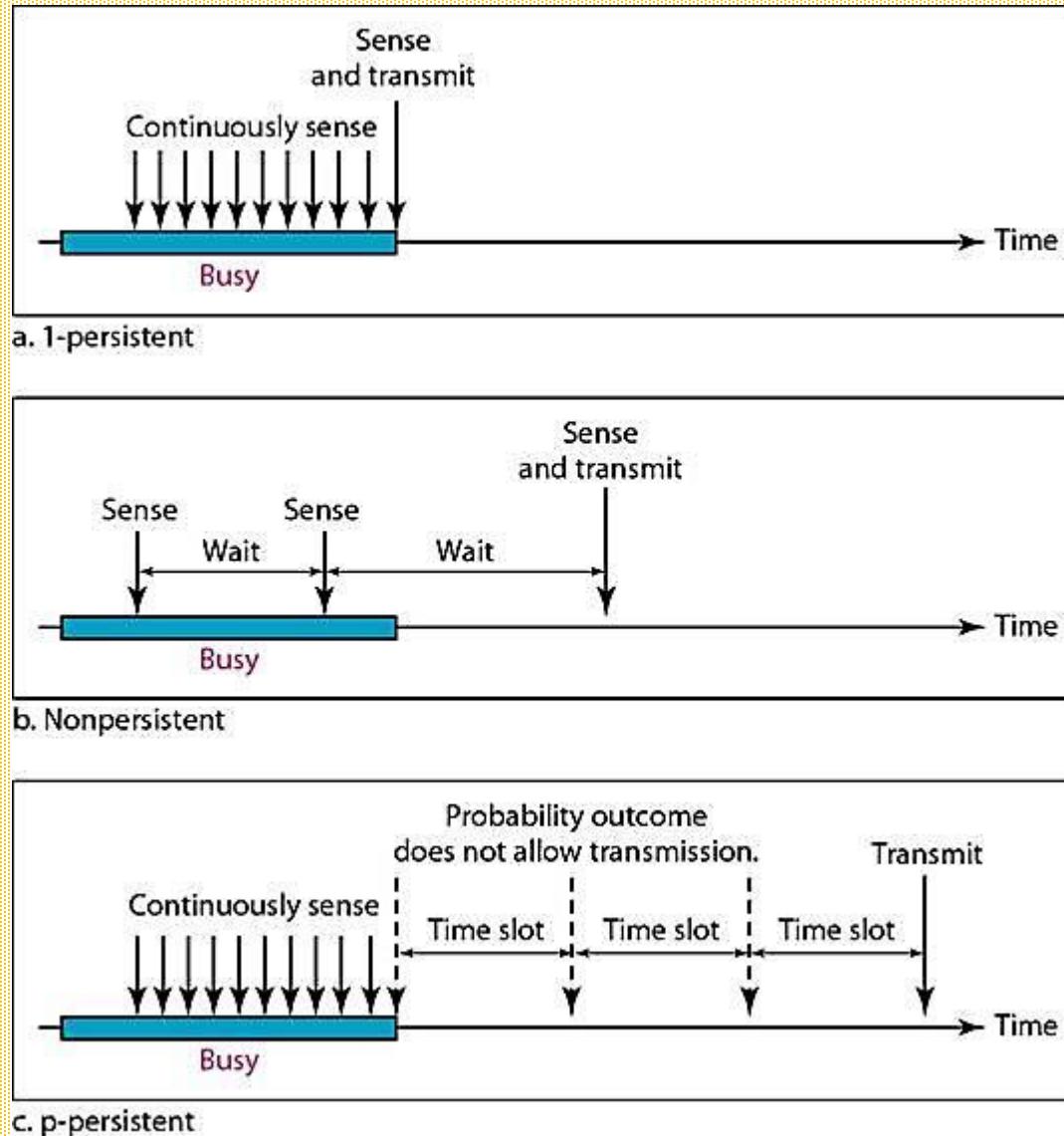


پروتکل CSMA مصرّ احتمالی (p-Persistent CSMA)

- حتی در صورت آزاد بودن خط با احتمال p ارسال و با احتمال $p-1$ تا آغاز برش زمانی بعدی صبر می‌کند.
- در صورت تداخل مدت زمان تصادفی صبر کرده و مجددًا تلاش می‌کند.
- تداخل کمتر و تأخیر بیشتر نسبت به غیر مصر با کاهش p .

زیرلایهی دسترسی به رسانه (MAC) در شبکه‌های محلی (چندپخشی)

مقایسه پروتکل‌ها



زیرلایهی دسترسی به رسانه (MAC) در شبکه‌های محلی (چندپخشی)

مقایسه‌ی پروتکلهای MAC

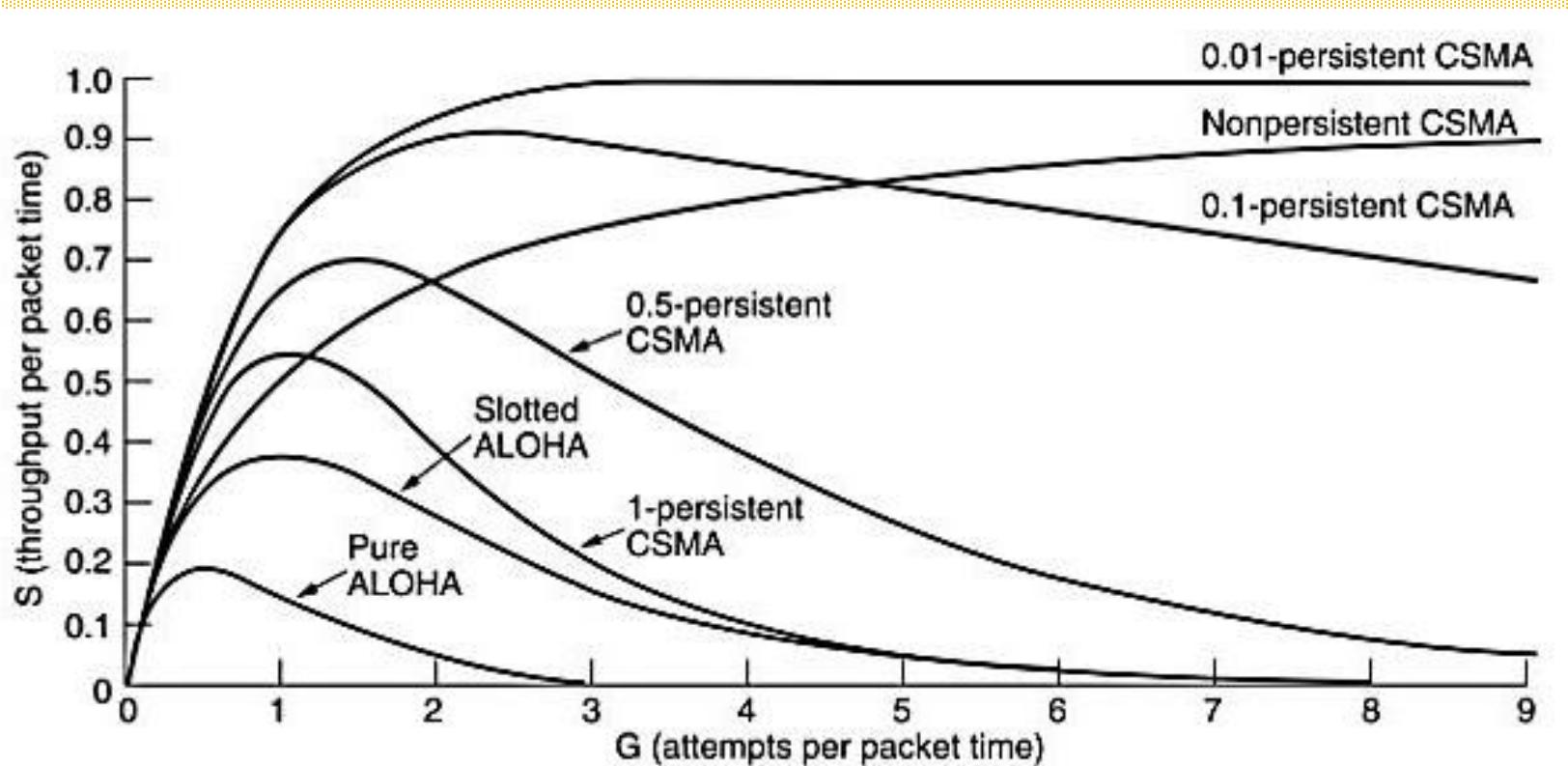


Fig. : Comparison of channel utilization versus load for various random access protocols

زیرلايهی دسترسی به رسانه (MAC) در شبکه های محلی (چندپخشی)

آدرس MAC

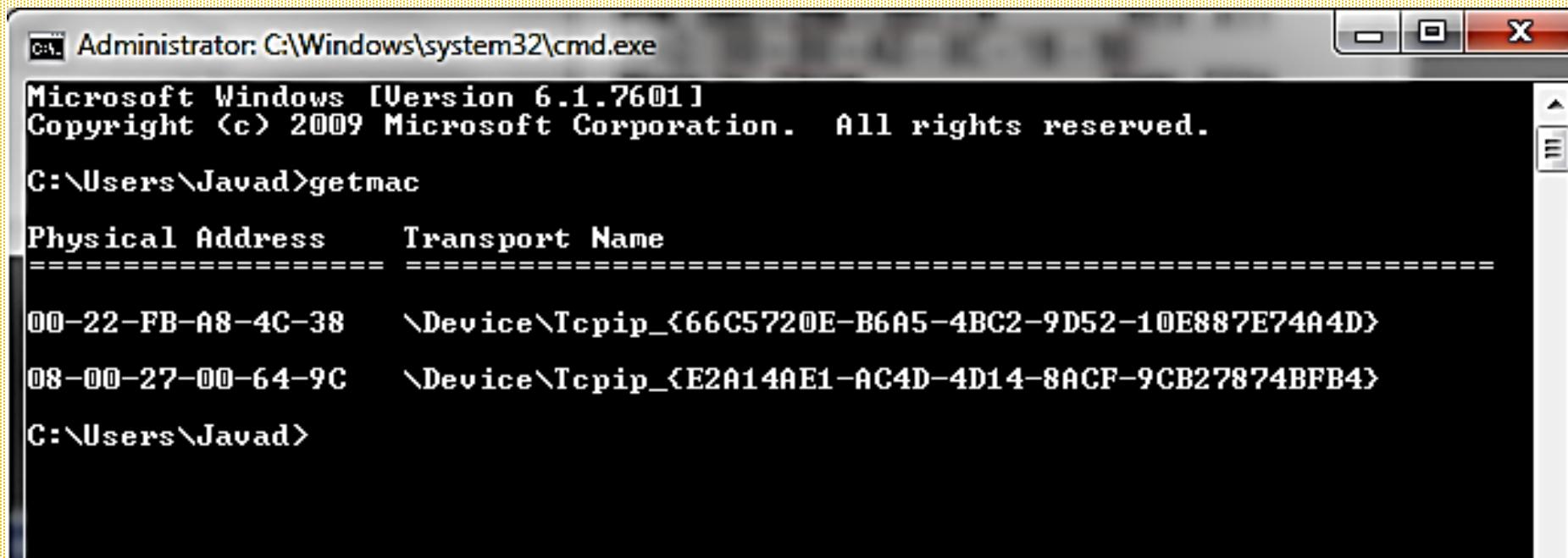
- آدرس ۴۸ بیتی منحصر به فرد برای همهی وسایل با قابلیت اتصال به شبکه
- در یک شبکه معنا دارد

Network Connection Details	
Network Connection Details:	
Property	Value
Connection-specific DN...	
Description	Intel(R) WiFi Link 5100 AGN
Physical Address	00-22-FB-A8-4C-38
DHCP Enabled	Yes
IPv4 Address	192.168.1.12
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Sunday, December 21, 2014 8:54:31 AM
Lease Expires	Monday, December 22, 2014 8:54:34 AM
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1

زیرلايهی دسترسی به رسانه (MAC) در شبکه های محلی (چندپخشی)

آدرس MAC

آدرس ۴۸ بیتی منحصر به فرد برای همهی وسایل با قابلیت اتصال به شبکه



A screenshot of a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window shows the following output:

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Javad>getmac

Physical Address      Transport Name
=====  =====
00-22-FB-A8-4C-38    \Device\Tcpip_{66C5720E-B6A5-4BC2-9D52-10E887E74A4D}
08-00-27-00-64-9C    \Device\Tcpip_{E2A14AE1-AC4D-4D14-8ACF-9CB27874BFB4}

C:\Users\Javad>
```

زیرلایهی دسترسی به رسانه (MAC) در شبکه‌های محلی (چندپخشی)

آدرس MAC

آدرس ۴۸ بیتی منحصر به فرد برای همهٔ وسایل با قابلیت اتصال به شبکه



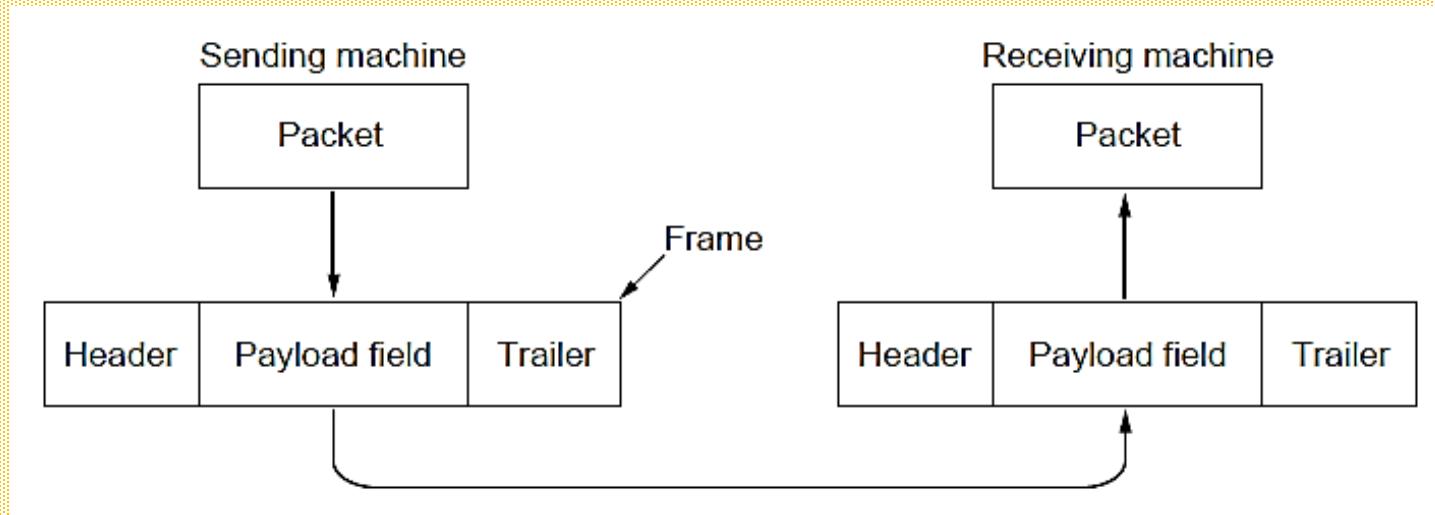
لایه شبکه

- سازماندهی اطلاعات بصورت بسته (Packet) و ارسال جهت انتقال مطمئن به لایه پیوند داده‌ها
- تعیین مسیر (مسیریابی - Routing) هر بسته ارسالی برای رسیدن به مقصد
- جلوگیری از ازدحام و ترافیک در بین مسیریابها و سوئیچها
- اختصاص آدرس‌های مشخص و استاندارد برای هر بسته آماده ارسال
- این لایه بدون اتصال است.

بسته IP

ساختمان داده‌ای است درون فیلد داده فریمها 😊

عدم تغییر بسته IP با وجود تغییر شبکه و تغییرات مداوم فریم 😊



Relationship between packets and frames.

لایه IP در شبکه اینترنت

لایه IP

هدایت بسته‌های اطلاعاتی از شبکه‌ای به شبکه‌های دیگر

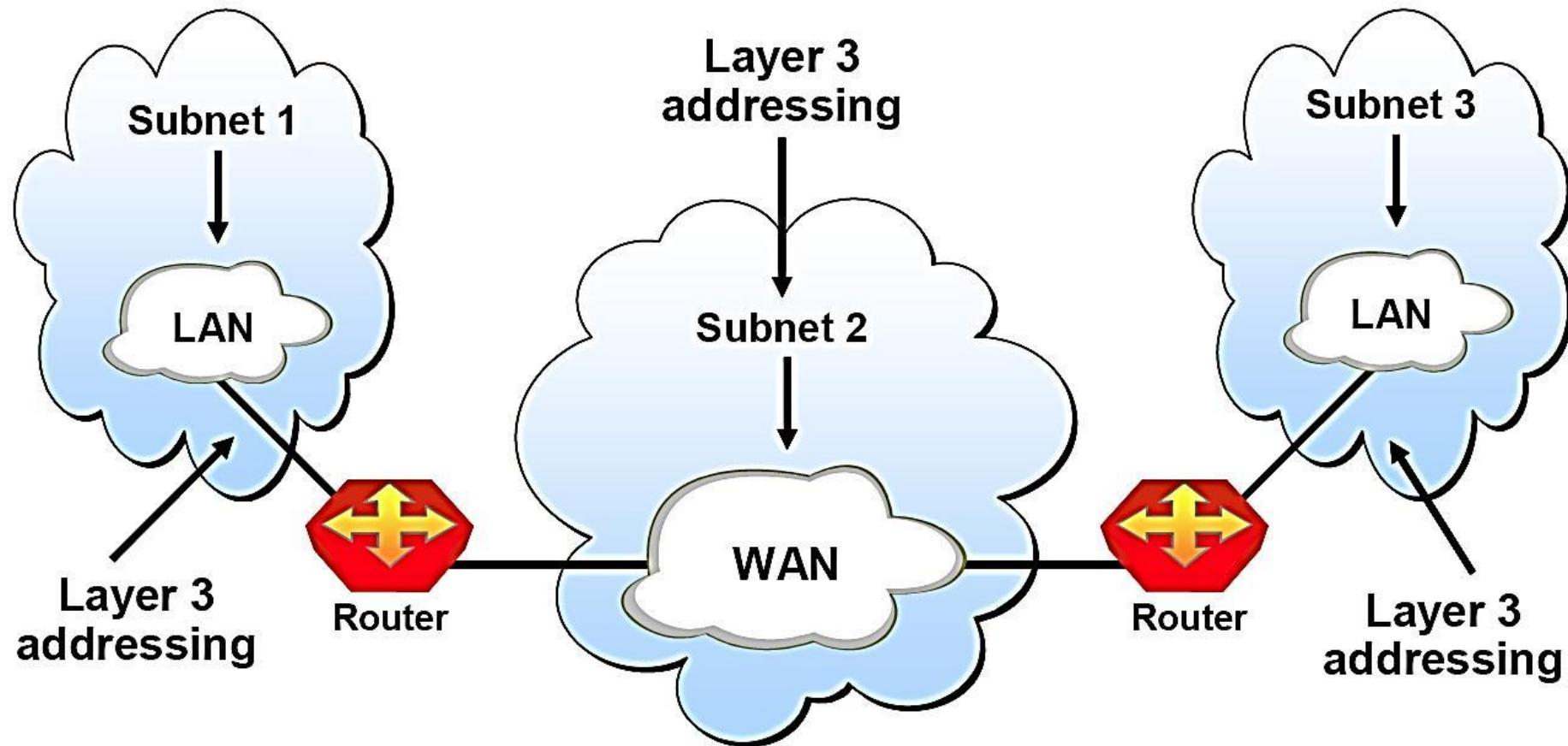
- تعریف آدرس‌های جهانی و استاندارد برای تمامی ایستگاهها
- ساختار یکسان بسته قرار گرفته درون فیلد داده از فریم هر شبکه
- عدم واپستگی بسته به نوع شبکه و سخت افزار

- بی‌نظمی در شبکه‌های مختلف
- نوع توپولوژی و پروتکلها
- تفاوت در روش‌های آدرس دهی

بسته IP

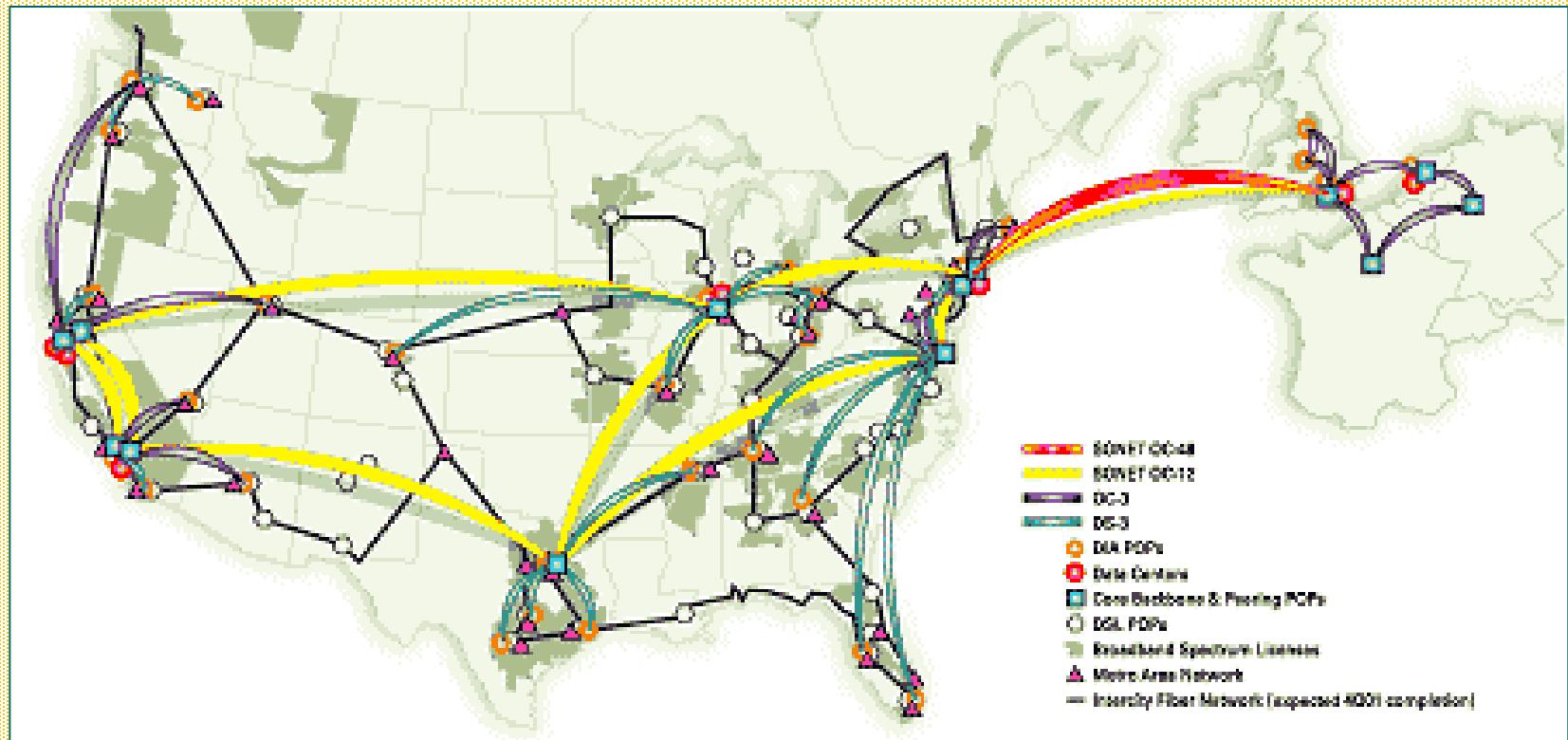
واحد اطلاعاتی که درون فیلد داده از فریم فیزیکی قرار گرفته و با عبور از یک شبکه به شبکه دیگر تغییر نمی‌کند.

لایه IP در شبکه اینترنت



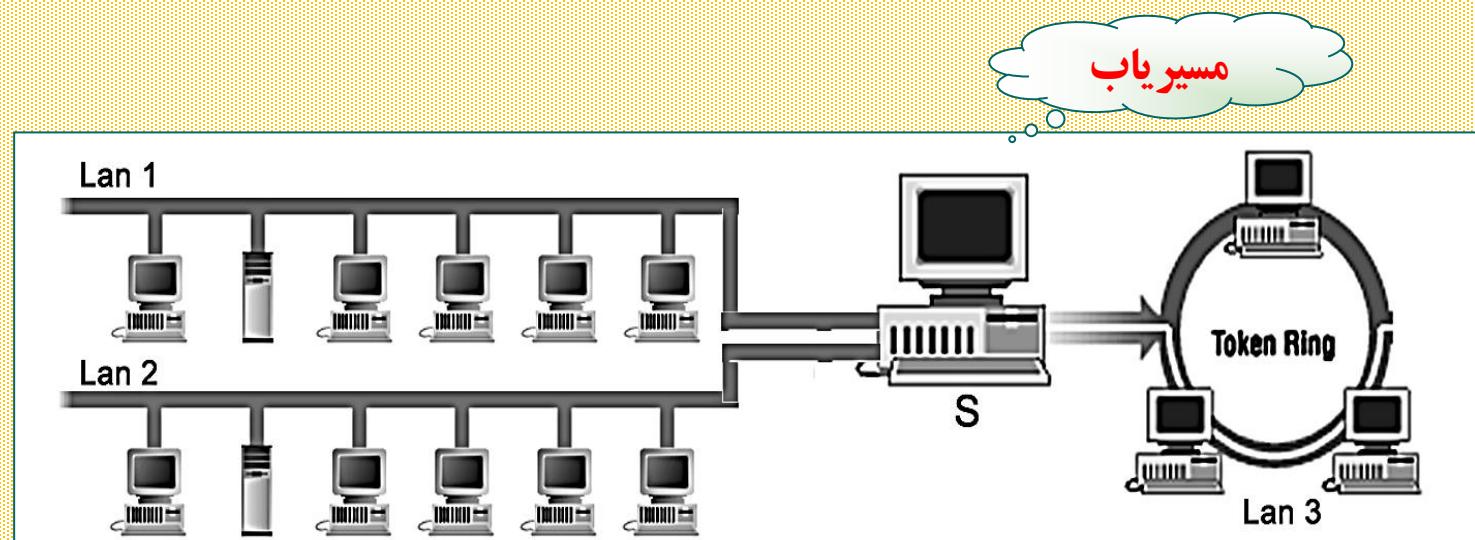
زیرشبکه (Subnet): زیر ساخت ارتباطی شبکه ها

ستون فقرات (Backbone) : خطوط ارتباطی با پهنهای باند (نرخ ارسال) بسیار بالا و مسیریابی های بسیار سریع و هوشمند در قسمت زیرشبکه

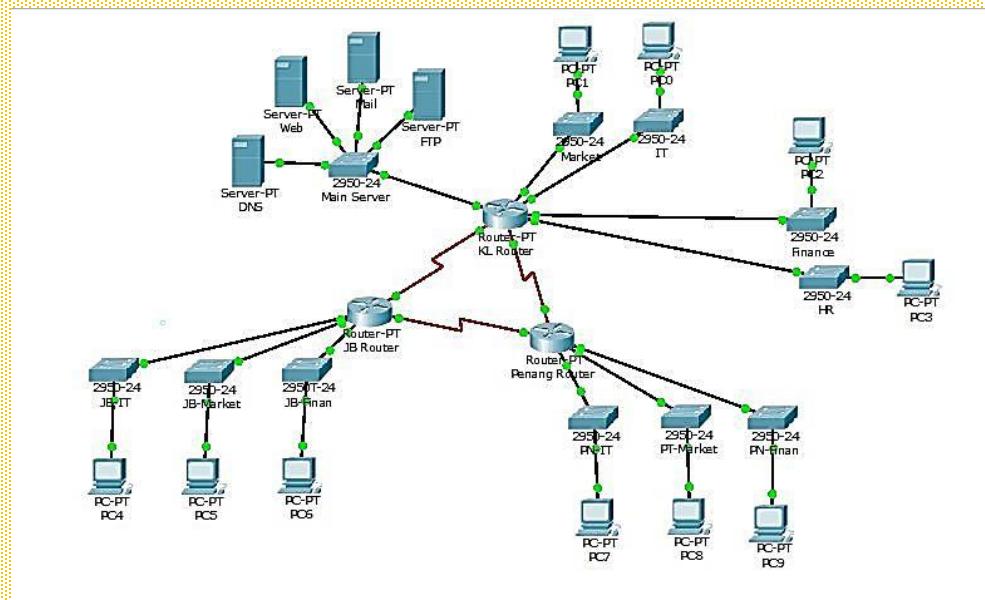
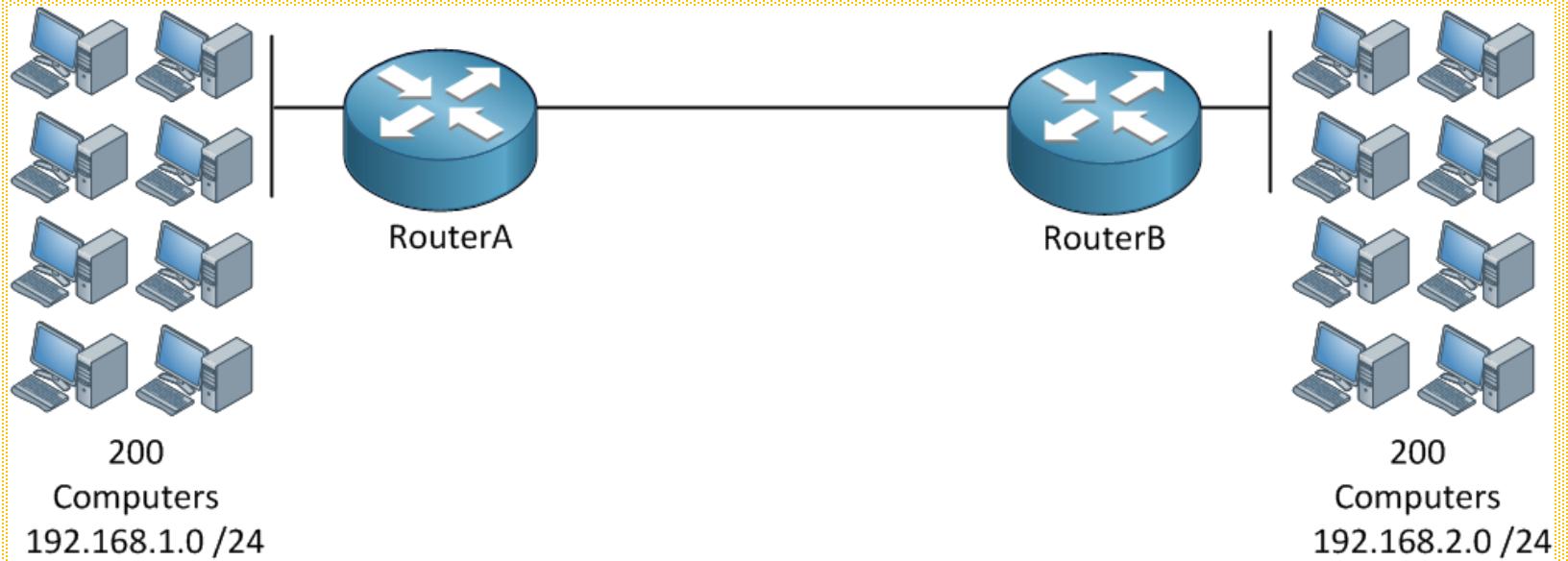


مسیریاب (Router)

- ماشینی با تعدادی ورودی و خروجی
- دریافت بسته‌های اطلاعاتی از ورودی و هدایت و انتخاب کanal خروجی مناسب بر اساس آدرس مقصد



مسیریابی در لایه شبکه

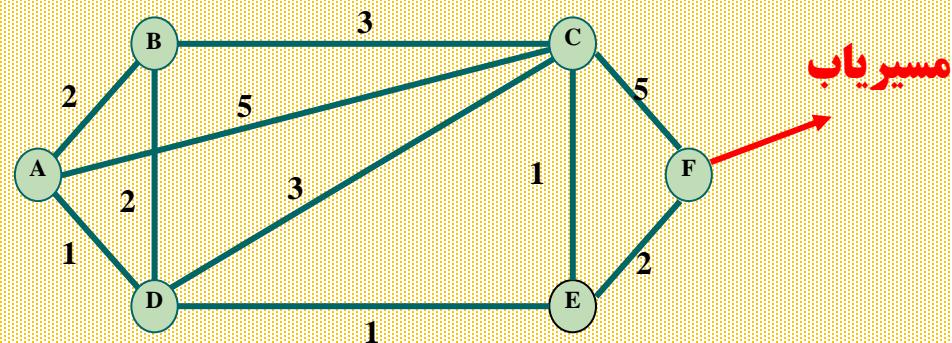


مسیریابی (Routing)

آدرس IP: آدرس جهانی و مشخص کننده ماشین به صورت یکتا و فارغ از ساختار شبکه‌ای (آدرس Mac مربوط به یک شبکه است و آدرس IP مربوط به Internetworking)

زیرساخت ارتباطی: مجموعه مسیریابها و کانالهای فیزیکی ما بین آنها

الگوریتم‌های مسیریابی: روش‌هایی برای پیدا کردن مسیری بهینه میان دو مسیریاب به گونه‌ای که هزینه کل مسیر به حداقل برسد.



زیرساخت ارتباطی یک شبکه فرضی

برخی اصطلاحات کلیدی در مسیریابی

مکاتبه با نام مدیر
سازمان یا با سمت
مدیر سازمان؟

آدرسهای MAC:

- آدرسهای لایه فیزیکی جهت انتقال فریمها بر روی کانال یک شبکه
- اندازه آدرس وابسته به پروتکل و توپولوژی شبکه
- تغییر آدرسهای MAC بسته‌های اطلاعاتی هنگام عبور از مسیریابهای موجود در مسیر

آدرسهای IP:

- آدرسهای جهانی و منحصر به فرد مربوط به اتصال شبکه‌ها
- مشخص کننده یک ماشین فارغ از نوع سخت افزار و نرم افزار آن
- ثابت بودن آدرسهای IP بسته‌های اطلاعاتی هنگام عبور از مسیریابهای موجود در مسیر

بسته IP:

- واحد اطلاعاتی با اندازه محدود

توپولوژی شبکه:

- مجموعه مسیریابها و کانالهای فیزیکی ما بین آنها در زیرساخت ارتباطی یک شبکه
- متغیر با زمان

ترافیک شبکه:

- تعداد متوسط بسته‌های اطلاعاتی ارسالی و یا دریافتی روی یک کanal در واحد زمان
- متغیر با زمان

گام یا Hop:

- عبور بسته از یک مسیریاب = گام
- تعداد مسیریابهای موجود در مسیر یک بسته = تعداد گام

ازدحام یا Congestion:

بیشتر بودن تعداد متوسط بسته‌های ورودی به یک مسیریاب از تعداد متوسط بسته‌های خروجی

بن بست Deadlock:

پایان طول عمر بسته‌ها

مسیریابی در لایه شبکه

Static and Dynamic Routes

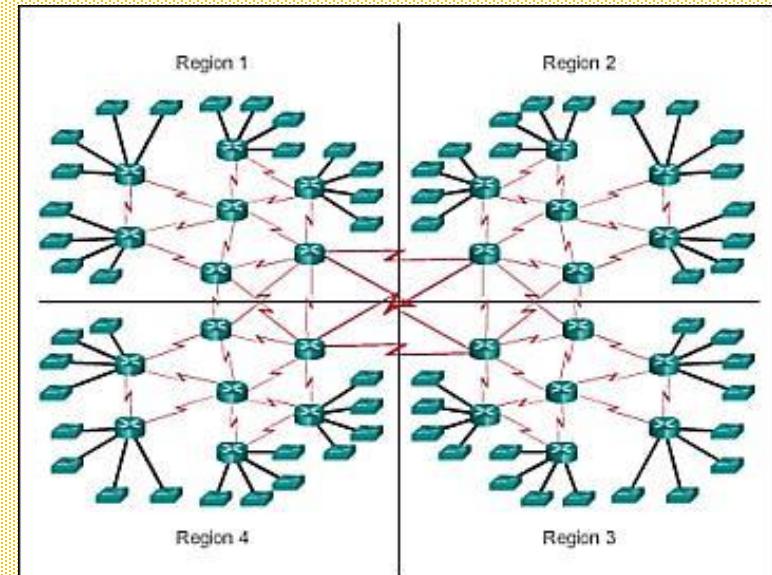
- **Static Route**

Uses a route that a network administrator enters into the router manually.

- **Dynamic Route**

Uses a route that a network routing protocol (i.e. OSPF, EIGRP, RIP) adjusts automatically for topology or traffic changes.

ماشین مسیریاب فقط تا همین لایه را دارد



انواع الگوریتمهای مسیریابی

ب) از دیدگاه چگونگی جمعآوری و پردازش طلاعات زیرساخت ارتباطی شبکه

غیرمتمرکز

سراسری / متمرکز

الف) از دیدگاه روش تصمیم‌گیری و میزان هوشمندی الگوریتم

پویا

ایستا

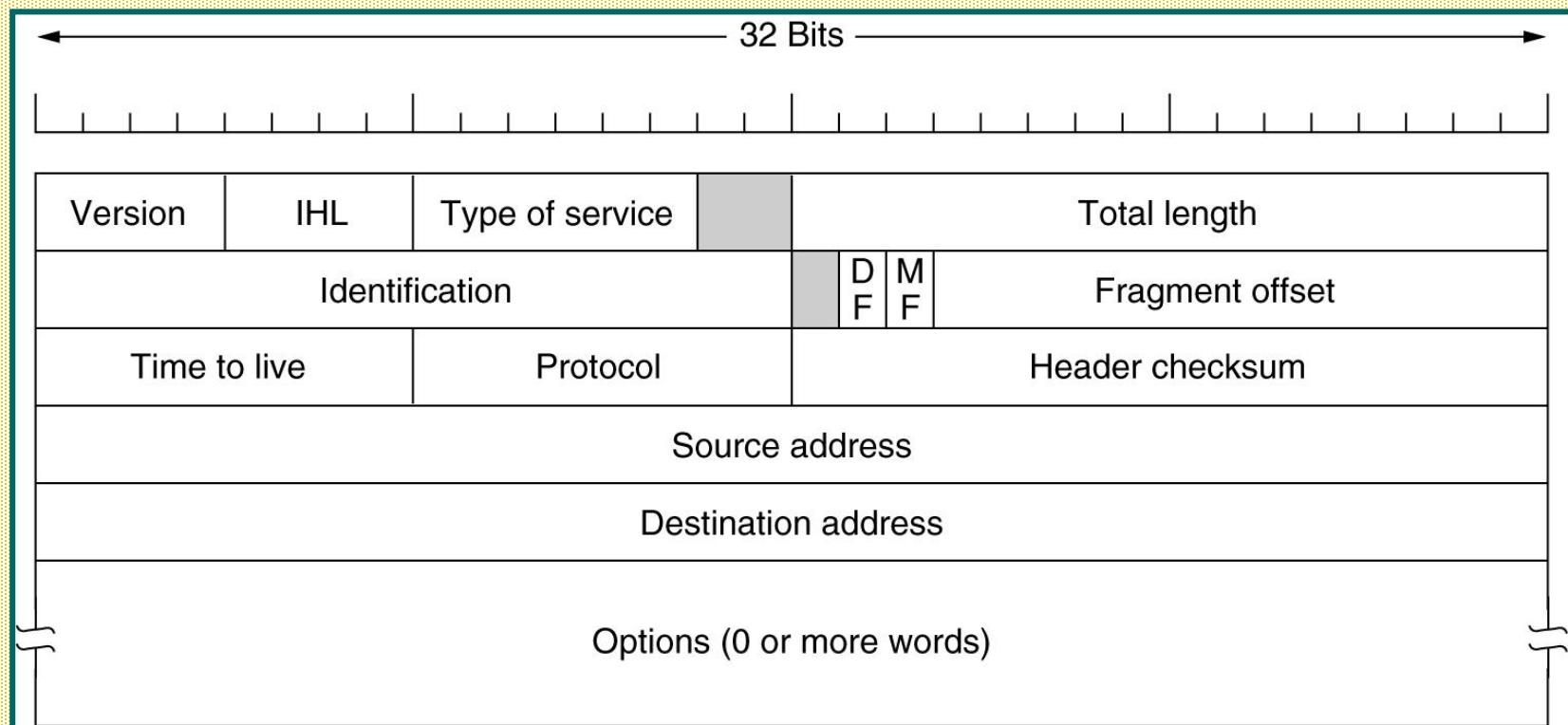
الگوریتم ایستا

- عدم توجه به شرایط توپولوژیکی و ترافیک لحظه‌ای شبکه
- جداول ثابت مسیریابی هر مسیریاب در طول زمان
- الگوریتم‌های سریع
- تنظیم جداول مسیریابی به طور دستی در صورت تغییر توپولوژی زیرساخت شبکه
- تغییر مسیرها به کندی در اثنای زمان

الگوریتم پویا

- به هنگام سازی جداول مسیریابی به صورت دوره‌ای بر اساس آخرین وضعیت توپولوژیکی و ترافیک شبکه
- تغییر سریع مسیرها
- تصمیم‌گیری بر اساس وضعیت فعلی شبکه جهت انتخاب بهترین مسیر
- ✗ ایجاد تأخیرهای بحرانی هنگام تصمیم‌گیری بهترین مسیر به جهت پیچیدگی الگوریتم

قالب بسته IP



Source Address فیلد

- فیلد ۳۲ بیتی
- مشخص کننده آدرس ماشین مبدأ

Destination Address فیلد

- فیلد ۳۲ بیتی
- مشخص کننده آدرس IP ماشین مقصد

آدرسها در اینترنت و اینترافت

شناسایی تمام ابزار شبکه (ماشینهای میزبان، مسیریابها، چاپگرهای شبکه) در اینترنت با یک آدرس IP

✓ نمی‌توان برای ارتباط در اینترنت از آدرس Mac استفاده کرد!

آدرس IP

۳۲ بیتی

نوشتن آدرس‌های IP به صورت چهار عدد ددهدی که با نقطه از هم جدا شده اند جهت سادگی نمایش

پرارزشترین بایت آدرس IP مشخص کننده کلاس آدرس

An IPv4 address (dotted-decimal notation)

172 . 16 . 254 . 1



10101100.00010000.11111110.00000001

One byte = Eight bits

Thirty-two bits ($4 * 8$), or 4 bytes

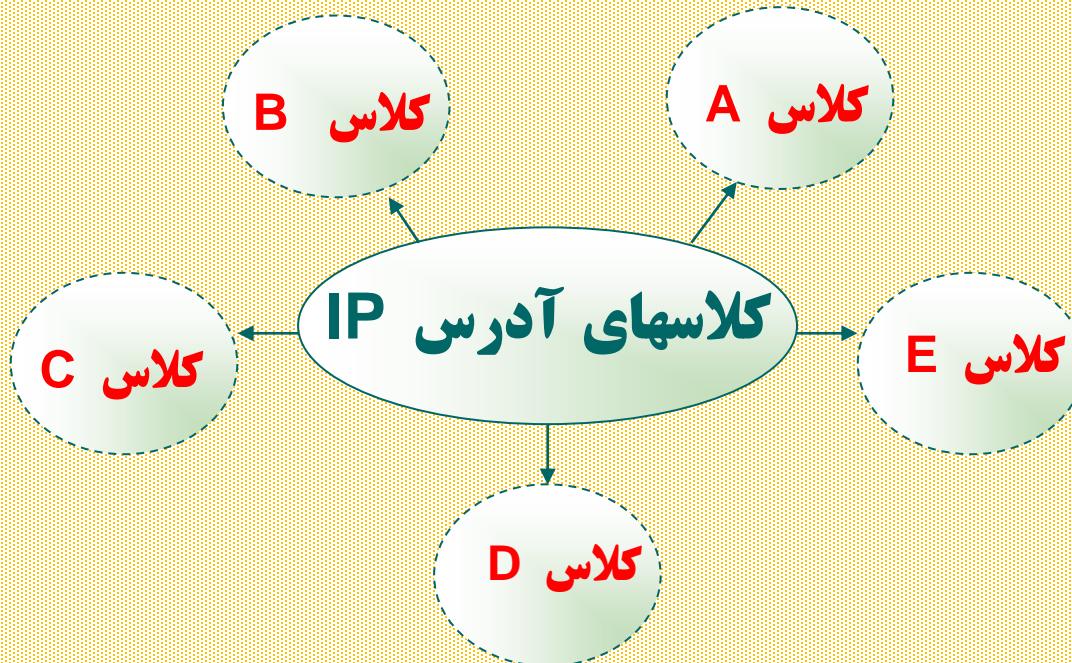
+۹۸ ۳۱ ۳۷۹۲ ۴۰۳۴



تقسیم ۳۲ بیت آدرس IP به قسمتهای :

آدرس ماشین / آدرس زیرشبکه / آدرس شبکه

Net ID / Subnet ID / Host ID



آدرسهای کلاس A

- مقدار پر ارزشترین بیت = صفر
- ۷ بیت از یک بایت اول = آدرس شبکه
- ۳ بایت باقیمانده مشخص کننده آدرس ماشین میزبان
- بایت پر ارزش در محدوده صفر تا ۱۲۷

Network ID = ۲ Bit

Net IDs: 0 & 127 are reserved



کلاس B

- مقدار دو بیت پر ارزش = ۱۰

- ۱۴ بیت از دو بایت سمت چپ = آدرس شبکه

- دو بایت اول از سمت راست = آدرس ماشین میزبان

Network ID = 14 Bit

10

Network ID

Host ID

192.0.0.0 to
239.255.255.255

32 bits

کلاس C

- مناسب ترین و پر کاربردترین کلاس از آدرس های IP
- مقدار سه بیت پر ارزش = ۱۱۰
- ۲۱ بیت از سه بایت سمت چپ = مشخص کننده آدرس شبکه
- ۸ بیت سمت راست = آدرس ماشین میزبان

Network ID = 21 Bit

110

Network ID

Host ID

240.0.0.0 to
247.255.255.255

32 bits

کلاس D

- مقدار چهار بیت پر ارزش = 1110
- 28 بیت = تعیین آدرس‌های چند مقصد (آدرس‌های گروهی)
- کاربرد = عملیات رسانه‌ای و چند پخشی

1110

Multicast Address

32 bits

کلاس E

• مقدار پنج بیت پر ارزش = 11110

11110

Unused Address Space

32 bits

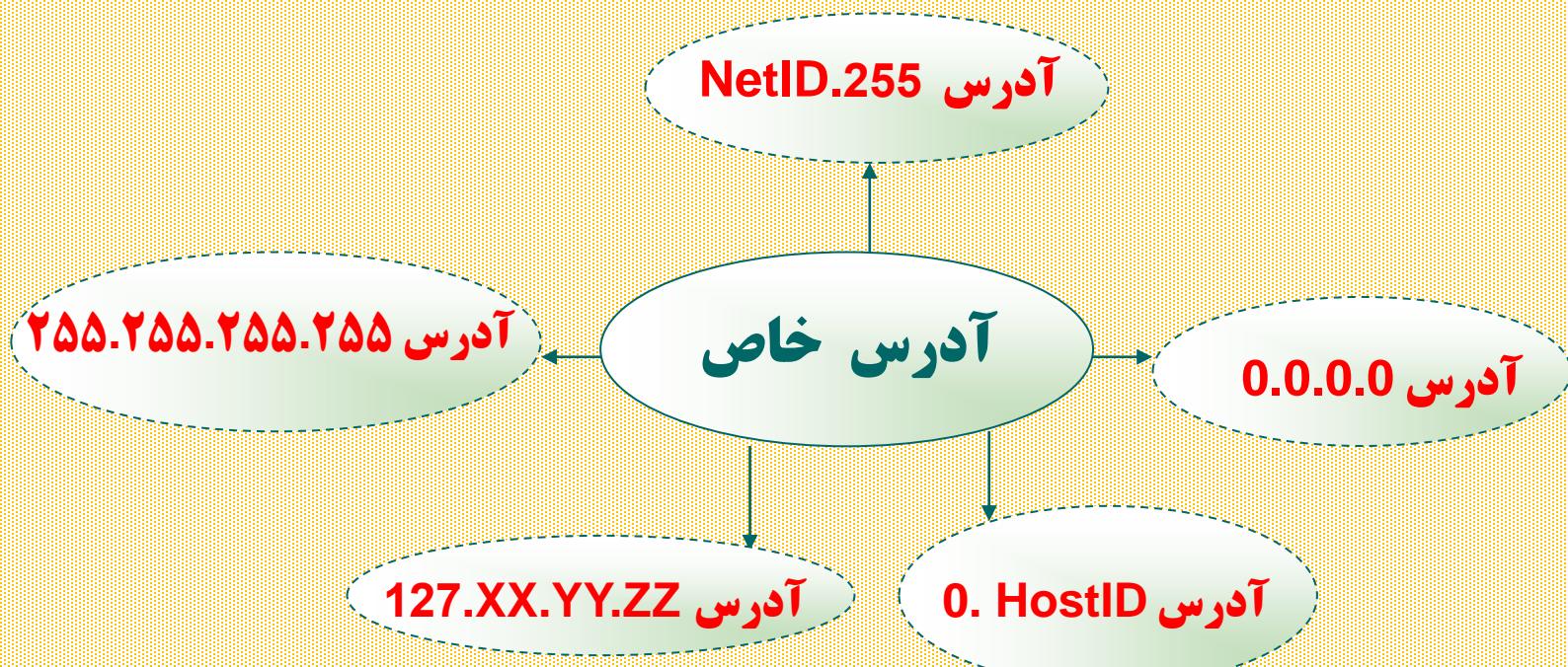
مقایسه کلاس‌های IP

کلاس	بیت‌های سمت چپ	تعداد بیت Net ID	تعداد بیت Host ID	بازه‌ی فیلد سمت چپ	تعداد شبکه‌های قابل تعریف	تعداد کامپیووتر در هر شبکه
A	0	7	24	1-126	126	۱۷ میلیون
B	10	14	16	128-191	$2^{14} = 16382$	۶۵۵۳۴
C	110	21	8	192-223	$2^{21} =$ بیش از دو میلیون	۲۵۶ °
D	1110	28	-	224-239	2^{28}	○ -
E	11110	27	-	-	-	○ -



آدرسهای خاص

در بین تمام کلاس‌های آدرس IP با پنج گروه از آدرسها نمی‌توان یک شبکه خاص را تعریف و آدرس‌دهی نمود.



آدرسهای خاص

در بین تمام کلاس‌های آدرس IP با پنج گروه از آدرسها نمی‌توان یک شبکه خاص را تعریف و آدرس‌دهی نمود.

آدرس :0.0.0.0

هر ماشین میزبان که از آدرس IP خودش مطلع نیست این آدرس را بعنوان آدرس خودش فرض می کند.

آدرس :0. HostID

این آدرس زمانی به کار می رود که ماشین میزبان ، آدرس مشخصه شبکه ای که بدان متعلق است را نداند. در این حالت در قسمت NetID مقدار صفر و در قسمت HostID شماره مشخصه ماشین خود را قرار می دهد.

آدرس :(Local Broadcast) 255.255.255.255

جهت ارسال پیامهای فرآگیر برای تمامی ماشینهای میزبان بر روی شبکه محلی که ماشین ارسال کننده به آن متعلق است .

آدرس :NetID.255

جهت ارسال پیامهای فرآگیر برای تمامی ماشینهای یک شبکه راه دور که ماشین میزبان فعلی متعلق به آن نیست .

آدرس :127.xx.yy.zz

این آدرس بعنوان "آدرس بازگشت" (Loop Back) شناخته می شود و آدرس بسیار مفیدی برای اشکالزدایی از نرم افزار می باشد .

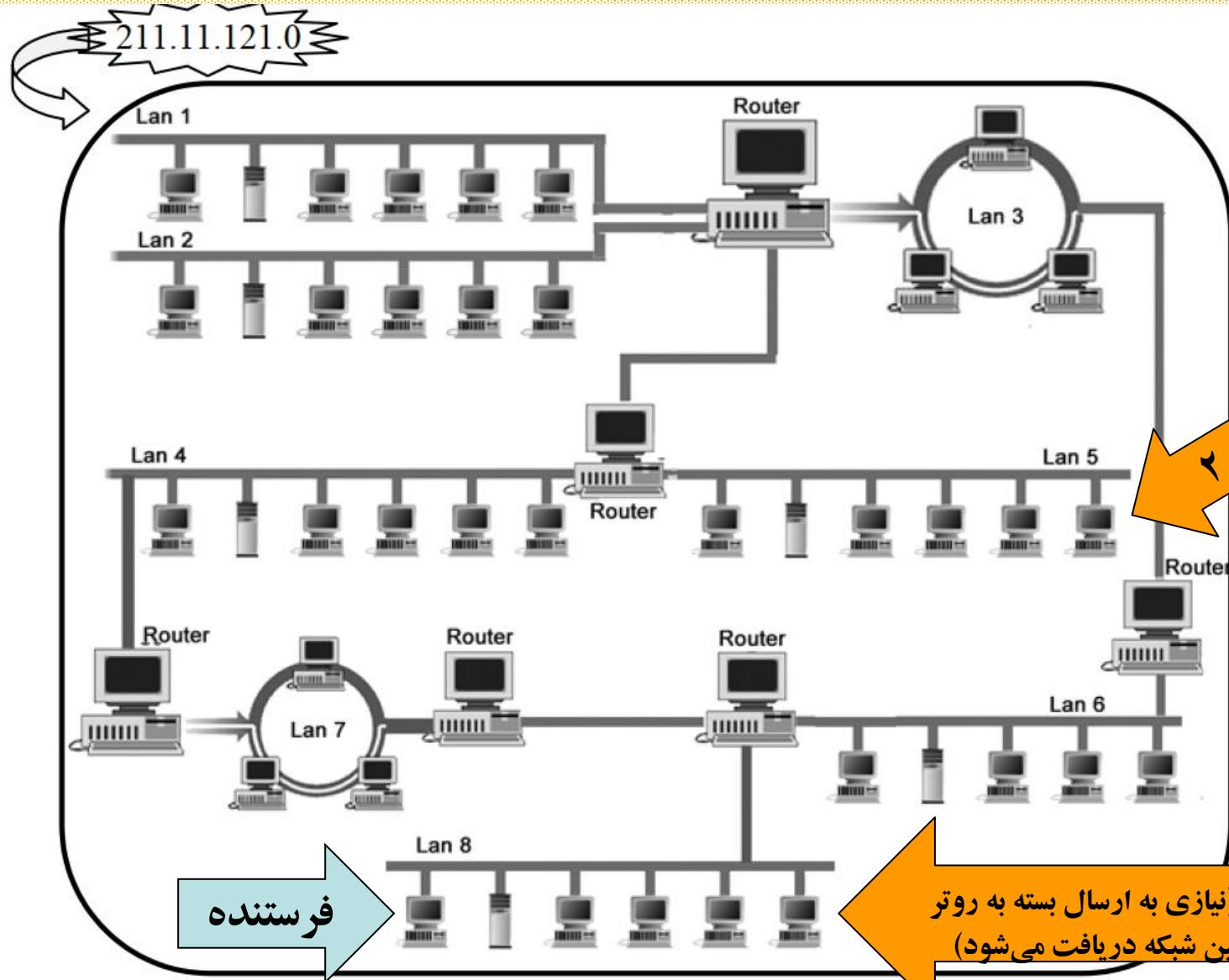
زیر شبکه (Subnet)

- در شبکه‌هایی که تعداد Host‌ها زیاد است، هر آدرس شبکه (مجموعه‌ای از Host‌ها) برای مدیریت بهتر به چند زیرشبکه‌ی کوچکتر تقسیم می‌شود که می‌توانند توپولوژی‌ها و تکنولوژی‌های متفاوت داشته باشند و از طریق مسیریاب‌ها به یکدیگر متصل هستند.
 - از دیدگاه بیرونی، کل شبکه با یک آدرس شناخته می‌شود و مسیریاب‌های بیرونی شناختی از ساختار شبکه‌بندی داخلی شبکه ندارند.
 - مثل وقتی که از بیرون دانشگاه برای شخصی داخل دانشگاه بسته‌ی پستی ارسال می‌شود. پستچی بیرون دانشگاه، فقط باجهی پست داخل دانشگاه را می‌شناسد و توزیع بسته‌های داخلی با پست دانشگاه است.
 - باید روشی وجود داشته باشد تا از طریق آدرس بتوان زیرشبکه‌ها را مشخص کرد و مسیریاب‌های داخلی هم بتوانند زیرشبکه‌های مختلف را شناسایی و تفکیک کنند.

C کلاس IP

زیرشبکه (Subnet)

گیرندگ ۲ (خارج از شبکه)



گیرندگ ۱ (نیازی به ارسال بسته به روتور
نیست و در همین شبکه دریافت می‌شود)

زیرشبکه (Subnet)

- تمامی ماشین‌های میزبان برای تشخیص مقصد یک بسته IP در شبکه، نیاز به الگوی زیرشبکه دارند که یک عدد ۳۲ بیتی است.
- میزبان از طریق الگوی زیرشبکه متوجه می‌شود آیا مقصد بسته در همین شبکه‌ی محلی است که خودش به آن تعلق دارد یا روی شبکه‌ای دیگر است؟ بر مبنای این اطلاعات است که بسته یا داخل شبکه توزیع می‌شود یا به روتر ارسال می‌شود.
- مثلاً آدرس 131.55.213.73 را در نظر گیرید که یک آدرس کلاس B با مشخصه‌ی شبکه‌ی 131.55.x.x و مشخصه‌ی میزبان x.x.213.73 است. این شبکه می‌تواند ۲^{۱۶} میزبان را ذیل مشخصه‌ی شبکه‌اش داشته باشد. اما تصمیم می‌گیرد آن را به ۲۵۶ زیرشبکه (در عمل ۲۵۴) که هر کدام ۲۵۶ کامپیوتر (در عمل ۲۵۴) داشته باشند تقسیم کند. بنابراین بخش مشخصه‌ی میزبان (۱۶ بیتی) را به دو بخش مشخصه‌ی زیرشبکه (۸ بیتی) و مشخصه‌ی میزبان (۸ بیتی) تقسیم می‌کند.

۲۱	۳۰	۲۹	۲۸	۲۷	۲۶	۲۵	۲۴	۲۳	۲۲	۲۱	۲۰	۱۹	۱۸	۱۷	۱۶	۱۵	۱۴	۱۳	۱۲	۱۱	۱۰	۹	۸	۷	۶	۵	۴	۳	۲	۱	۰
1	0	Network ID					Subnet ID					Host ID																			

الگوی زیرشبکه (Subnet Mask)

- زمانی که ماشین فرستنده بسته‌ای را ارسال می‌کند، برای تصمیم‌گیری اینکه آیا باید بسته را برای روتر بفرستد یا در همین زیرشبکه‌ای که خودش در آن است باید ارسال شود، باید بخش مشخصه‌ی شبکه و مشخصه‌ی زیرشبکه‌ی خودش را با IP گیرنده مقایسه کند.
- این کار از طریق AND کردن آدرس IP فرستنده و گیرنده با الگویی که در آن، بخش مشخصه‌ی شبکه و زیرشبکه ۱ و بقیه (مشخصه‌ی میزبان) صفر است و مقایسه‌ی نتایج انجام می‌شود.

۲۱	۳۰	۲۹	۲۸	۲۷	۲۶	۲۵	۲۴	۲۳	۲۲	۲۱	۲۰	۱۹	۱۸	۱۷	۱۶	۱۵	۱۴	۱۳	۱۲	۱۱	۱۰	۹	۸	۷	۶	۵	۴	۳	۲	۱	۰	
۱	۰	Network ID								Subnet ID								Host ID														
۲۱	۳۰	۲۹	۲۸	۲۷	۲۶	۲۵	۲۴	۲۳	۲۲	۲۱	۲۰	۱۹	۱۸	۱۷	۱۶	۱۵	۱۴	۱۳	۱۲	۱۱	۱۰	۹	۸	۷	۶	۵	۴	۳	۲	۱	۰	
۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۱	۰	۰	۰	۰	۰	۰	۰

تمرین) فرض کنید یک شبکه‌ی کلاس C خریداری کرده‌اید. الگوی زیرشبکه‌ی 255.255.255.192/26 چه اطلاعاتی به شما می‌دهد؟ (۲۶ تعداد بیت‌های یک در الگوی زیرشبکه است)

تمرین) برای تقسیم شبکه‌ی بالا به‌طوری که در هر زیرشبکه ۳۲ (عملاً ۳۰) کامپیوتر قرار بگیرد، از چه الگوی زیرشبکه‌ای استفاده می‌کنیم؟

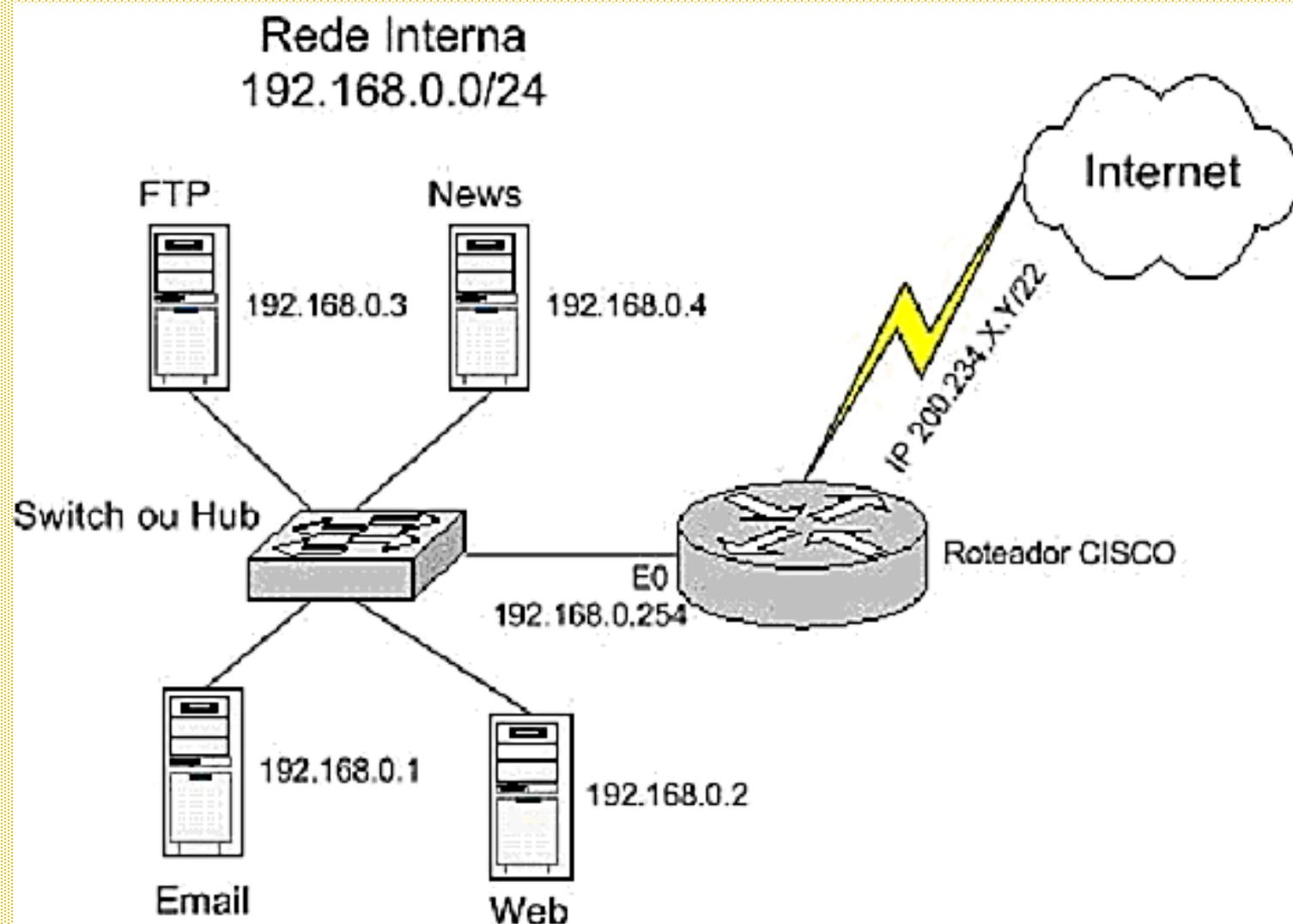
آدرس IP : 192.168.X.X

آدرس‌های IP نامعتبر (Invalid) که برای ماشین‌هایی که مستقیم به اینترنت متصل نیستند (در شبکه‌های خصوصی مستقل) مورد استفاده قرار می‌گیرد.

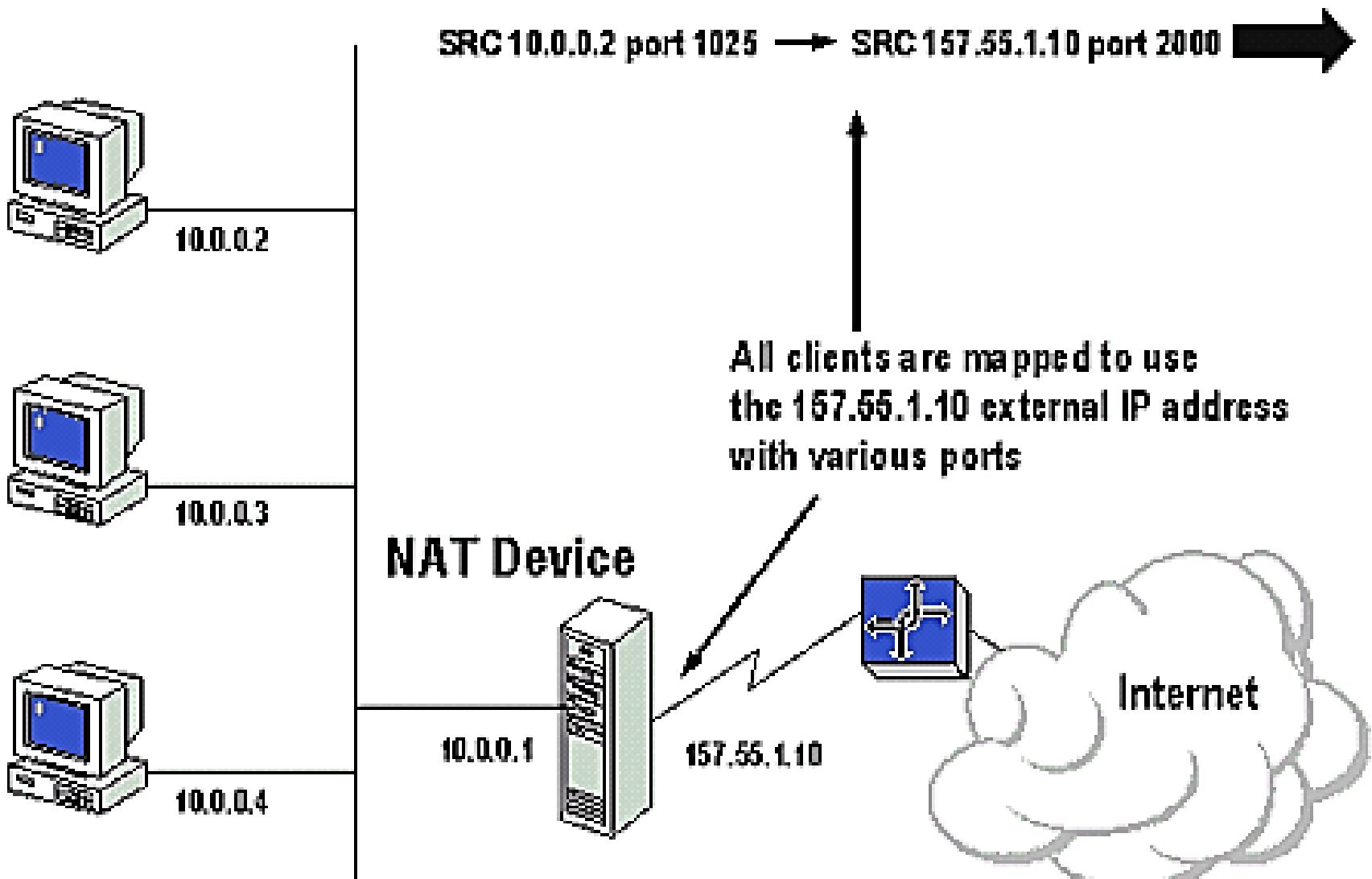
معتبر (Valid) بودن IP توسط بنیادهای IANA و InterNIC تضمین می‌شود.

Network Connection Details	
Network Connection Details:	
Property	Value
Connection-specific DN...	
Description	Intel(R) WiFi Link 5100 AGN
Physical Address	00-22-FB-A8-4C-38
DHCP Enabled	Yes
IPv4 Address	192.168.1.12
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Sunday, December 21, 2014 8:54:31 AM
Lease Expires	Monday, December 22, 2014 8:54:34 AM
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1

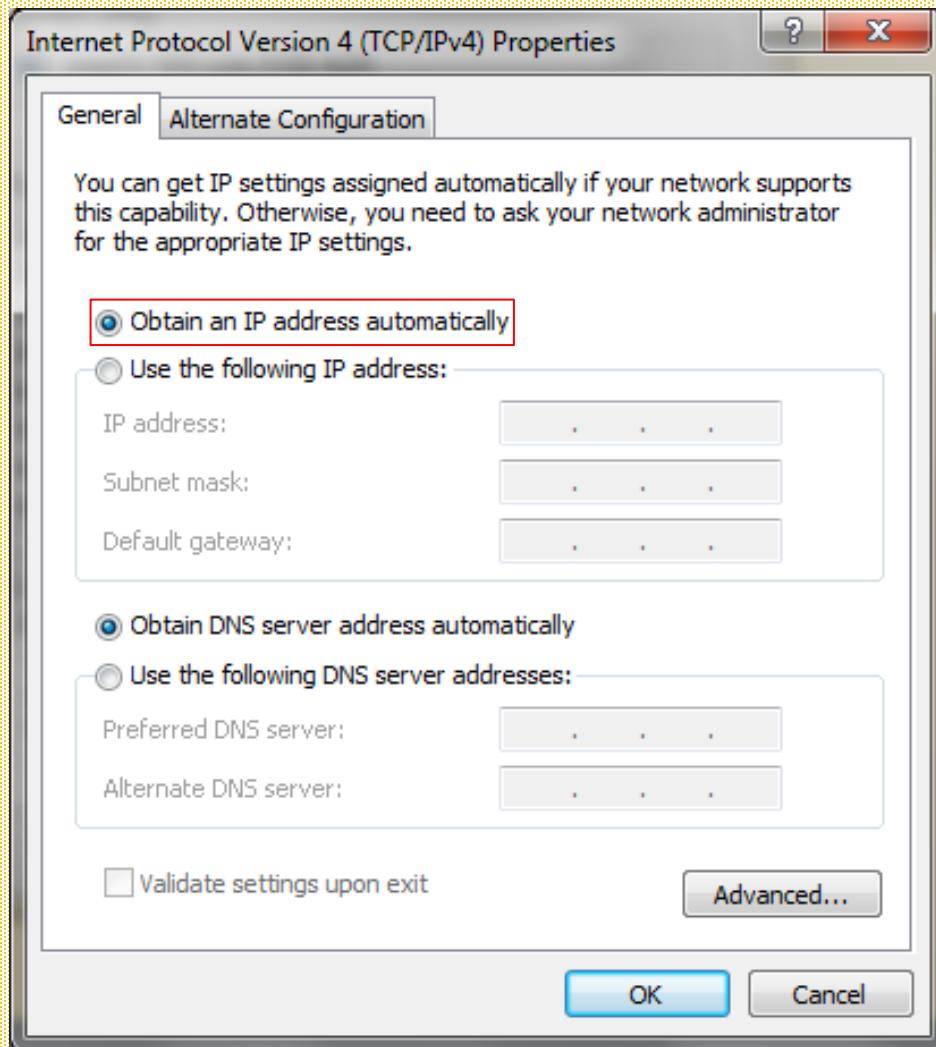
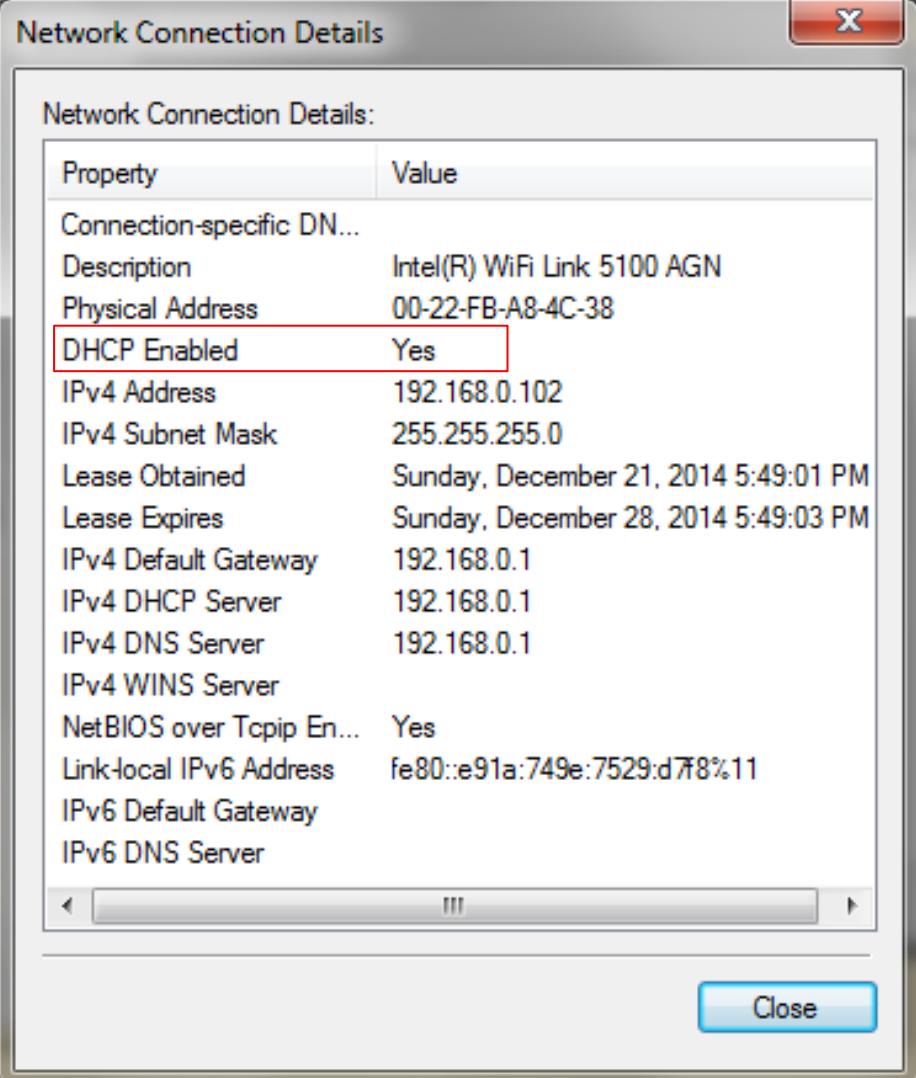
Nat Server



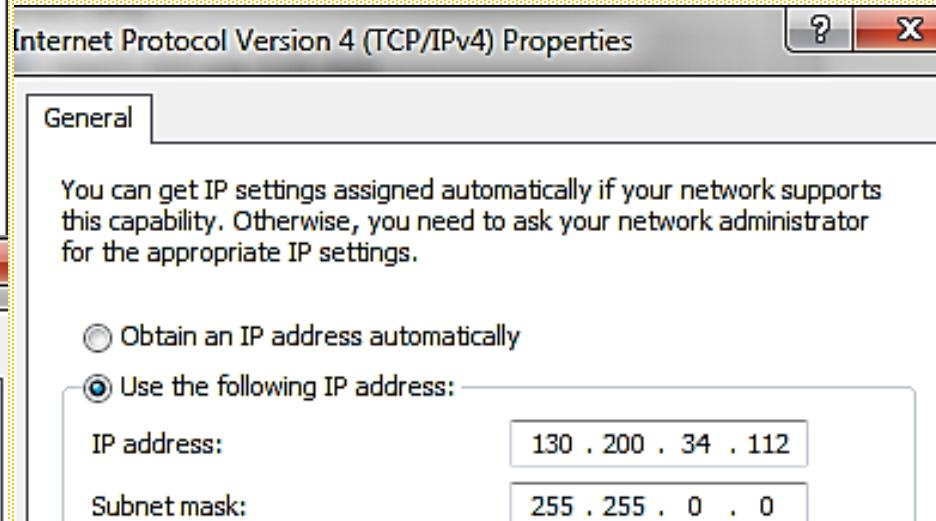
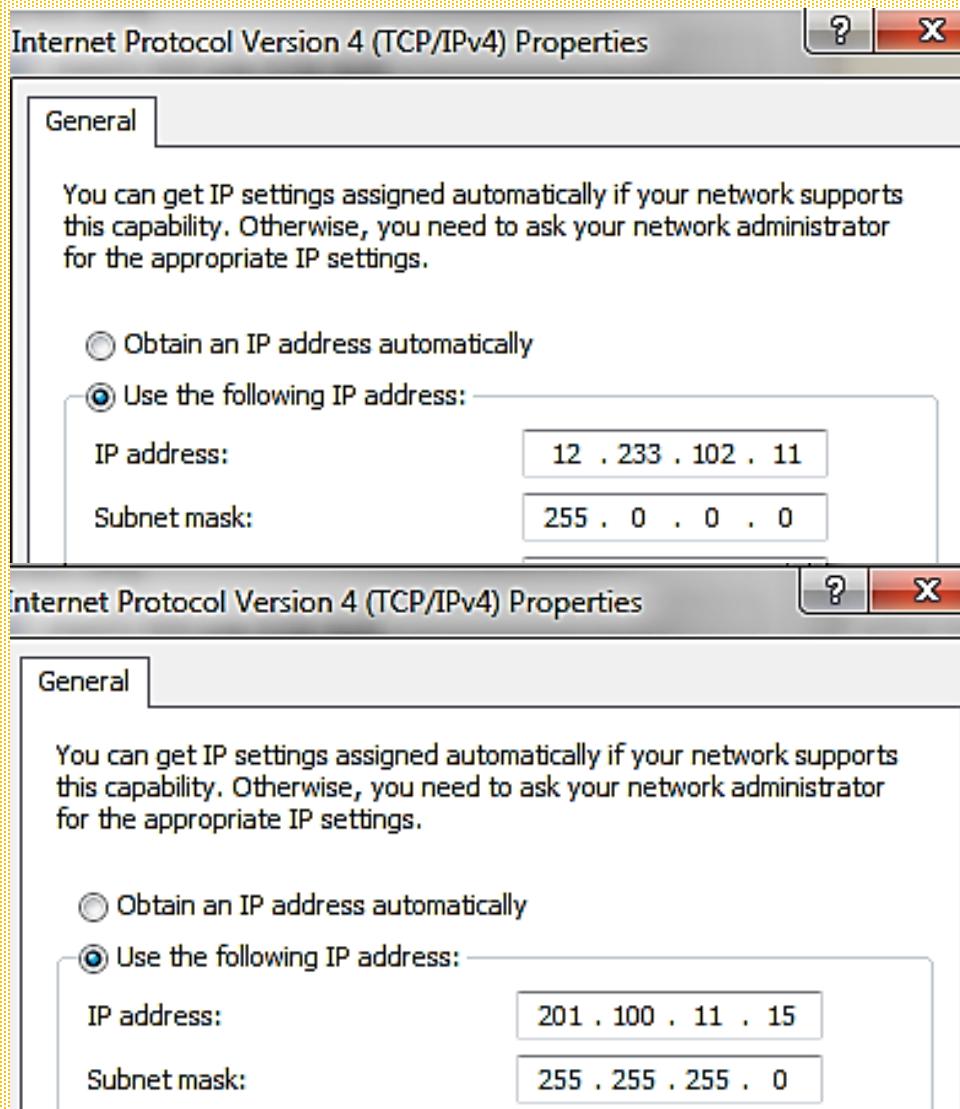
Nat Server



تخصیص IP: پویا

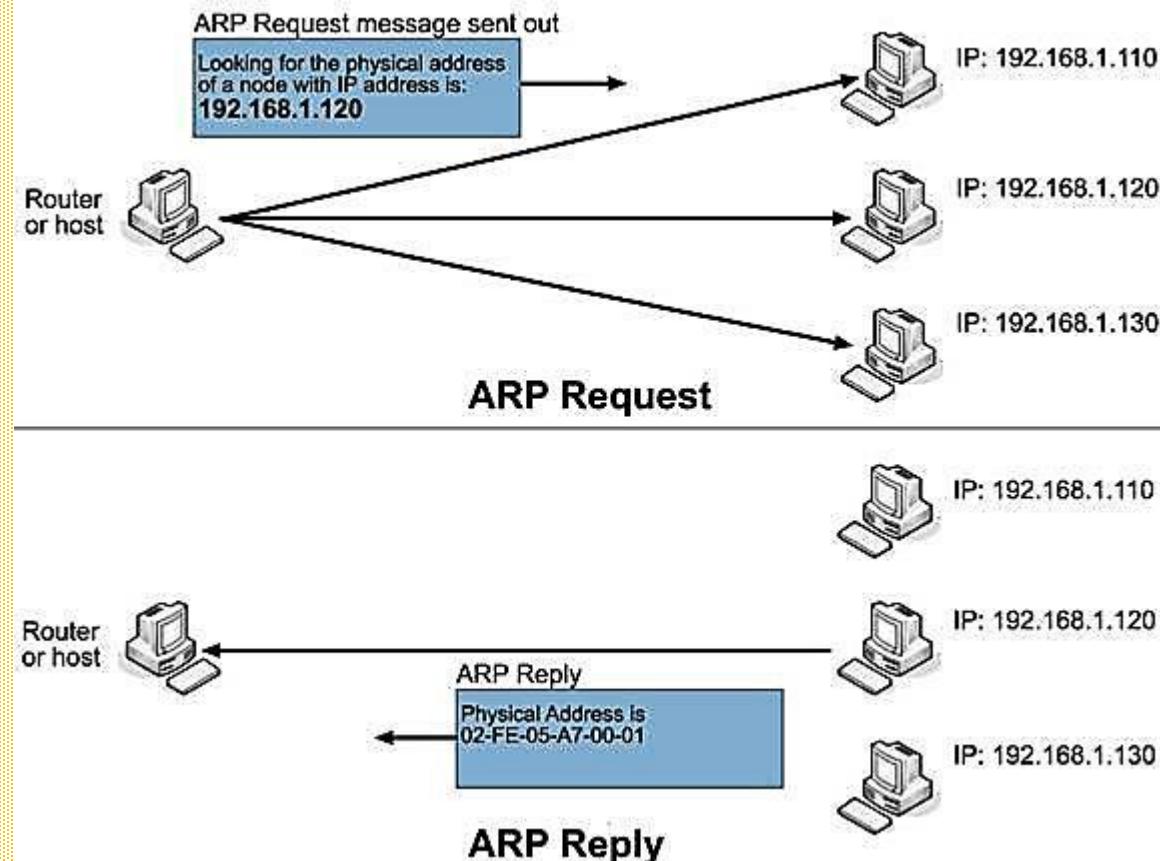


تخصیص IP: ایستا



پروتکل آدرس حل : ARP

- بی معنابودن آدرس‌های IP روی کانال انتقال
- دانستن آدرس IP ماشین مقصد و نیاز به داشتن آدرس فیزیکی آن جهت ارسال بسته
- وظیفه پروتکل ARP: ارسال بسته فرآگیر روی کل شبکه محلی که در آن آدرس IP ماشین مورد نظر قرار دارد. پاسخ ماشین با آدرس IP موجود در بسته ارسالی و ارسال آدرس فیزیکی خود برای ارسال‌کننده بسته ARP



پروتکل Reverse Address Resolution Protocol : *RARP*

- ایستگاه آدرس فیزیکی مورد نظرش را می‌داند ولیکن آدرس IP آن را نمی‌داند
- ارسال یک بسته فراگیر روی خط
- تمامی ایستگاههایی که از پروتکل RARP حمایت می‌کنند و بسته‌های مربوطه را تشخیص می‌دهند، در صورتی که آدرس فیزیکی خودشان را درون بسته ببینند در پاسخ به آن، آدرس IP خود را در قالب یک بسته RARP Reply برمی‌گردانند.

توجه: بسته‌های RARP, ARP از نوع فراگیر محلی Local Broadcast هستند و بالطبع توسط مسیریابها منتقل نمی‌شوند و فقط در محدوده شبکه محلی عمل می‌کنند.

.

نام حوزه (Domain Name) آدرس (Uniform Resource Locator) URL

- ✓ تشکیل نام حوزه از بخش‌هایی به نام سطح
- ✓ تفکیک سطح‌ها در نام حوزه با علامت •
- ✓ اشاره هر سطح از نام حوزه به یک قسمت از بانک اطلاعاتی توزیع شده
- ✓ تحلیل یک نام حوزه از سطوح سمت راست به چپ جهت پیدا نمودن سرویس‌دهنده متناظر

www.eng.ui.ac.ir/~rasti :مثال

www.jrasti.ir/Courses/Network/slides.zip

- ✓ تفاوت دامنه (Host) و میزبان (Domain)

هفت حوزه عمومی

.edu

موسسات علمی یا دانشگاهی
educational

.gov

آژانس‌های دولتی آمریکا
government

.org

سازمانهای غیر انتفاعی
organization

.net

ارائه دهنده خدمات شبکه
Network Service provider

.com

موسسات اقتصادی و تجاری
commercial

.int

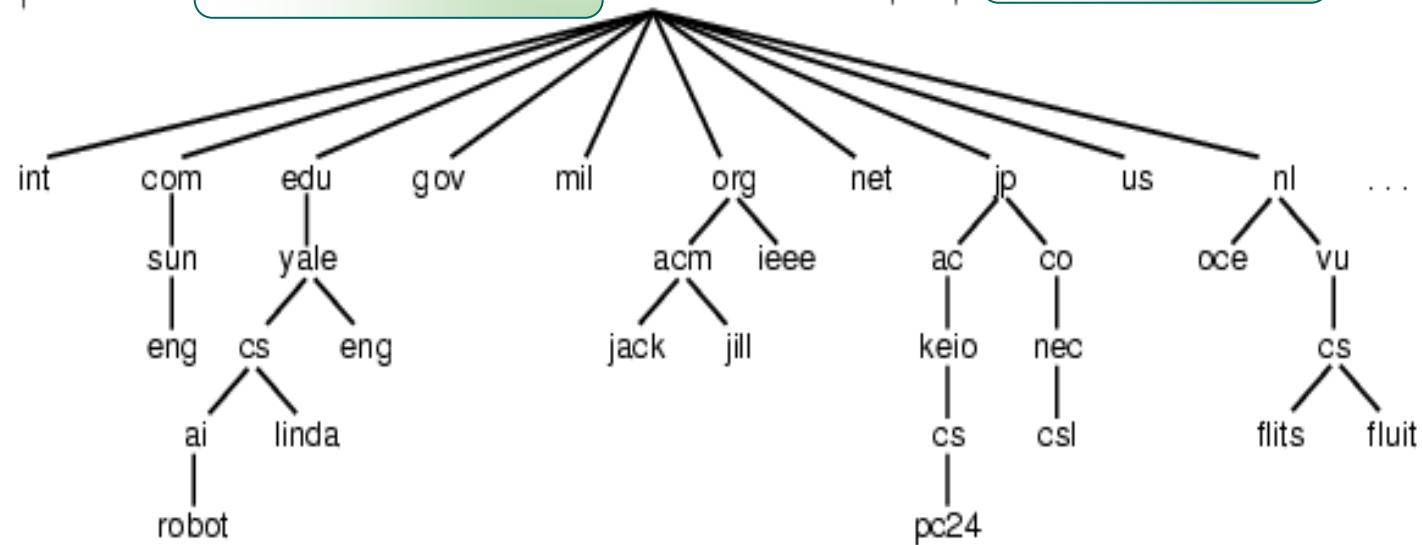
سازمانهای بین المللی
international

.mil

سازمانهای نظامی دنیا
military

حوزه‌های عمومی

حوزه‌های کشوری



حوزه‌های عمومی و حوزه‌های کشوری

سرویس دهنده نامهای حوزه (Domain Name System)

آدرسها در دنیای واقعی = آدرسهای اینترنت = آدرسهای نمادین = نام حوزه

مانند: www.ibm.com

ترجمه آدرسهای نمادین به آدرسهای IP

- ۱) روش متمرکز: - تعریف تمام نامها و آدرسهای IP معادل در یک فایل به نام **hosts.txt**
- استفاده از فایل **hosts.txt** جهت ترجمه یک نام نمادین به آدرس IP معادل آن توسط تابع مترجم نام موجود در هر ماشین میزبان

کاربرد در شبکه ARPANET

و شبکه های کوچک و داخلی

(۲) DNS یا سیستم نامگذاری حوزه:

- روشی سلسله مراتبی
- توزیع بانک اطلاعاتی مربوط به نامهای نمادین و معادل IP آنها در کل شبکه اینترنت
- معرفی این سیستم در سال ۱۹۸۴
- کاربرد در شبکه‌های بزرگ مانند اینترنت

روش ترجمه نام در DNS

- فراخوانی تابع تحلیلگر نام Name Resolver توسط برنامه کاربردی
- پارامتر ورودی تابع تحلیلگر نام آدرس نمادین
- ارسال بسته UDP (بسته درخواست) به آدرس یک سرویس‌دهنده DNS (به صورت پیش فرض مشخص می‌باشد) توسط تابع
- تحویل آدرس IP معادل با آدرس نمادین از طرف سرویس‌دهنده به تابع تحلیلگر
- تحویل آدرس IP به برنامه کاربردی درخواست‌کننده

پیدا کردن IP یک سایت:

۱) آن سایت را ping کنید.

۲) در محیط Command سایت را tracert کنید.

<https://www.ip-adress.com/whois-lookup> (۳)

<https://www.site24x7.com/find-ip-address-of-web-site.html> (۴)

پیدا کردن IP خود سیستم در اینترنت و نمایش محل روی نقشه:

<http://www.ip-adress.com/>

نمونه‌ی tracert یک سایت خارجی

```
C:\Users\Abolfazl>tracert google.com
```

```
Tracing route to google.com [172.217.169.238] ←  
over a maximum of 30 hops:
```

1	228 ms	226 ms	223 ms	172.16.72.1
2	230 ms	208 ms	190 ms	172.16.1.110
3	226 ms	232 ms	*	172.16.1.1
4	219 ms	208 ms	232 ms	172.16.1.6
5	234 ms	199 ms	193 ms	logout.ui.ac.ir [192.168.25.16]
6	232 ms	218 ms	197 ms	asmanfaraz.1.40.126.93.in-addr.arpa [93.126.40.1]
7	105 ms	102 ms	99 ms	172.16.199.233
8	57 ms	47 ms	42 ms	172.22.13.1
9	94 ms	99 ms	105 ms	172.16.19.2
10	73 ms	*	111 ms	172.17.2.29
11	184 ms	205 ms	198 ms	10.202.6.32
12	214 ms	198 ms	207 ms	10.202.4.176
13	228 ms	238 ms	243 ms	10.21.21.10
14	240 ms	239 ms	224 ms	10.21.0.11
15	269 ms	272 ms	261 ms	213.202.4.172
16	258 ms	229 ms	236 ms	213.202.5.239
17	112 ms	118 ms	123 ms	216.239.48.87
18	106 ms	107 ms	111 ms	172.253.51.131
19	239 ms	202 ms	200 ms	mct01s10-in-f14.1e100.net [172.217.169.238]

```
Trace complete.
```

نمونه‌ی tracert یک سایت خارجی با VPN

```
C:\Users\Abolfazl>tracert google.com
```

```
Tracing route to google.com [142.250.186.78] ←  
over a maximum of 30 hops:
```

1	105 ms	178 ms	200 ms	100.120.201.1
2	102 ms	101 ms	107 ms	r-1-45-234-77.ff.avast.com [77.234.45.1]
3	103 ms	102 ms	101 ms	5.62.25.1
4	104 ms	102 ms	101 ms	10.26.0.18
5	102 ms	125 ms	168 ms	border3.ae15.avast-25.fra002.pnap.net [95.172.67.121]
6	103 ms	102 ms	102 ms	core1-0-0-0-0.fra002.pnap.net [95.172.67.3]
7	103 ms	101 ms	102 ms	te0-0-0-3.rcr21.b015749-1.fra03.atlas.cogentco.com [149.11.106.41]
8	163 ms	103 ms	102 ms	be2501.ccr41.fra03.atlas.cogentco.com [154.54.39.177]
9	*	125 ms	204 ms	be3186.agr41.fra03.atlas.cogentco.com [130.117.0.2]
10	210 ms	201 ms	102 ms	tata.fra03.atlas.cogentco.com [130.117.15.86]
11	113 ms	112 ms	135 ms	72.14.196.162
12	115 ms	115 ms	113 ms	108.170.251.129
13	103 ms	102 ms	103 ms	142.250.214.187
14	164 ms	102 ms	102 ms	fra24s05-in-f14.1e100.net [142.250.186.78]

```
Trace complete.
```

نمونه‌ی tracert یک سایت داخلی

```
C:\Users\Abolfazl>tracert aparat.com
```

```
Tracing route to aparat.com [185.147.178.13] ←  
over a maximum of 30 hops:
```

1	217 ms	226 ms	230 ms	172.16.72.1
2	206 ms	207 ms	214 ms	172.16.1.110
3	201 ms	206 ms	219 ms	172.16.1.1
4	180 ms	188 ms	188 ms	172.16.1.6
5	227 ms	210 ms	188 ms	logout.ui.ac.ir [192.168.25.16]
6	224 ms	226 ms	229 ms	asmanfaraz.1.40.126.93.in-addr.arpa [93.126.40.1]
7	228 ms	247 ms	230 ms	172.16.199.233
8	221 ms	238 ms	241 ms	172.22.13.1
9	234 ms	*	208 ms	10.201.219.110
10	*	*	*	Request timed out.
11	240 ms	243 ms	239 ms	185.147.178.13

• سازماندهی اطلاعات به صورت قطعه (Segment)

- ارسال یک بسته ویژه قبل از ارسال بسته‌ها برای اطمینان از آمادگی گیرنده برای دریافت اطلاعات
- شماره‌گذاری بسته‌های ارسالی برای جلوگیری از گم شدن یا ارسال دوباره بسته‌ها
- حفظ ترتیب جریان بسته‌های ارسالی
- آدرس‌دهی پروسه‌های مختلفی که روی یک ماشین واحد اجرا می‌شوند.
- تقسیم پیامهای بزرگ به بسته‌های اطلاعاتی کوچکتر
- بازسازی بسته‌های اطلاعاتی و تشکیل یک پیام کامل
- شماره‌گذاری بسته‌های کوچکتر جهت بازسازی
- تعیین و تبیین مکانیزم نامگذاری ایستگاههای موجود در شبکه

جبران ضعف‌های لایه‌ی IP

- عدم تضمین آماده بودن ماشین مقصد
 - عدم تضمین حفظ ترتیب و صحت داده‌ها
 - عدم تضمین تکراری نبودن بسته‌ها
 - ارسال فله‌ای بسته‌های مربوط به ماشین
- هماهنگی بین فرستنده و گیرنده قبل از ارسال داده
 - شماره‌گذاری و مکانیسم کشف خطا
 - شماره‌گذاری
 - جداسازی بسته‌های مربوط به هر پروسه

سرویس‌های لایه‌ی انتقال

(Transfer Control Protocol) TCP: سرویس مطمئن با اتصال

(User Datagram Protocol) UDP: سرویس نامطمئن بی‌اتصال

TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement

سرویس‌های لایه‌ی انتقال

(Transfer Control Protocol) TCP: سرویس مطمئن با اتصال

(User Datagram Protocol) UDP: سرویس نامطمئن بی‌اتصال

	Reliable	Best-Effort
Connection Type	Connection-oriented	Connectionless
Protocol	TCP Data Stream	UDP Datagram
Sequencing	Yes	No
Uses	<ul style="list-style-type: none">▪ E-mail▪ File sharing▪ Downloading	<ul style="list-style-type: none">▪ Voice streaming▪ Video streaming

سرویس‌های اتصال‌گرا و بدون اتصال

اتصال‌گرایی ربطی به سوییچینگ بسته و مدار ندارد و روی هر لایه‌ای از همین شبکه‌های سوییچینگ بسته هم می‌تواند پیاده شود.

- **لایه فیزیکی:** مذاکره بر سر سرعت نماد اتصال‌گرایی است. در حالت بدون اتصال، داده‌ها بر اساس مشخصات از پیش توافق‌شده ارسال می‌شوند.
- **لایه پیوند داده:** اگر مانند اترنوت بر اساس قراردادهای استاندارد اطلاعات ارسال شود بدون اتصال است. اگر مثل Wifi چند فریم کنترلی در ابتدا ارسال شود و پس از اطمینان از آمادگی و حضور گیرنده فریم‌های داده ارسال شوند، اتصال‌گرا است.

سرویس‌های اتصال‌گرا و بدون اتصال

اتصال‌گرایی ربطی به سوییچینگ بسته و مدار ندارد و روی هر لایه‌ای از همین شبکه‌های سوییچینگ بسته هم می‌تواند پیاده شود.

- **لایه شبکه:** اگر مثل شبکه‌های ATM تمام مسیریاب‌های بین فرستنده و گیرنده ثبت و تنظیم شوند و تمهیدات لازم را پیش‌بینی کنند اتصال‌گرا است. شبکه‌ی اینترنت بدون اتصال است تا سربار کمی داشته باشد.
- **لایه انتقال:** در ارتباط TCP با ارسال بسته‌های کنترلی خاص بین دو لایه‌ی انتقال، هماهنگی اولیه انجام و سپس بسته‌های داده ارسال می‌شوند. در ارتباط UDP، پروسه فرستنده بدون هماهنگی داده‌ها را ارسال می‌کند و اگر لایه انتقال گیرنده قادر به دریافت نباشد، آن‌ها را دور می‌ریزد.

لایه جلسه Session Layer

- برقراری و مدیریت یک جلسه (مجموعه عملیاتی که پس از برقراری ارتباط بین دو پرسه با یک توافق اولیه آغاز و با انجام چند تراکنش ادامه می‌یابد و در روالی هماهنگ قطع می‌شود مانند Remote Login (ادامه‌ی یک نشست نافرجام شناسائی طرفین Authentication) (Authorization) (مشخص نمودن اعتبار پیامها) (Accounting) (حسابداری مشتریها)

لایه ارائه (نمایش) Presentation Layer

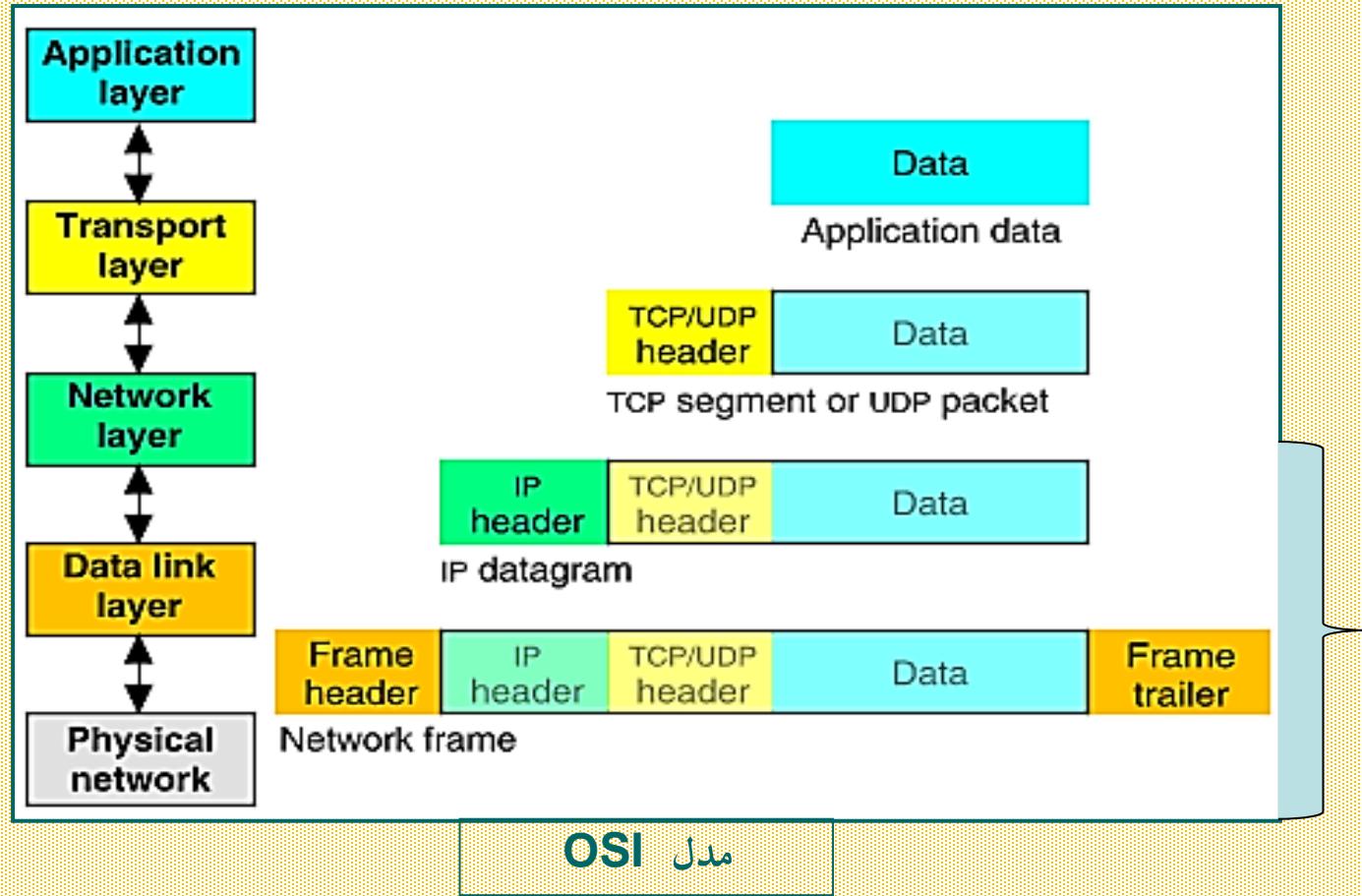
- فشرده‌سازی فایل
- رمزنگاری برای ارسال داده‌های محرمانه
- رمزگشائی
- تبدیل کدها به یکدیگر هنگام استفاده دو ماشین از استانداردهای مختلفی برای متن

لایه کاربرد Application Layer

تعریف استانداردهائی نظری :

- انتقال نامه‌های الکترونیکی
 - انتقال مطمئن فایل
 - دسترسی به بانکهای اطلاعاتی راه دور
 - مدیریت شبکه
 - انتقال صفحه وب
- پروتکل‌های telnet, pop3, pop2, smtp, ftp, https, http و ...

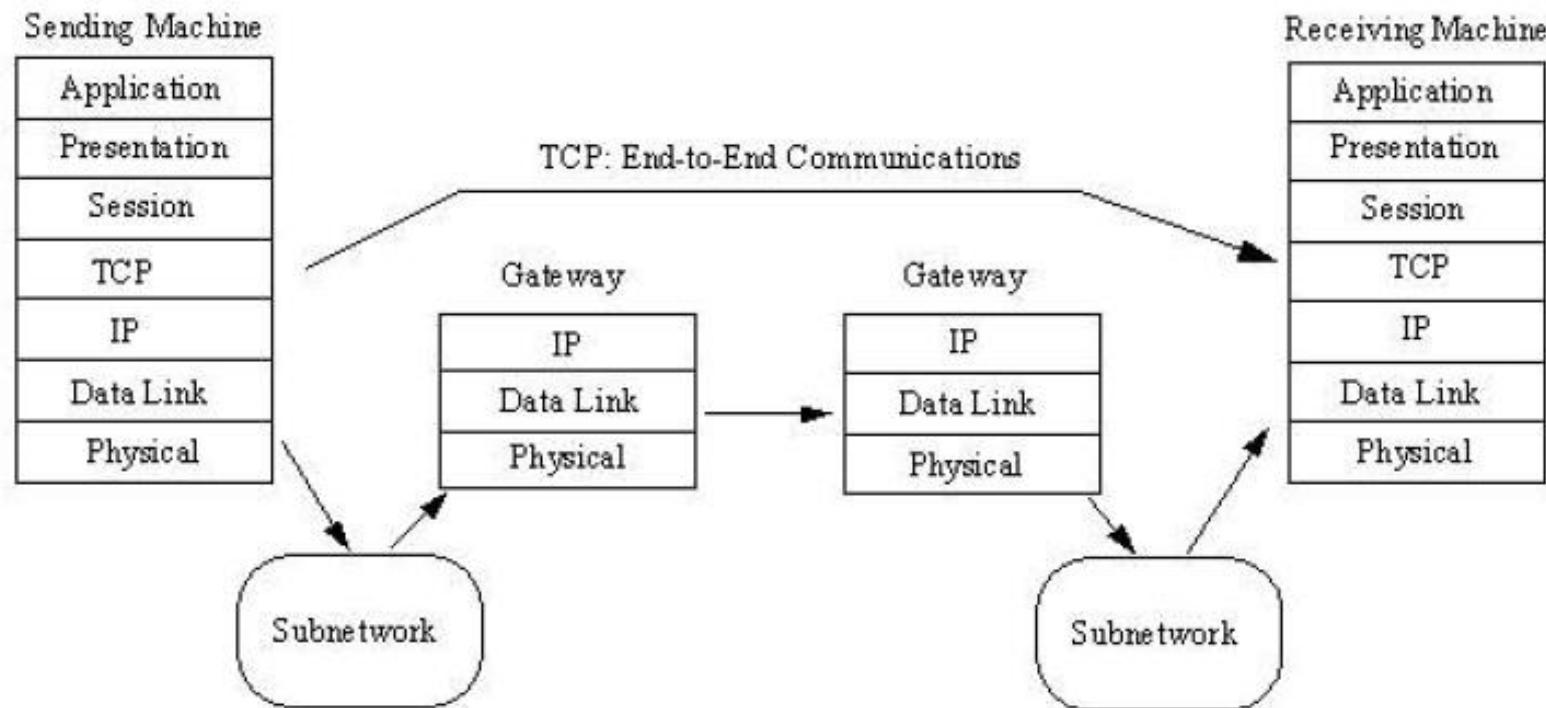
روند حذف و اضافه شدن سرآیند در هر لایه



لایه هایی که سرآیند را اضافه کرده اند

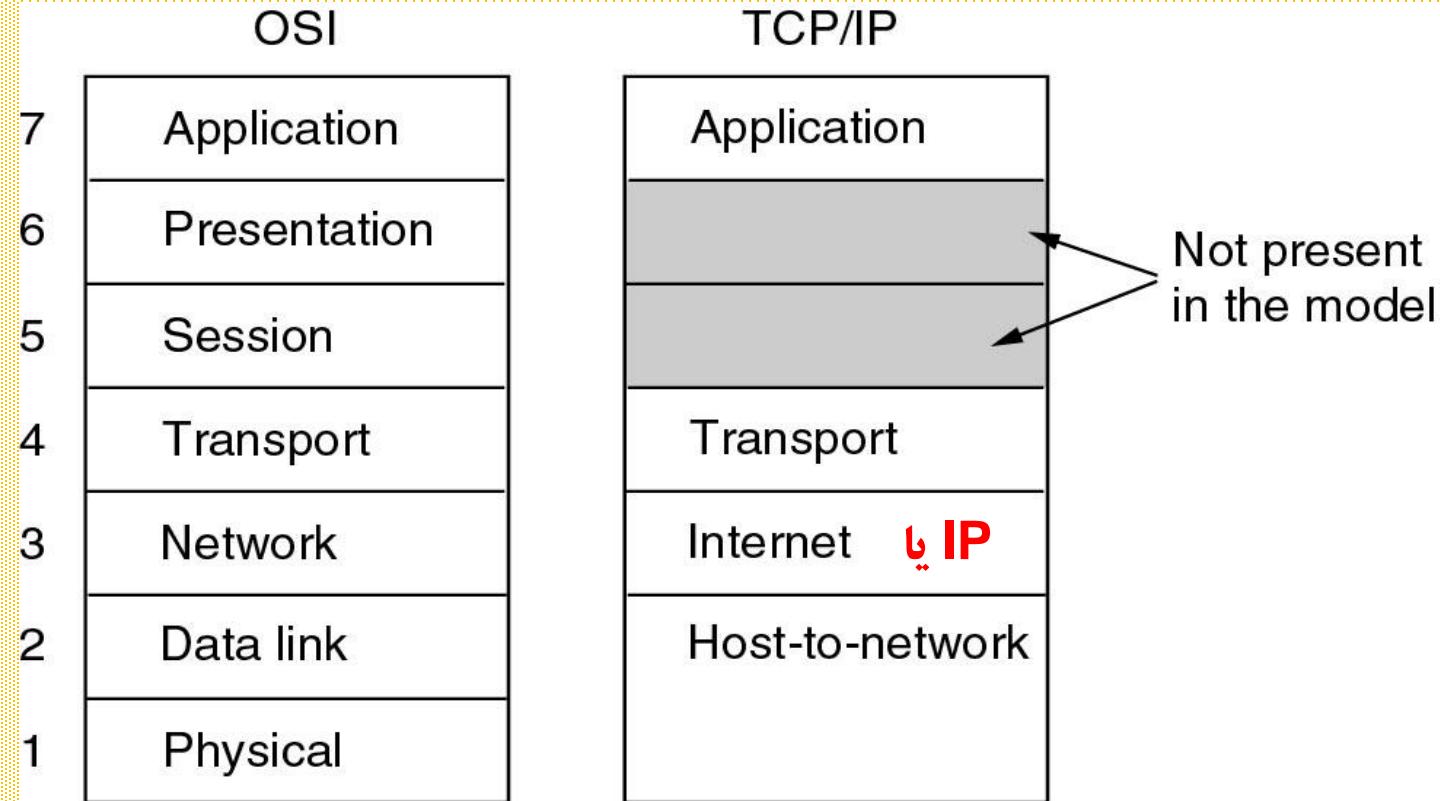
ارتباطات انتهایه‌هایها (End to End)

لایه‌های یک تا سه را لایه‌های گام به گام (Hop to Hop) گویند. یعنی ارتباط در این لایه‌ها مستقیماً با لایه‌های متناظر در ماشین مقصد برقرار نمی‌شود بلکه در طول مسیر بین مسیریاب‌های مختلف تا رسیدن به مقصد به صورت زنجیره‌ای برقرار است. اما در لایه چهار تا لایه هفت ارتباط انتهایها به انتهایها (End to End) وجود دارد یعنی این لایه‌ها به صورت مستقیم با لایه‌های متناظر خود در ماشین مقصد ارتباط برقرار می‌کنند.



Worst!
but Best!

مدل چهار لایه‌ای TCP/IP



لایه‌های مدل TCP/IP

نامهای معادل در برخی از کتب	لایه‌ها
لایه سرویس‌های کاربردی	لایه کاربرد Application layer
لایه ارتباط میزبان به میزبان (Host to Host) (End to End Connection)	لایه انتقال Transport layer
لایه اینترنت لایه ارتباطات اینترنت	لایه شبکه Network layer
لایه میزبان به شبکه (Host to Network) لایه رابط شبکه	لایه دسترسی به شبکه Network Interface

لایه اول از مدل TCP/IP: لایه واسط شبکه

تعریف لایه‌های استاندارد سخت‌افزار، نرم‌افزارهای راه‌انداز و پروتکلهای شبکه در این لایه پروتکلهایی که در لایه اول از مدل **TCP/IP** تعریف می‌شوند، می‌توانند مبتنی بر ارسال رشته بیت یا مبتنی بر ارسال رشته بایت باشند.

لایه دوم از مدل TCP/IP: لایه شبکه

- بسته‌های IP بسته‌های اطلاعاتی در این لایه
- هدایت بسته‌های IP روی شبکه از مبدأ تا مقصد که این عمل از نوع نامطمئن بدون اتصال می‌باشد. در صورت نیاز به سرویس‌های دیگر در لایه‌های بالاتر باید ارائه شود.
- مسیریابی بسته‌های لایه‌ی بالاتر به صورت Hop-to-Hop (انتقال از یک مسیریاب به مسیریاب دیگر)
- پروتکلهایی که در این لایه استفاده می‌شوند عبارتند از: **IP , IGMP , BOOTP , ARP , RARP , RIP , ICMP ..**

لایه سوم از مدل TCP/IP : لایه انتقال

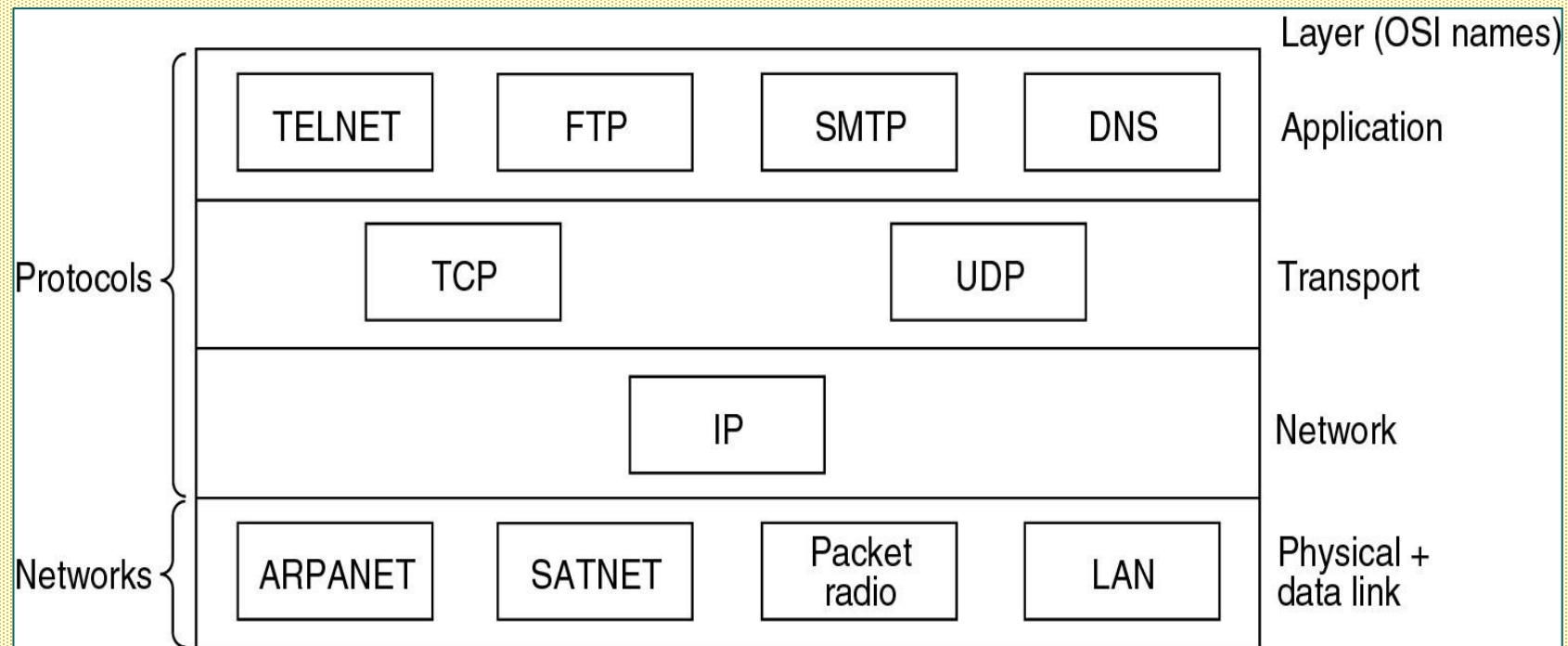
برقراری ارتباط از طریق یک سرویس اتصال‌گرا و مطمئن با ماشین‌های انتهایی یا میزبان.
ارسال و یا دریافت داده‌های تحویلی به این لایه توسط برنامه‌های کاربردی و از طریق توابع سیستمی

لایه چهارم از مدل TCP/IP : لایه کاربرد

خدماتی که در این لایه صورت می‌گیرد در قالب پروتکلهای استاندارد زیر
به کاربر ارائه می‌شود :

- شبیه‌سازی ترمینال
- FTP
- مدیریت پست الکترونیکی
- خدمات انتقال صفحات ابرمنته

پروتکل‌های رایج در لایه‌ها



مدل‌های ارتباطی بین کامپیوترها

مدل سرور/مشتری (Clint/Server)

- سرور برنامه کامپیوتری است که دارای اطلاعات است و یا برای دیگر کامپیوترها سرویس و خدمات فراهم می‌کند. کلاینت (مشتری) برنامه کامپیوتری است که نیاز به اطلاعات دارد و یا از سرویس ارائه شده توسط سرور استفاده می‌کند.
- ارتباط بین دو برنامه کلاینت و سرور با درخواست از طرف کلاینت و ارائه سرویس (پاسخ) از طرف سرور انجام می‌شود.
- بعد از برباسازی سخت‌افزار، بایستی نرم‌افزار سرور روی یک کامپیوتر و روی دیگر کامپیوترها نرم‌افزار کلاینت نصب شود.
- تمام اطلاعات شبکه و فایلها به صورت مت مرکز بر روی سرور قرار می‌گیرد.

مدل‌های ارتباطی بین کامپیوترها

مدل نظیر به نظیر (Peer to Peer)

- در این مدل هر کامپیوتر هم به صورت کلاینت و هم به صورت سرور عمل می‌نماید. پس از برپاسازی سخت‌افزار، نرم‌افزارهای لازم شبکه نظیر به نظیر بایستی روی تمامی کامپیوترها نصب شوند و اطلاعات به صورت توزیعی بر روی تمامی کامپیوترها پخش شوند.
- در واقع در این شبکه ایستگاه ویژه‌ای جهت نگهداری فایل‌های اشتراکی و سیستم عامل شبکه وجود ندارد و به تجهیزات اضافی به جز یک سیستم عامل بر روی هر یک از کامپیوترها نیازی نخواهد بود.

مدل‌های ارتباطی بین کامپیوترها

مقایسه‌ی دو مدل

- در مدل نظیر به نظری، با توجه به اینکه کاربران مسئولیت کنترل منابع خود را به عهده دارند، به مدیریت متمن کز نیازی نیست.
- مدیریت منابع نظیر تغییر فایل‌ها، نصب نرم‌افزارهای جدید، ایجاد کاربران جدید، ایجاد مجوزهای دسترسی در مدل سرور/مشتری به صورت متمن کز و بسیار راحت است. بنابراین برای شبکه‌های بزرگ با تعداد کاربران زیاد مناسب است.
- در مدل نظیر به نظیر تعداد کامپیوترها معمولاً کمتر از ۱۰ دستگاه است.
- با خرابی سرور در مدل سرور/مشتری کل شبکه از کار می‌افتد. در حالی که در مدل نظیر به نظیر چنین نیست؛ به همین علت در بعضی از شبکه‌ها از چندین سرور به جای تک سرور استفاده می‌گردد.
- هزینه برپاسازی و مدیریت شبکه‌های سرور/مشتری نسبت به شبکه‌های نظیر به نظیر به مراتب بیشتر است.

Socket Programming

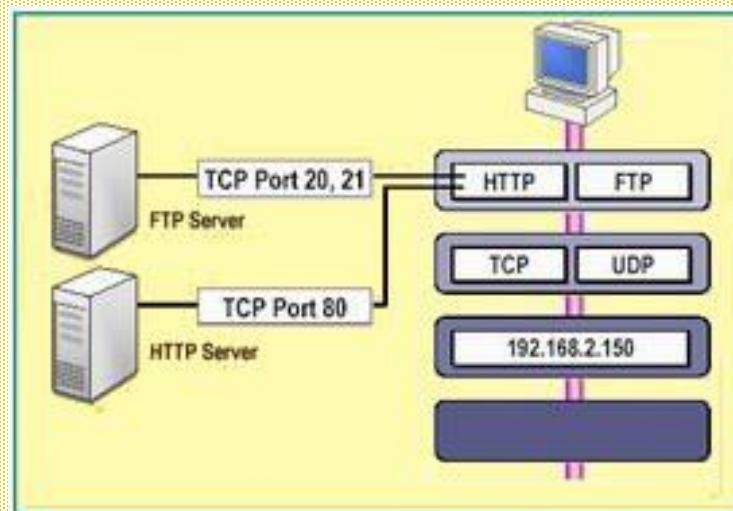
ارتباط بین برنامه‌ی روی دو کامپیوتر با استفاده از پروتکل‌های لایه‌ی انتقال

تعريف سوکت

زمانیکه چندین برنامه بر روی یک کامپیوتر فعال می‌گردند، روشی به منظور تمایز یک برنامه از برنامه دیگر مورد استفاده قرار گیرد. سوکت (Socket) به منظور مشخص کردن یک برنامه خاص روی یک کامپیوتر خاص استفاده می‌شود که شامل ترکیب IP:Port (مثلاً 80.247.3.100:8000) است.

پورت

لایه انتقال برای اینکه بداند هر بسته متعلق به کدام برنامه‌ی کاربردی در لایه‌ی هفتم است، به آن یک شماره‌ی یکتا از صفر تا ۶۵۵۳۵ اختصاص می‌دهد که شماره پورت نامیده می‌شود.



Socket Programming

Well-Known Ports

The port numbers in the range from 0 to 1023 are the well-known, also known as System ports. They are used by system processes that provide widely-used types of network services. Examples of some of the most common well-known ports are:

Port	Service	Protocol	Description
20	ftp	tcp/udp/sctp	File Transfer Data
21	ftp	tcp/udp/sctp	File Transfer Control
22	ssh	tcp/udp/sctp	Secure Shell
23	telnet	tcp/udp	Telnet
25	smtp	tcp/udp	Simple Mail Transfer
42	name	tcp/udp	Name Server (WINS)
67	bootps	udp	Bootstrap (BOOTP/DHCP) Server
68	bootpc	udp	Bootstrap (BOOTP/DHCP) Client
69	tftp	udp	Trivial File Transfer
80	http	tcp	Hypertext Transfer Protocol
88	kerberos	tcp	Kerberos
110	pop3	tcp	Post Office Protocol v3
119	nntp	tcp	Network News Transfer Protocol
123	ntp	udp	Network Time Protocol
135	epmap	tcp/udp	DCE Endpoint Mapper/RPC
137	netbios-ns	tcp/udp	NETBIOS Name Service
138	netbios-dgm	tcp/udp	NETBIOS Datagram Service
139	netbios-ssn	tcp/udp	NETBIOS Session Service
143	imap	tcp/udp	Internet Message Access Protocol
161	snmp	udp	Simple Network Management Protocol
162	snmptrap	tcp/udp	Simple Network Management Protocol Trap
443	https	tcp	Internet Message Access Protocol
445	microsoft-ds	tcp	SMB File Sharing

برنامه نویسی سوکت TCP با فرم‌های ویندوز در C#

برای برقراری یک ارتباط TCP، به یک برنامه سرویس‌دهنده (Server) و یک برنامه مشتری (Client) نیاز داریم:

- در برنامه سرویس‌دهنده، یک سوکت تعریف می‌شود که باید به درخواست‌های احتمالی روی یک پورت مشخص «گوش کند» و پس از دریافت درخواست آن را پذیرد.
- در برنامه مشتری باید درخواست اتصال به سوکت مذبور (IP:Port Number) ارسال شود و پس از پذیرش توسط سرویس‌دهنده، تبادل اطلاعات آغاز گردد.

دو نوع برنامه سرویس‌دهنده وجود دارد:

۱) برنامه سرویس‌دهنده سنکرون

این برنامه در حال انتظار برای دریافت درخواست اتصال، قفل (Block) می‌شود و توانایی انجام هیچ کاری را ندارد؛ اما نوشتمن و درک آن ساده است.

۲) برنامه سرویس‌دهنده آسنکرون

این برنامه به کمک threadها، وظیفه پذیرش درخواست‌های اتصال و دریافت داده‌ها را بدون قفل شدن انجام می‌دهد. این برنامه نسبت به نسخه سنکرون پیشرفته‌تر و در عین حال پیچیده‌تر است.