# شبکه‌های مخابراتی

**سید حمید صفوی**
دانشکده فنی و مهندسی
دانشگاه محقق اردبیلی
نیمسال دوم ۹۸-۹۹

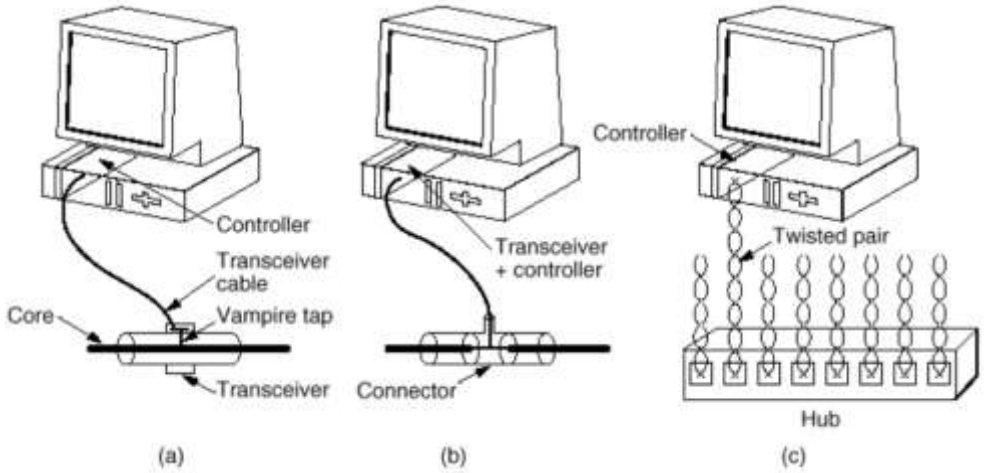
# استانداردها

# استانداردهای گروه IEEE 802

- گروه IEEE 802 فعال‌ترین مجموعه استانداردسازی بین‌المللی است که در تدوین استانداردهای لایه MAC فعالیت کرده است.

IEEE 802: Overview & Architecture
IEEE 802.1 Bridging & Management
IEEE 802.2: Logical Link Control
IEEE 802.3: CSMA/CD Access Method (Ethernet)
IEEE 802.5: Token Ring Access Method
IEEE 802.11: Wireless Local Area Networks (LAN)
IEEE 802.15: Wireless Personal Area Networks (PAN)
IEEE 802.16: Broadband Wireless Metropolitan Area Networks (MAN)
IEEE 802.17: Resilient Packet Rings (RPR)
IEEE 802.20: Mobile Broadband Wireless Access
IEEE 802.21: Media Independent Handoff
IEEE 802.22: Wireless Regional Area Network
IEEE 802.23: Emergency Services Working Group

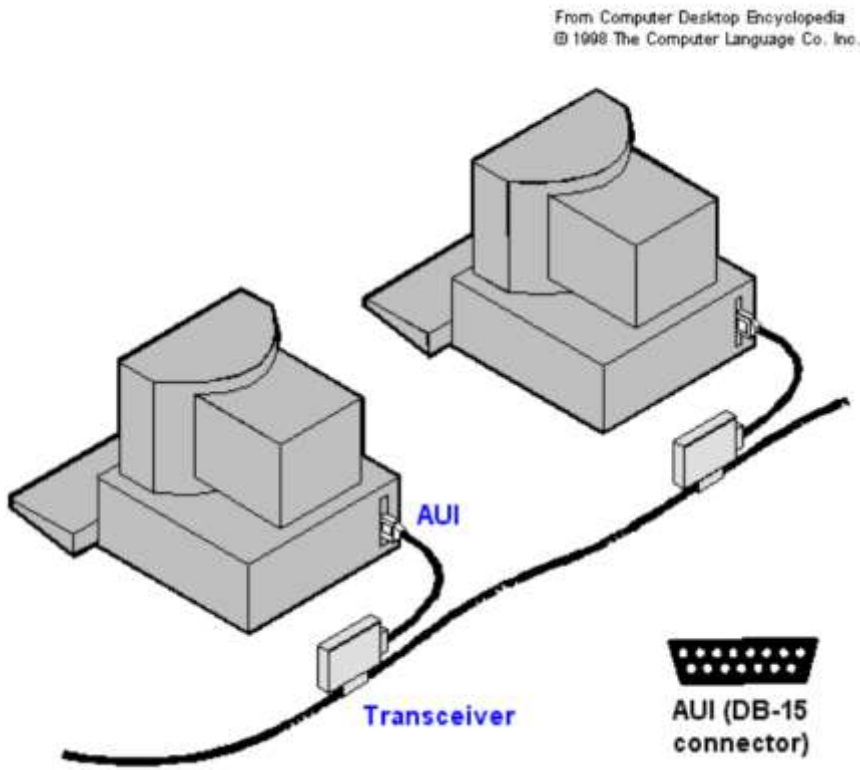
# استاندارد گروه IEEE 802 برای LAN

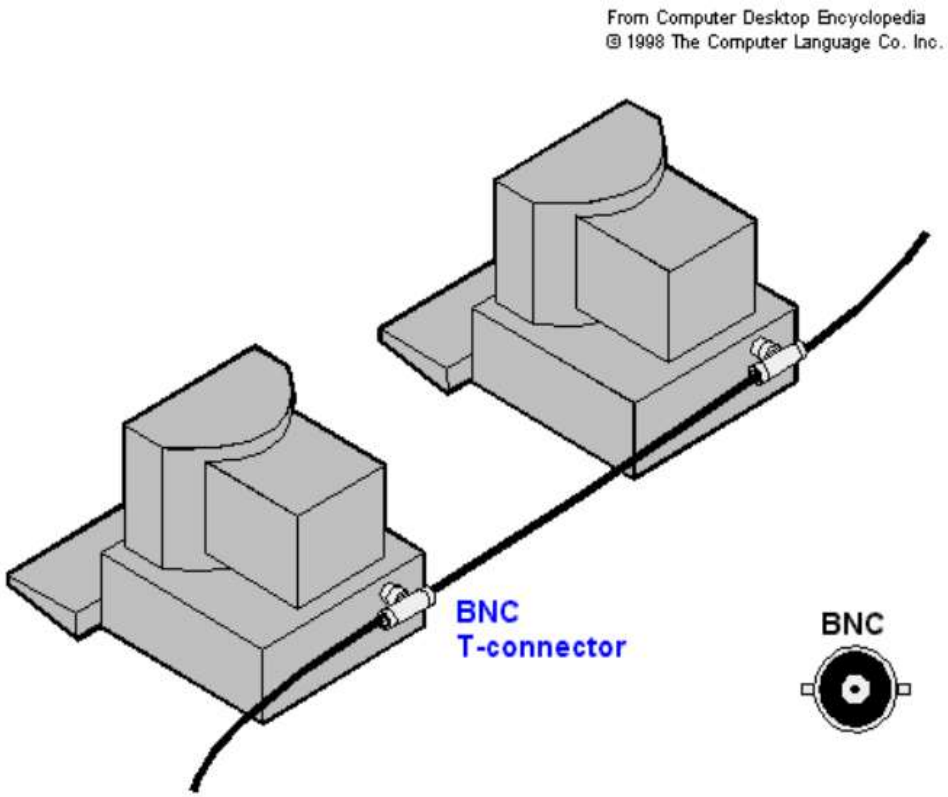



| Name | Cable | Max. segment | Nodes/seg. | Advantages |
|---|---|---|---|---|
| 10Base5 | Thick coax | 500 m | 100 | Good for backbones |
| 10Base2 | Thin coax | 200 m | 30 | Cheapest system |
| 10Base-T | Twisted pair | 100 m | 1024 | Easy maintenance |
| 10Base-F | Fiber optics | 2000 m | 1024 | Best between buildings |

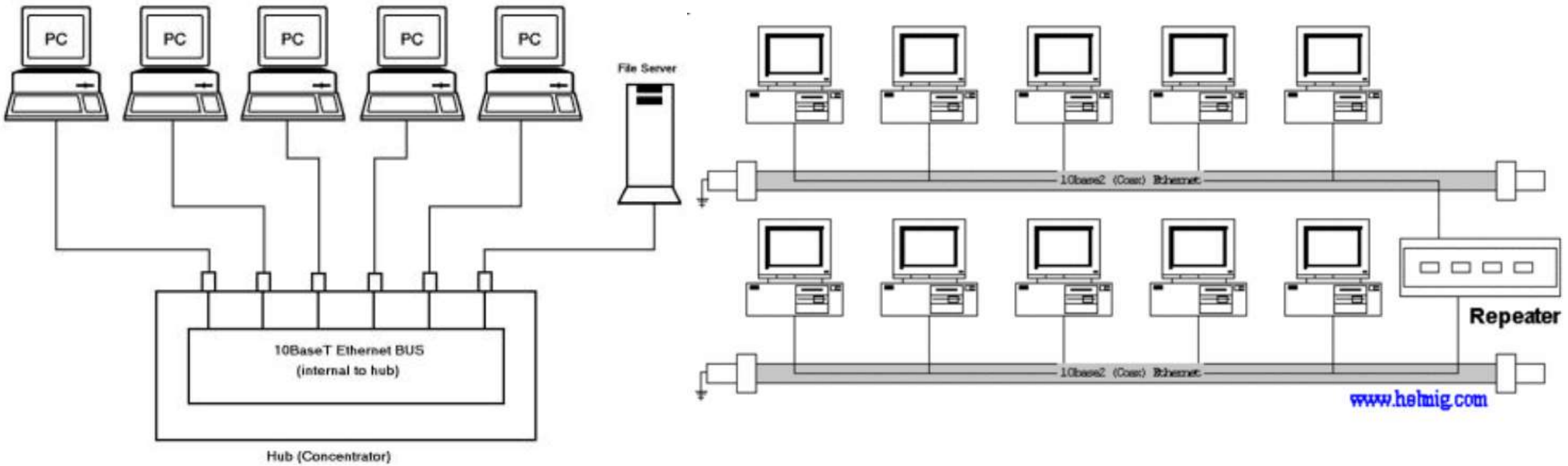
- **اترنت 802.3:**
  - تمام پروتکل‌های خانواده 1-Persistent از CSMA/CD
  - در اصل برای **نرخ‌های ۱ تا ۱۰ مگابیت برثانیه** طراحی شده بود.
  - واسط‌های مختلفی را می‌توان استفاده کرد. در ابتدا بر روی کابل کواکسیال ۵۰ اهم استفاده شده است.
  - با شروع روش ALOHA از جزایر هاوایی، این پروتکل هم شروع شد.
  - قابلیت carrier sensing توسط شرکت xerox افزوده شد.

# توپولوژی اترنت



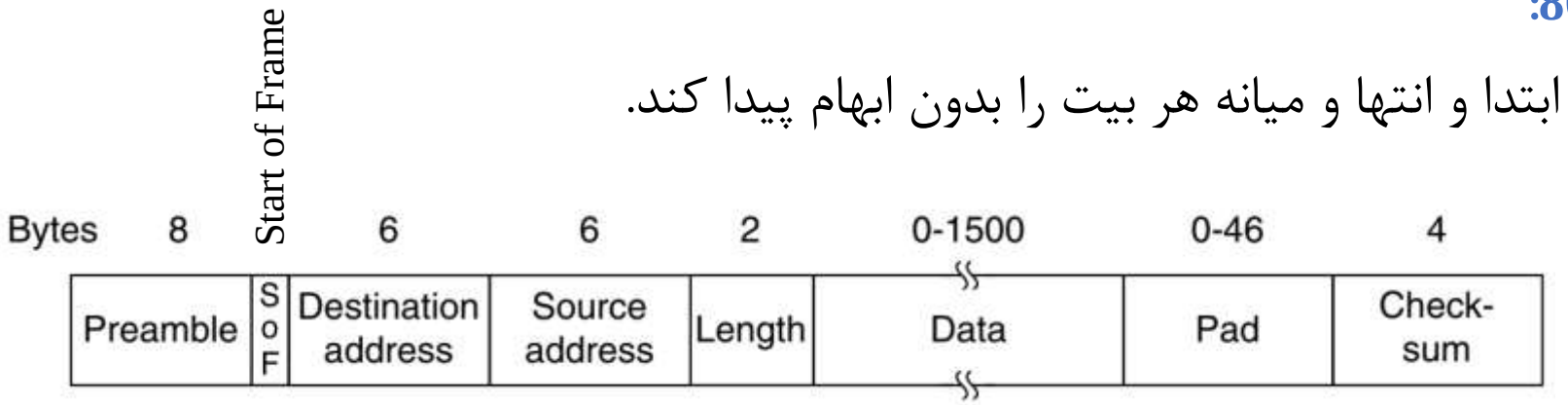



# توپولوژی اترنت



# استاندارد 802.3 LAN

- **نحوه Encoding استاندارد 802.3:**
- بدون نیاز به کلاک خارجی، بتواند ابتدا و انتها و میانه هر بیت را بدون ابهام پیدا کند.
- دو نوع Encoding استفاده شده:
  - Manchester Encoding
  - Differential Encoding




- **ساختار فریم:**
  - الگوی Preamble هفت بایتی (۷ تا 10101010)
  - فیلد شروع: 10101011
  - به منظور تشخیص تصادم، طول فریم باید بیشتر از دو برابر تأخیر انتشار باشد. ماکزیموم طول کابل LAN با ۵ سگمنت (۴ تکرارکننده) می‌تواند ۲۵۰۰ متر باشد. اترنت اولیه برای سرعت ۱۰ مگابیت بر ثانیه طراحی شده است. با این مشخصات حداقل طول فریم باید ۵۱.۲ میکروثانیه باشد. در نتیجه حداقل طول فریم باید ۶۴ بایت شود. بدین منظور، **فیلد Pad** اضافه شده‌است.

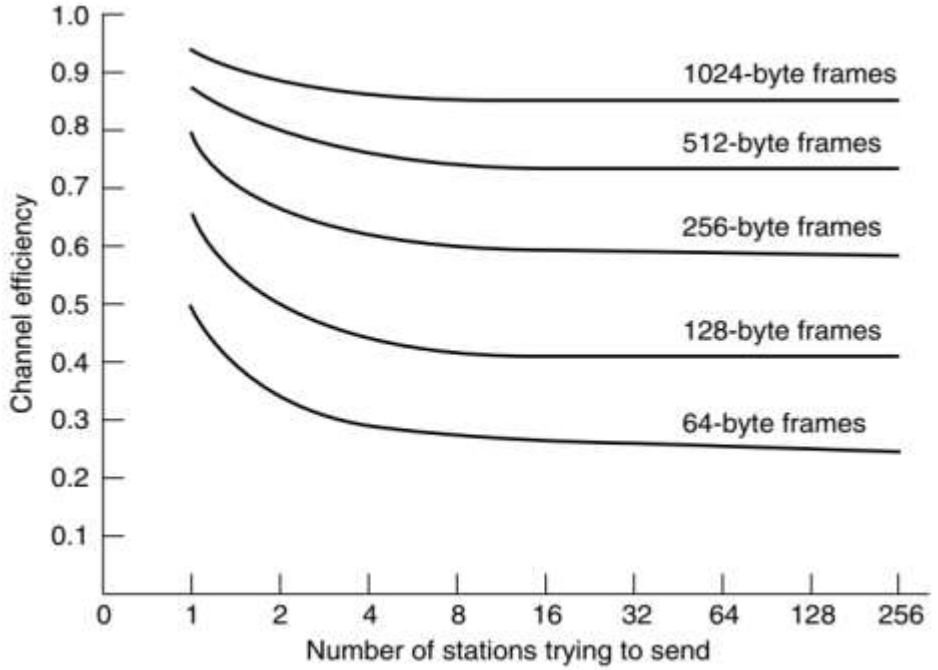
# استاندارد 802.3 LAN

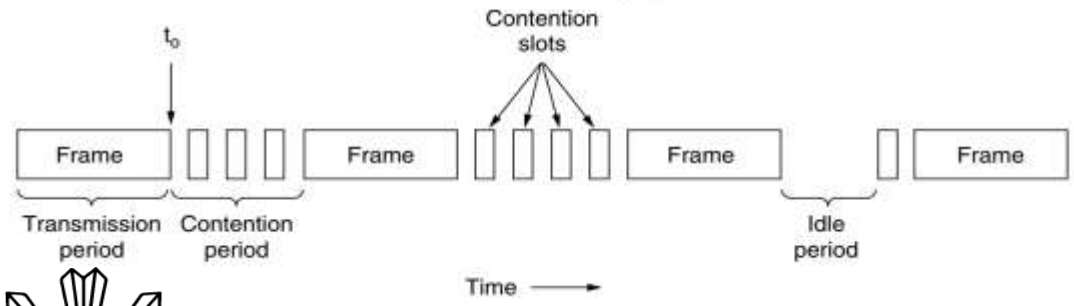
- **آدرس‌دهی:**
- طول آدرس ۶ بایت است که توسط IEEE تخصیص داده می‌شود.
- اولین بیت ارسالی آدرس گیرنده برابر 0 باشد بدین معناست که آدرس از نوع عادی است و 1 به معنای آدرس گروهی است. بدین ترتیب می‌توان پیام را به گروه خاصی از کاربران ارسال کرد (Multicasting)
- آدرس تمام یک برای حالت پخش (Broadcast) درنظر گرفته شده است.

# استاندارد 802.3 LAN

- **Binary Exponential Back off:**
  - بعد از تصادم به مدت صفر و یا چندین اسلات زمانی (۵۱.۲ میکروثانیه) منتظر باش. نحوه انتخاب چند اسلات به شرح زیر است:
  - اولین تصادم: 0 یا 1 اسلات به صورت تصادفی منتظر باش.
  - دومین تصادم: 0 یا 1 و یا 2 و یا 3 اسلات زمانی به صورت تصادفی منتظر باش.
  - تصادم N ام: به صورت تصادفی از بین 0 تا $2^N - 1$ اسلات زمانی یک عدد را انتخاب کن و به همان مقدار منتظر باش.
  - ماکزیموم N برابر 10 است. به عبارتی بین صفر و 1023 اسلات زمانی
  - پس از ۱۶ بار تلاش، دیگر ادامه نده و روند بازیابی فریم را برای لایه‌های بالاتر واگذار کن.
- این الگوریتم تأخیر کم برای بارهای کم را تضمین می‌کند و به صورت مناسبی تصادم‌ها را در بار زیاد مدیریت می‌کند.

# تحلیل عملکرد 802.3



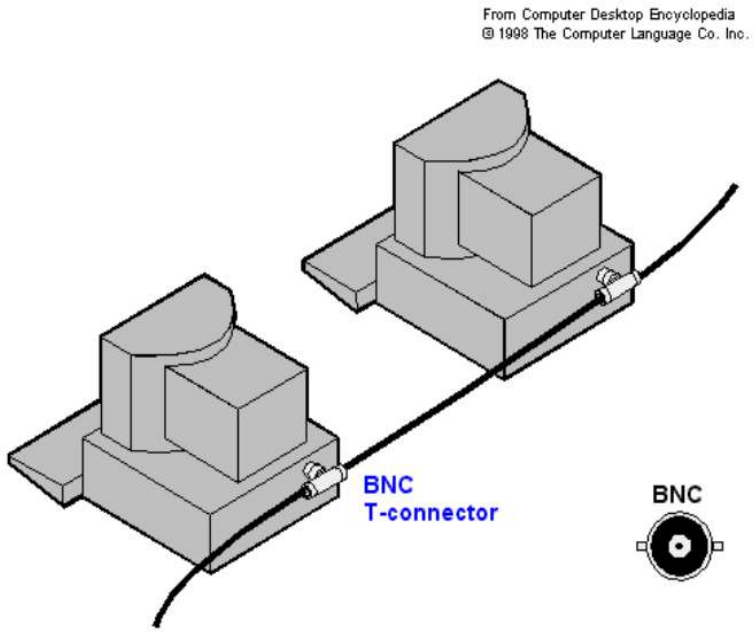

- **بحث Channel Utilization:**
- فرض کنید T ثانیه طول می‌کشد تا فریم ارسال شود.
- همچنین فرض کنید دوره رقابت مدت زمان  طول بکشد.
- هنگامی که کاربران زیادی، فریم برای ارسال داشته باشند:

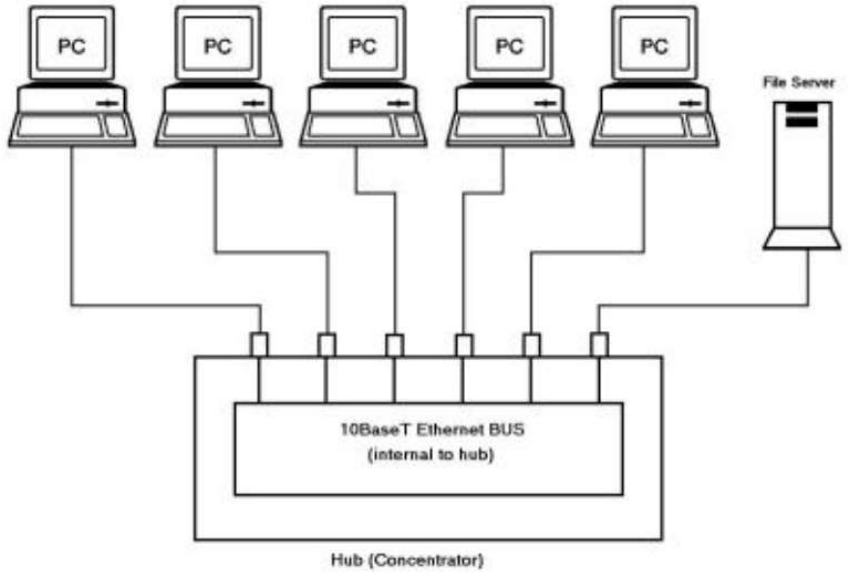
$$U = \frac{T}{T + T_{cp}} = \frac{T}{T + 2\tau / A} = \frac{1}{1 + 2BLe / cF}$$

- F = Frame Length,  L = Cable Length
- B = Network Rate,  c = Propagation Speed
- e = Contention Slots per Frame
- (Note $\tau = L / c$ and $T = F / B$ )

# Switched Ethernet

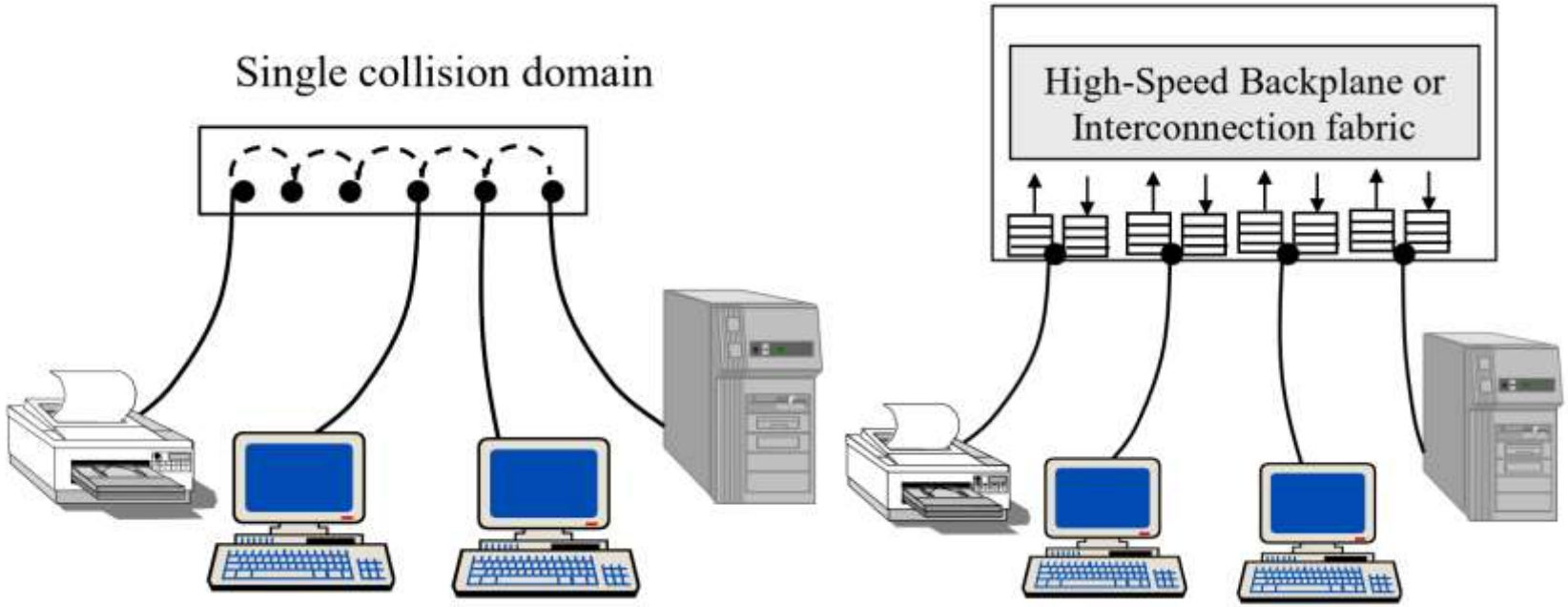
- مسئله عملی موجود در اترنت:
- اگر هر کدام از T-connector ها به هر دلیلی (مثلا باز شود) اتصال را برقرار نکند، چه مشکلی رخ می‌دهد؟ آیا بقیه کاربران می‌توانند از شبکه استفاده کنند؟



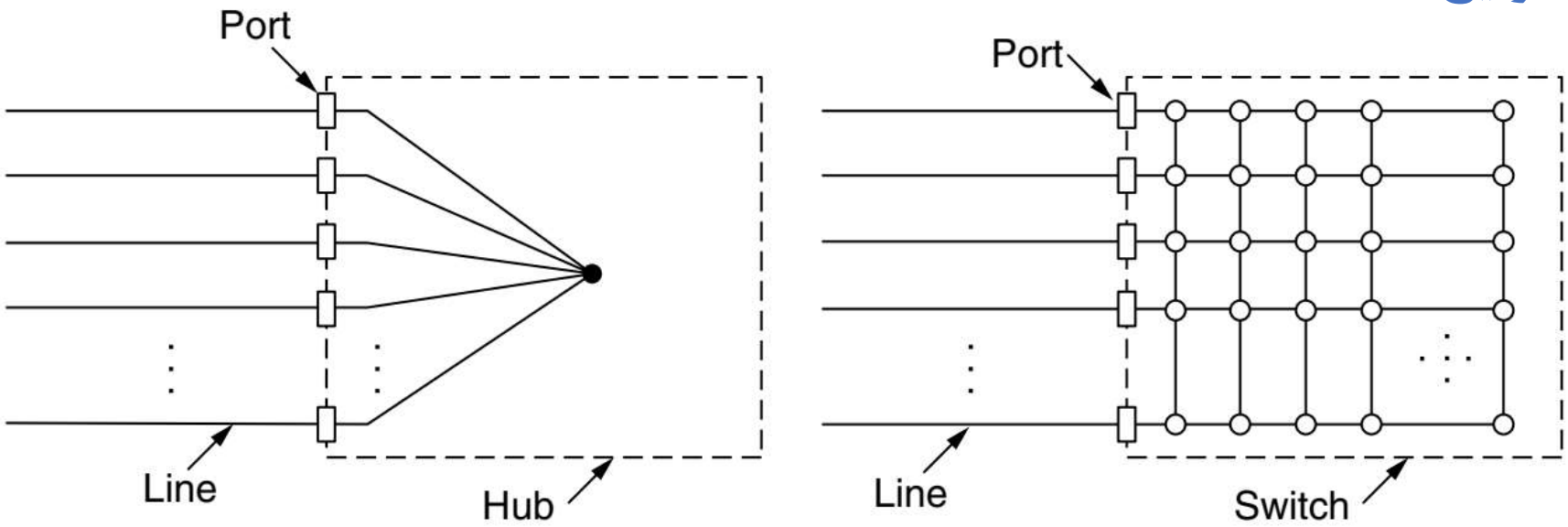
# (2) Switched Ethernet

- **ایده:** به جای استفاده از هاب، از سوئیچ استفاده کنیم و برای هر پورت بافر ورودی و خروجی در نظر بگیریم.
- هاب، توزیع‌شده نیست. یک موجود واحد است که نقش محیط مشترک را بازی می‌کند. بنابراین، حال که از حالت توزیع‌شده خارج شدیم، نمی‌توانیم هوشمندی به خرج دهیم؟!



# (3) Switched Ethernet

- در حالتی که از سوئیچ استفاده شود، ظرفیت به خاطر تصادم از بین نمی‌رود. چون تصادمی رخ نمی‌دهد.
- **دو چالش اصلی:**
  - **الگوی ترافیکی**
  - **سرعت سوئیچ**

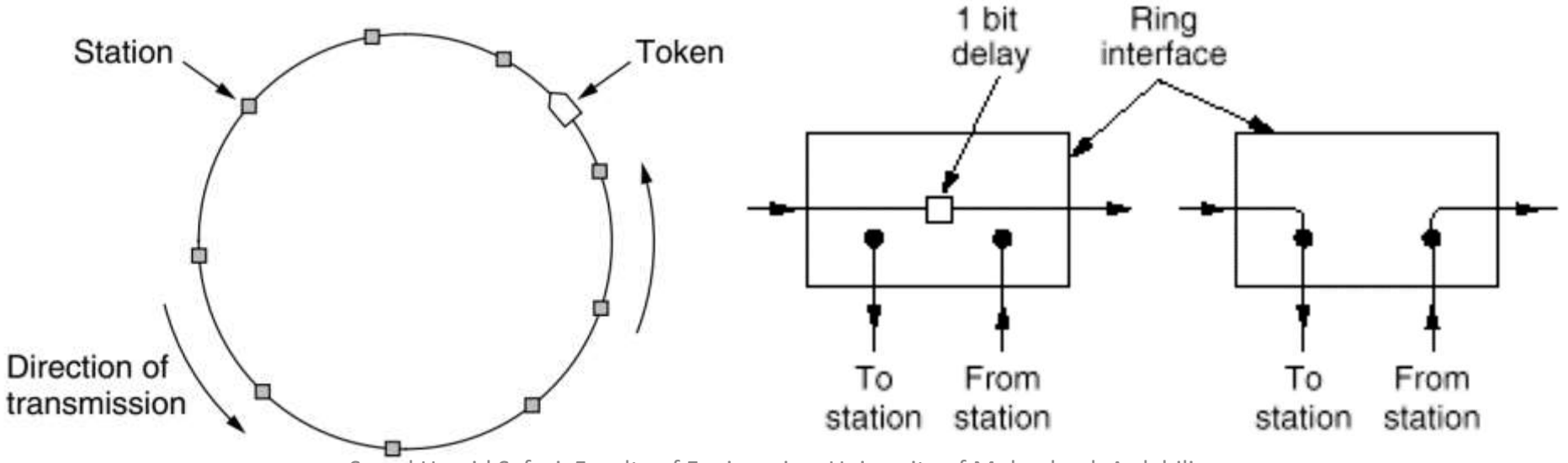


# Switched Ethernet Evolution

- **مراحل رشد اترنت:**
- **Classic Ethernet:** نرخ ۱۰ مگابیت بر ثانیه، استفاده از منچستر کدینگ
- **Fast Ethernet:** نرخ ۱۰۰ مگا بیت بر ثانیه، از منچستر کدینگ استفاده نمی‌شود. سال ۲۰۰۵.
- **Gigabit Ethernet:** دو نوع مبتنی بر سیم مسی و فیبر نوری، اجازه frame bursting
- **10-Gigabit Ethernet**

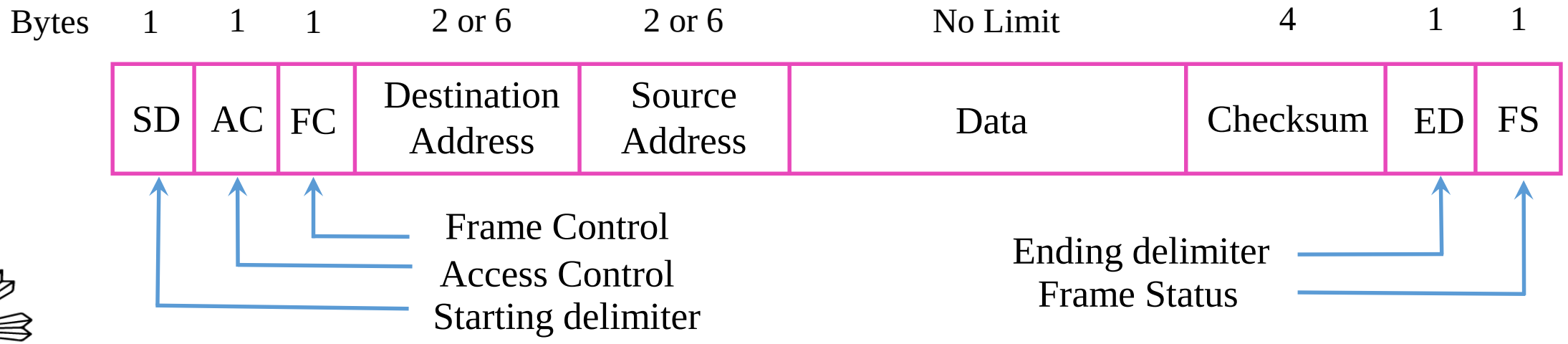
# استاندارد 802.5 LAN (Token Ring)

- می‌توان کاربران را در یک توپولوژی حلقوی به همدیگر متصل کرد. نحوه به اشتراک گذاشتن کاربران توسط ابزاری به نام Token انجام می‌شود. به عبارت دیگر نوبت ارسال را مشخص می‌کند.
- **گام‌های پروتکل:**
  - فرستنده پس از گرفتن Token، واسط (Interface) را در وضعیت ارسال قرار می‌دهد.
  - پس از ارسال آخرین بیت، Token مجدداً تولید می‌شود.



# استاندارد (Token Ring) 802.5 LAN

- **ساختار فریم در Token Ring:**
- فیلد یک بایتی AC:
  - توسط این بایت Token رزرو شده و اولویت بندی هم می‌شود. برای ارسال فریم با اولویت N، باید Token آزاد با اولویت کمتر از N مشاهده شود.
- فیلد یک بایتی FC: نوع فریم (داده و یا کنترلی) را مشخص می‌کند.

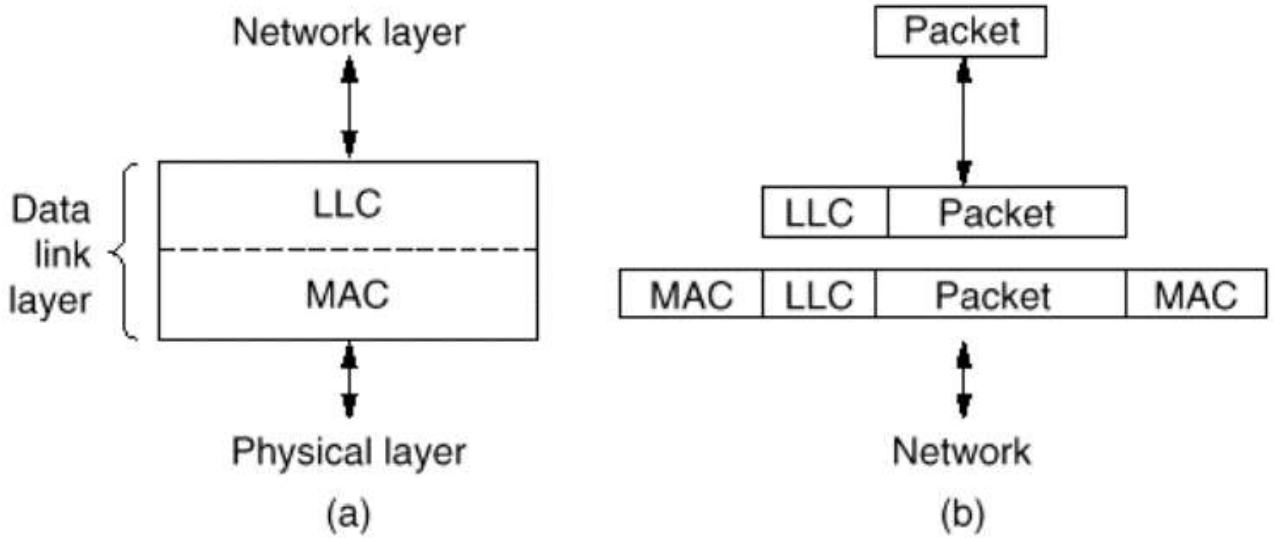


# استاندارد 802.5 LAN (Token Ring) (۲)

- **ساختار فریم در Token Ring:**
- فیلد یک بایتی FS:
  - شامل بیت‌های A و C به منظور ACK
  - فرستنده هنگام ارسال هر دو بیت را صفر می‌کند.
    - اگر A=0 و C=0 باشد، به معنای آن است که گیرنده وجود ندارد.
    - اگر A=1 و C=0 باشد، گیرنده حضور دارد، اما فریم پذیرش نشده است.
    - اگر A=1 و C=1 باشد، گیرنده حضور دارد و فریم نیز پذیرش شده است.
- **نتیجه مهم:** با دو بیت هم کنترل جریان انجام شد و هم تأییدیه!

# Logical Link Control: استاندارد 802.2

- لایه لینک در استاندارد 802.2 شامل دو بخش است:
  - LLC
  - MAC
- وظایف LLC:
  - کنترل جریان
  - مدیریت خطا (تشخیص و یا تصحیح خطا)
- سرویس‌هایی که فراهم می‌کند:
  - Unreliable datagram service
  - Acknowledged datagram service
  - Reliable connection-oriented service




(a) Poaition of LLC. (b) Protocol Formats

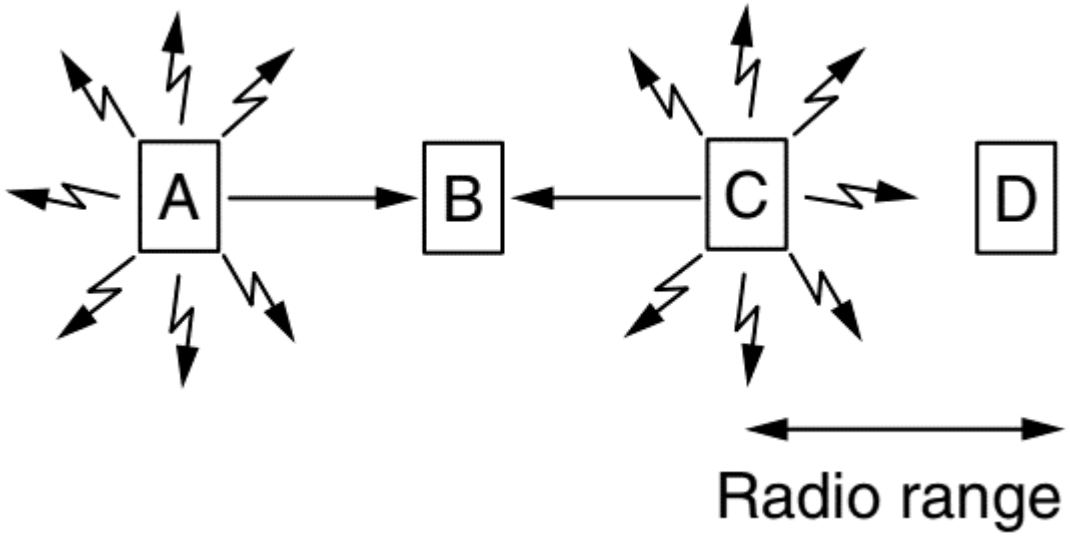
# استانداردهای ارتباط بی‌سیم

# پروتکل‌های LAN بی‌سیم

- پروتکل‌های بی‌سیم، ذاتاً دسترسی چندگانه هستند!
- در شبکه بی‌سیم، تشخیص تصادم **به هنگام وقوع آن** خیلی سخت و گاهاً ناممکن است. قدرت سیگنال دریافتی کاربرها می‌تواند خیلی کوچک باشد. به مانند یافتن سوزن در انبار کاه!!! بنابراین بهترین راه ممکن، تشخیص تصادم و خطا از طریق **دریافت تأییدیه پس از اتمام ارسال** است.
- بُرد سیگنال رادیویی ایستگاه‌ها:
  - ایستگاه‌ها به دلیل بُرد رادیویی محدود، نمی‌توانند به همه ایستگاه‌های دیگر داده ارسال کرده و یا دریافت کنند.
- رویکرد ساده برای LAN بی‌سیم، می‌تواند CSMA باشد. به کانال گوش کنیم و هر زمان خالی بود، ارسال کنیم. اما مشکلاتی پیش می‌آید!
  - آنچه که مهم است، تصادم در گیرنده است و نه فرستنده.

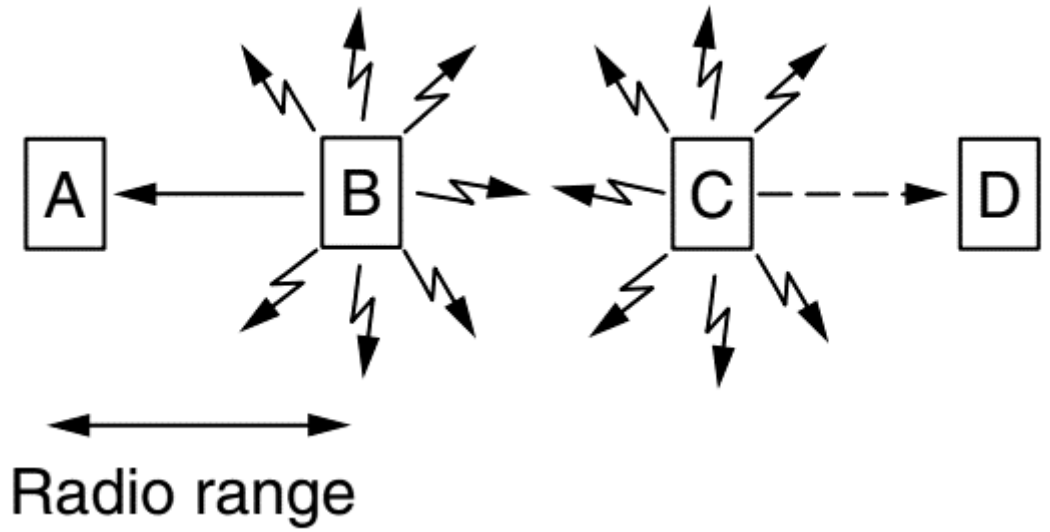
# پروتکل‌های LAN بی‌سیم (۲)

- **مسئله ایستگاه مخفی (Hidden Station Problem)**
- حالتی که یک ایستگاه، قادر نیست دیگر ایستگاه‌هایی که در حال رقابت برای تصاحب کانال هستند را تشخیص دهد، مسئله ترمینال‌های مخفی گویند.
  - کاربر C نمی‌تواند کاربر A را Sense کند. اگر هر دو بخواهند برای B ارسال کنند، تصادم رخ می‌دهد.



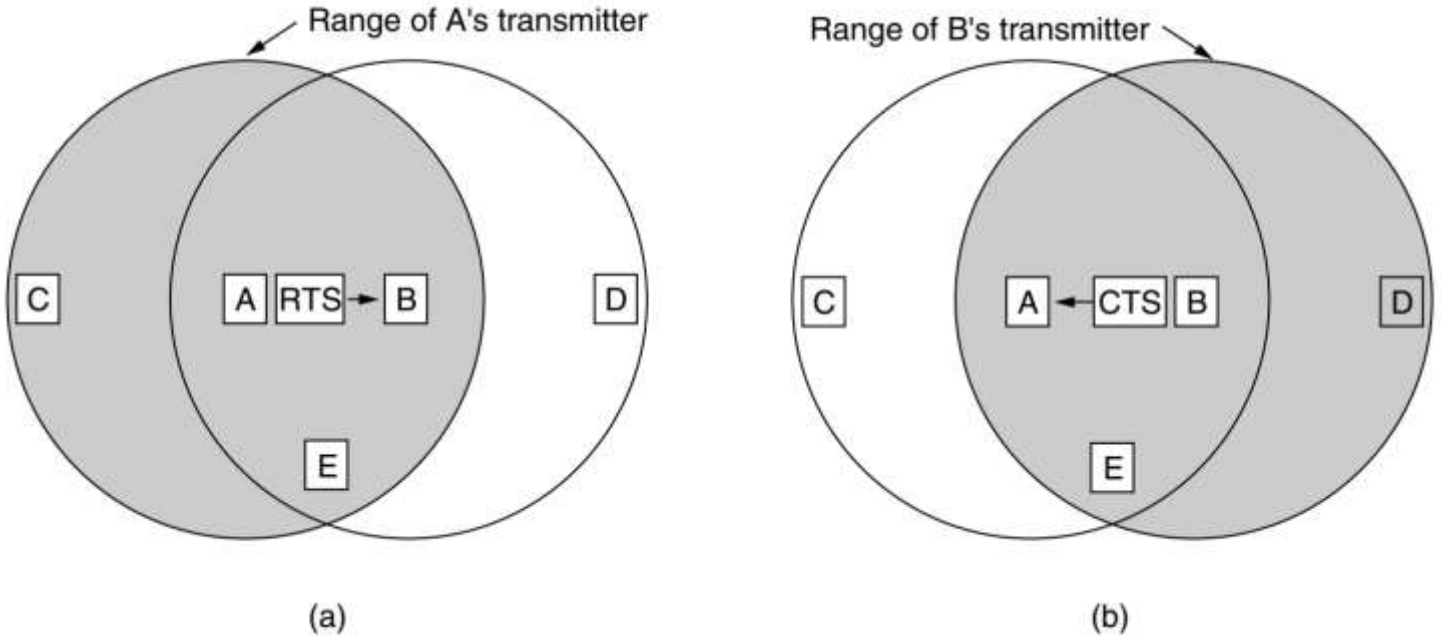
# پروتکل‌های LAN بی‌سیم (۳)

- **مسئله ایستگاه آشکار (Exposed Station Problem)**
  - کاربر B در حال ارسال به کاربر A است. در همین حین کاربر C نیز می‌خواهد به کاربر D داده ارسال کند. طبق قواعدی که یاد گرفته‌ایم، کاربر C قبل از شروع به ارسال، کانال را Sense می‌کند و متوجه می‌شود که کانال پُر است. بنابراین ارسال نمی‌کند! در حالی که اگر ارسال می‌کرد، تصادمی رخ نمی‌داد.



# پروتکل‌های LAN بی‌سیم (۴)

- **MACA: Multiple Access with Collision Avoidance**
  - فرستنده: Request to Send (RTS) ارسال می‌کند.
  - گیرنده: Clear to Send (CTS) ارسال می‌کند.
  - RTS و CTS حاوی طول پیامی هستند که باید ارسال شود.

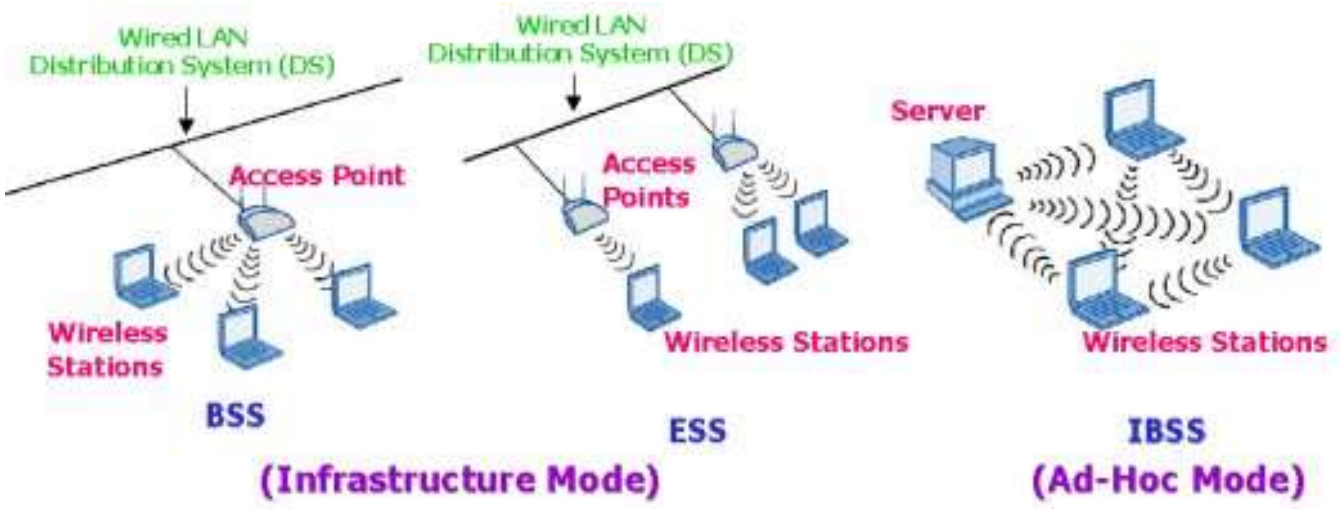


# پروتکل‌های LAN بی‌سیم (۵)

- **MACA: Multiple Access with Collision Avoidance**
  - هر ایستگاهی که RTS شنید، باید در طول فاز بعدی ارسال داده ساکت بماند.
  - هر ایستگاهی که CTS شنید، باید در طول پیام بعدی ساکت بماند.
- علی رغم همه این محدودیت‌هایی که برای جلوگیری از ایجاد تصادم گذاشته شد، باز هم امکان وقوع تصادم وجود دارد! چرا؟
  - برای مثال فرض کنید هر دو ایستگاه B و C به صورت همزمان به ایستگاه A، RTS ارسال کنند. بنابراین پس از این تصادم، مدت زمان رندمی باید صبر کنند و مجددا برای ارسال تلاش کنند.

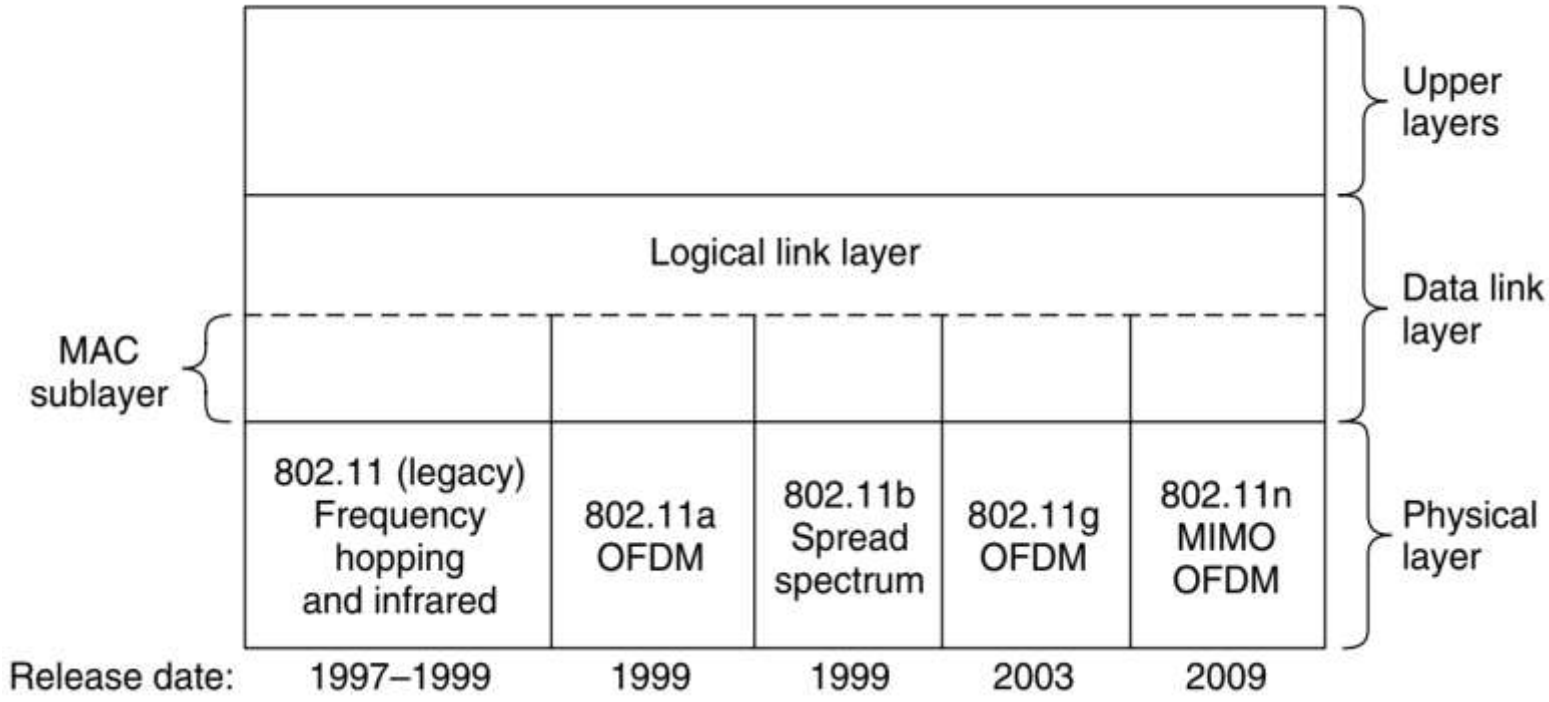
# پروتکل‌های LAN بی‌سیم (۵)

- **پیکربندی شبکه‌های بی‌سیم:**
  - **مبتنی بر زیرساخت (Infrastructure Mode):** ایستگاه‌ها از طریق یک دستگاه مرکزی به نام Access Point (AP) با یکدیگر ارتباط دارند.
  - **شبکه‌های اقتضائی (Ad-hoc Mode):** هر ایستگاه بدون زیرساخت مشخص و به صورت مستقیم با دیگر ایستگاه‌ها در ارتباط است.

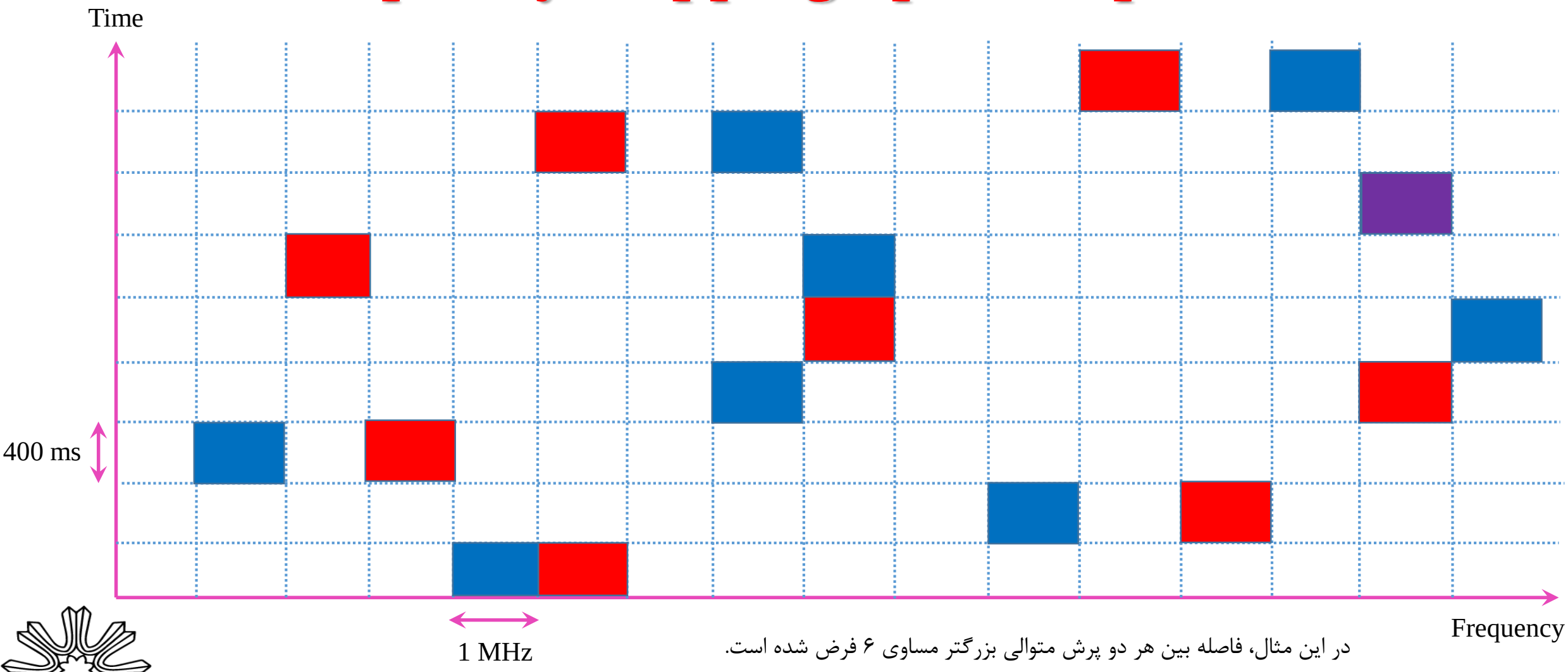


# پروتکل‌های LAN بی‌سیم (۶)

- استانداردهای مختلفی در سالیان گذشته گسترش یافته است:
- استانداردهای قدیمی
  - 802.11 Infrared
  - 802.11 DSSS
  - 802.11 FHSS
- استانداردهای جدیدتر
  - 802.11a OFDM
  - 802.11b Spread Spectrum
  - 802.11g OFDM
  - 802.11n MIMO-OFDM



# Frequency Hopping Spread Spectrum




در این مثال، فاصله بین هر دو پرش متوالی بزرگتر مساوی ۶ فرض شده است.

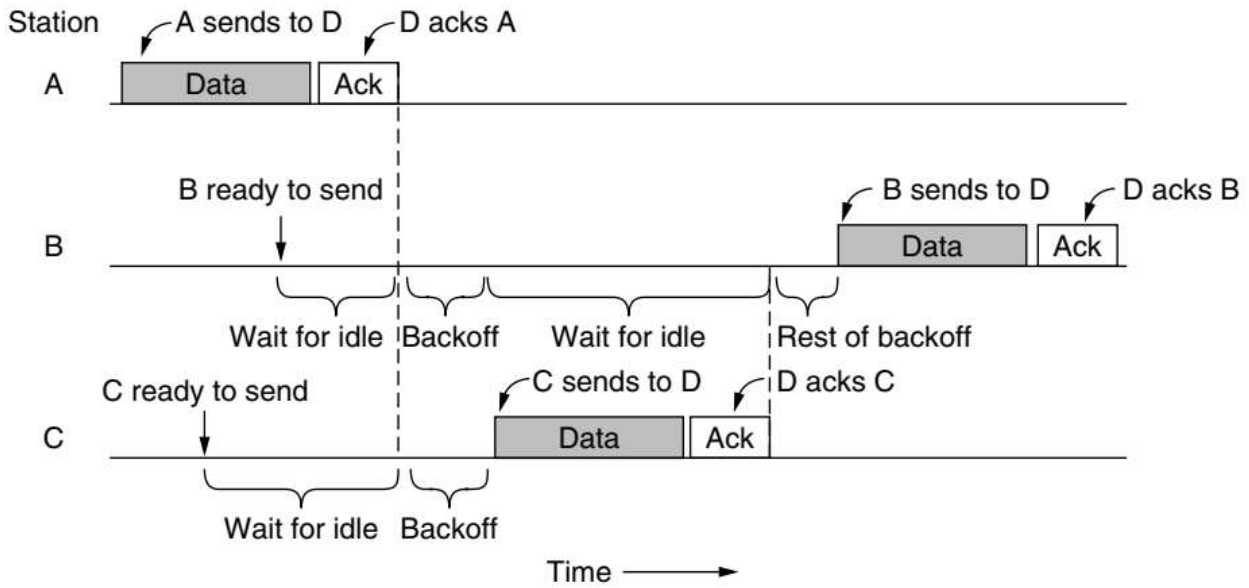
# Frequency Hopping Spread Spectrum

- **مزایای پرش فرکانسی:**
  - الگوی پرش فرکانسی را فقط فرستنده و گیرنده می‌داند. بنابراین کاربر دیگری نمی‌تواند به صحبت بین فرستنده و گیرنده گوش کند.
  - اگر کاربری قصد ایجاد اختلال داشت و به نحوی توانسته بود فرکانس کاری را بداند، در روش‌های قبلی می‌توانست کل ارتباط را که در یک باند فرکانسی بود، مختل کند. در FHSS به دلیل پرش فرکانسی، مدت زمانی کمی از یک فرکانس استفاده می‌شود و سپس فرکانس عوض می‌شود. بنابراین تشخیص فرکانس کاری سخت است و در صورت اختلال بخش کوچکی از پیام دچار اختلال می‌شود.

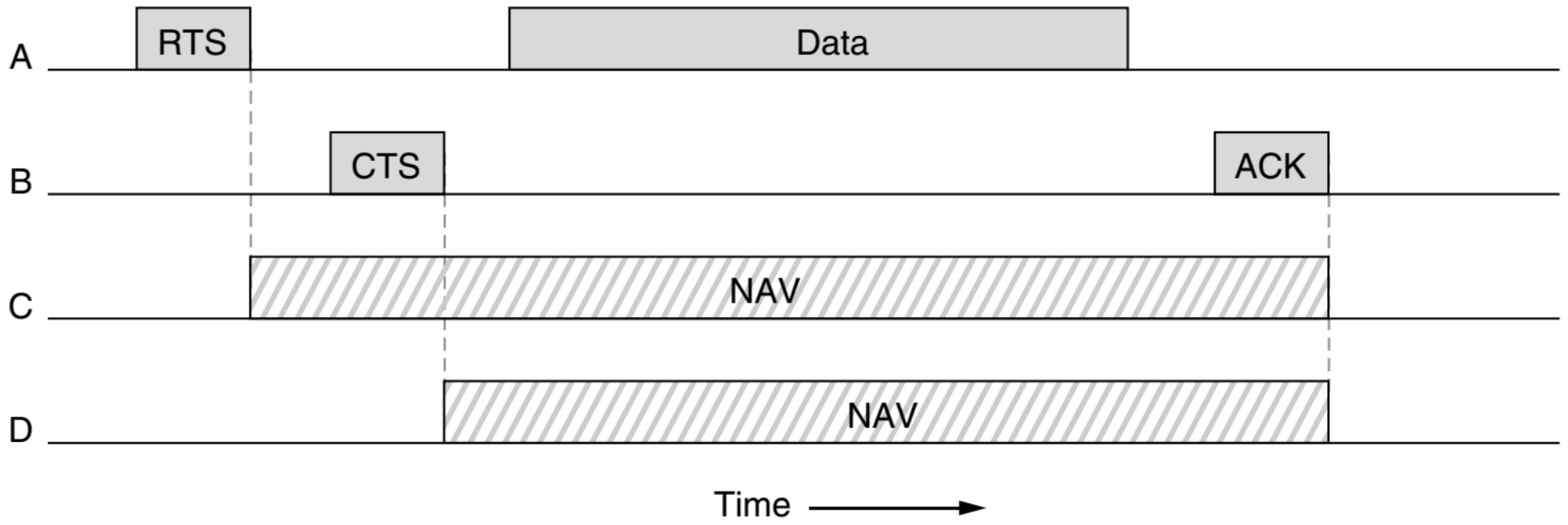
# کنترل دسترسی چندگانه در 802.11

# کنترل دسترسی چندگانه در 802.11

- دو تفاوت عمده ارسال فریم با روش CSMA/CA در حالت بی‌سیم و روش CSMA/CD در اترنت
  - در روش CSMA/CA قبل از ارسال مدت زمان رندم منتظر می‌مانیم. در روش CSMA/CD پس از وقوع تصادم مدت زمان رندمم منتظر می‌ماندیم.
  - در روش CSMA/CA، تشخیص تصادم توسط ACK صورت می‌گیرد.



# کنترل دسترسی چندگانه در 802.11 (۲)




- NAV (Network Allocation Vector): به زبان ساده مدتی که ایستگاه باید ساکت باشد!

# کنترل دسترسی چندگانه در 802.11 (۳)

- در مثال اسلاید قبل، A می‌خواهد به B ارسال کند. C در محدوده رادیویی A است (ممکن است در محدوده رادیویی B نیز باشد) و همچنین D در محدوده رادیویی B است.
- نود C صدای RTS نود A را می‌شنود و به اندازه‌ای که مشخص شده (با در نظر گرفتن ACK) ساکت می‌ماند. بردار NAV خود را به اندازه مشخص شده آپدیت می‌کند.
- نود D صدای CTS را شنیده و به اندازه مدتی که مشخص شده ساکت می‌ماند. بردار NAV خود را به اندازه مشخص شده آپدیت می‌کند.
- دقت کنید که سیگنال‌های NAV ارسال نمی‌شوند. بلکه برای یادآوری این هستند که ایستگاه باید به مدت مشخصی ساکت بماند.

# کنترل دسترسی چندگانه در 802.11 (۴)

- **کنترل دسترسی چندگانه در 802.11 از دو مود عملکرد پشتیبانی می‌کند:**
  - مود Distributed Coordination Function (DCF): در شبکه‌های اقتضایی به کار می‌رود.
  - مود Point Coordination Function (PCF): در شبکه‌های مبتنی بر زیرساخت (شامل AP) به کار می‌رود.

# کنترل دسترسی چندگانه در 802.11 (۵)

- محدودیت‌های عملیاتی
  - قابلیت اطمینان (Reliability)
  - صرفه‌جویی در توان مصرفی (Power Saving)
  - کیفیت سرویس (Quality of Service)

# کنترل دسترسی چندگانه در 802.11 (۶)

- **قابلیت اطمینان:**
  - بر خلاف شبکه‌های مبتنی بر سیم، شبکه‌های بی‌سیم به شدت دارای نویز و غیر قابل اطمینان هستند.
  - در صورتی که احتمال ارسال موفقیت‌آمیز فریم کم باشد، استفاده از گرفتن تأییدیه و ارسال مجدد کمک چندانی نمی‌کند.
  - استراتژی عمده در بالابردن احتمال موفقیت در ارسال فریم‌ها، **کاهش نرخ ارسال** است. نرخ‌های پایین از مدولاسیون‌های مقاوم‌تری استفاده می‌کنند و احتمال موفقیت افزایش می‌یابد.
  - استراتژی دیگر **کاهش طول فریم‌ها** است.
    - مثال: احتمال خطای BER=0.0001 را در نظر بگیرید. برای طول فریم اترنت 12144 بیت، احتمال موفقیت کمتر از ۳۰ درصد است! در صورتی که طول فریم‌ها 4048 بیت باشد، احتمال موفقیت حدود ۶۵ درصد خواهد بود.

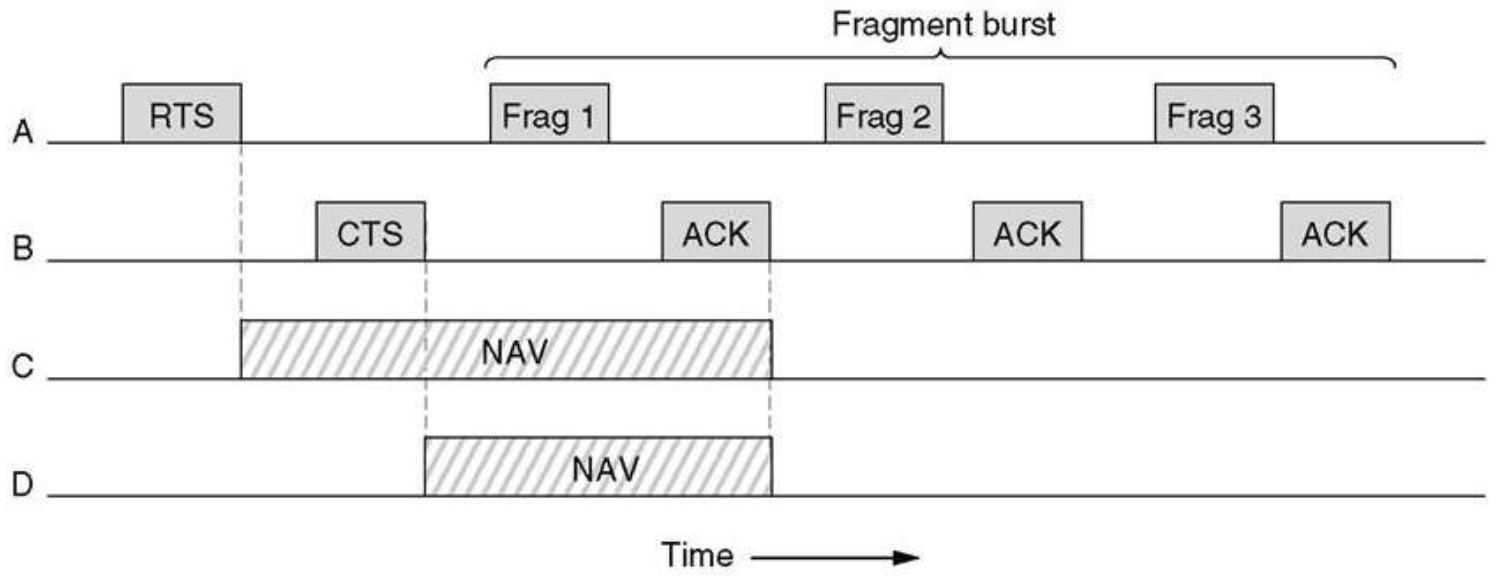
$$p = 10^{-4} \qquad \text{Bit Error Rate (BER)}$$

$$12144\,Bits \Rightarrow P_{success} = \left(1-10^{-4}\right)^{12144} \approx 0.297$$

$$4048\ \ Bits \Rightarrow P_{success} = \left(1-10^{-4}\right)^{4048} \approx 0.667$$

# کنترل دسترسی چندگانه در 802.11 (۷)

- کاهش طول فریم با استفاده از ارسال Fragment هایی که هر فریم را تشکیل می‌دهند، انجام می‌گیرد.



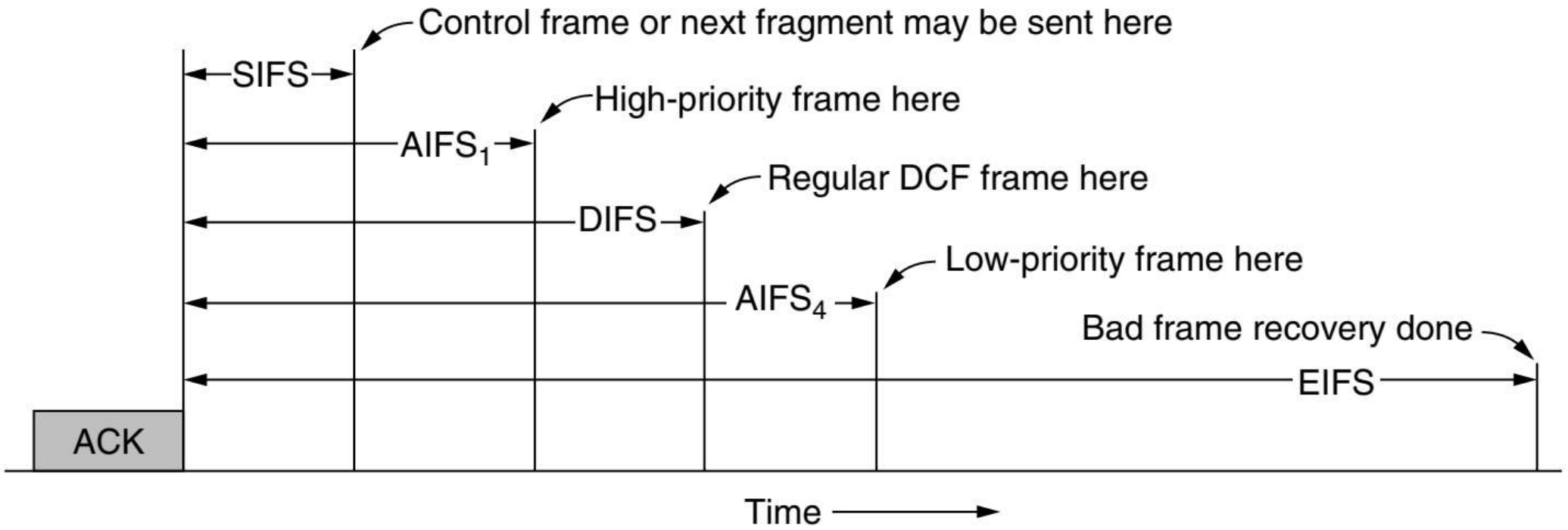

- **سوال:** آیا مدت زمان ارسال کل Fragment ها مشخص است؟ نودهای C و D چه مدت زمانی باید ساکت بمانند؟ به اندازه یک Fragment. راه حل در دو اسلاید بعدی بیان خواهد شد.

# کنترل دسترسی چندگانه در 802.11 (۸)

- **کیفیت سرویس**
  - فرض کنید دو نوع ترافیک در حال رقابت برای به دست گرفتن کانال هستند.
    ترافیک VOIP و ترافیک Peer to Peer.
  - به دلیل پهنای باند بالای ترافیک Peer to Peer، ترافیک VOIP به دلیل رقابت دچار تأخیر خواهد شد که برای این نوع سرویس خوشایند نیست. بنابراین مطلوب است که ترافیک VOIP نسبت به ترافیک Peer to Peer از اولویت بالاتری برخوردار باشد.
- برای حل این مشکل و ایجاد قابلیت اولویت دادن، IEEE 802.11 مکانیزم هوشمندانه‌ای در نظر گرفته است که در اسلاید بعدی توضیح داده می‌شود.

# کنترل دسترسی چندگانه در 802.11 (۹)

- فواصل زمانی فریم‌ها در 802.11



# کنترل دسترسی چندگانه در 802.11 (۱۰)

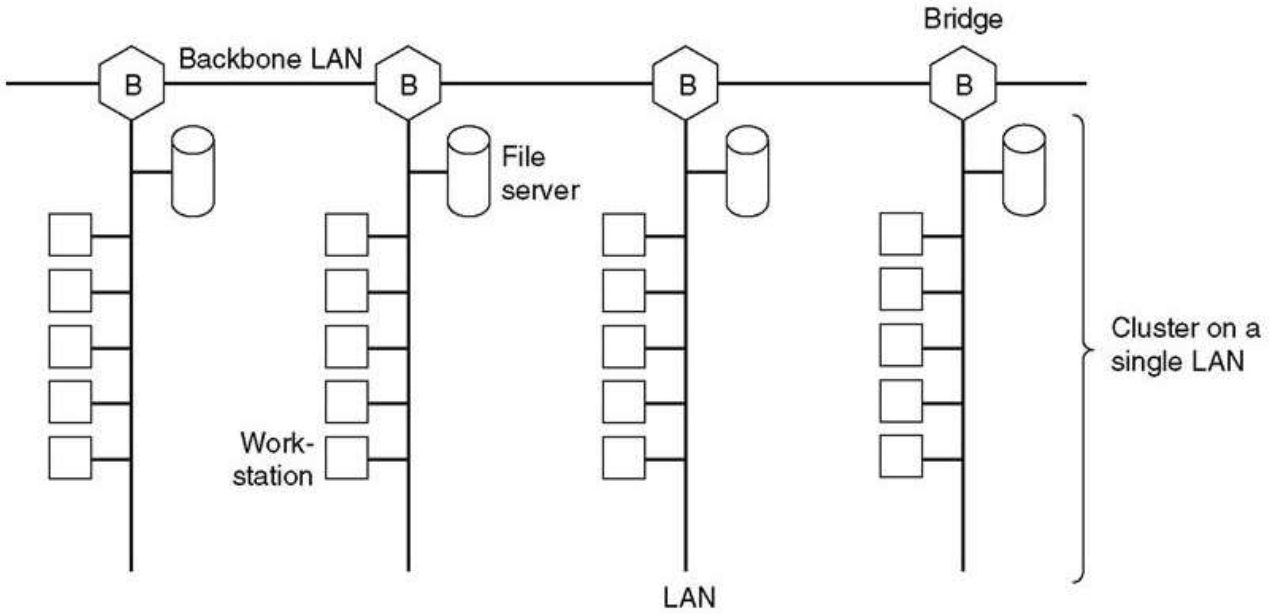
## فواصل زمانی فریم‌ها در 802.11

- DIFS (DCF InterFrame Spacing):
  - فاصله زمانی برای فریم‌های عادی DCF
- SIFS (Short InterFrame Spacing):
  - به منظور ارسال فریم‌های کنترلی و یا ارسال Fragment بعدی
- AIFS (Arbitration InterFrame Spacing):
  - به منظور دادن اولویت بالاتر و یا پایین تر استفاده می‌شود.
- EIFS (Extended InterFrame Spacing):
  - در مواقعی که فریم به درستی دریافت نشده باشد، برای گزارش استفاده می‌شود.

# سوئیچینگ در لایه پیوند داده

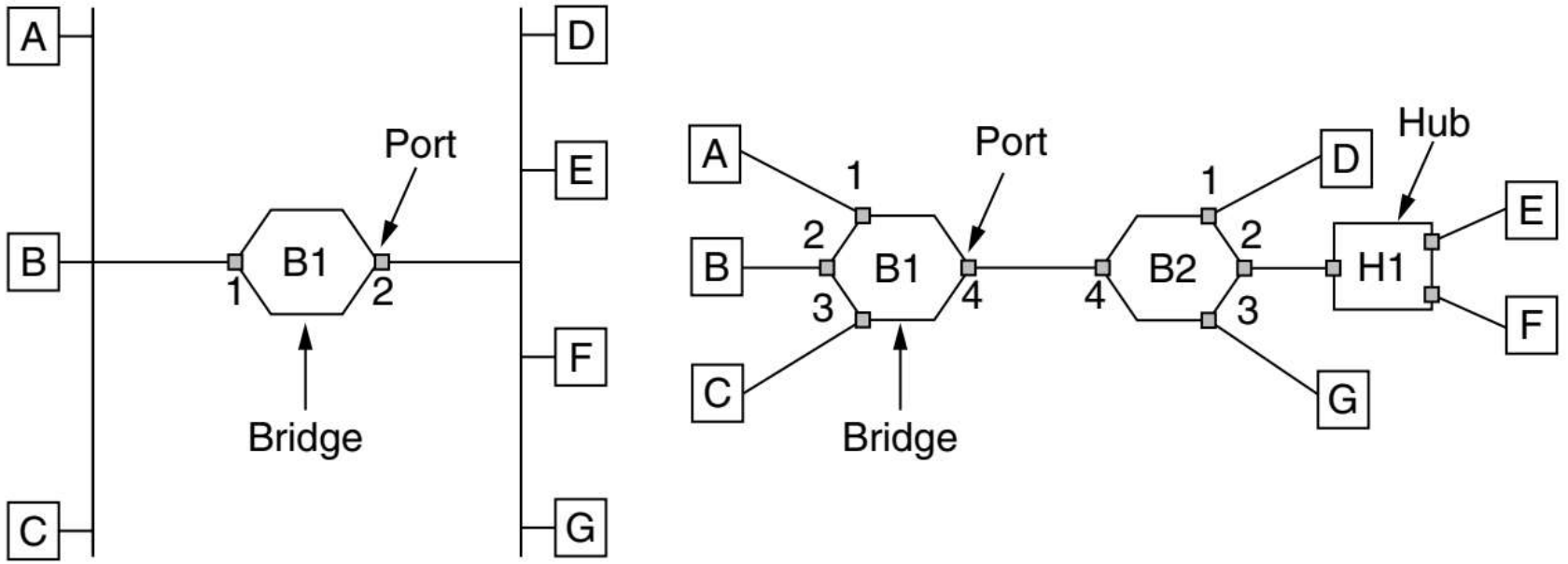
# سوئیچینگ در لایه پیوند داده

- بسیاری از سازمان‌ها چندین شبکه LAN دارند و مایل هستند آن‌ها را به هم متصل کنند. اما چگونه؟
- پل (Bridge) قطعه‌ای است که ما را در این امر کمک می‌کند. سوئیچ نام مدرن Bridge است.
- **سوال:** در صورتی که نودهای داخل یک سگمنت با همدیگر مکالمه داشته باشند، چه نیازی است مکالمه آن‌ها به خارج از سگمنت ارسال شده و باعث تصادم شود؟!



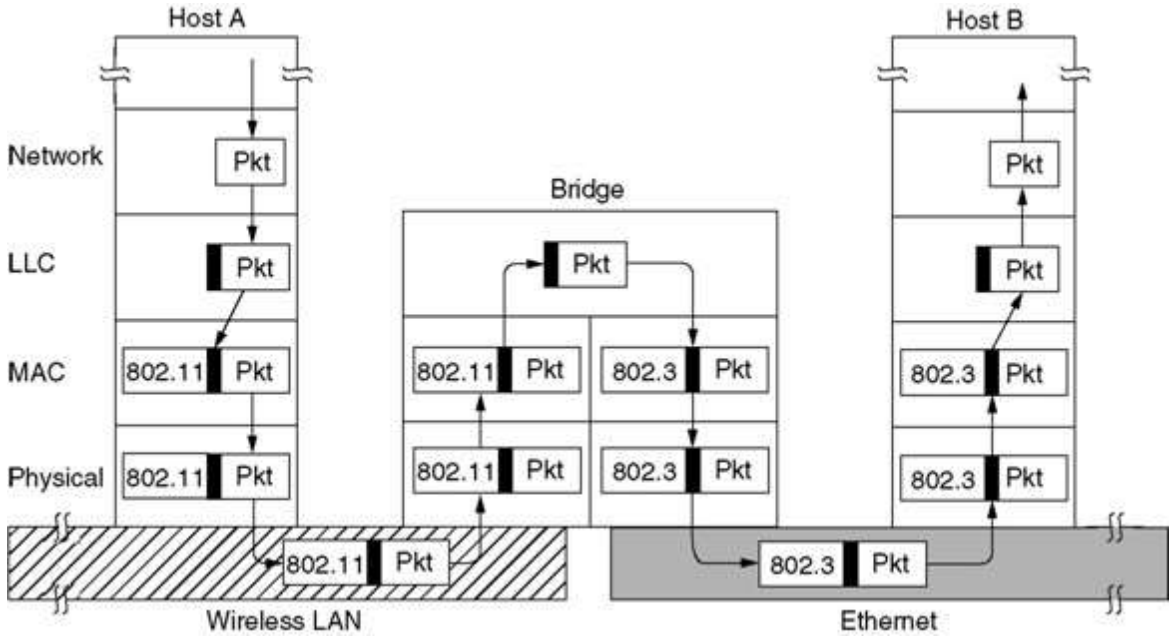
# سوئیچینگ در لایه پیوند داده (۲)

- Bridge ها در لایه پیوند داده عمل می‌کنند. در نتیجه از آدرس لایه پیوند داده برای فوروارد کردن فریم‌ها استفاده می‌کنند.
- Bridge ها می‌توانند LAN های multidrop و همچنین LAN های نقطه به نقطه را به همدیگر متصل کنند.




(a) Connecting two multidrop LANs (b) Connecting 7 point-to-point LANs

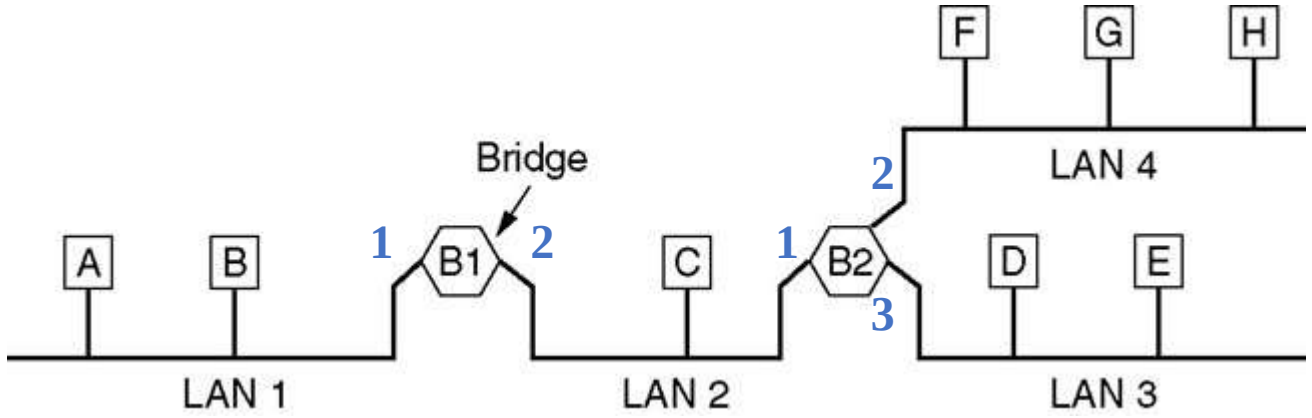
# سوئیچینگ در لایه پیوند داده (۳)




- **شمای پشته پروتکل در Bridge:**
- کاری که Bridge انجام می‌دهد این است که هر فریمی را که به یک پورت Bridge متصل است، می‌پذیرد. حال تصمیم می‌گیرد که این فریم را باید فوروارد کند یا نکند. اگر تصمیم به فوروارد است، برای کدام پورت فوروارد کند؟

# سوئیچینگ در لایه پیوند داده (۴)

- الگوریتم آموزش آدرس Bridge: فرض کنید نود A می‌خواهد به نود G داده ارسال کند.




**Bridge B1**

| Address | Port | Time Expiary |
|---|---|---|
| A | 1 | T |
| G | 2 | T |

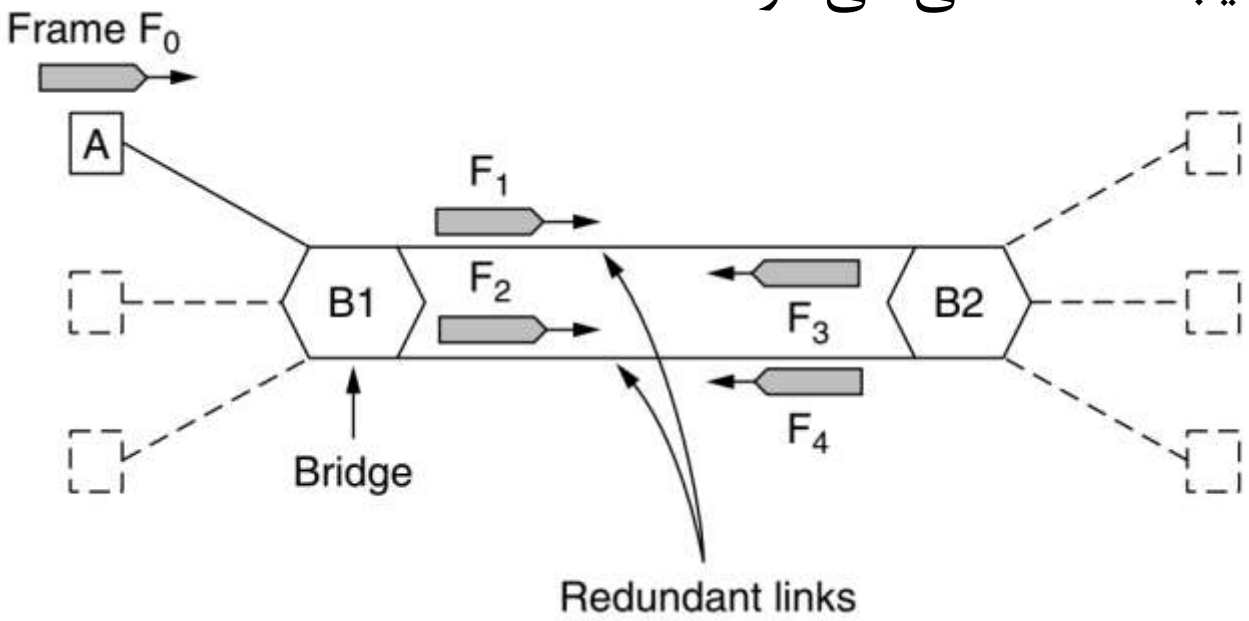
**Bridge B2**

| Address | Port | Time Expiary |
|---|---|---|
| A | 1 | T |
| G | 2 | T |

- **سه قانون کلی Bridge:**
  - اگر پورت آدرس مقصد با پورت آدرس مبدأ یکی بود، فریم را رها کن.
  - اگر پورت آدرس مقصد با پورت آدرس مبدأ متفاوت بود، فریم را از پورت مبدأ به پورت مقصد فوروارد کن.
  - اگر پورت مقصد ناشناخته است، فریم را در همه پورت‌ها به جز پورت مبدأ، فوروارد کن.

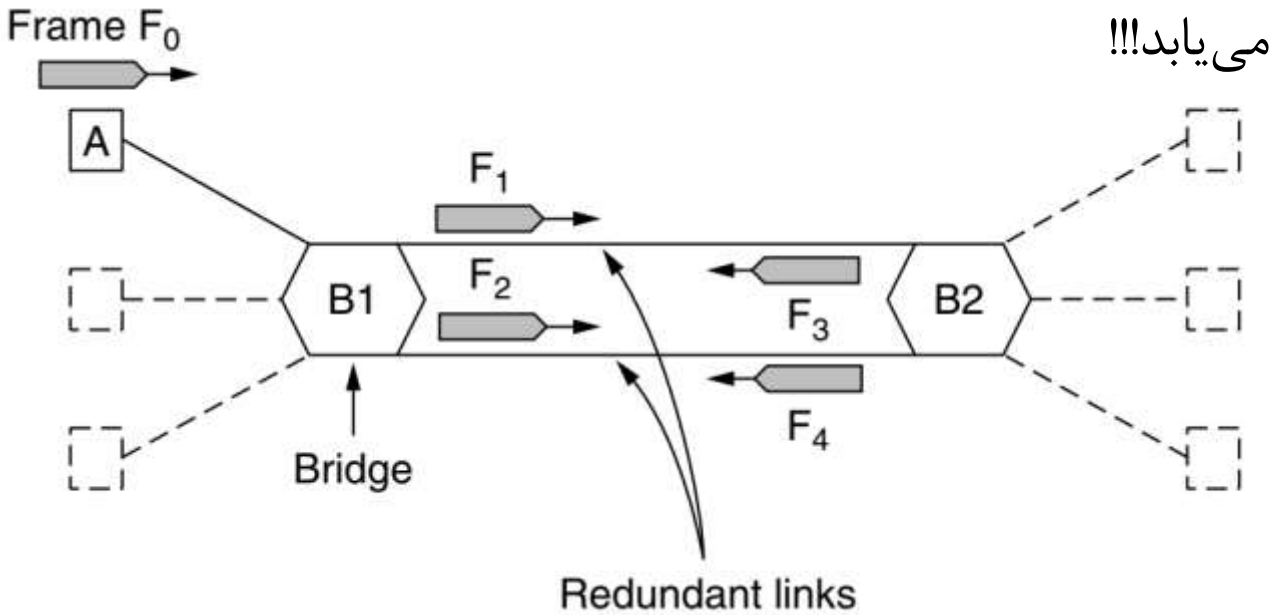
# سوئیچینگ در لایه پیوند داده (۵)

- به منظور افزایش قابلیت اطمینان، لینک‌های اضافی بین Bridge ها در نظر گرفته می‌شود. زمانی که یکی از لینک‌ها از کار بیفتد، لینک دیگر همچنان قابل استفاده است. در شکل زیر دو لینک موازی هم در نظر گرفته شده‌است.
- این افزونگی باعث ایجاد مشکلاتی می‌شود!



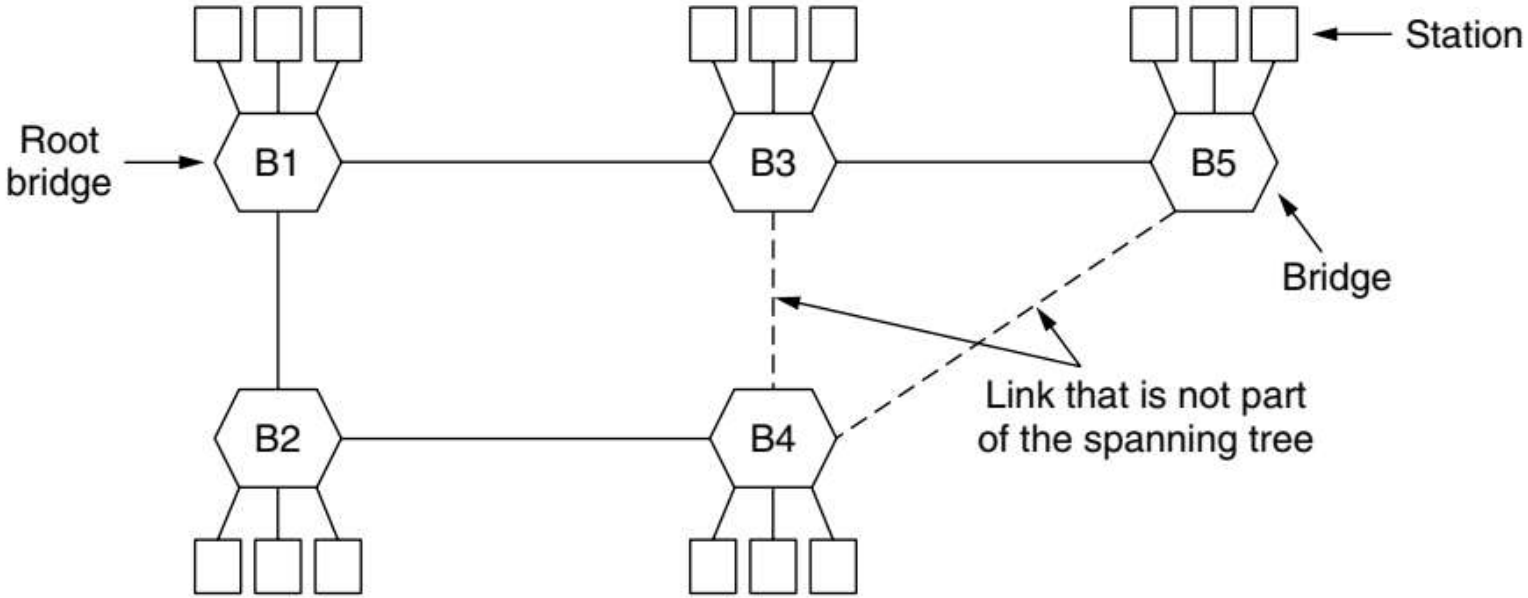
# سوئیچینگ در لایه پیوند داده (۶)

- فرض کنید نود A، فریم F0 را به مقصدی که قبلاً پورت آن مشخص نشده است، ارسال می‌کند.
- پل B1 دو کپی از فریم را در لینک‌های موازی هم قرار می‌دهد. (فریم‌های F1 و F2)
- پل B2 نیز نمی‌داند فریم‌های F1 و F2 کپی همدیگر هستند و به دلیل اینکه پورت فریم ارسالی برای پل B2 ناشناخته است، آن‌ها را در لینک‌ها کپی می‌کند. (F3 و F4)
- این روند تا ابد ادامه می‌یابد!!!



# Spanning Tree

- لینک‌هایی که باعث ایجاد حلقه شده‌اند، در ساختار درختی وجود ندارند. اما در صورتی که یکی از لینک‌ها از کار بیفتد، لینک‌هایی که در توپولوژی درخت استفاده نشده بودند و الان قابلیت استفاده دارند، می‌توانند به ساختار درخت اضافه شوند.



# Spanning Tree

- الگوریتم Spanning Tree توسط Radia Perlman ابداع شده‌است. برای فهم ساده موضوع، ایشان شعری سروده‌اند:

*I think that I shall never see*
*A graph more lovely than a tree.*
*A tree whose crucial property*
*Is loop-free connectivity.*
*A tree which must be sure to span.*
*So packets can reach every LAN.*
*First the Root must be selected*
*By ID it is elected.*
*Least cost paths from Root are traced*
*In the tree these paths are placed.*
*A mesh is made by folks like me*
*Then bridges find a spanning tree.*