Chapter 4

The Medium Access Control Sublayer
（介质访问子层）

The Medium Access Control Sublayer

- The categories of networks

  (based on Transmission Technology)

  - **Point-to-point connections（点到点连接）**
  - **Broadcast channels（广播信道）**
- Broadcast channels（广播信道网络），也称：
  - Multiaccess Channel（多路访问信道）
  - or: Random Access Channel(随机访问信道）
- Medium Access Control（介质访问控制， **MAC**)
  - The bottom part of the data link layer

4.1 The Channel Allocation Problem

- Static Channel Allocation in LANs and MANs
  （局域网和城域网中信道的静态分配）
- Dynamic Channel Allocation in LANs and MANs
  （局域网和城域网中信道的动态分配）

4.1.1 Static Channel Allocation in LANs and MANs

- Defect： if the spectrum is cut up into N regions,and fewer than N users are currently interested in communicating, a large piece of valuable spectrum will be wasted

  缺陷：无通信量时信道白白浪费
- The performance of static FDM is poor
- The mean time delay： $T_{FDM} = NT$
  - N---number of Sub-Channel after FDM
  - T---original mean delay of frame before FDM
- The same arguments that apply to FDM also apply to TDM

4.1.2 Dynamic Channel Allocation in LANs and MANs

Five key assumptions（5个关键假设）：

1. Independent Traffic. Station model（站）

- N independent stations、the frame be generated、waiting for transmittal、until the frame has been successfully transmitted

2. Single Channel （单通道）

- A single channel is available for all communication

3. Observable Collision （冲突）

- A collided frame must be transmitted again later

4. Continuous or Slotted Time

a. Continuous time（连续时间）

- Frame transmission can begin at any instant.

b. Slotted time（时隙）

- Frame transmissions always begin at the start of a slot.A slot may contain 0,1,or more frames

5. Carrier Sense or No Carrier Sense

a. Carrier sense（载波侦听）

- Stations can tell if the channel is in use before trying to use it

b. No carrier sense（非载波侦听）

- Only later can they determine whether or not the transmission was successful

4.2 MULTIPLE ACCESS PROTOCOLS

- ALOHA(Additive Link On-Line Hawaii system)
- Carrier Sense Multiple Access Protocols
- Collision-Free Protocols
- Limited-Contention Protocols
- Wavelength Division Multiple Access Protocols
- Wireless LAN Protocols

4.2.1 ALOHA

- ALOHA(Additive Link On-Line Hawaii system)--- How are you？
  - Pure ALOHA
  - Slotted ALOHA
- Pure ALOHA-[see fig 4-1]
  - The **basic idea：** let users transmit whenever they have data to be sent. Assumed: Fixed frame length。

    基本思想：只要有待发数据，就让他们发
  - After collision,waiting for random time,then retransmit
  - Vulnerable period for the shaded frame-[see fig 4-2]
  - The throughput of system: $\mathbf{S=G*e^{-2G}}$
    - G---Load, total generated mean frame numbers(old and new) per <u>frame time</u>，每帧时内传送的帧数
    - S---successfully transmitted frames per frame time, $S\leq1$
  - The maximum throughput occurs at G=0.5,with S=1/(2e),which is about **0.184.**
  - In other words ,the best we can hope for is a channel utilization of 18 percent.

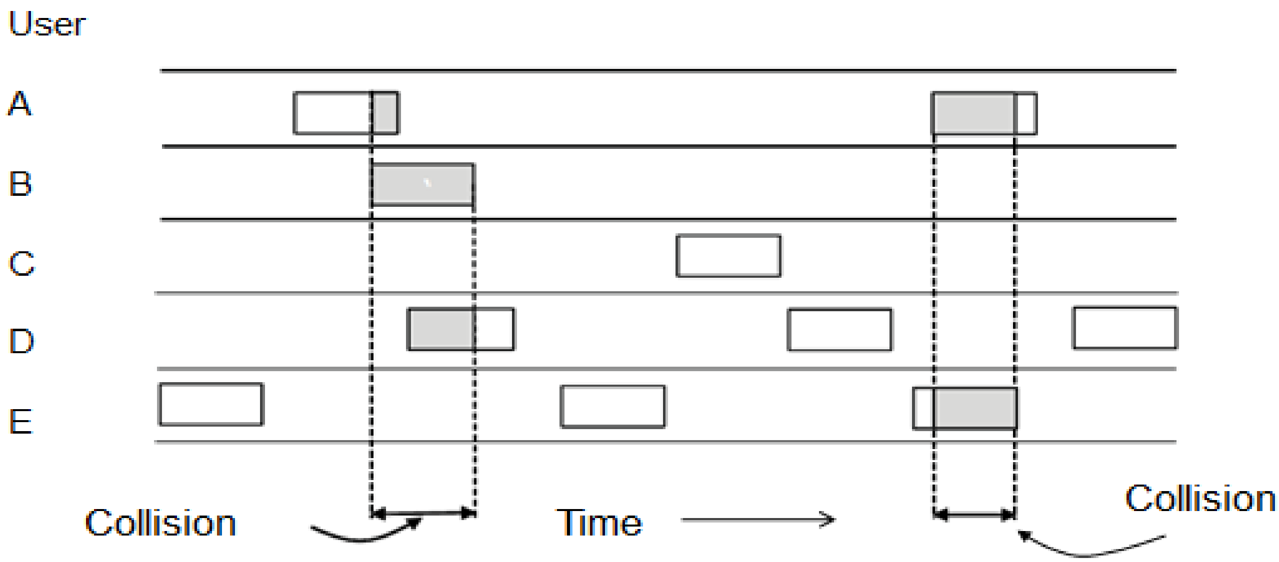


Fig. 4-1. In pure ALOHA, frames are transmitted at completely arbitrary times

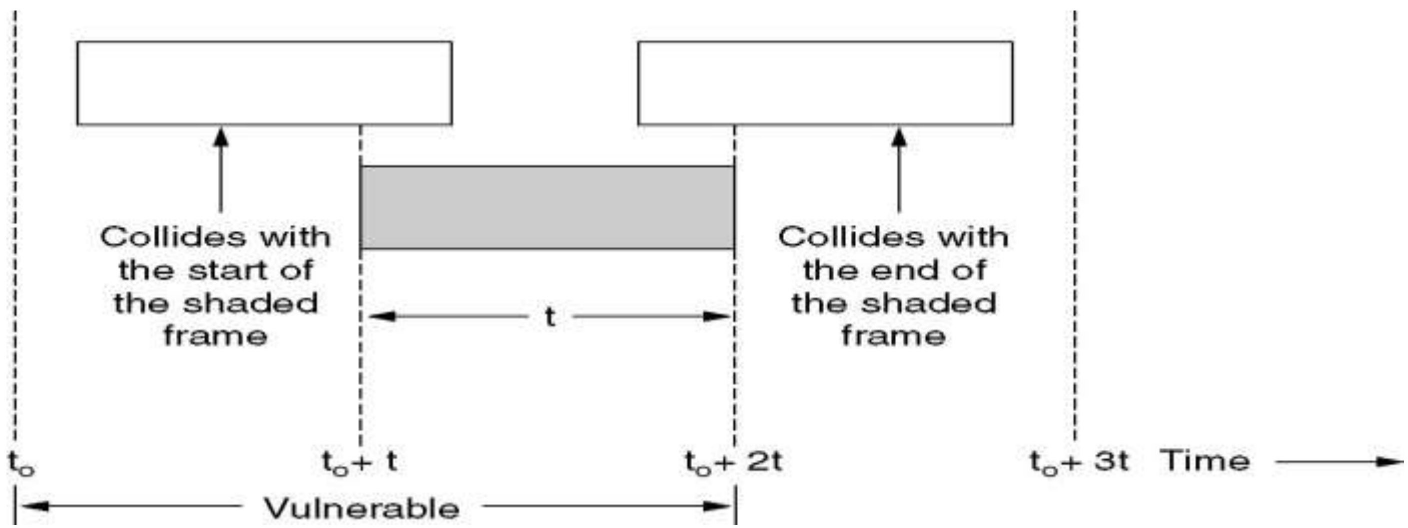


Fig. 4-2. Vulnerable period for the shaded frame

4.2.1 ALOHA

- Slotted ALOHA
  - **The basic idea：** divide time up into discrete intervals ,each interval corresponding to one frame

    基本思想：把时间分为离散的时间片(slot)，每段对应一帧
  - The approach requires the users to agree of slot boundaries.
  - Danger of collision reduce a half
  - The throughput : **$S=Ge^{-G}$**
  - Slotted ALOHA at G=1,with a throughput s=1/e or about **0.368**,twice that of pure ALOHA.
  - The best we can hope for using slotted ALOHA is 37 percent of the slots.
  - The relation between the offered traffic and the throughput is shown in [Figure 4-3]

4.2.1 ALOHA

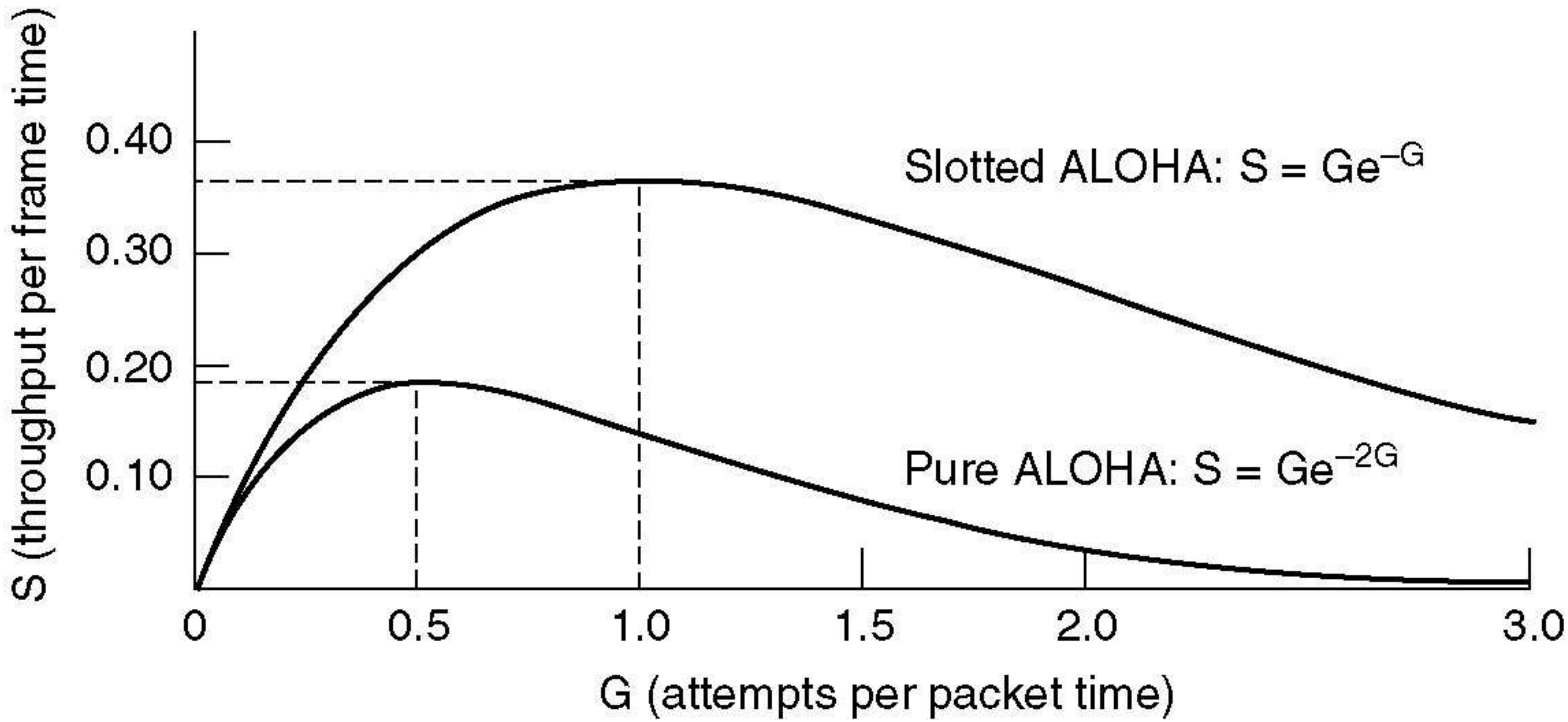


Fig.4-3.Throughput versus offered traffic for ALOHA systems

4.2.2 Carrier Sense Multiple Access Protocols（载波侦听多路访问协议　）

- **Basic Idea：** detect what other stations are doing， adapt their behavior accordingly， achieve a much better utilization

基本思想：检测其它站点，调整自己的动作，大大提高利用率

- Carrier Sense Protocols: protocols in which stations listen for a carrier(i.e., a transmission) and act accordingly
- **Bandwidth-delay product：** the number of frames that fit on the channel.
  - **The larger the bandwidth-delay product, the more important this effect becomes, and the worse the performance of the protocol.**
- Persistent and Nonpersistent CSMA
  - **1-persistent CSMA**
    - listen to the channel, if the channel is busy, the station waits until it becomes idle, then transmits the frame. If idle, the station transmit it immediately.
    - If a collision occurs ,the station waits a random amount of time and starts all over again.
  - **Nonpersistent CSMA**
    - listening, if the channel is busy, waits a random amount of time and starts listening. If idle, the station transmit it immediately.
    - Better Channel utilization than 1-persistent CSMA, but longer delays.

– **p-persistent CSMA**
  - Applies to slotted channels
  - listening, if it is idle,it transmits with a probability p , and defers with a probability 1-p .If busy,Continue listening.

- Comparison of various protocol-[see fig 4-4]

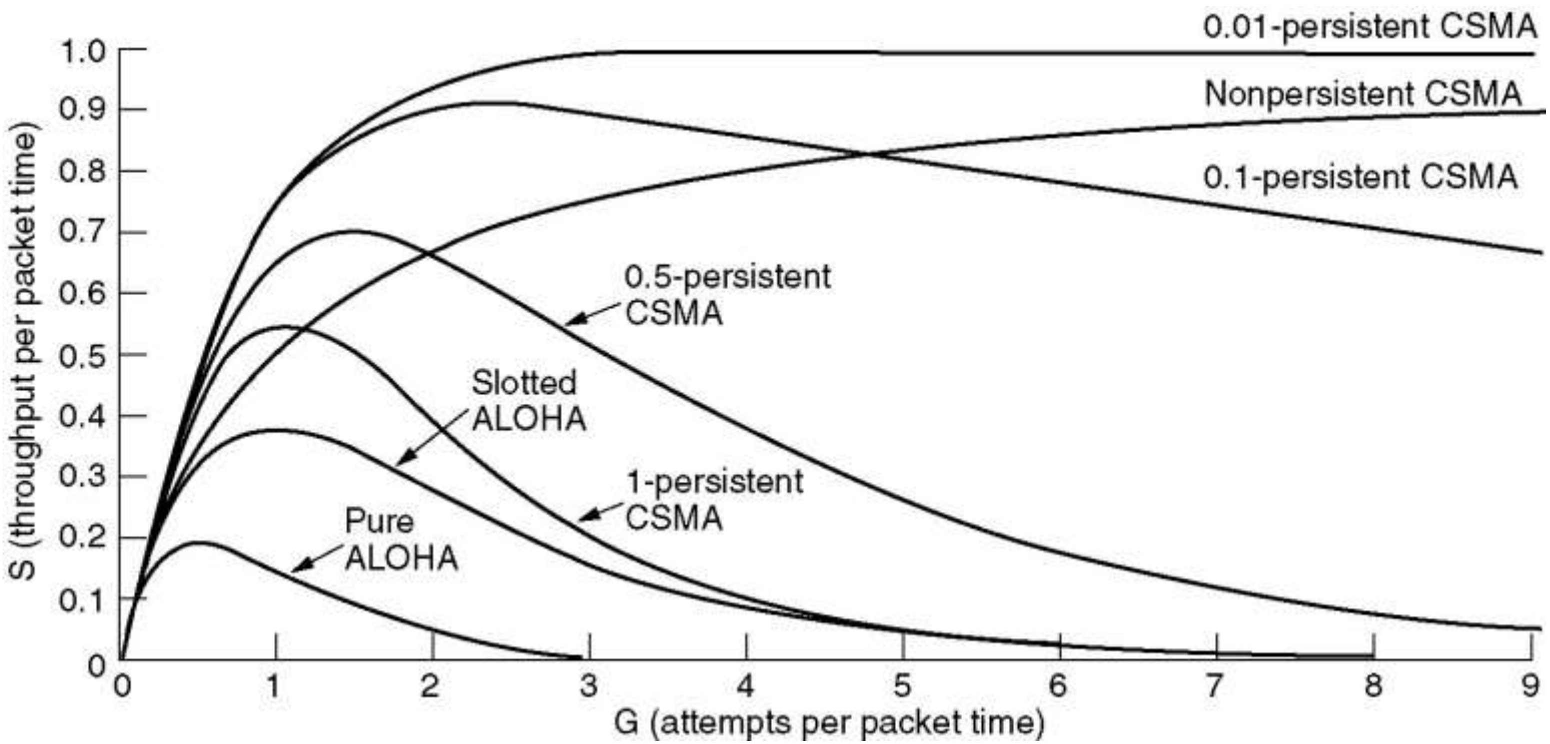


Fig.4-4.Comparison of the channel utilization versus load for various random access protocols

4.2.2 Carrier Sense Multiple Access Protocols

- CSMA with Collision Detection（带冲突检测的CSMA）
  - Improvement： abort their transmissions as soon as they detect a collision.
  - Carrier Sense Multiple Access with Collision Detection（**CSMA/CD**)
  - The conceptual model-[see fig 4-5]
  - **Three states： contention,transmission,or idle**
  - CSMA/CD is an important protocol. One version of it： IEEE 802.3(Ethernet),which is an international standard.

(补充)

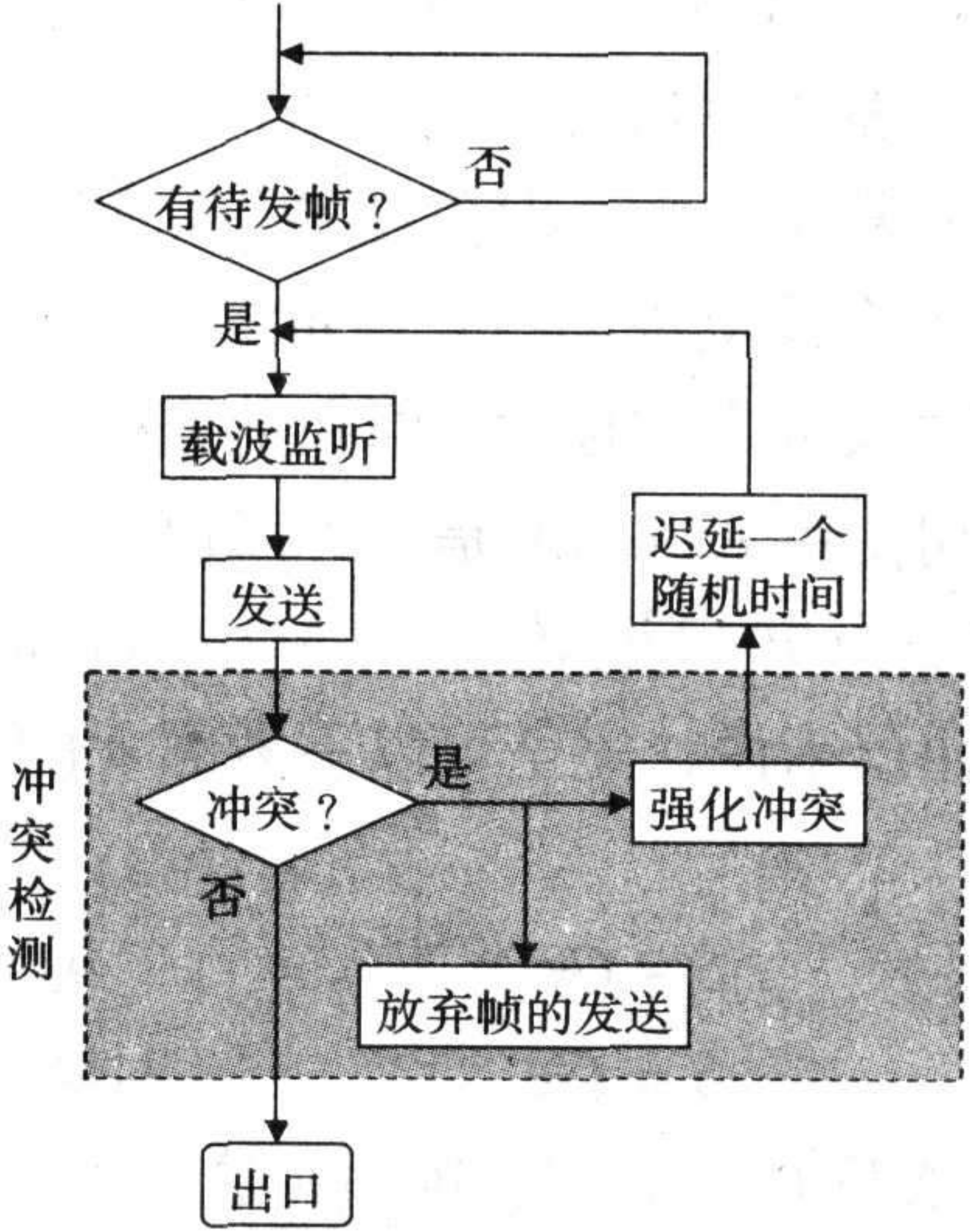


图 4-10　CSMA/CD 的流程图

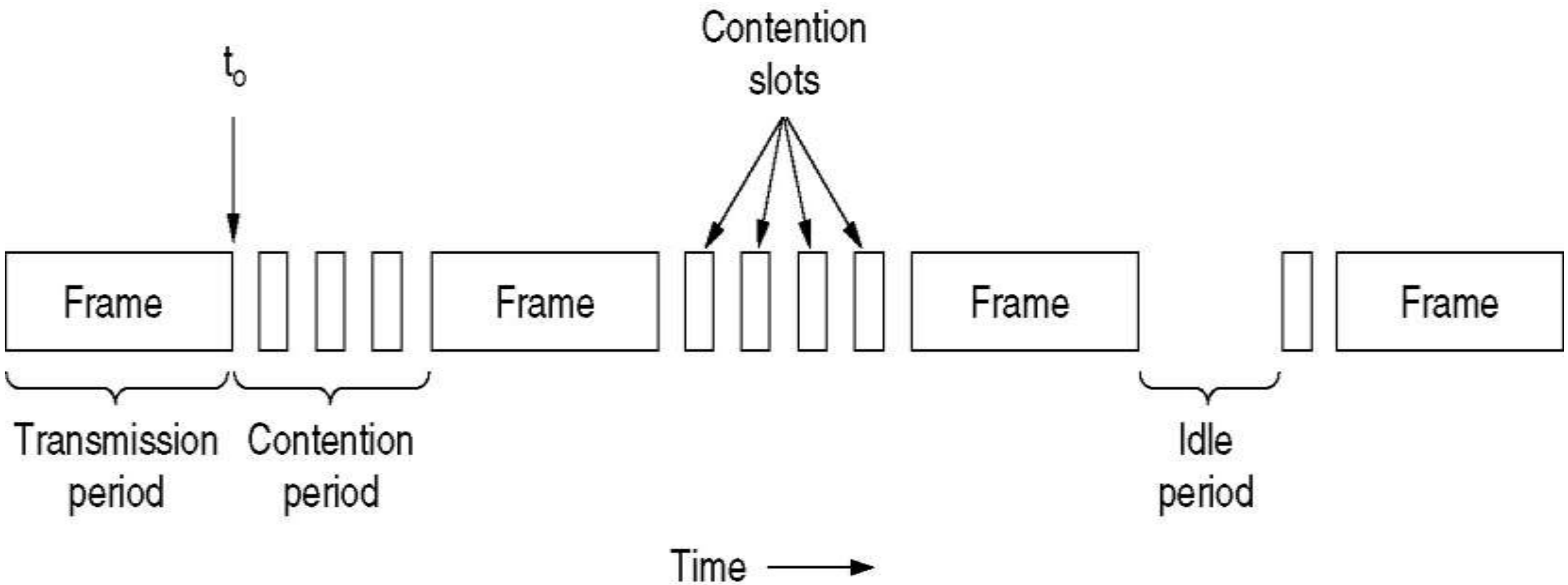


Fig.4-5 CSMA/CD can be in one of three states: contention, transmission, or idle.

4.2.3 Collision-Free Protocols

- A Bit-Map Protocol
  - Each contention period consists of exactly N slots.
  - In general, station *j* may announce the fact that it has a frame to send by inserting a *1* bit into slot *j*.
  - After all *N* slots have passed by, each station has complete knowledge of which stations wish to transmit.
  - At that point, they begin transmitting in numerical order. **Since everyone agrees on who goes next, there will never by any collisions**.
  - After the last ready station has transmitted its frame, an event all stations can easily monitor, another *N* bit contention period is begun.

4.2.3 Collision-Free Protocols

- A Bit-Map Protocol

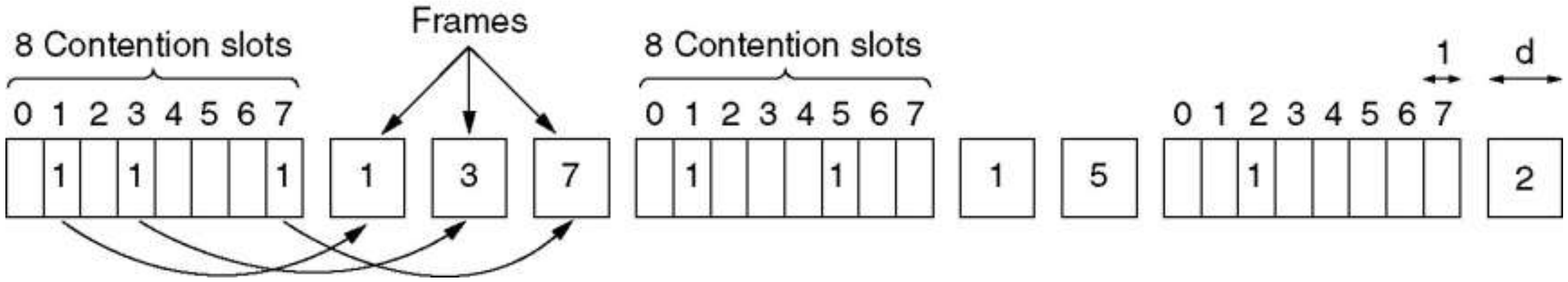


Fig 4-6. The basic bit-map protocol.

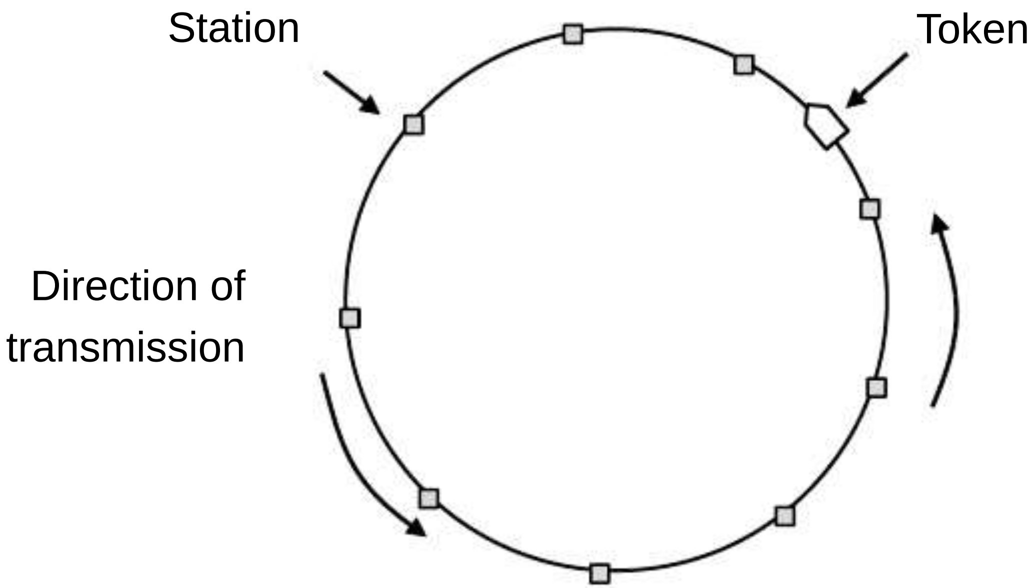
4.2.3 Collision-Free Protocols

Performance analysis: Assume data frames consisting of d time units where one time unit is one contention bit slot.

- At low load: The mean delay is N slots. The overhead per frame is N bits, and the amount of data is d bits, for an efficiency of ***$d/(N+d)$*.**
- At high load: When all the stations have something to send all the time, the N bit contention period is prorated over N frames, yielding an overhead of only 1 bit per frame, or an efficiency of ***$d/(d+1)$*.** The mean delay for a frame is equal to the sum of the time it queues inside its station, plus an additional $N(d+1)/2$ once it gets to the head of its internal queue.

4.2.3 Collision-Free Protocols

- Token Passing

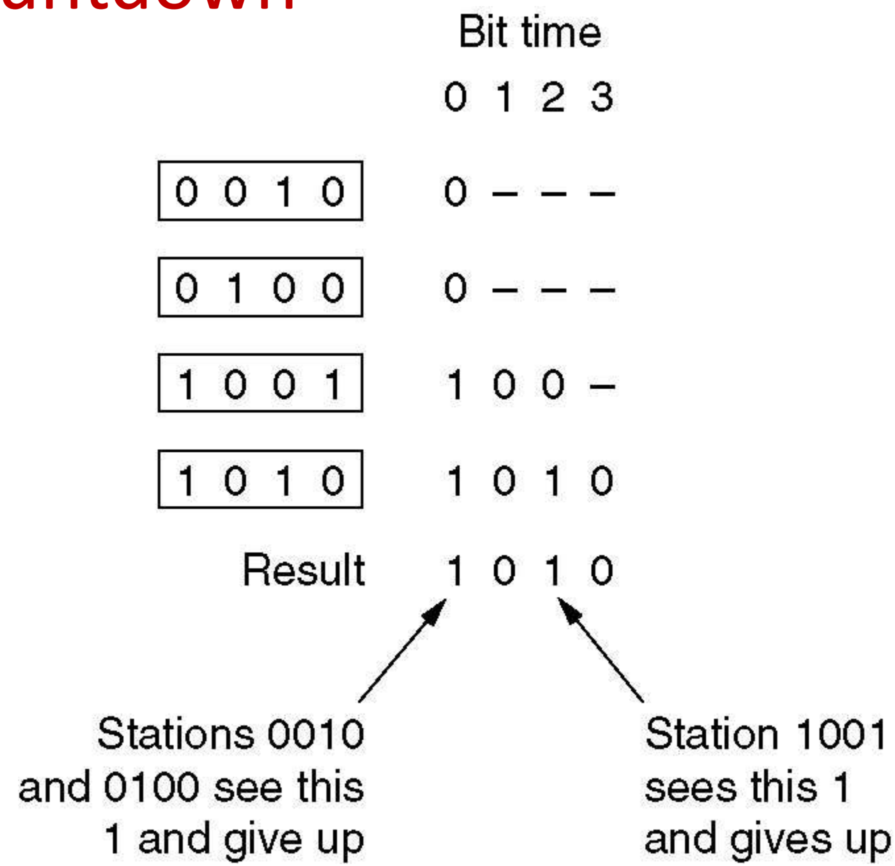


Token ring.

- Token bus, 1980s
- FDDI, 1990s
- RPR(Resilient Packet Ring, a token ring), 2000s, IEEE 802.17

4.2.3 Collision-Free Protocols

- Binary Countdown



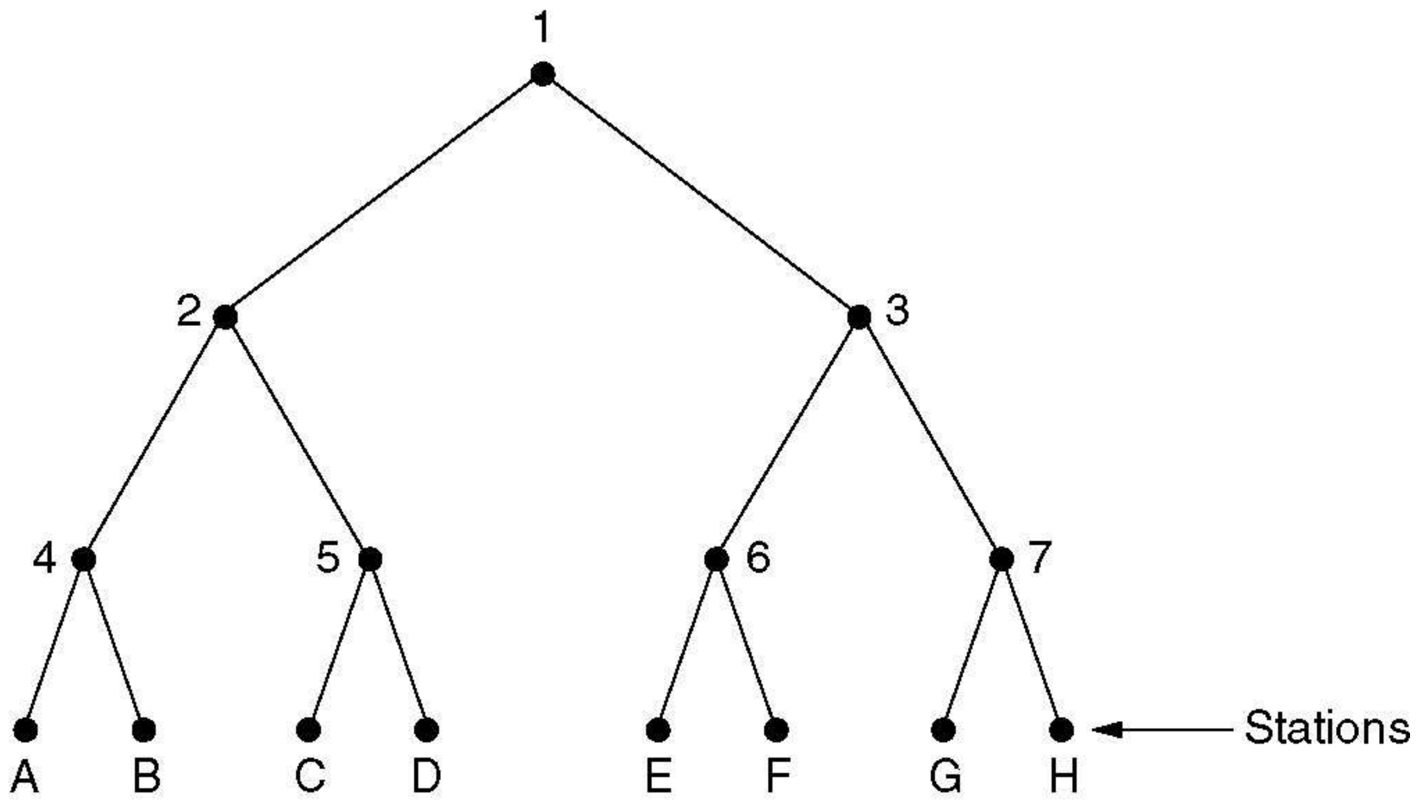
The binary countdown protocol. A dash indicates silence.

4.2.4 Limited-Contention

- Contention method
  - Under low load, the contention method (i.e., pure or slotted ALOHA, CSMA) is preferable due to its low delay.
  - Under high load, the contention method becomes increasingly less efficient.
- Collision-free method
  - Under low load, the collision-free method has high delay.
  - Under high load, the collision-free method becomes increasingly more efficient.
- → Limited-Contention Protocols

4.2.4 Limited-Contention

- Adaptive Tree Walk Protocol
  （适应数搜索协议）
  - The tree for eight stations.



4.2.4 Limited-Contention

- Adaptive Tree Walk Protocol
  - At what level in the tree should the search begin? Clearly, the heavier the load, the farther down the tree the search should begin.
  - Begin at $i=log_2\, q$ where q is the estimate of the number of ready stations.
  - Numerous improvements to the basic algorithm have been discovered (Bersekas and Gallager, 1992)

4.2.5 Wireless LAN Protocols

- Unlike cellular telephone systems,each cell has only one channel,covering the entire available band width，usually its bandwidth is 11-54Mb/s
- Hidden station problem-[see fig 4-11(a)]
  - A->B, C will not hear A，thus falsely conclude that C can transmit,collision occur.
- Exposed station problem-[see fig 4-11(b)]
  - B->A, C is listening,falsely conclude that it may not send to D

Fig.4-11.A wireless LAN.(a) A transmitting.(b) B transmitting.

Wireless LAN Protocols (2)

- Multiple Access with Collision Avoidance(MACA) -[see fig 4-12]
  - IEEE 802.11
  - The basic idea： the sender stimulate the receiver（RTS)，make it send a frame(CTS)， all stations nearby can detect this transmission ， avoid collision.

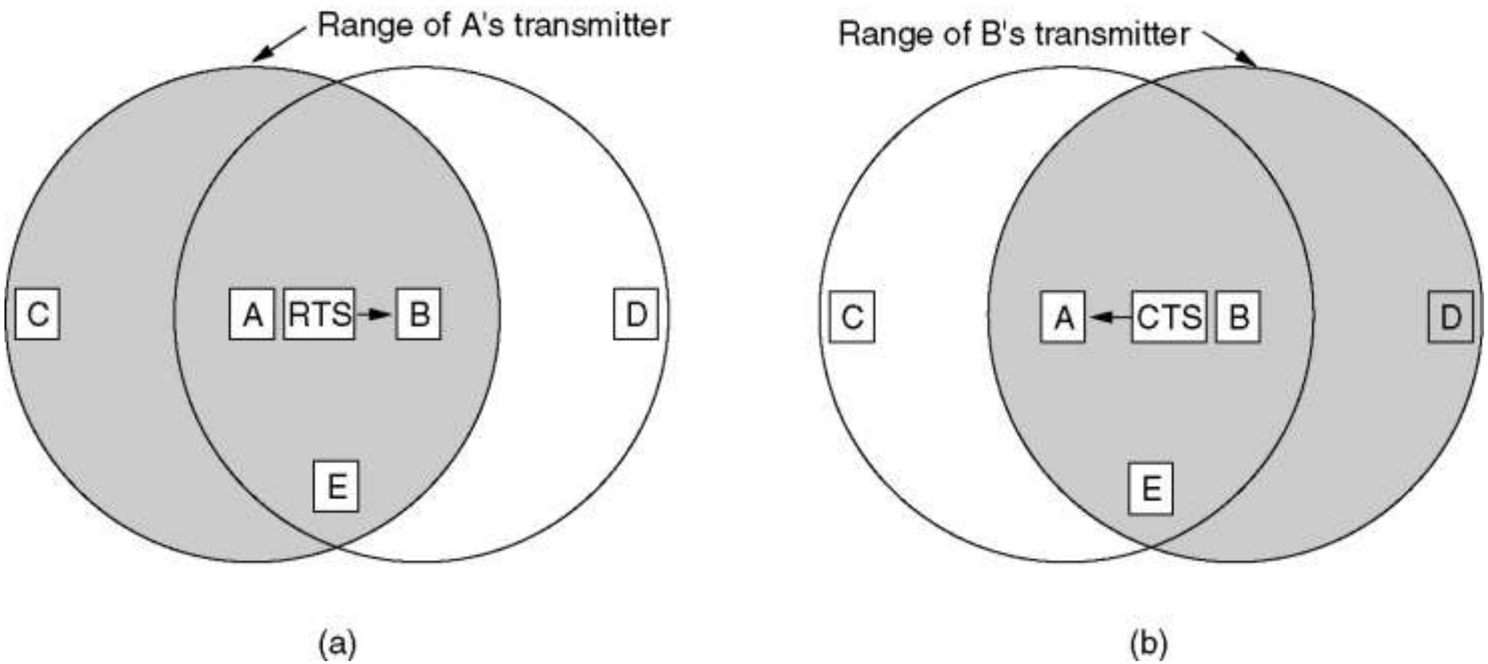


Fig.4-12.The MACA protocol.(a) A sending an RTS to B
(b) B responding with a CTS to A

- **Conclusion （CSMA／CA Rule）：**
  - If station X received RTS,but did not receive CTS,then X can transmit its data and will not interfere with other stations. 。
  - If station X has not received RTS, but received CTS,then X may not transmit its data.
  - If station X has received both RTS and CTS,then X may not transmit its data.
- Although the use of RTS and CTS will decrease the efficiency of network,but the influence is little because they are very short. e.g, frame length of RTS is 30 byte while the maximal length of data frame is 2346 bytes.
- **MACA** can not prevent collision from happening. e.g, A and C transmit RTS to B in the same time, their RTS frame will collision.
- **MACAW**: tune MACA to improve its performance.
  - MAC for Wireless
  - introducing an ACK after each successful data frame， avoid losing the frame

WLAN Protocols

- IEEE 802.11 2.4GHz, 1997
  - 1/2M
- IEEE 802.11b 2.4GHz, 1999
  - 11M
- IEEE 802.11a 5GHz, 1999
  - 54M
- IEEE 802.11g 2.4GHz, July 2003
  - 11M/54M
- IEEE 802.11i （WLAN的 802.1x）新一代WLAN安全标准
- IEEE 802.11n 2.4G/5GHz, Sept.11,2009
  - 300, 600Mbps
- IEEE 802.11ac (draft), 5GHz, Nov. 2011
  - 1G

802.11标准比较

IEEE 标准	最大速度	最大室内范围	频率	向后兼容
802.11a	54 Mb/s	35 米（115 英尺）	5 GHz	—
802.11b	11 Mb/s	35 米（115 英尺）	2.4 GHz	—
802.11g	54 Mb/s	38 米（125 英尺）	2.4 GHz	802.11b
802.11n	600 Mb/s	70 米（230 英尺）	2.4 GHz 和 5 GHz	802.11a/b/g
802.11ac	1.3 Gb/s (1300 Mb/s)	35 米（115 英尺）	5 GHz	802.11a/n

4.3 Ethernet

- Physical layer
- MAC sublayer protocol
- Ethernet performance
- Switched Ethernet
- Fast Ethernet
- Gigabit Ethernet
- 10 Gigabit Ethernet
- IEEE 802.2: Logical Link Control
- Retrospective on Ethernet

4.3.1 Classic Ethernet Physical Layer

- Classic Ethernet
- Switched Ethernet

- DIX standard
- Thick Ethernet
- Thin Ethernet
- Repeater

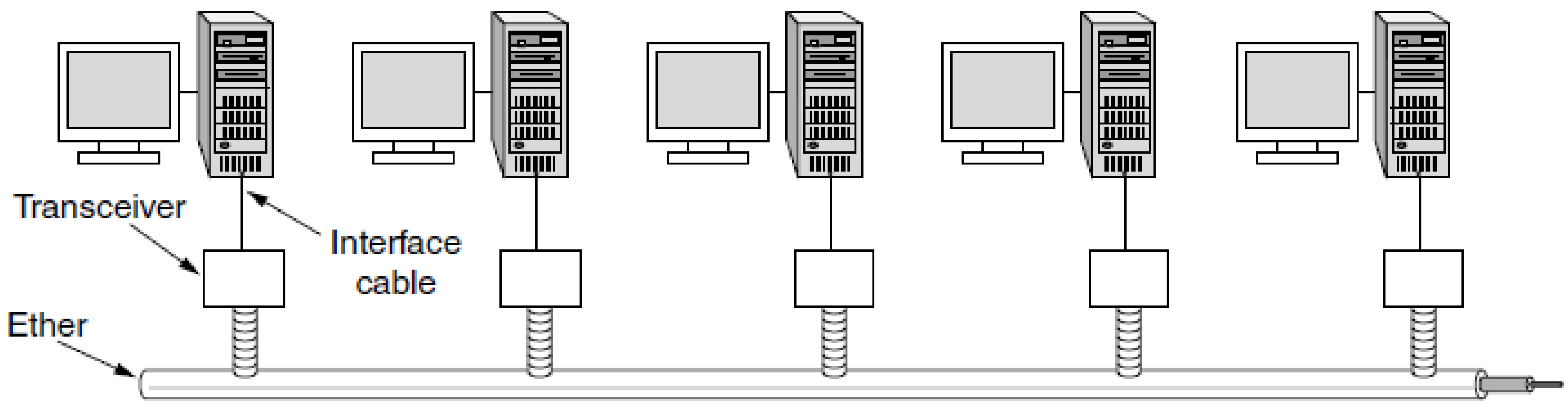


Figure 4-13. Architecture of classic Ethernet

- Four types of cabling are commonly used: (Figure 4-13,14,15)

Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

Figure 4-xx. The most common kinds of Ethernet cabling.

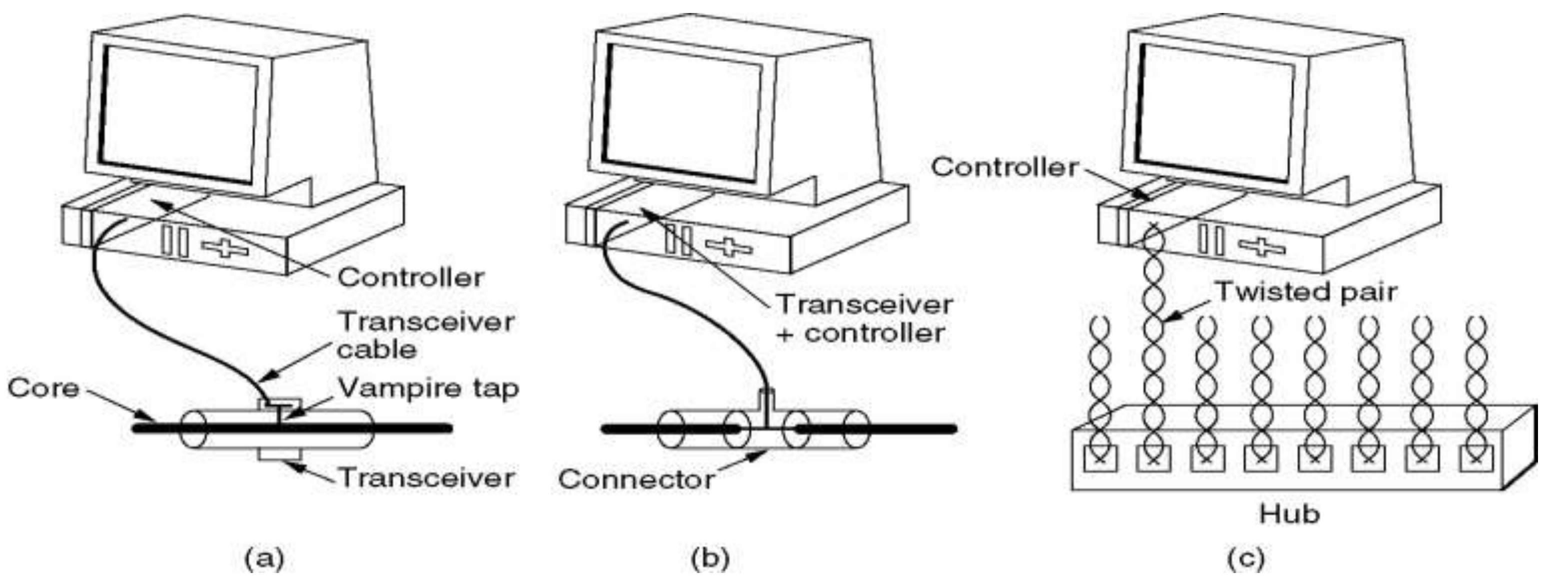


Figure 4-xxThree kinds of Ethernet cabling. (a) 10Base5, (b) 10Base2, (c) 10Base-T.

4.3.2 Classic Ethernet MAC Sublayer Protocol

Bytes	8	6	6	2	0-1500	0-46	4
(a)	Preamble	Destination address	Source address	Type	Data	Pad	Check-sum
(b)	Preamble | SoF	Destination address	Source address	Length	Data	Pad	Check-sum

Figure 4-14. Frame formats. (a) Ethernet (DIX). (b) IEEE 802.3.

？？Manchester Encoding

- Problem: bit 0--0 volts , bit 1--5 volts , then ambiguities arise: an idle sender(0 volts) or a 0 bit (0 volts).
- Method: using +1 volts for a 1 and –1 volts for a 0, but there is still a problem: different clock speeds
- key issue: to unambiguously determine the start, end, or middle of each bit without reference to an external clock. Two such approaches: **Manchester encoding** and differential Manchester encoding.
- **Manchester encoding**: Each bit period is divided into two equal intervals(1—high during the first interval and low in the second one. 0—just the reverse).
  - Advantage: easy for the receiver to synchronize with the sender
  - Disadvantage: twice as much bandwidth as straight binary encoding

？？ Manchester Encoding

- Differential Manchester encoding: 1—absence of a transition(跳变) at the start of the interval, 0—presence of a transition at the start of the interval
  - The differential scheme requires more complex equipment but offers better noise immunity
- All Ethernet systems use Manchester encoding due to its simplicity

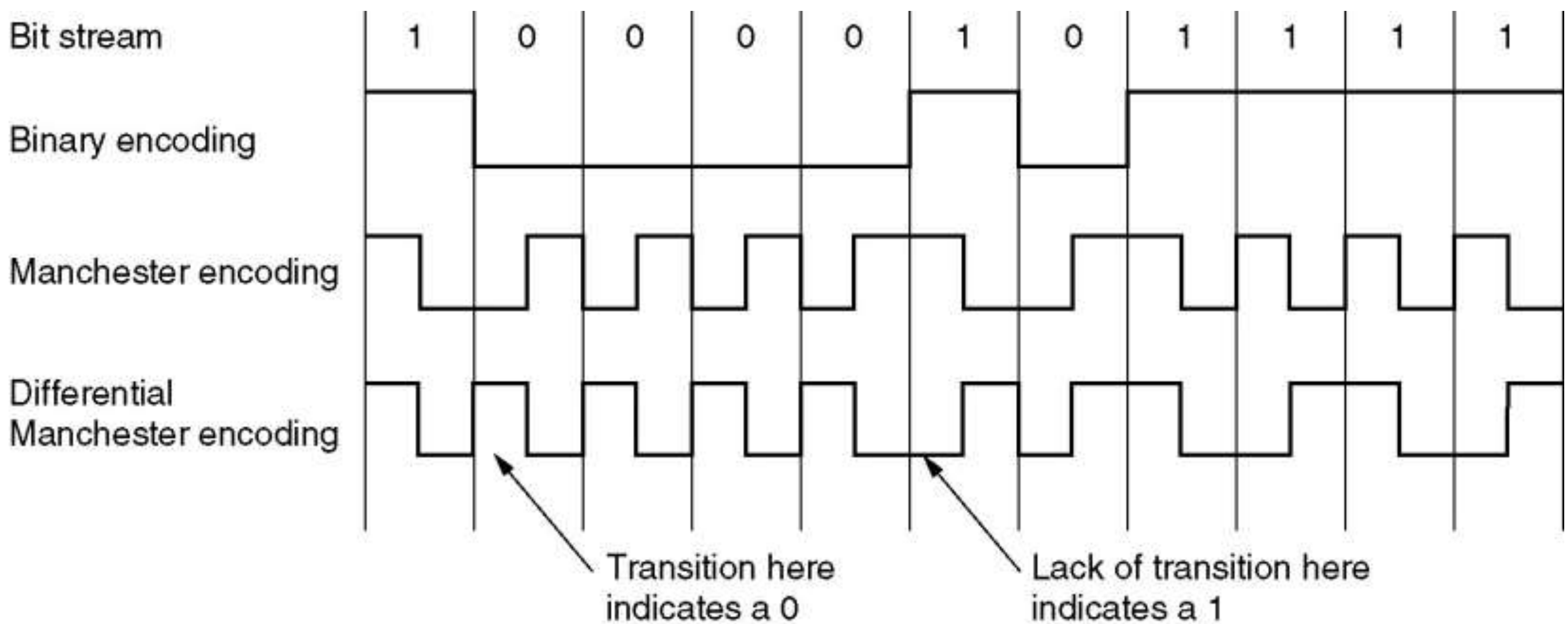


Figure 4-16. (a) Binary encoding, (b) Manchester encoding, (c) Differential Manchester encoding.

4.3.2 Classic Ethernet MAC Sublayer Protocol

- Original DIX frame structure-[see fig 4-14(a)]
  - Preamble of 8 bytes, containing bit pattern 10101010
  - high-order bit of destination address: 0-ordinary, 1- group
  - minimum frame length: 64 bytes (512bits)
    - to distinguish valid frames from garbage
    - collision detection -[see fig 4-15]
  - CRC check
- two changes IEEE made: [see fig 4-14(b)]
  - Preamble of 7 bytes, last byte for a Start of Frame(SOF) delimiter (7+1=8)
  - to change Type field into Length field
- Multicasting: Sending to a group
- Broadcasting: Special address, all 1
- OUI (Organizationally Unique Identifier, MAC)
- LLC

DEC, Intel, Xerox

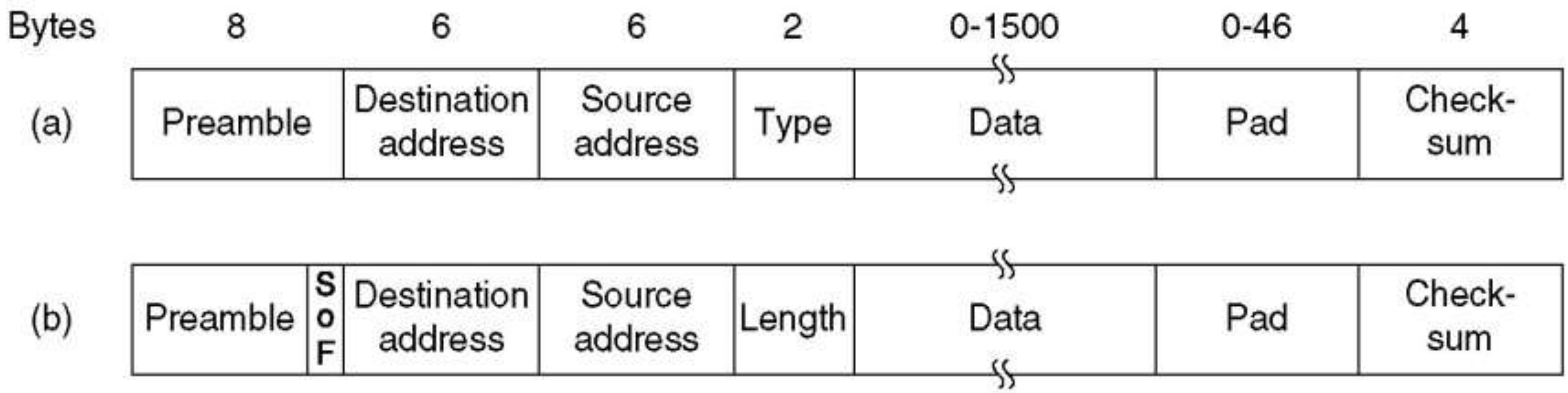
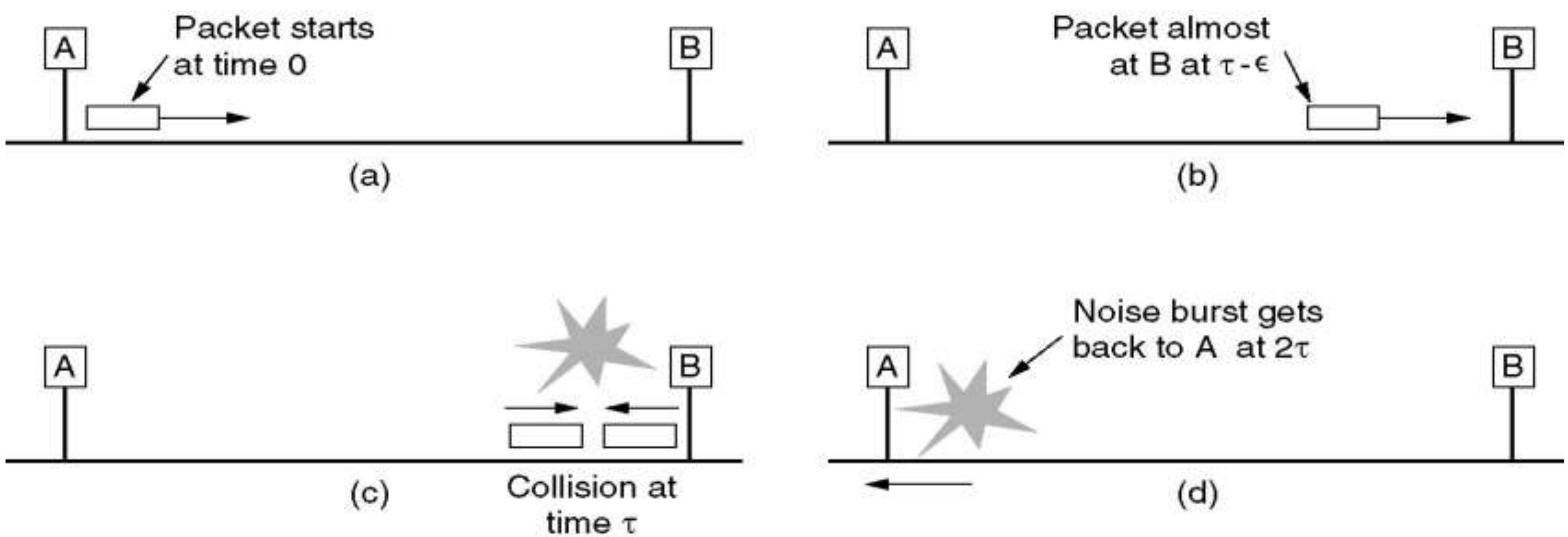


Figure 4-14. Frame formats. (a) DIX Ethernet, (b) IEEE 802.3.



Collision detection can take as long as 2τ.

CSMA/CD with Binary Exponential Backoff

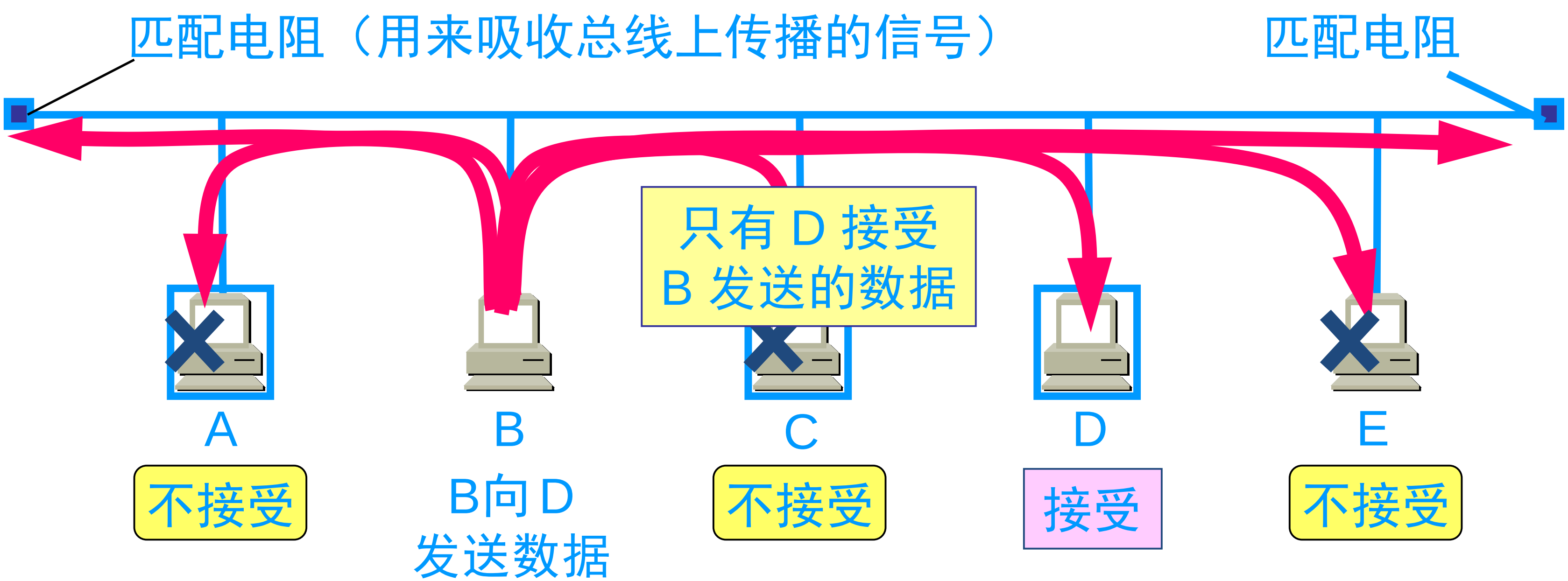
- delay=k*2τ
- slot time(round-trip delay): 2τ=51.2 μs
- after i collisions, a random number k between 0 and 2^i-1 is chosen.
- After 10 collisions have been reached, the randomization interval is frozen at a maximum of 1023 slots. After 16 collisions, the controller throws in the towel and reports failure back to the computer.

Goto 4.3.3

CSMA/CD 协议

Optional

- 最初的以太网是将许多计算机都连接到一根总线上。当初认为这样的连接方法既简单又可靠，因为总线上没有有源器件。



两个标准

- DIX Ethernet V2 是世界上第一个局域网产品（以太网）的规约。
- IEEE 的 802.3 标准。
- DIX Ethernet V2 标准与 IEEE 的 802.3 标准只有很小的差别，因此可以将 802.3 局域网简称为“以太网”。
- 严格说来，“以太网”应当是指符合 DIX Ethernet V2 标准的局域网

为了通信的简便
以太网采取了两种重要的措施

- 采用较为灵活的无连接的工作方式，即不必先建立连接就可以直接发送数据。
- 以太网对发送的数据帧不进行编号，也不要求对方发回确认。
  - **这样做的理由是局域网信道的质量很好，因信道质量产生差错的概率是很小的。**

以太网提供的服务

- 以太网提供的服务是不可靠的交付，即尽最大努力的交付。
- 当目的站收到有差错的数据帧时就丢弃此帧，其他什么也不做。差错的纠正由高层来决定。
- 如果高层发现丢失了一些数据而进行重传，但以太网并不知道这是一个重传的帧，而是当作一个新的数据帧来发送。

载波监听多点接入/碰撞检测（CSMA/CD）

- **CSMA/CD 表示 Carrier Sense Multiple Access with Collision Detection。**
- “多点接入”表示许多计算机以多点接入的方式连接在一根总线上。
- “载波监听”是指每一个站在发送数据之前先要检测一下总线上是否有其他计算机在发送数据，如果有，则暂时不要发送数据，以免发生碰撞。
- 总线上并没有什么“载波”。因此，“载波监听”就是用电子技术检测总线上有没有其他计算机发送的数据信号。

碰撞检测

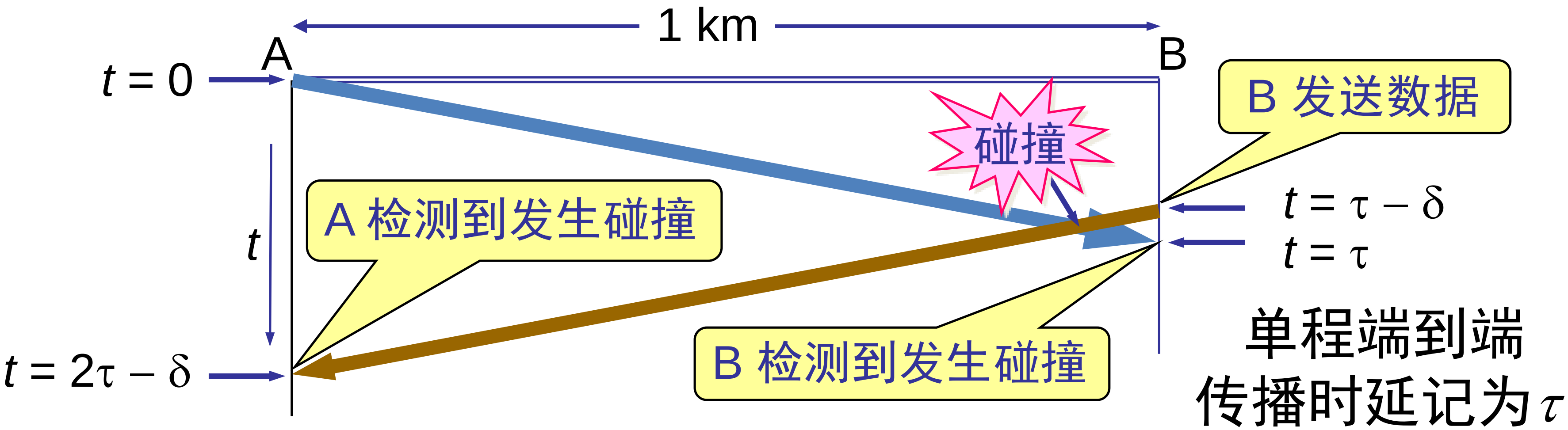
- “碰撞检测”就是计算机边发送数据边检测信道上的信号电压大小。
- 当几个站同时在总线上发送数据时，总线上的信号电压摆动值将会增大（互相叠加）。
- 当一个站检测到的信号电压摆动值超过一定的门限值时，就认为总线上至少有两个站同时在发送数据，表明产生了碰撞。
- 所谓“碰撞”就是发生了冲突。因此“碰撞检测”也称为“冲突检测”。

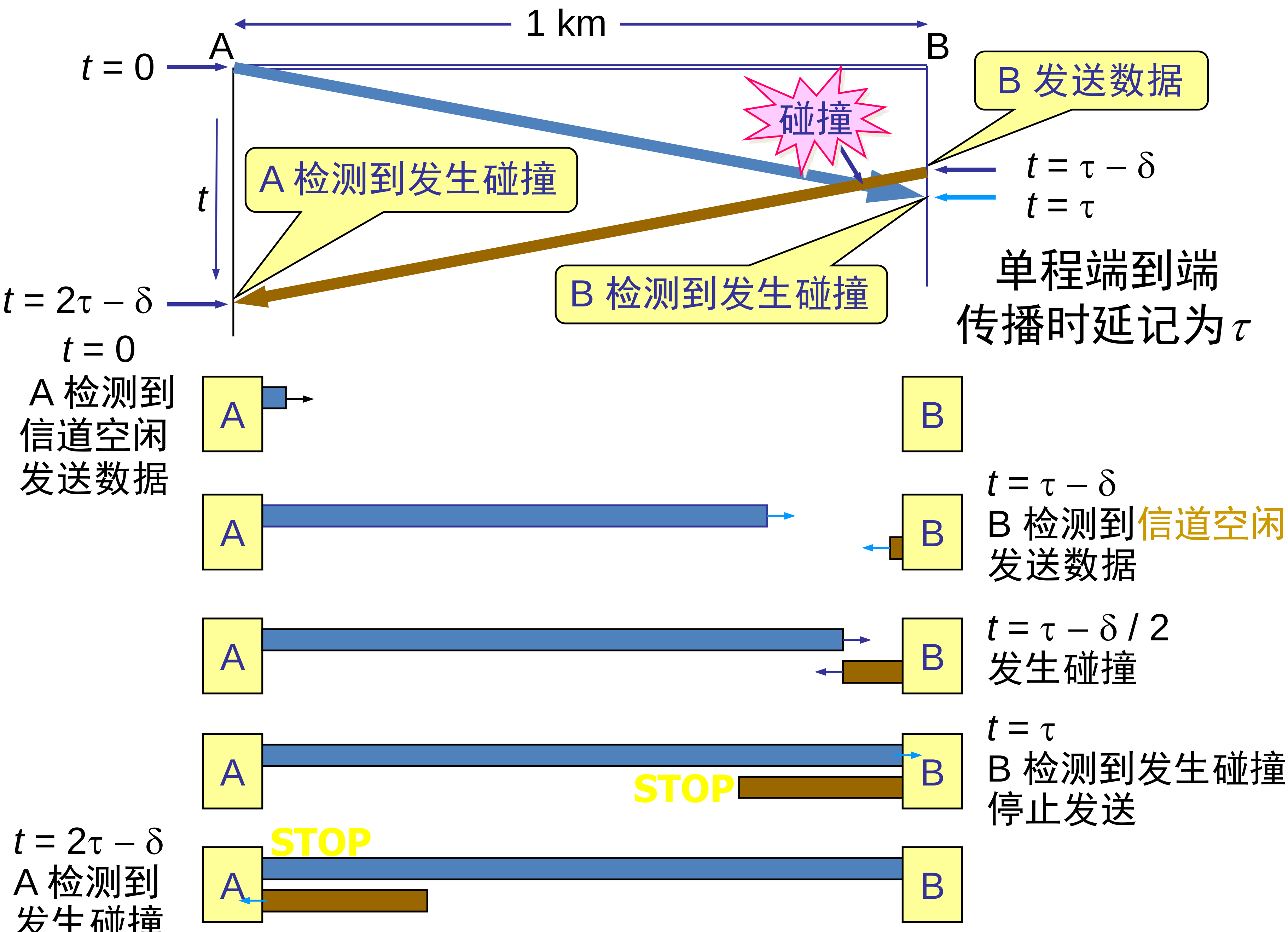
检测到碰撞后

- 在发生碰撞时，总线上传输的信号产生了严重的失真，无法从中恢复出有用的信息来。
- 每一个正在发送数据的站，一旦发现总线上出现了碰撞，就要立即停止发送，免得继续浪费网络资源，然后等待一段随机时间后再次发送。

电磁波在总线上的
有限传播速率的影响

- 当某个站监听到总线是空闲时，也可能总线并非真正是空闲的。
- A 向 B 发出的信息，要经过一定的时间后才能传送到 B。
- B 若在 A 发送的信息到达 B 之前发送自己的帧(因为这时 B 的载波监听检测不到 A 所发送的信息)，则必然要在某个时间和 A 发送的帧发生碰撞。
- 碰撞的结果是两个帧都变得无用。


1 km
A
B
$t = 0$
B 发送数据
碰撞
t
A 检测到发生碰撞
$t = \tau - \delta$
$t = \tau$
B 检测到发生碰撞
$t = 2\tau - \delta$
单程端到端
传播时延记为τ


1 km
A
B
t = 0
t
t = 2τ – δ
碰撞
B 发送数据
A 检测到发生碰撞
t = τ – δ
t = τ
B 检测到发生碰撞
单程端到端
传播时延记为τ
t = 0
A 检测到
信道空闲
发送数据
A
B
A
B
t = τ – δ
B 检测到信道空闲
发送数据
A
B
t = τ – δ / 2
发生碰撞
A
B
STOP
t = τ
B 检测到发生碰撞
停止发送
t = 2τ – δ
A 检测到
发生碰撞
STOP
A
B

重要特性

- 使用 CSMA/CD 协议的以太网不能进行全双工通信而只能进行双向交替通信（半双工通信）。
- 每个站在发送数据之后的一小段时间内，存在着遭遇碰撞的可能性。
- 这种发送的不确定性使整个以太网的平均通信量远小于以太网的最高数据率。

争用期

- 最先发送数据帧的站，在发送数据帧后至多经过时间 **2**τ（两倍的端到端往返时延）就可知道发送的数据帧是否遭受了碰撞。
- 以太网的端到端往返时延 **2**τ称为争用期，或碰撞窗口。
- 经过争用期这段时间还没有检测到碰撞，才能肯定这次发送不会发生碰撞。

二进制指数类型退避算法
(truncated binary exponential type)

- 发生碰撞的站在停止发送数据后，要推迟（退避）一个随机时间才能再发送数据。
  - 确定基本退避时间，一般是取为争用期 2τ。
  - 定义重传次数 k ，$k \leq 10$，即

$$k = \text{Min}[\text{重传次数},\ 10]$$

  - 从整数集合$[0, 1, \cdots, (2^k - 1)]$中随机地取出一个数，记为 r。重传所需的时延就是 r 倍的基本退避时间。
  - 当重传达 16 次仍不能成功时即丢弃该帧，并向高层报告。

争用期的长度

- 以太网取 **51.2 μs** 为争用期的长度。
- 对于 **10 Mb/s** 以太网，在争用期内可发送**512 bit**，即 **64** 字节。
- 以太网在发送数据时，若前 **64** 字节没有发生冲突，则后续的数据就不会发生冲突。

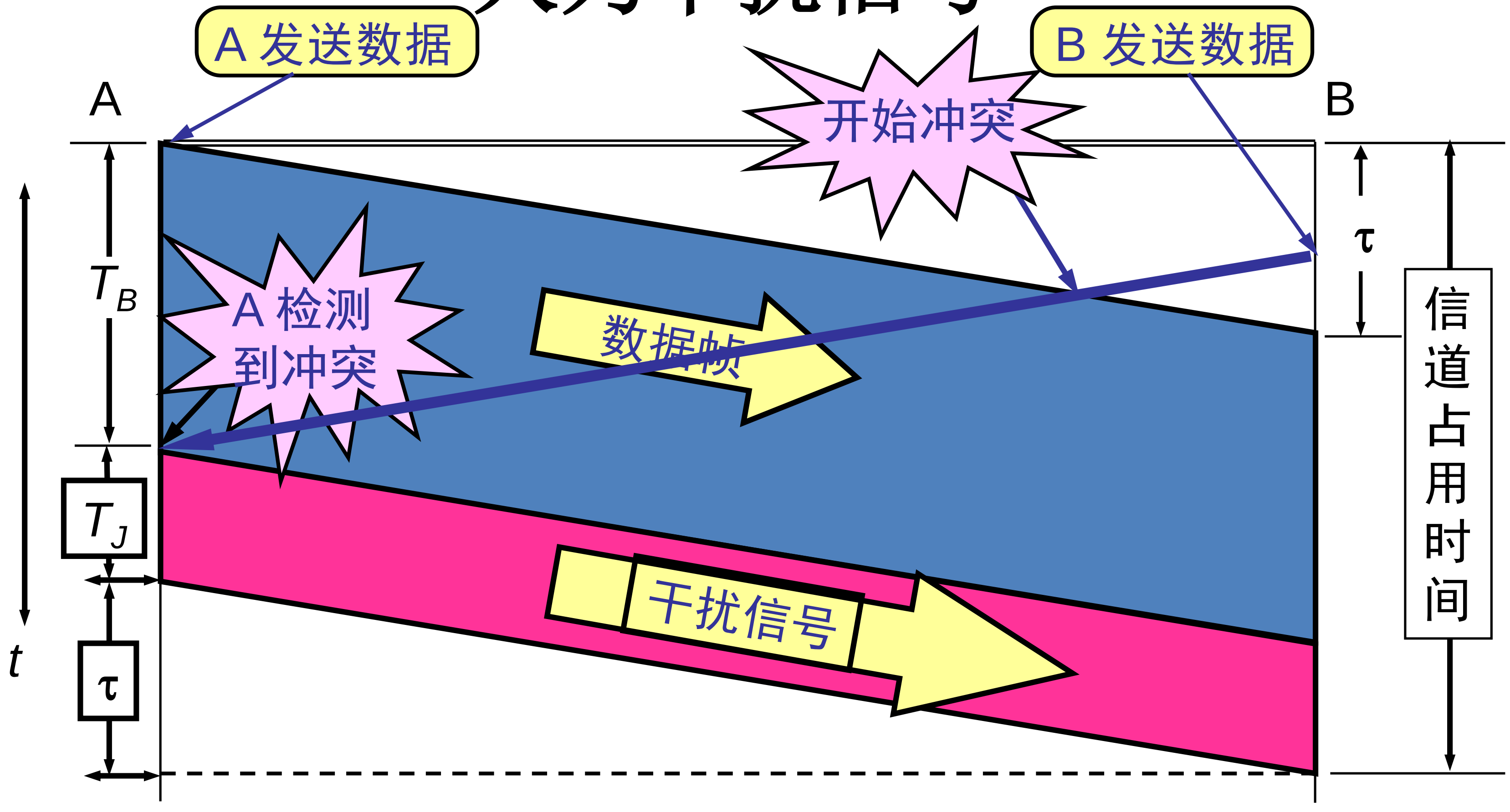
最短有效帧长

- 如果发生冲突，就一定是在发送的前 **64** 字节之内。
- 由于一检测到冲突就立即中止发送，这时已经发送出去的数据一定小于 **64** 字节。8 bytes for frame header/footer, and 46 bytes for the data.
- 以太网规定了最短有效帧长为 **64** 字节，凡长度小于 **64** 字节的帧都是由于冲突而异常中止的无效帧。

强化碰撞

- 当发送数据的站一旦发现发生了碰撞时，除了立即停止发送数据外，还要再继续发送若干比特的**人为干扰信号(jamming signal)**，以便让所有用户都知道现在已经发生了碰撞。

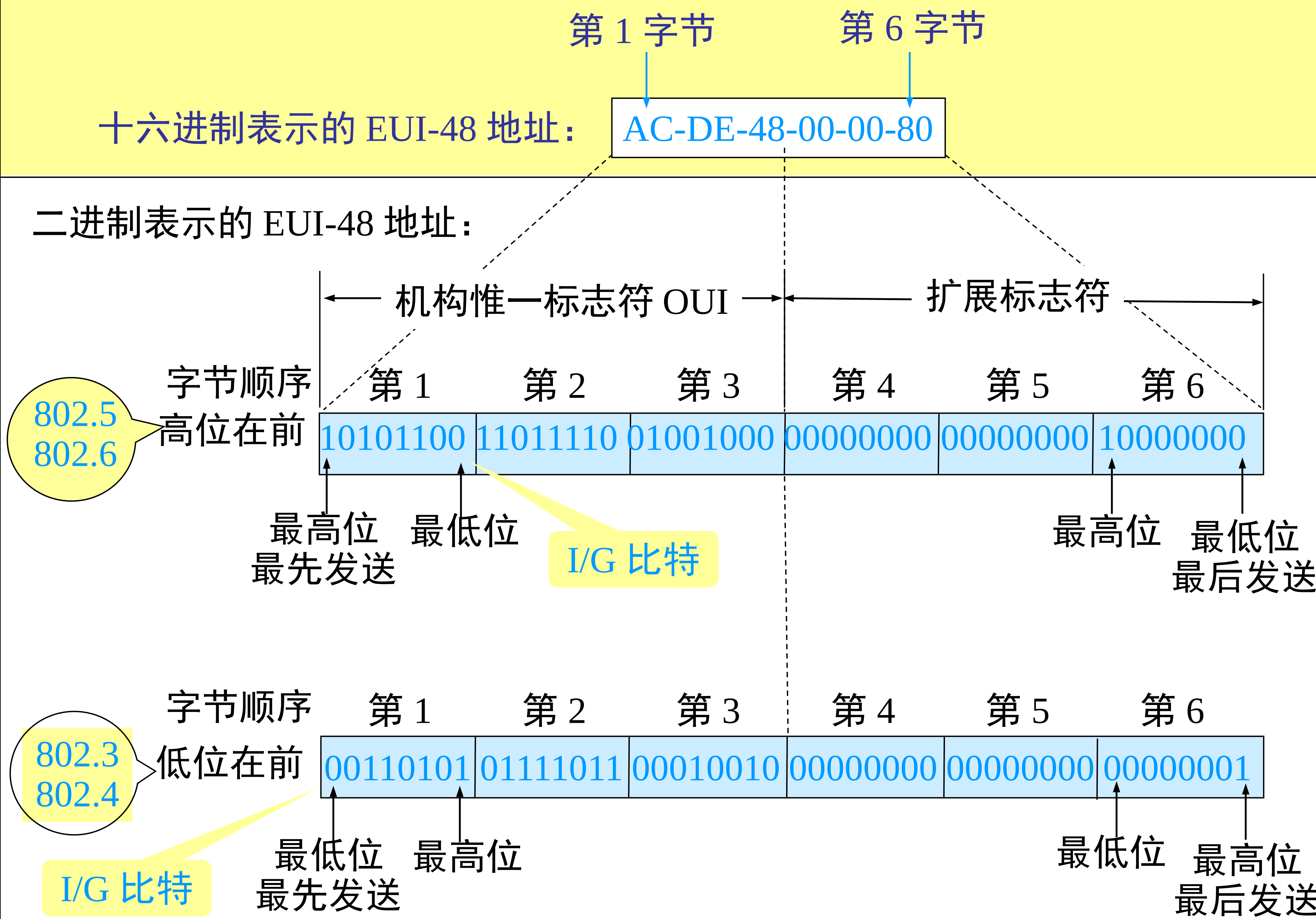
人为干扰信号



B 也能够检测到冲突，并立即停止发送数据帧，接着就发送干扰信号。这里为了简单起见，只画出 A 发送干扰信号的情况。

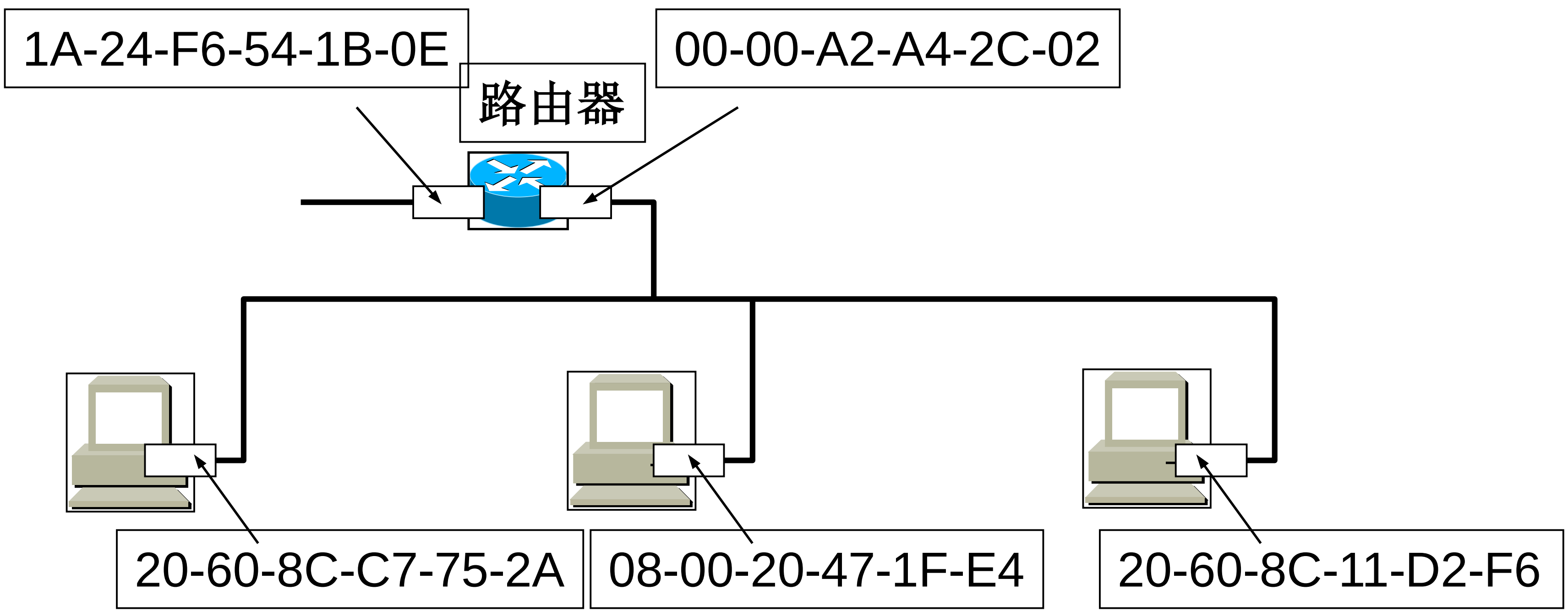
4.3 以太网的 MAC 层（*）
4.3.1 MAC 层的硬件地址

- 在局域网中，硬件地址又称为物理地址，或 MAC 地址。
- 802 标准所说的“地址”严格地讲应当是每一个站的“名字”或标识符。
- 但鉴于大家都早已习惯了将这种 48 bit 的“名字”称为“地址”，所以本书也采用这种习惯用法，尽管这种说法并不太严格。


第 1 字节
第 6 字节
十六进制表示的 EUI-48 地址：
AC-DE-48-00-00-80
二进制表示的 EUI-48 地址：
机构惟一标志符 OUI
扩展标志符
字节顺序
第 1
第 2
第 3
第 4
第 5
第 6
802.5
802.6
高位在前
10101100 11011110 01001000 00000000 00000000 10000000
最高位
最先发送
最低位
I/G 比特
最高位
最低位
最后发送
字节顺序
第 1
第 2
第 3
第 4
第 5
第 6
802.3
802.4
低位在前
00110101 01111011 00010010 00000000 00000000 00000001
最低位
最先发送
最高位
I/G 比特
最低位
最高位
最后发送

网卡上的硬件地址

路由器由于同时连接到两个网络上，因此它有两块网卡和两个硬件地址。

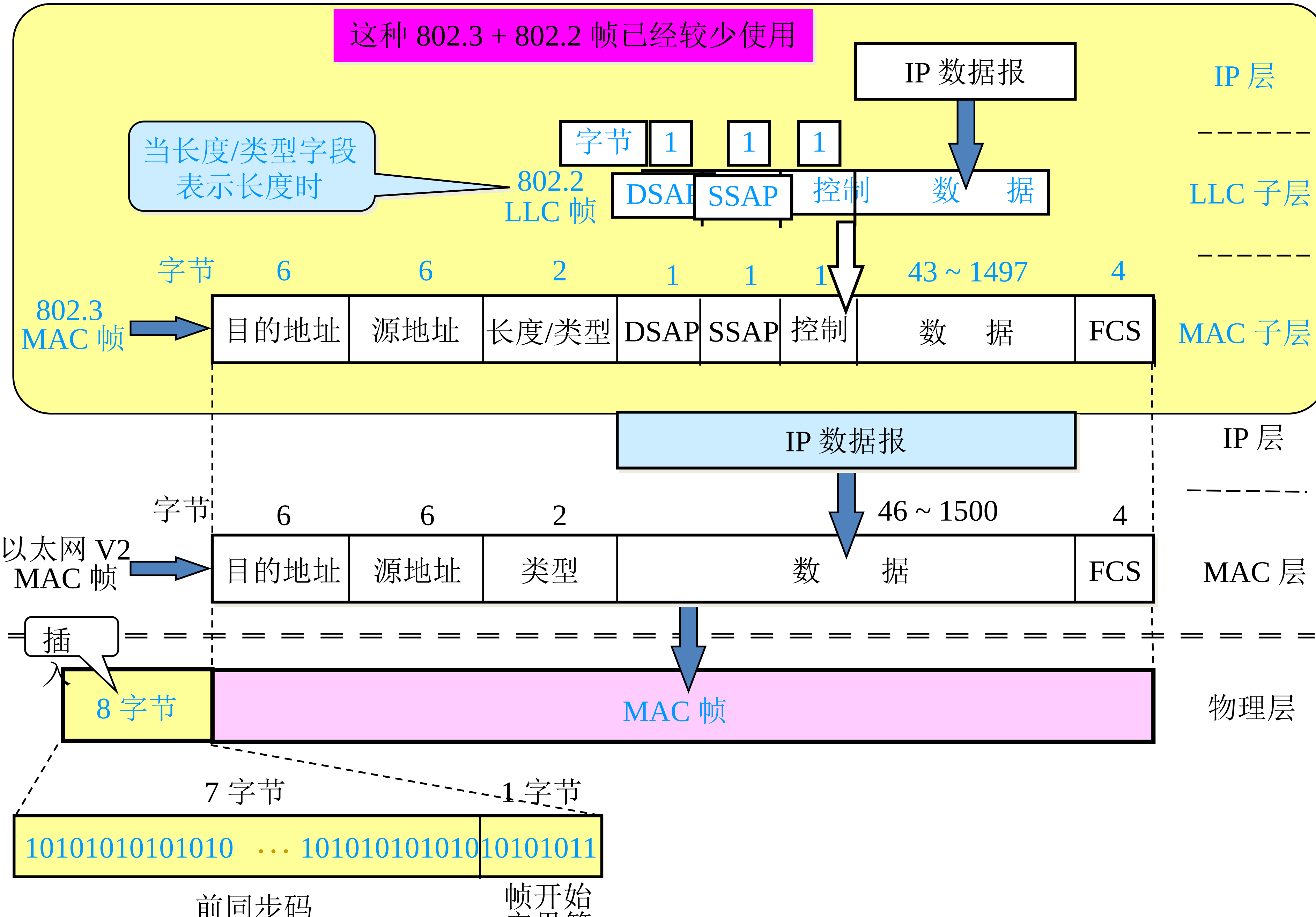


网卡检查 MAC 地址

- 网卡从网络上每收到一个 MAC 帧就首先用硬件检查 MAC 帧中的 MAC 地址.
  - 如果是发往本站的帧则收下，然后再进行其他的处理。
  - 否则就将此帧丢弃，不再进行其他的处理。
- “发往本站的帧”包括以下三种帧：
  - 单播(unicast)帧（一对一）
  - 广播(broadcast)帧（一对全体）
  - 多播(multicast)帧（一对多）

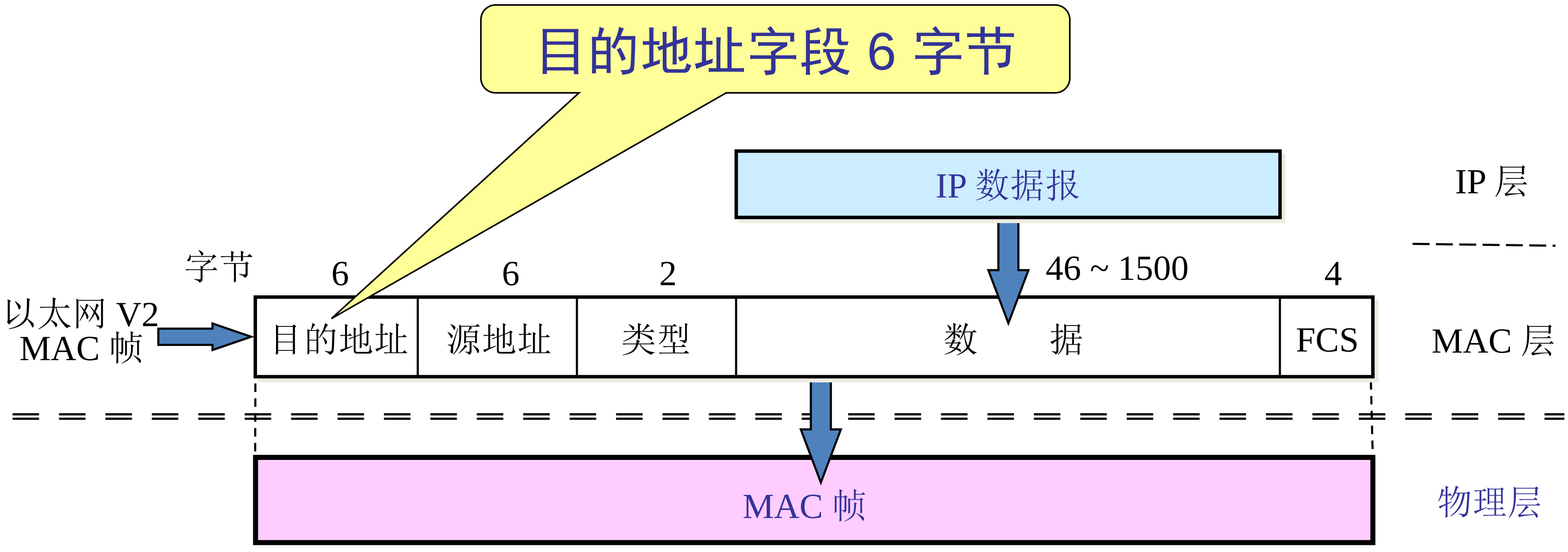
4.3.2 两种不同的 MAC 帧格式 （*）

- 常用的以太网MAC帧格式有两种标准：
  - DIX Ethernet V2 标准
  - IEEE 的 802.3 标准
- 最常用的 MAC 帧是以太网 V2 的格式。

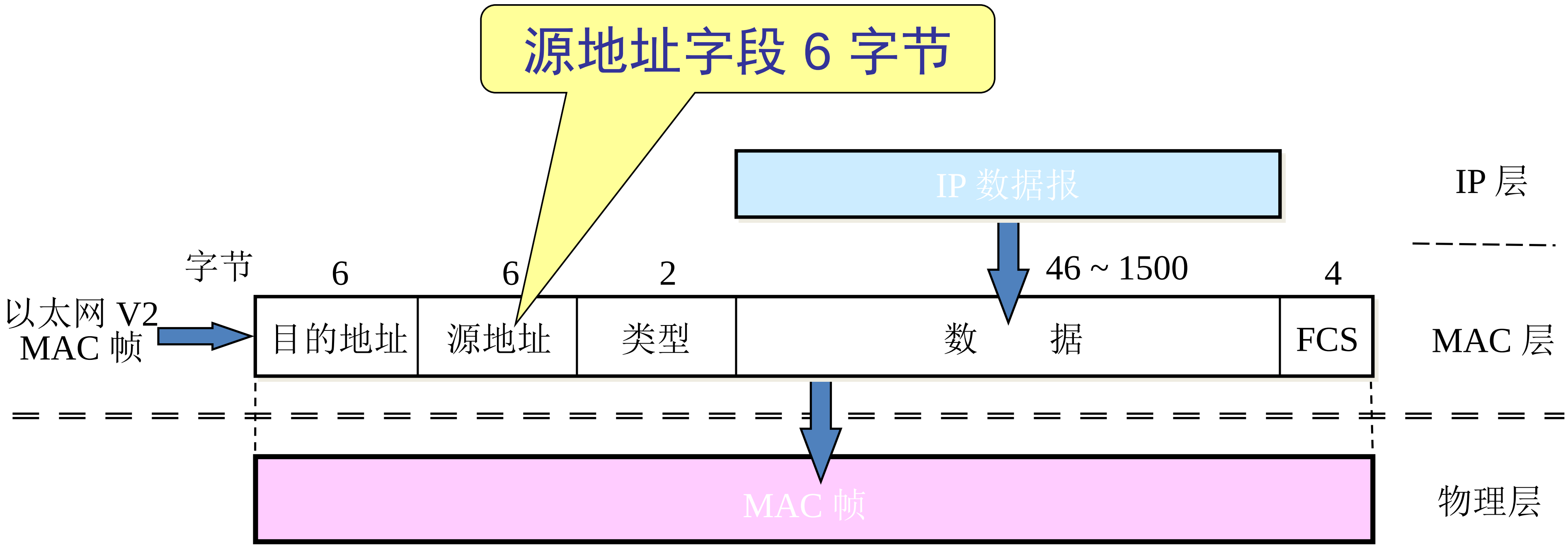


这种 802.3 + 802.2 帧已经较少使用
IP 数据报
IP 层
LLC 子层
MAC 子层
当长度/类型字段
表示长度时
802.2
LLC 帧
字节
1
1
1
DSAP
SSAP
控制
数 据
802.3
MAC 帧
字节
6
6
2
1
1
1
43 ~ 1497
4
目的地址
源地址
长度/类型
DSAP
SSAP
控制
数 据
FCS
IP 数据报
IP 层
以太网 V2
MAC 帧
字节
6
6
2
46 ~ 1500
4
目的地址
源地址
类型
数 据
FCS
MAC 层
插
入
8 字节
MAC 帧
物理层
7 字节
1 字节
1010101010101010 … 1010101010101010101011
前同步码
帧开始
定界符

以太网 V2 的 MAC 帧格式

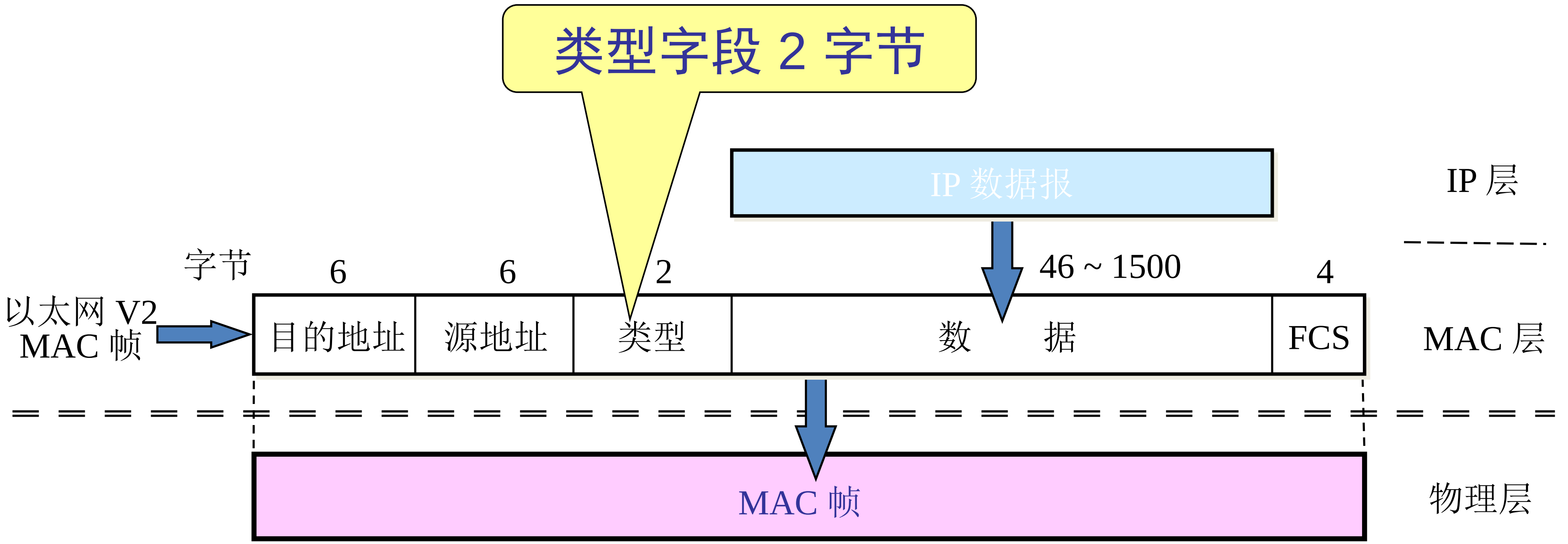


以太网 V2 的 MAC 帧格式



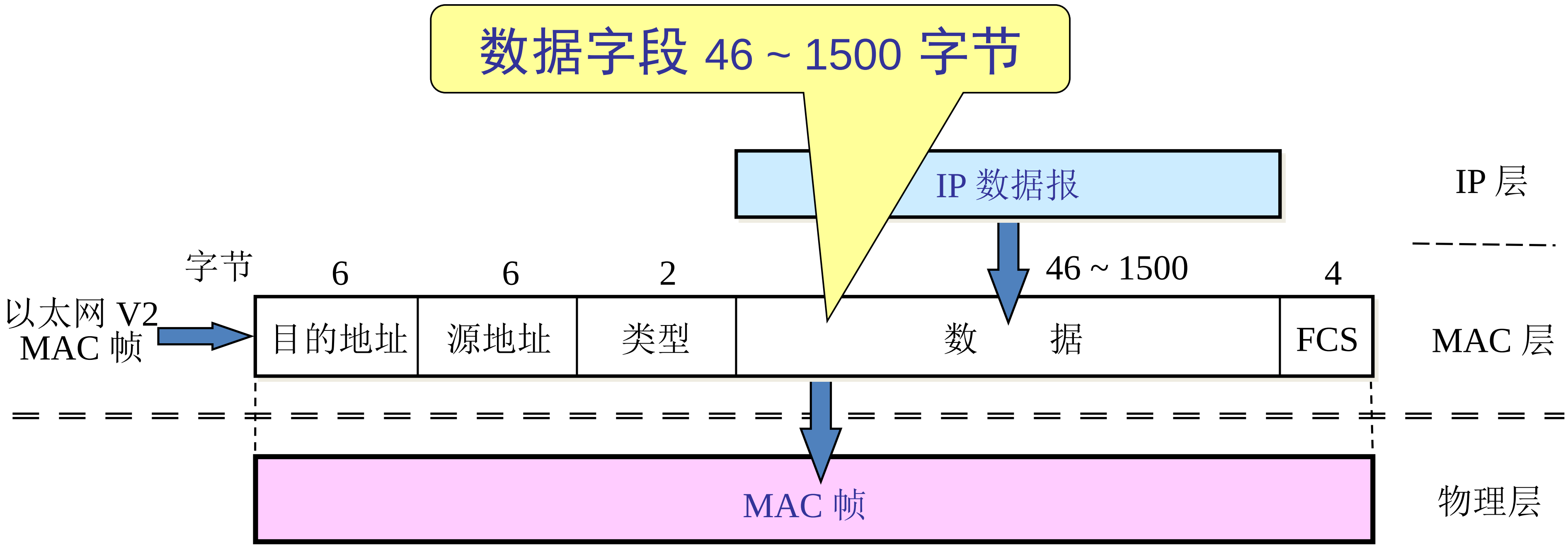
以太网 V2 的 MAC 帧格式

类型字段用来标志上一层使用的是什么协议，
以便把收到的 MAC 帧的数据上交给上一层的这个协议。



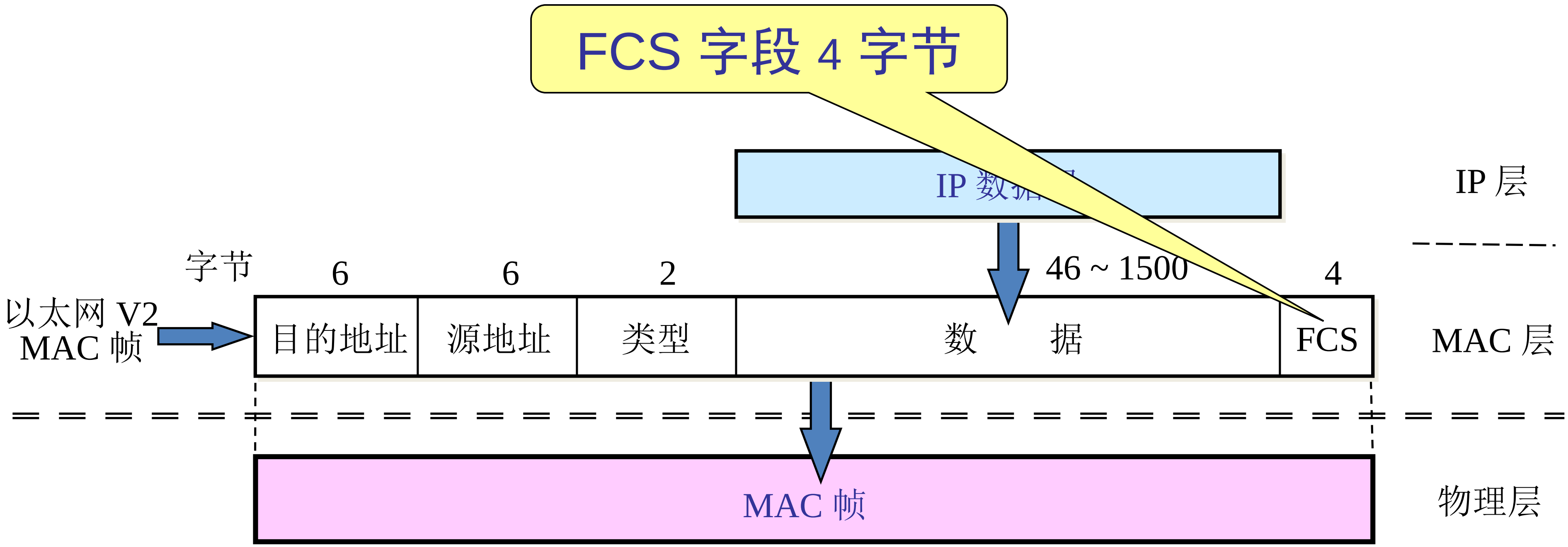
以太网 V2 的 MAC 帧格式

数据字段的正式名称是 MAC 客户数据字段
最小长度 64 字节 – 18 字节的首部和尾部 = 数据字段的最小长度



以太网 V2 的 MAC 帧格式

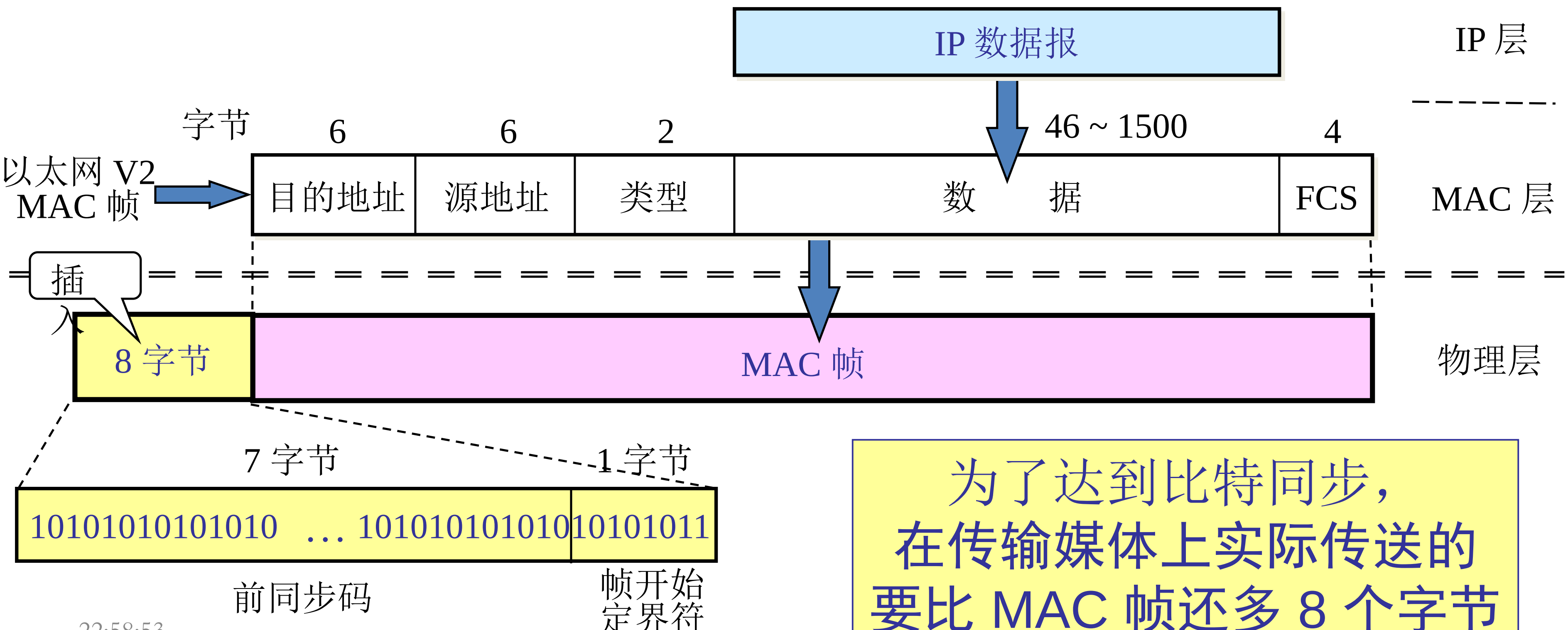
当传输媒体的误码率为 1×10^{-8} 时，
MAC 子层可使未检测到的差错小于 1×10^{-14}。



当数据字段的长度小于 46 字节时，
应在数据字段的后面加入整数字节的填充字段，
以保证以太网的 MAC 帧长不小于 64 字节。

以太网 V2 的 MAC 帧格式

在帧的前面插入的 8 字节中的第一个字段共 7 个字节，
是前同步码，用来迅速实现 MAC 帧的比特同步。
第二个字段是帧开始定界符，表示后面的信息就是MAC 帧。



为了达到比特同步，
在传输媒体上实际传送的
要比 MAC 帧还多 8 个字节

22:58:53

无效的 MAC 帧

- 数据字段的长度与长度字段的值不一致；
- 帧的长度不是整数个字节；
- 用收到的帧检验序列 FCS 查出有差错；
- 数据字段的长度不在 46 ~ 1500 字节之间。
- 有效的 MAC 帧长度为 64 ~ 1518 字节之间。
- 对于检查出的无效 MAC 帧就简单地丢弃。以太网不负责重传丢弃的帧。

帧间最小间隔

- 帧间最小间隔为 9.6 μs，相当于 96 bit 的发送时间。
- 一个站在检测到总线开始空闲后，还要等待 9.6 μs 才能再次发送数据。
- 这样做是为了使刚刚收到数据帧的站的接收缓存来得及清理，做好接收下一帧的准备。

4.3.3 Ethernet Performance

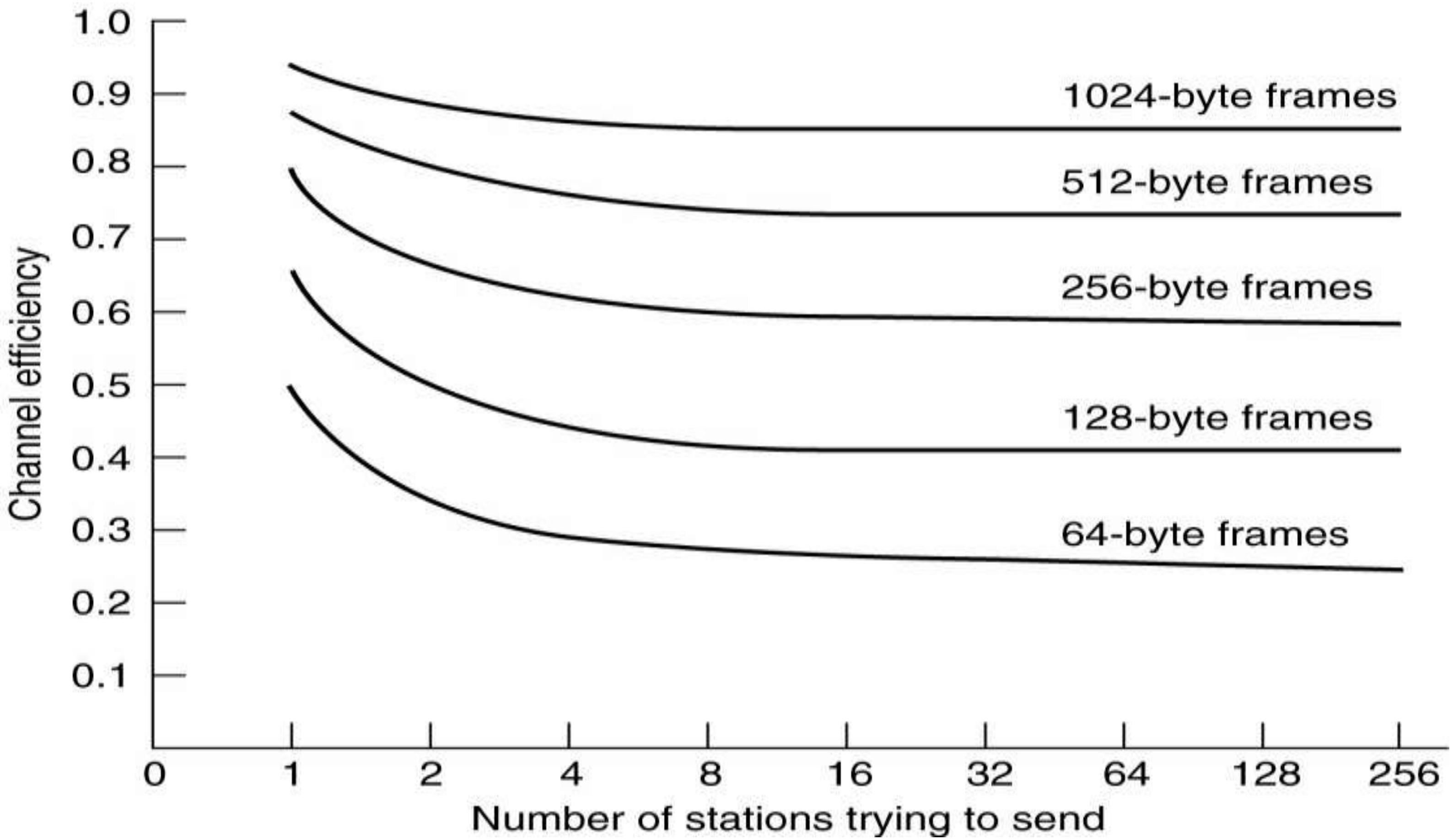


Figure 4-16. Efficiency of Ethernet at 10 Mbps with 512-bit slot times.

4.3.4 Switched Ethernet

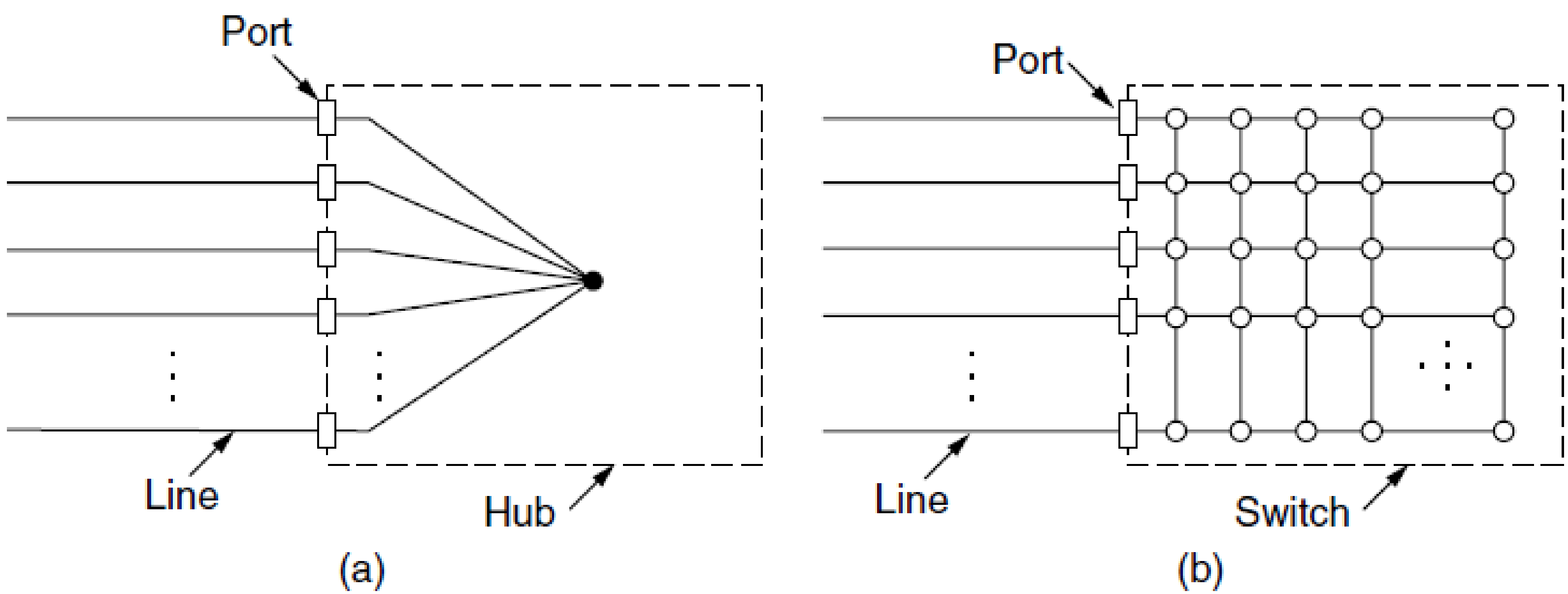


Figure 4-17. (a) Hub. (b) Switch.

Switched Ethernet (2)

- Collision Domain： In a hub, all stations are in the same collision domain; while in a switch, each port is a collision domain.

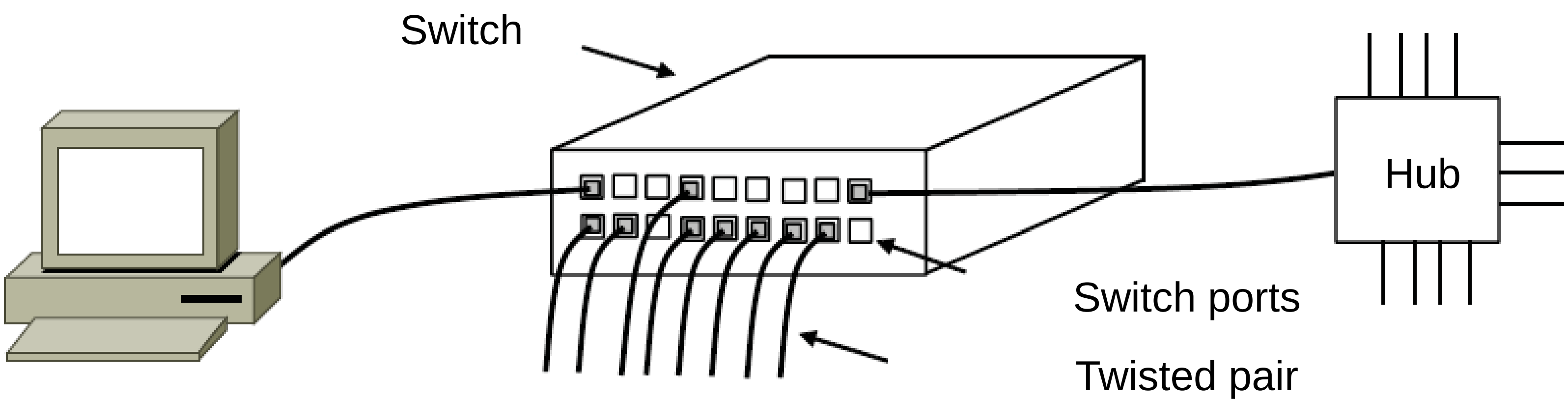


Figure 4-18. An Ethernet switch.

4.3.5 Fast Ethernet

- FDDI (Fiber Distributed Data Interface)
- Fibre Channel (note: Fibre, not Fiber, as British editor)
- Disadvantage of optical LANs(such as FDDI) make IEEE come up with **Fast Ethernet.** **[802.3(1980) based on Ethernet]**
- The basic idea: all **802.3u (1995)** use hubs and switches
- Wire types to support：
  - Category 3 twisted pair： 100Base-T4 （4 twisted pairs）
    - Advantage and disadvantage
  - Category 5 twisted pair： 100Base-TX （2 twisted pairs）
  - Often 100Base-T4 and 100Base-TX are called 100Base-T
  - Fiber： 100Base-FX

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

4.3.5 Fast Ethernet(2)

- Category 3 UTP scheme：100Base-T4 （4 twisted pairs）
  - 25MHz signaling speed
  - Transmitting 4 bits in each of the 25MHz to give 100Mbps
  - 10Base-T Ethernet
    - 20MHz signaling speed,
    - Manchester encoding,
    - Two clock periods for each bit of the 10Mbps
- Category 5 UTP scheme：100Base-TX （2 twisted pairs）
  - 125MHz signaling speed
  - 4B/5B:
    - 5 clock periods,
    - each contain one of two values,
    - yields 32 combinations
    - 16 of these combinations are used to transmit the four bit groups 0000,0001,… ,1111
  - Full duplex
  - Autonegotiation (10 or 100Mbps, half or full duplex)

4.3.5 Fast Ethernet(3)

- Hub：
  - Shared hub
  - Switched hub

4.3.6 Gigabit Ethernet

- Gigabit Ethernet ------**802.3z** (1998)
- Goals(the same as 802.3u): make Ethernet go 10 times faster yet remain backward compatible with existing Ethernet standards.
- All configurations of gigabit Ethernet are point-to-point rather than multidrop as in the original 10Mbps standard (see Fig.4-20)

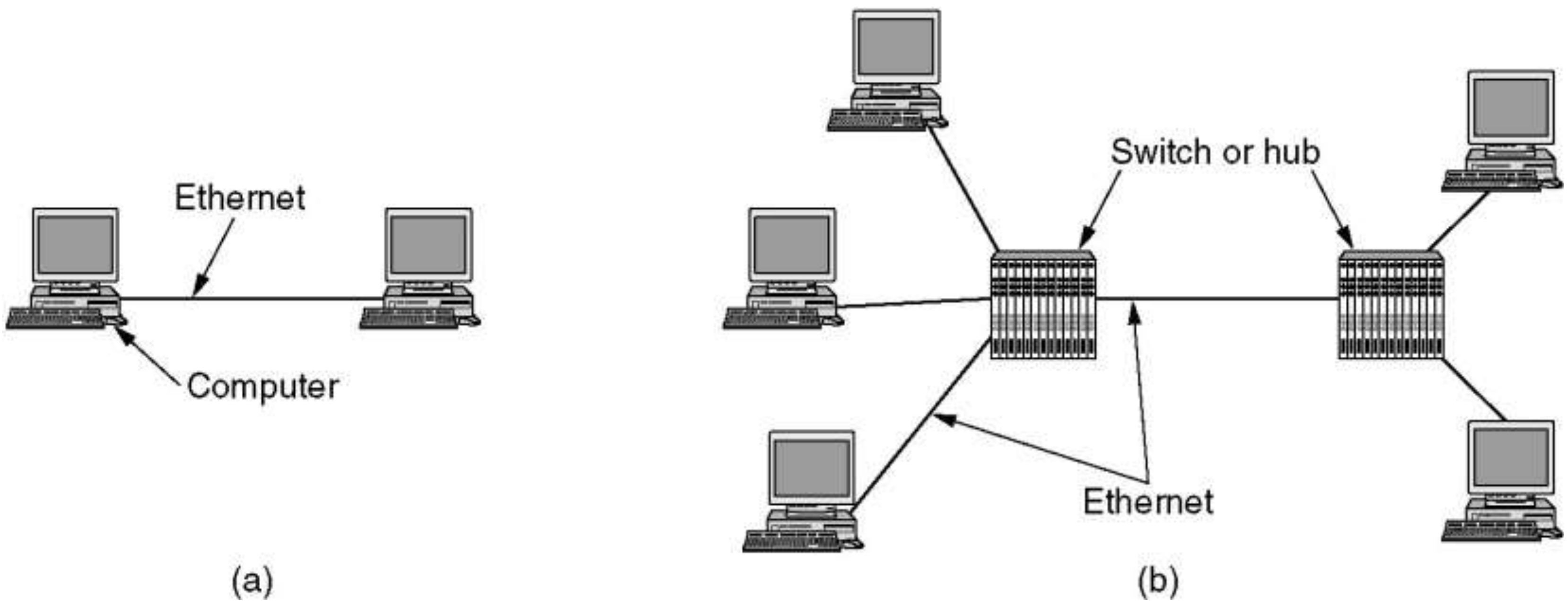


Fig4-20 (a) A two-station Ethernet. (b) A multistation Ethernet.

4.3.6 Gigabit Ethernet(2)

- Two different modes of operation:
  - **Full-duplex mode**: “normal” mode. Used in central switch. buffered. No contention, no CSMA/CD
  - **Half-duplex mode:** used with a hub. A hub does not buffer incoming frames. Collisions are possible, CSMA/CD protocol required. A minimum frame can now be transmitted 100 times faster than in classic Ethernet(10M→1000M), and the maximum distance is 100 times less, or 25 meters (2500m→25m).
- Two features to the standard to increase the radius:
  - **Carrier extension:** tells the hardware to add its own padding after the normal frame(64 bytes) to extend the frame to 512 bytes.
  - **Frame bursting:** allows a sender to transmit a concatenated sequence of multiple frames in a single transmission.
  - **➔These two features extend the radius of the network to 200 meters**

4.3.6 Gigabit Ethernet(3)

- Gigabit Ethernet supports both copper and fiber cabling, as listed in Fig.4-21.

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

Figure 4-21. Gigabit Ethernet cabling.

- **Three fiber diameters are permitted: 10μm,50μm and 62.5μm (microns).**

4.3.6 Gigabit Ethernet(4)

- **8B/10B:** 8-bit byte encoded as 10 bits. The following rules were used in choosing codewords:
  - No codeword may have more than four identical bits in a row.
  - No codeword may have more than six 0s or six 1s.
  - Need to balance 0s and 1s
- Gigabit Ethernets using 1000Base-T use a different scheme: four category 5 twisted pairs to allow four symbols to be transmitted in parallel. Each symbol is encoded using one of five voltage levels.
  - 125MHz
  - 4 pair x 2 data bits per clock cycle/pair x 125MHz =1000Mbps
  - Five voltage levels instead of four is to have combinations left over for framing and control purposes

4.3.6 Gigabit Ethernet(5)

- Flow control: PAUSE frame. Type: 0x8808; the first two bytes of the data field give the command; succeeding bytes provide the parameters, if any.

4.3.7 10 Gigabit Ethernet

- 10-Gigabit Ethernet-----802.3ae (2002)
- 10 Gigabit以太网与 10 Mb/s，100 Mb/s 和 1 Gb/s 以太网的帧格式完全相同。
- 10 Gigabit以太网还保留了 802.3 标准规定的以太网最小和最大帧长，便于升级。
- 10 Gigabit以太网不再使用铜线而只使用光纤作为传输媒体。
- 10 Gigabit以太网只工作在全双工方式，因此没有争用问题，也不使用 CSMA/CD 协议。

- Coming on new standard for **40Gbps and 100Gbps**

4.3.7 10 Gigabit Ethernet(2)

Name	Cable	Max. segment	Advantages
10GBase-SR	Fiber optics	Up to 300 m	Multimode fiber (0.85μ)
10GBase-LR	Fiber optics	10 km	Single-mode fiber (1.3μ)
10GBase-ER	Fiber optics	40 km	Single-mode fiber (1.5μ)
10GBase-CX4	4 Pairs of twinax	15 m	Twinaxial copper
10GBase-T	4 Pairs of UTP	100 m	Category 6a UTP

Figure 4-22. 10-Gigabit Ethernet cabling

4.3.x 40/100 Gigabit Ethernet

- **THE IEEE** Standards Association has ratified the IEEE Standard **802.3ba** that covers 40 gigabit and 100 gigabit Ethernet (40GbE and 100GbE).
- It was ratified **in June 17,2010**.

IEEE 802.2: Logical Link Control (*)

- **LLC(Logical Link Control)**: upper half of the data link layer

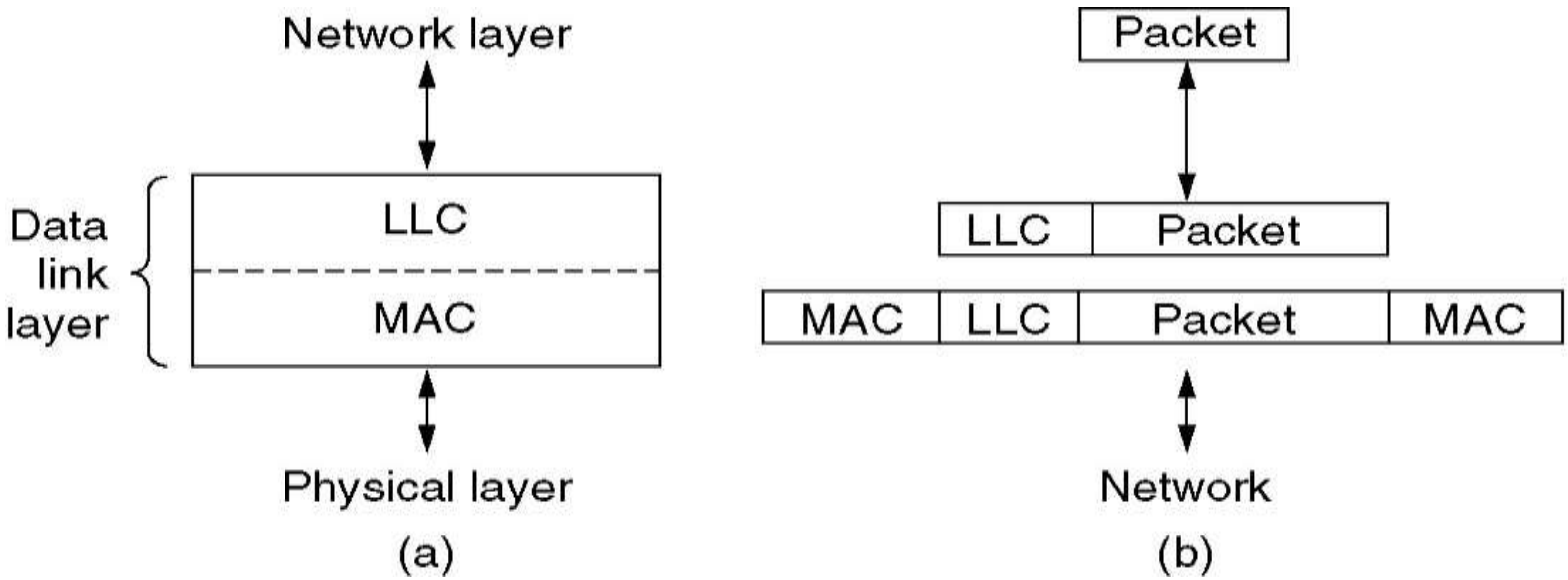


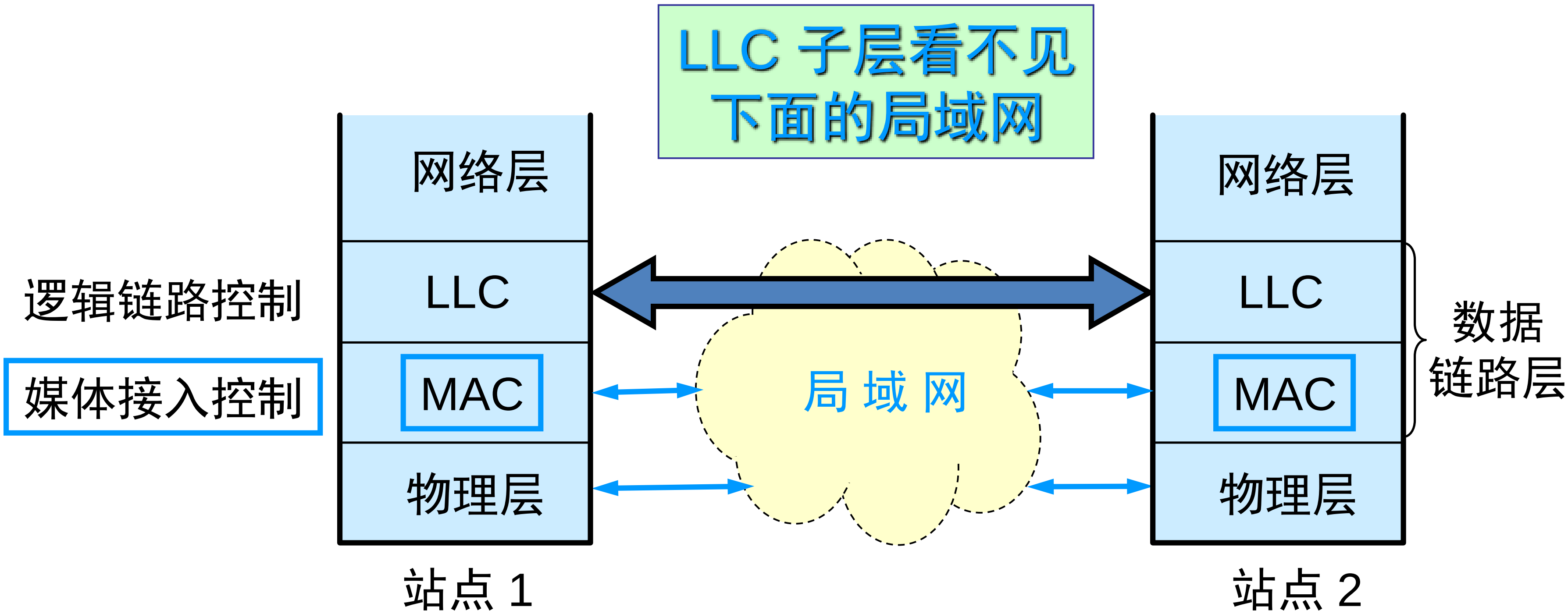
Figure 4-24. (a) Position of LLC. (b) Protocol formats.

- Service options:
  - unreliable datagram service
  - acknowledged datagram service
  - reliable connection-oriented service

数据链路层的两个子层

- 为了使数据链路层能更好地适应多种局域网标准，802 委员会就将局域网的数据链路层拆成两个子层：
  - 逻辑链路控制 LLC (Logical Link Control)子层
  - 媒体接入控制 MAC (Medium Access Control)子层。
- 与接入到传输媒体有关的内容都放在 MAC 子层，而 LLC 子层则与传输媒体无关，不管采用何种协议的局域网对 LLC 子层来说都是透明的

局域网对 LLC 子层是透明的



以后一般不考虑 LLC 子层

- 由于TCP/IP 体系经常使用的局域网是 DIX Ethernet V2 而不是 802.3 标准中的几种局域网，因此现在 802 委员会制定的逻辑链路控制子层 LLC（即 802.2 标准）的作用已经不大了。
- 很多厂商生产的网卡上就仅装有 MAC 协议而没有 LLC 协议。

4.3.8 Retrospective on Ethernet

- Simple and flexible
- cheap
- easy to maintain
- internetworking easily with TCP/IP

4.4 Wireless LANs

- The 802.11 Protocol Stack
- The 802.11 Physical Layer
- The 802.11 MAC Sublayer Protocol
- The 802.11 Frame Structure
- Services
- Products: Cisco, Aruba, H3C, Huawei, Linksys, D-Link, Netgear …

4.4.1 802.11 Architecture and Protocol Stack (1)

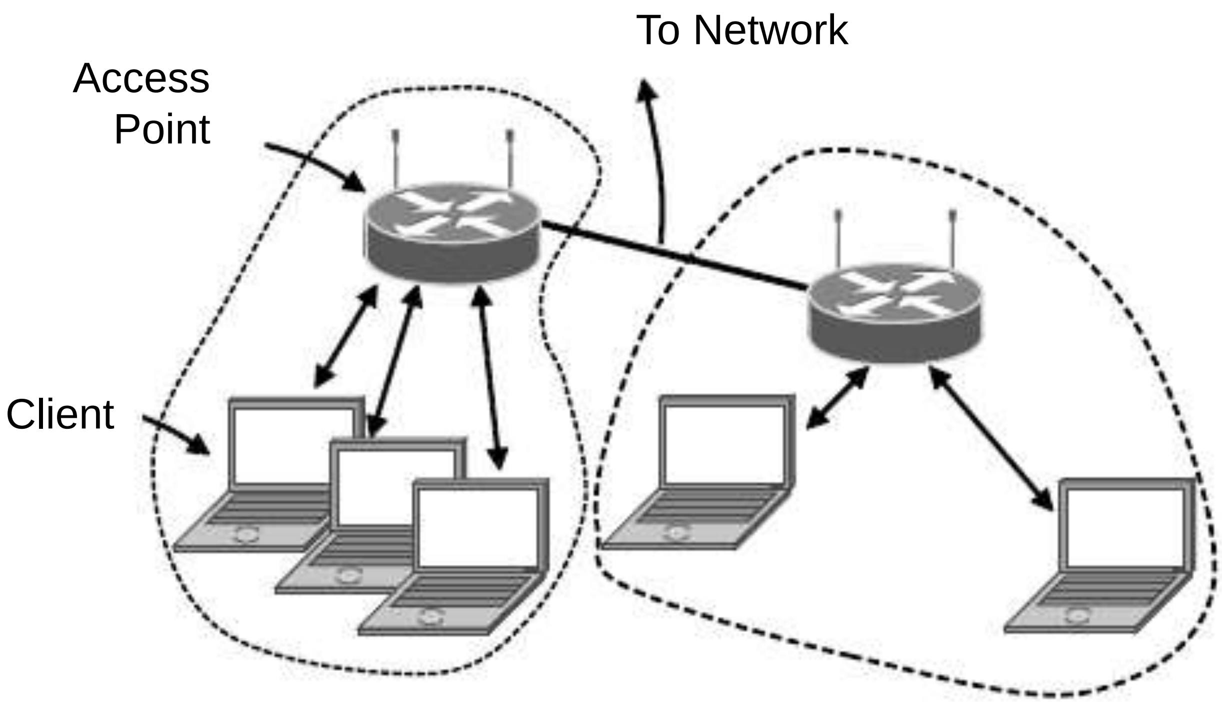


Figure 4-23 802.11 architecture – (a) infrastructure mode

4.4.1 802.11 Architecture and Protocol Stack (2)

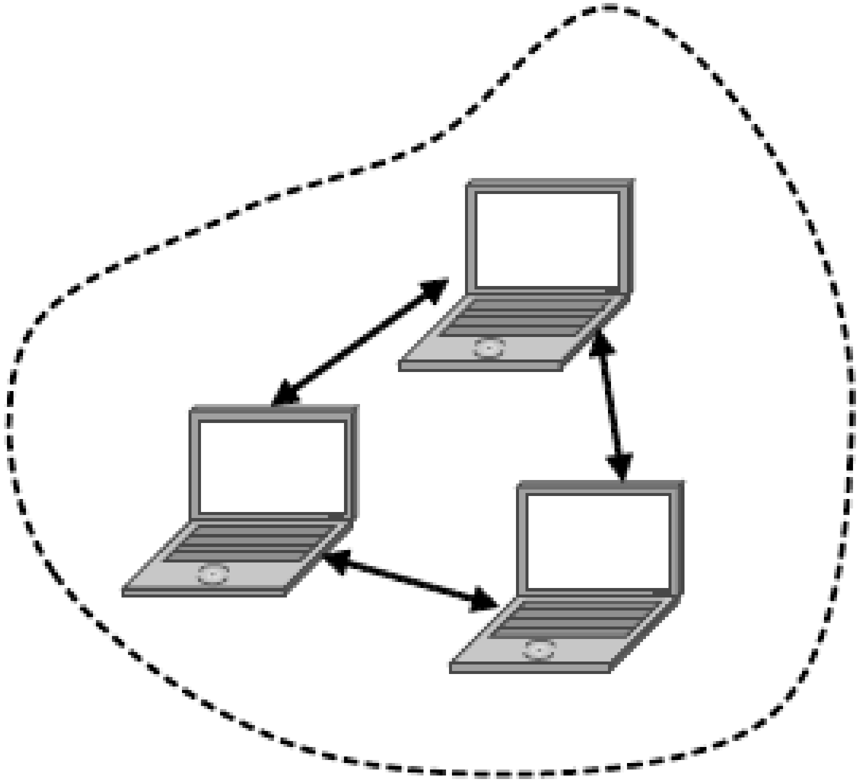


Figure 4-23 Figure 4-23 802.11 architecture – (b) ad-hoc mode

4.4.1 The 802.11 Architecture and Protocol Stack(3)

- Protocol stack structure [see fig.4-24]
  - MAC sublayer determines how the channel is allocated
  - LLC sublayer hide the difference between 802 variants

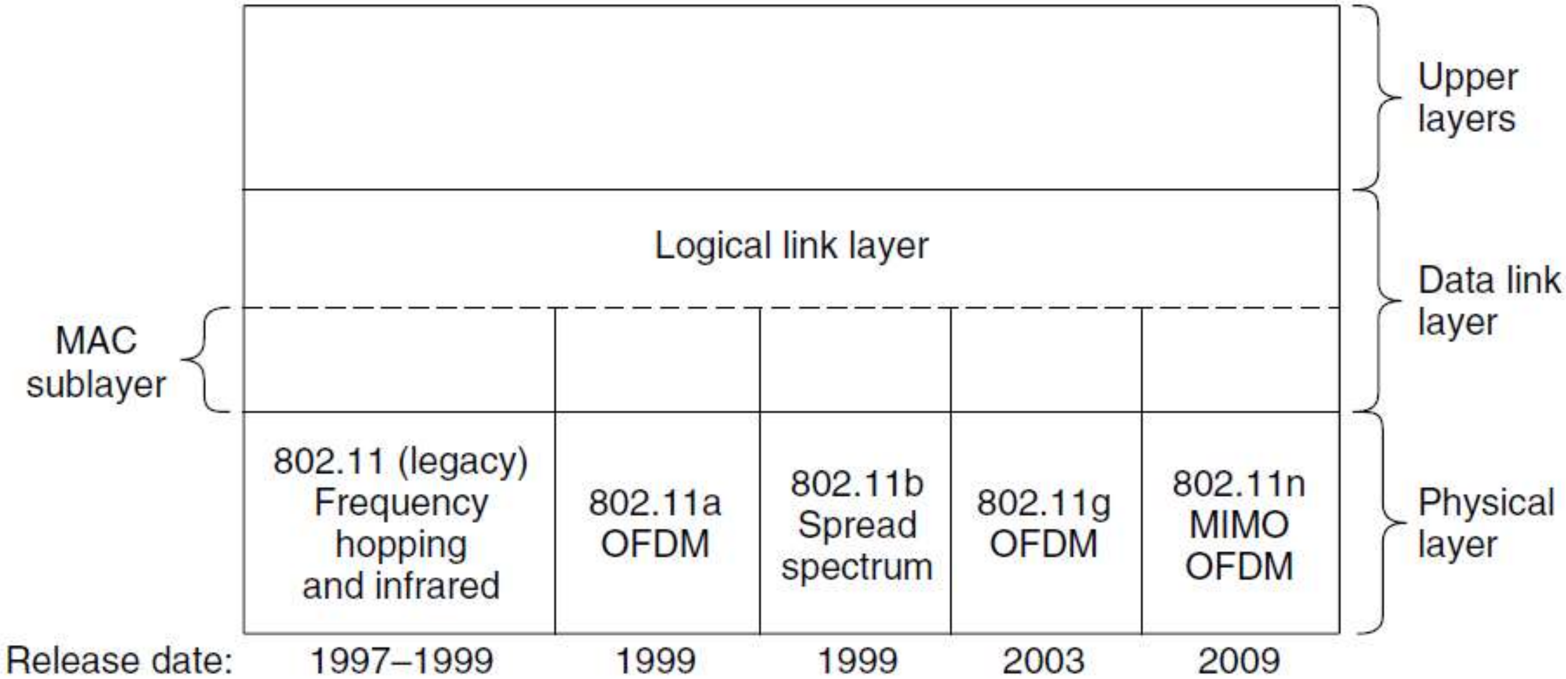


Figure 4-24 Part of the 802.11 protocol stack.

- FHSS(Frequency Hopping Spread Spectrum，跳频扩频技术)
- DSSS (Direct Sequence Spread Spectrum，直接序列扩频技术)
- OFDM (Orthogonal Frequency Division Multiplexing， 正交频分复用)
- HR-DSSS (High Rate Direct Sequence Spread Spectrum，高速直接序列扩频技术)
- **MIMO OFDM** (Multiple Input Multiple Output OFDM) , 802.11n, ratifed in Oct. 2009, use 4 antennas, rates up to 600Mbps

4.4.2 The 802.11 Physical Layer

- Infrared: diffused transmission, two speeds:
  - 1 Mbps: takes 2 bits and produces a 16-bit codeword containing fifteen 0s and a single 1, Gray code
  - 2 Mbps: takes 2 bits and produces a 4-bit codeword, also only a single 1
- FHSS(Frequency Hopping Spread Spectrum,跳频扩频技术):
  - uses 79 channels, each 1 MHz wide, starting at the low end of the 2.4-GHz ISM band. (ISM: Industrial, Scientific, Medical)
  - Pseudorandom number generator,dwell time
- DSSS(Direct Sequence Spread Spectrum,直接序列扩频技术):
  - Each bit as 11 chips, Barker sequence, phase shift modulation
  - Similar to the CDMA technology
  - 1 or 2Mbps

4.4.2 The 802.11 Physical Layer

- OFDM(Orthogonal Frequency Division Multiplexing,正交频分复用):
  - IEEE 802.11a
  - Splitting signal into many narrow bands, better immunity to narrowband interference and possibility of using noncontiguous bands
  - Up to 54Mbps in the wider 5 GHz ISM band
  - 216 data bits are encoded into 288-bit symbols
- HR-DSSS(High Rate Direct Sequence Spread Spectrum,高速直接序列扩频技术):
  - IEEE 802.11b
  - Uses 11 million chips/sec to achieve 11 Mbps in the 2.4-GHz band
  - Data rates supported: 1, 2, 5.5, and 11 Mbps.
  - For 1 and 2Mbps, run at 1M baud with 1 and 2 bits per baud
  - For 5.5 and 11Mbps, run at 1.375M baud with 4 and 8 bits per baud

4.4.2 The 802.11 Physical Layer

- IEEE 802.11g, uses OFDM modulation method of 802.11a but operates in the narrow 2.4-GHz ISM band along with 802.11b
  - OFDM modulation method but run at 2.4GHz ISM band
  - An enhanced version of 802.11b, compatible with 802.11b
  - In theory it can operate at up to 54 Mbps
  - 54Mbps, 11Mbps …
- **MIMO** (Multiple Input Multiple Output)
  - 802.11n, ratifed in Oct. 2009
  - use 4 antennas， 40MHz
  - 802.11ac, ratifed in Feb.18, 2012

4.4.3 The 802.11 MAC Sublayer Protocol

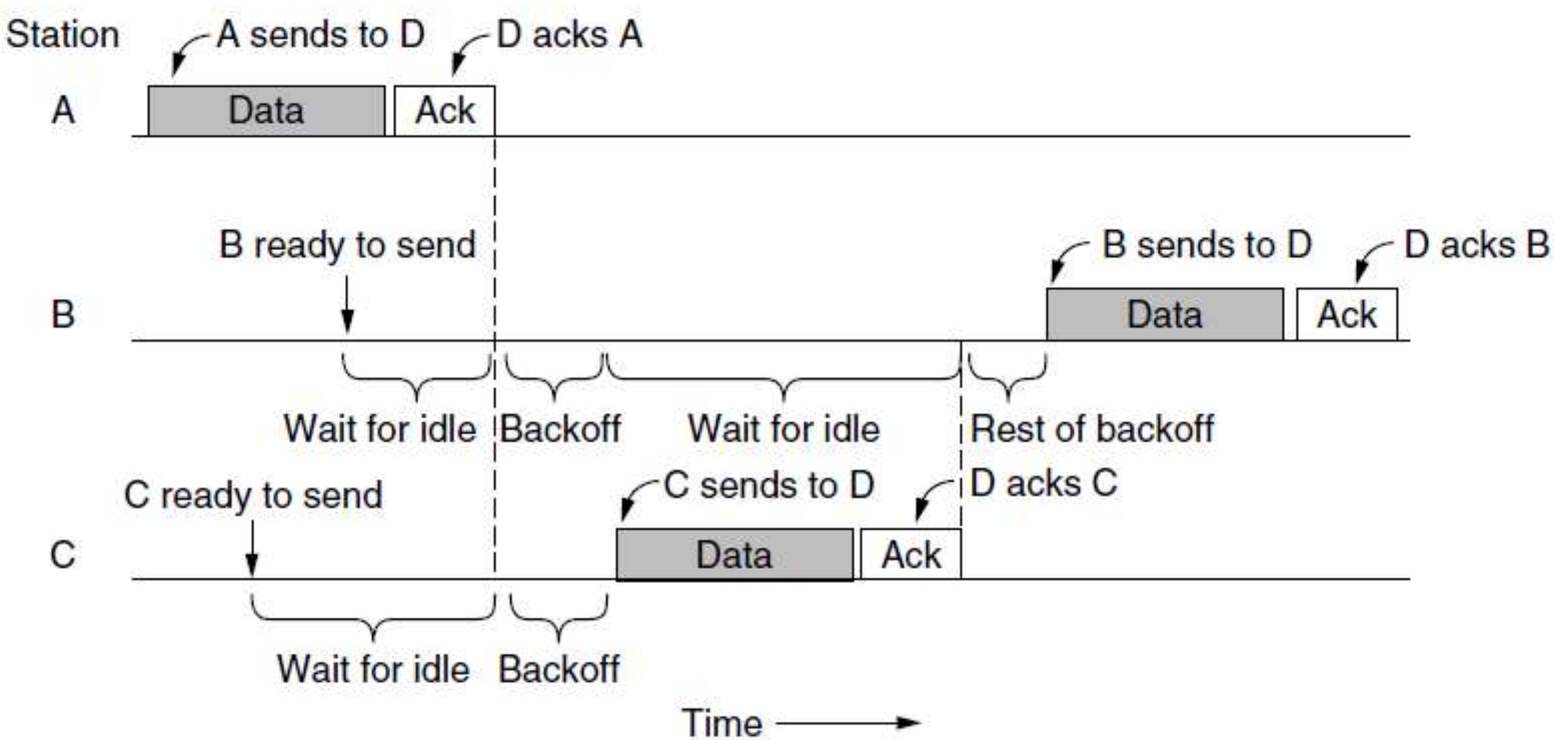


Figure 4-25 Sending a frame with CSMA/CA.

4.4.3 The 802.11 MAC Sublayer Protocol

- Problems with wireless:
  - Hidden station problem: transmissions in one part of a cell may not be received elsewhere in the same cell [see Fig.4-26(a)]
  - Exposed station problem: just the reverse [see Fig.4-26(b)]
  - half duplex, cannot transmit and listen for noise bursts at the same time on a single frequency.

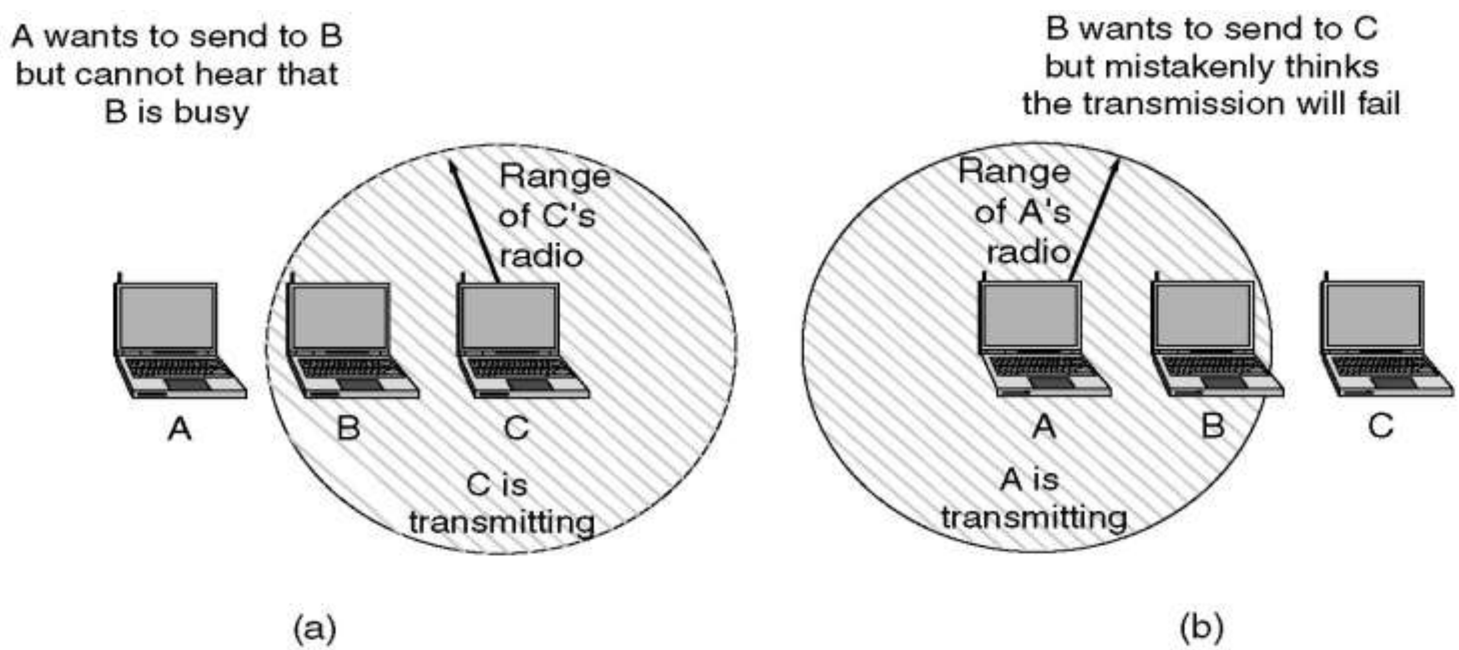
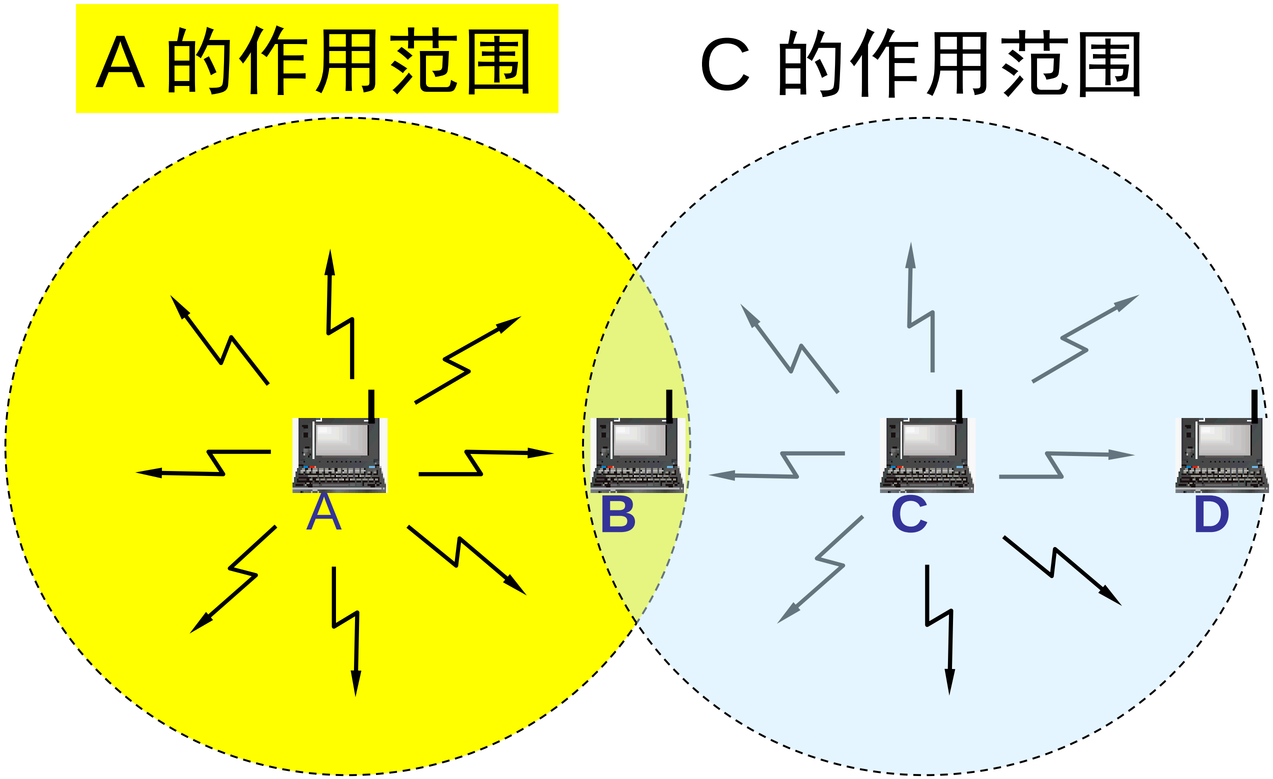


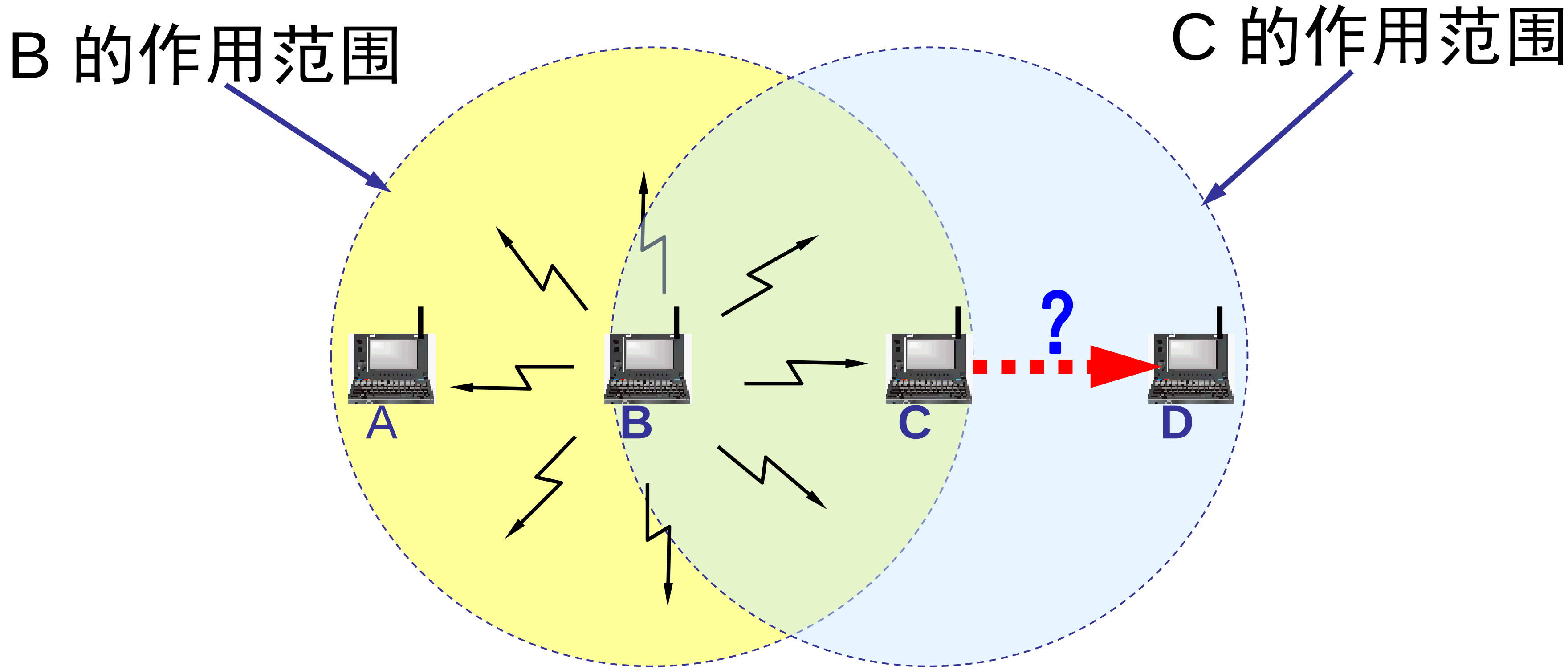
Figure 4-26. (a) The hidden station problem. (b) The exposed station problem.

这种未能检测出媒体上已存在的信号的问题叫做**隐蔽站问题**(hidden station problem)



当 A 和 C 检测不到无线信号时，都以为 B 是空闲的，因而都向 B 发送数据，结果发生碰撞。

其实 B 向 A 发送数据并不影响 C 向 D 发送数据
这就是暴露站问题(exposed station problem)



B 向 A 发送数据，而 C 又想和 D 通信。
C 检测到媒体上有信号，于是就不敢向 D 发送数据。

4.4.3 The 802.11 MAC Sublayer Protocol

- Two modes of opertion to deal with hidden/ exposed station problem :
  - **DCF**(Distributed Coordination Function): not use central control
  - **PCF**(Point Coordination Function): uses the base station to control all activity in its cell.
  - All must support DCF but PCF is optional.
- **CSMA/CA**(CSMA with Collision Avoidence): employs DCF, uses both physical and virtual channel sensing
  - **method 1**: senses channel, if idle, just starts transmitting. Does not sense channel while transmitting. If collision occurs, wait random time, using Ethernet binary exponetial backoff algorithm
  - **method 2**: based on MACAW, ues virtual channel sensing[see Fig.4-27]
    - situation: A wants to send to B. C is a station within range of A. D is a station within range of B but not within range of A.

4.4.3 The 802.11 MAC Sublayer Protocol

- A sends RTS frame to B to request permission, B sends CTS frame back to grant permission. Then A sends data, and starts an ACK timer. (假定: C在A附近，D在B附近）
- C receives RTS frame ----->assert NAV(Network Allocation Vector)
- D hears CTS----->assert NAV (NAV 是大致估计的时间）

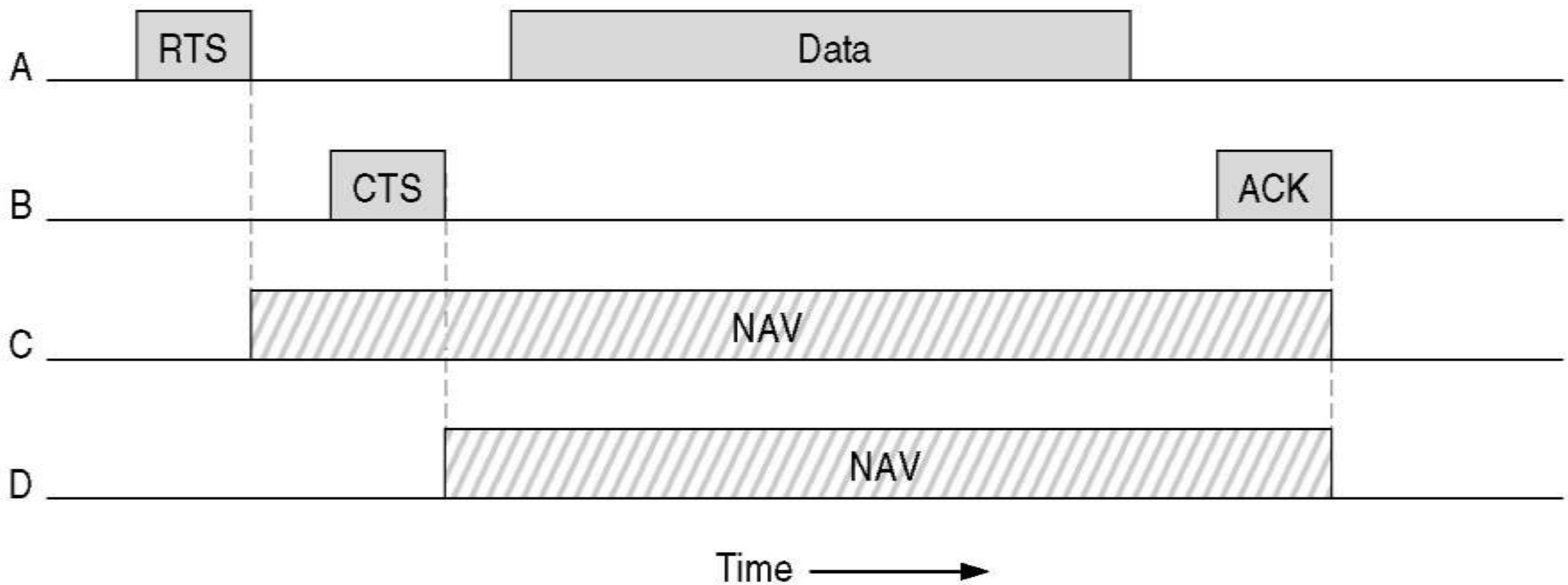


Figure 4-27. The use of virtual channel sensing using CSMA/CA.

4.4.3 The 802.11 MAC Sublayer Protocol

- Wireless networks are noisy and unreliable. If a frame is too long, it is very difficult to getting through undamaged.
- Fragment: individually numbered and acknowledged using stop-and-wait protocol.
- Fragment burst. [see Fig. 4-xx.]
- Fragment increases the throughput by restricting retransmissions to bad fragments rather than the entire frame

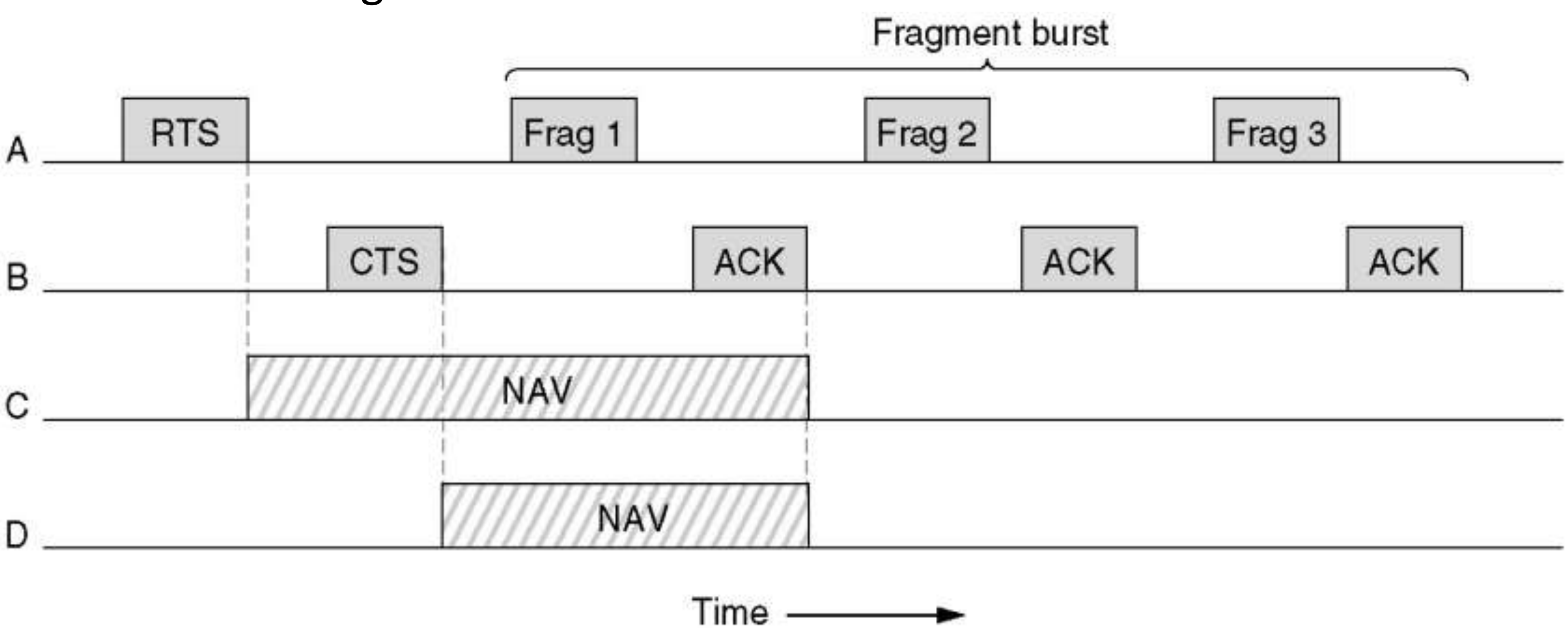


Figure 4-xx. A fragment burst.

4.4.3 The 802.11 MAC Sublayer Protocol

- PCF mode: polling, no collisions
  - base station broadcast a beacon frame periodically
  - power management: tells a station to go to sleep
- coexistence of PCF and DCF: [see Fig. 4-28]（优先等级）
  - SIFS(Short InterFrame Spacing): allow the parties in a single dialog the chance to go first
  - PIFS(PCF InterFrame Spacing): the base station may send a **beacon frame** or **poll frame**. sends data frame or fragment sequence to finish, gives base station a chance to grab the channel when done.
  - DICF(DCF InterFrame Spacing): apply usual contension rules, binary exponential backoff if needed.
  - EIFS(Extended InterFrame Spacing): report the bad frame

4.4.3 The 802.11 MAC Sublayer Protocol

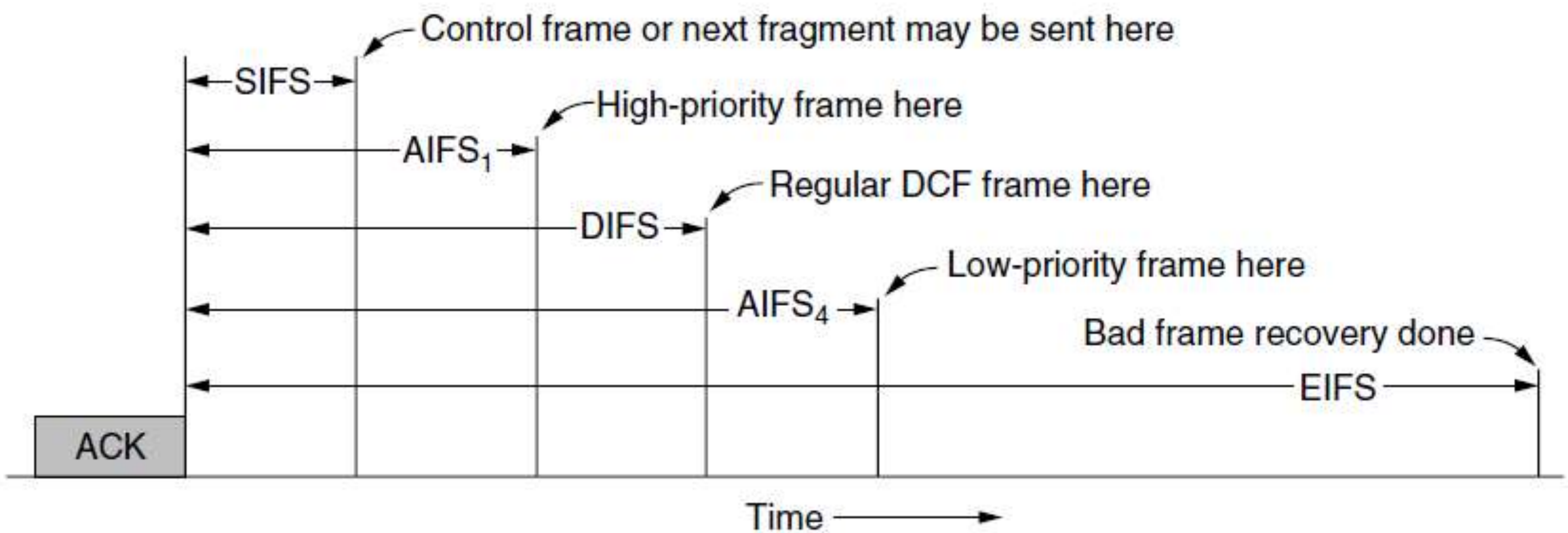


Figure 4-28. Interframe spacing in 802.11.

4.4.4 The 802.11 Frame Structure(1)

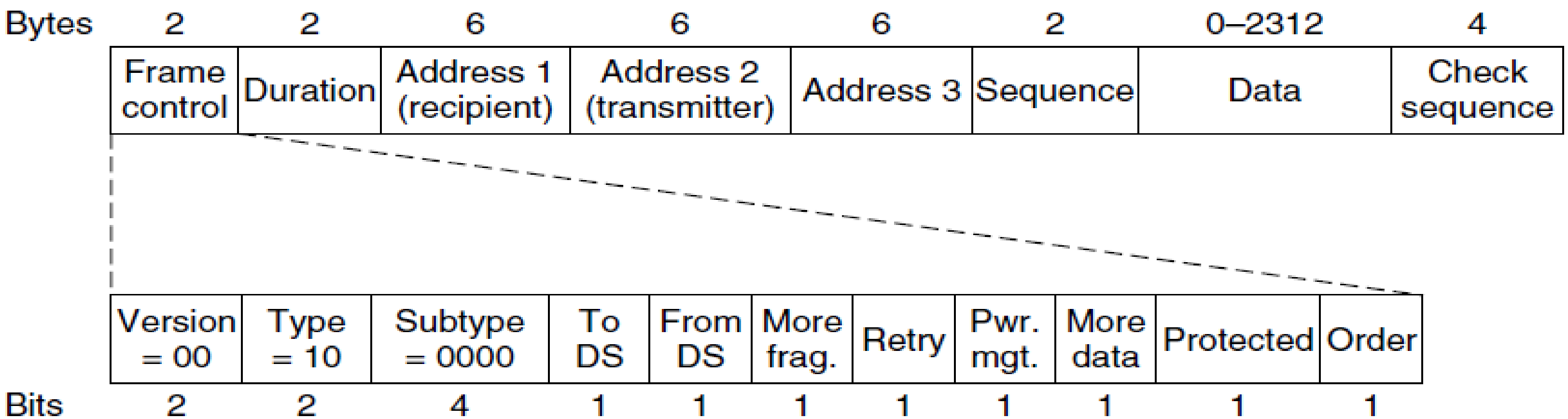


Figure 4-29. The 802.11 data frame.

- **Data frame:**
  - *Type*: **data, control, or management**; *Subtype*: RTS or CTS;
  - *MF*: more fragments will follow; *Retry*: retransmission;
  - *Pwr*: sleep state; *More*: additional frames;
  - *W*: encrypted usign WEP(Wired Equivalent Privacy); *O*: processed strictly in order
  - *Druation*: time the frame and acknowledgement takes (occupy the channel);
  - *four Address*: source and destination, and those for base station
  - *Sequence*: 16 bits, 12 for frame, 4 for fragment.

4.4.4 The 802.11 Frame Structure(2)

- Management frames: similar to data frames, except without one of the base station addresses, because management frames are restricted to a single cell.
- Control frames: shorter still
  - only one or two addresses
  - no *Data* field, and no *Sequence* field
  - *Subtype* field: usually **RTS, CTS**, OR **ACK**
  - Note: **RTS** means Request To Send
    CTS means Clear To Send

4.4.5 Services

- **Distribution services**: relate to managing cell membership and interacting with stations outside the cell
  - Association（连接）
  - Disassociation（取消连接）
  - Reassociation （重新连接）
  - Distribution （分配）
  - Integration （整合）
- **Intracell Services:** relate to activity within a single cell
  - Authentication （身份认证）-- WPA2(WiFi Protected Access 2) -- AES
  - Deauthentication （取消身份认证）
  - Privacy （ 加密）
  - Data Delivery （数据传递）

  - QoS traffic scheduling service
  - Transmit power control
  - Dynamic frequency selection

4.5 Broadband Wireless (*)

- Comparison of 802.11 and 802.16
- The 802.16 Protocol Stack
- The 802.16 Physical Layer
- The 802.16 MAC Sublayer Protocol
- The 802.16 Frame Structure

4.5.1 Comparison of 802.11 and 802.16

- Both were designed to provide high-bandwidth wireless communications
- differences:
  - 802.16 serves buildings, not mobile. Much of 802.11 deals with mobility
  - buildings can have many computers, so full-duplex; while notebook(802.11) avoids full-duplex to keep cost low
  - 802.16: varying distances, multiple modulation schemes, open communication, security and privacy
  - more users in each cell, so more spectrum is needed
  - quality of service:
    - 802.11 provides some support for real-time traffic, but not really designed for telephony and heavy-duty multimedia usage
    - 802.16 is expected to support these applications completely
  - In short, 802.11: mobile Ethernet, while 802.16: wireless, but stationary, cable television

4.5.2 The 802.16 Protocol Stack

- Physical layer: [see Fig. 4-31]
  - bottom sublayer: deals with transmission.
  - Convergence sublayer: to hide the different technologies from the data link layer
  - Two physical layer protocols: 802.16a standard support OFDM in the 2-to-11 GHz frequency range; 802.16b operate in the 5-GHz ISM band
- Data link layer consists of three sublayers:
  - Bottom one deals with privacy and security
  - MAC sublayer common part: main protocol such as channel management located. The model is that the base station controls the system
  - service-specific convergence sublayer: take the place of the logical link sublayer. Interface to the network layer. Integrate with both datagram protocols (e.g. PPP, IP and Ethernet) and ATM.

Comparison of 802.16 with 802.11 and 3G

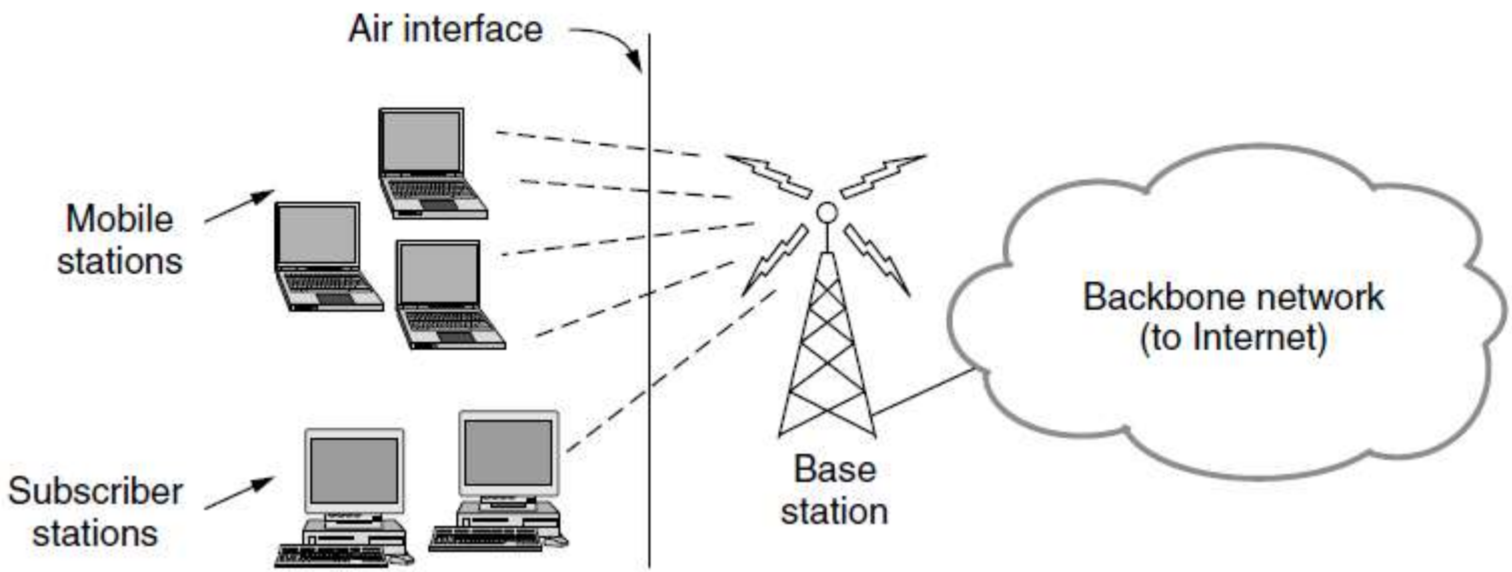


Figure 4-30. The 802.16 Architecture

4.5.2 The 802.16 Protocol Stack

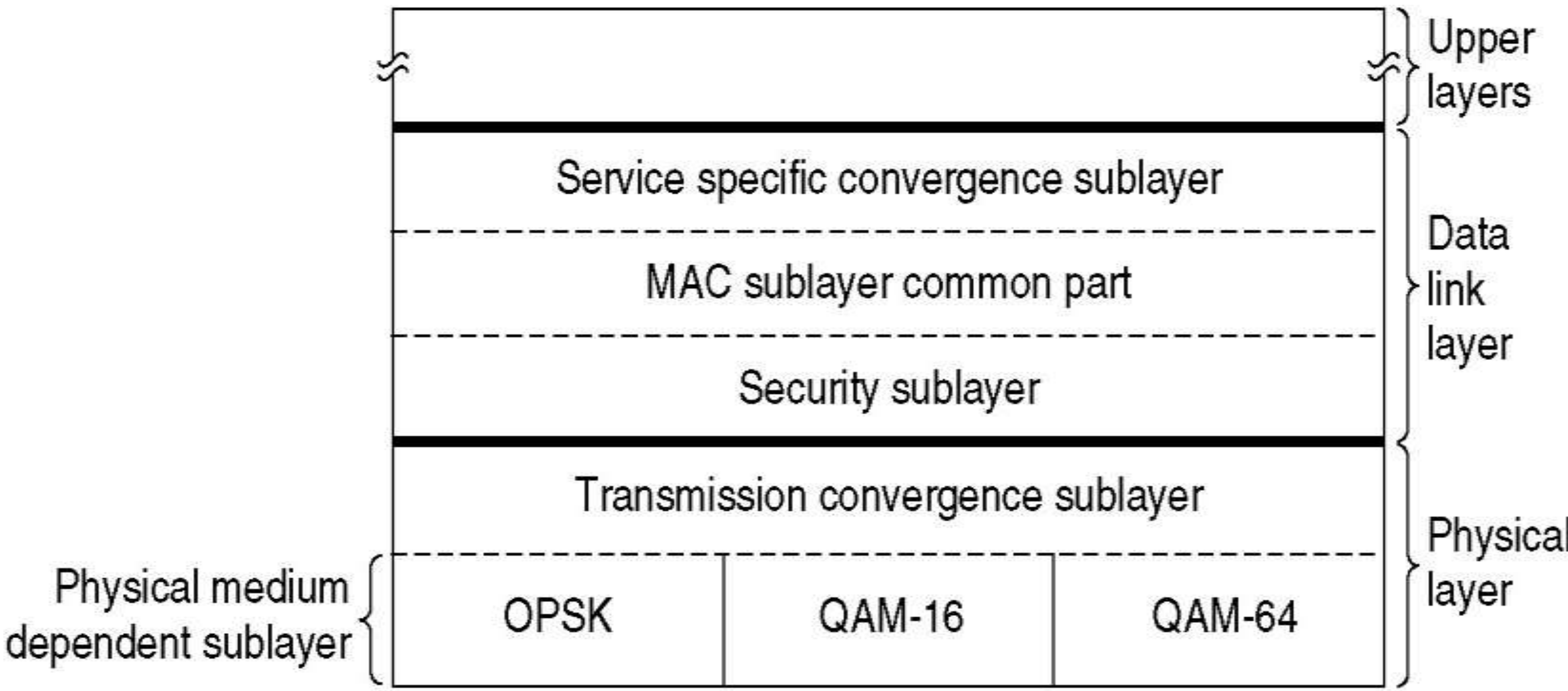


Figure 4-31. The 802.16 Protocol Stack.

4.5.3 The 802.16 Physical Layer

- Most WiMAX spectrum around either: 3.5GHz or 2.5GHz
  - these millimeter waves travel straight, so base station have multiple antennas, each pointing at a different sector, see Fig. 4-32. Each sector is independent.
- 802.16 operate from 2GHz to 11GHz

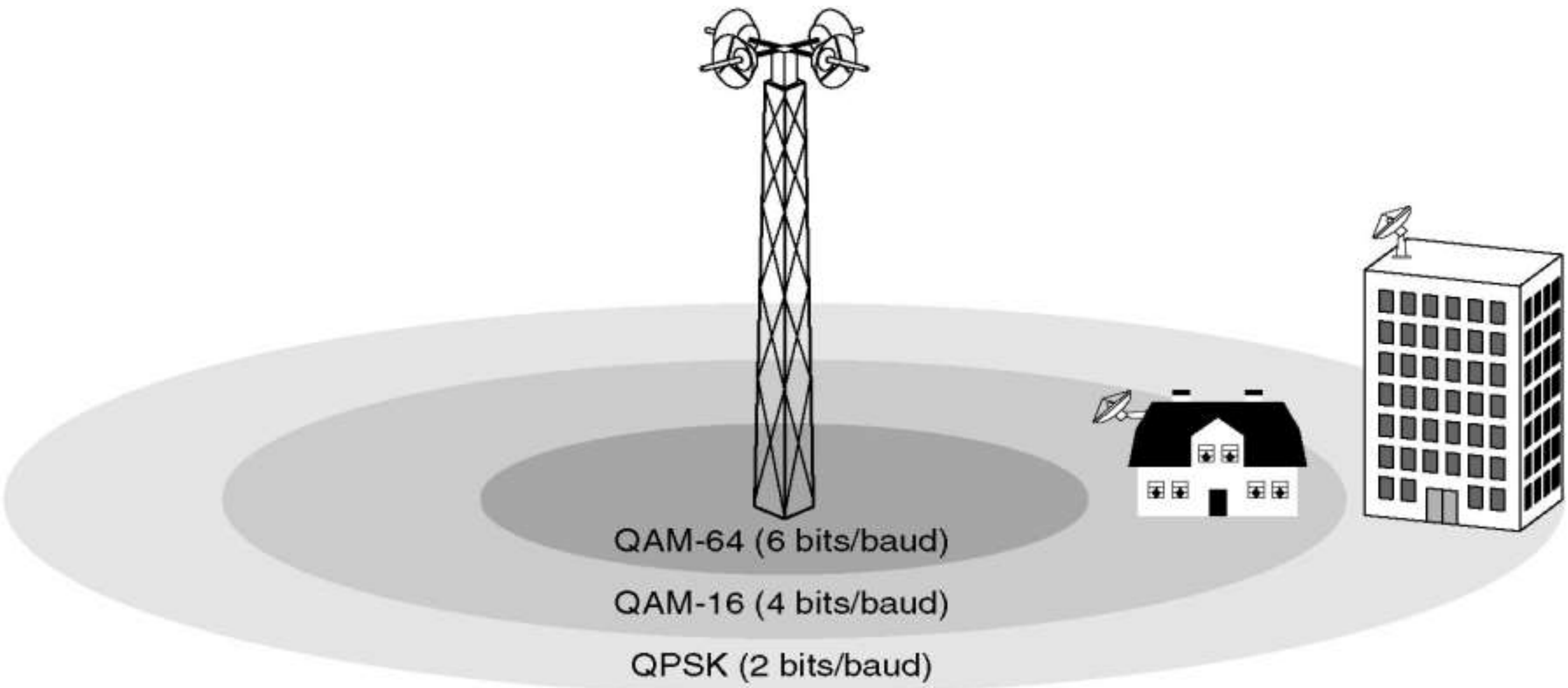


Figure 4-xx The 802.16 transmission environment.

4.5.3 The 802.16 Physical Layer

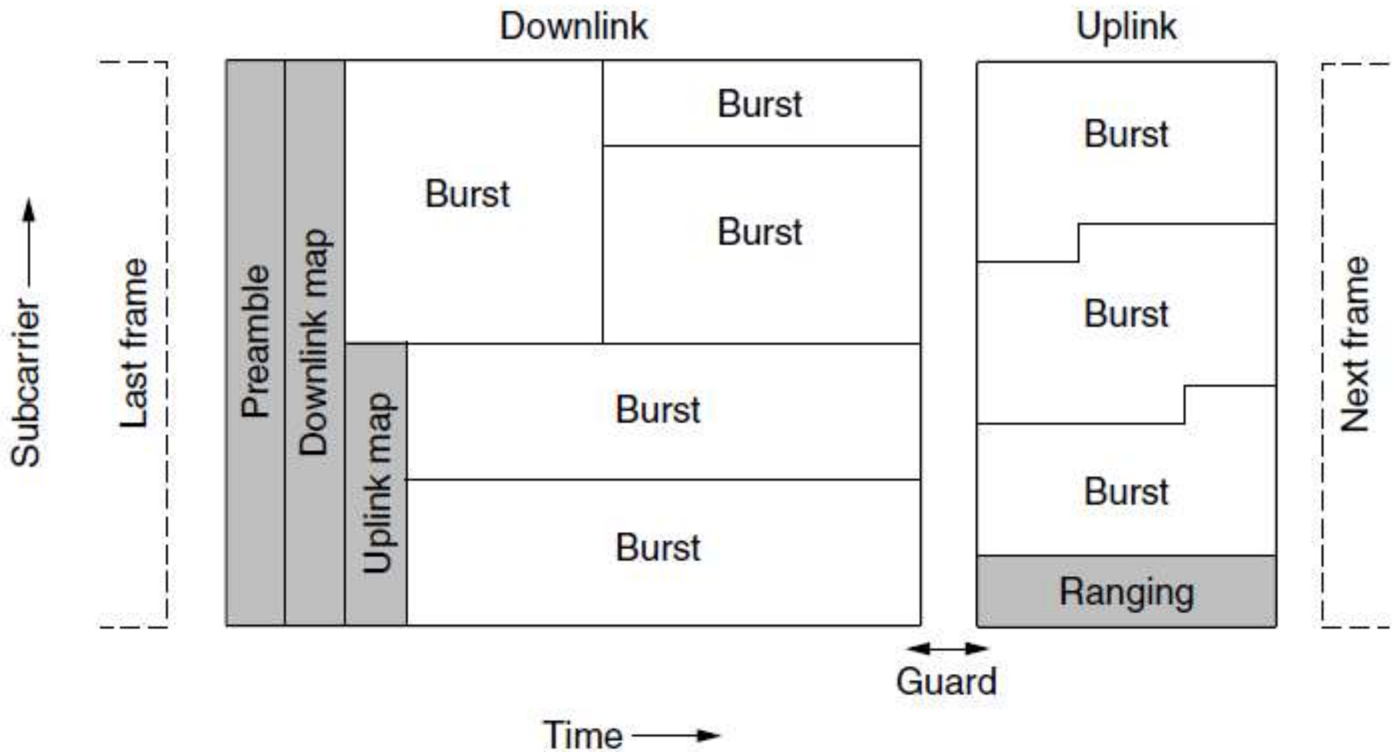


Figure 4-32 Frames structure for OFDMA with time division duplexing.

4.5.3 The 802.16 Physical Layer

- Signal length in the millimeter band falls off sharply with distance from base station, and signal-to-noise ratio also drops. So, 802.16 employs different modulation schems:
  - close-in: QAM-64 is used, with 6 bits/baud
  - medium-distance: QAM-16 is used, with 4 bits/baud
  - distant: QPSK is used, with 2 bits/baud
- 802.16 provides a more flexible way to allocate the bandwidth:
  - FDD(Frequency Division Duplexing)
  - TDD(Time Division Duplexing) [see Fig. 4-xx]

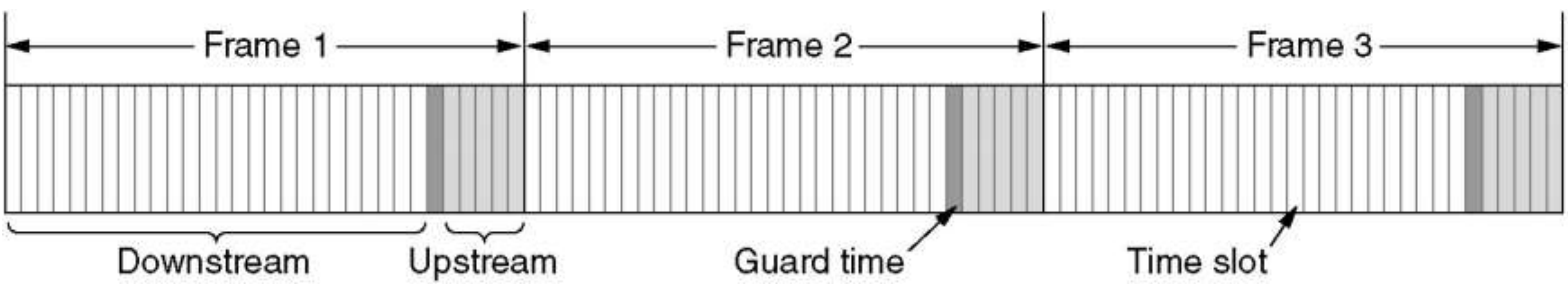


Figure 4-xx. Frames and time slots for time division duplexing.

4.5.4 The 802.16 MAC SubLayer Protocol

- Security sublayer: only the frame payload encrypted, not the headers
- MAC sublayer common part: physical layer time slots, subframes, downstream and upstream maps. Four classes of services for upstream channel allocation:
  - Constant bit rate service
  - Real-time variable bit rate service
  - Non-real-time variable bit rate service
  - Best-efforts service
- bandwidth allocation:
  - per station: subscriber station aggregates the needs of all the users, and makes collective requests
  - per connection: base station manages each connection directly

4.5.4 The 802.16 Frame Structure

- generic header, followed by an optional payload and an optional checksum (CRC): [see Fig.4-33]
  - *EC bit*-----tells whether the payload is encrypted
  - *Type*-----frame type, packing and fragment
  - *CI*--------the presence or absence of the final checksum
  - *EK*-------which encryption key is used
  - *Length*---complete length of the frame, including the header
  - *Connection identifier*---which connection this frame belongs to
  - *HeaderCRC*----chechsum of header only
- bandwidth request frame: [see Fig.4-33(b)]
  - starts with 1 bit instead of 0 bit
  - *Bytes needed*: how much bandwidth is needed
  - do not carry a payload or full-frame CRC.

4.5.4 The 802.16 Frame Structure

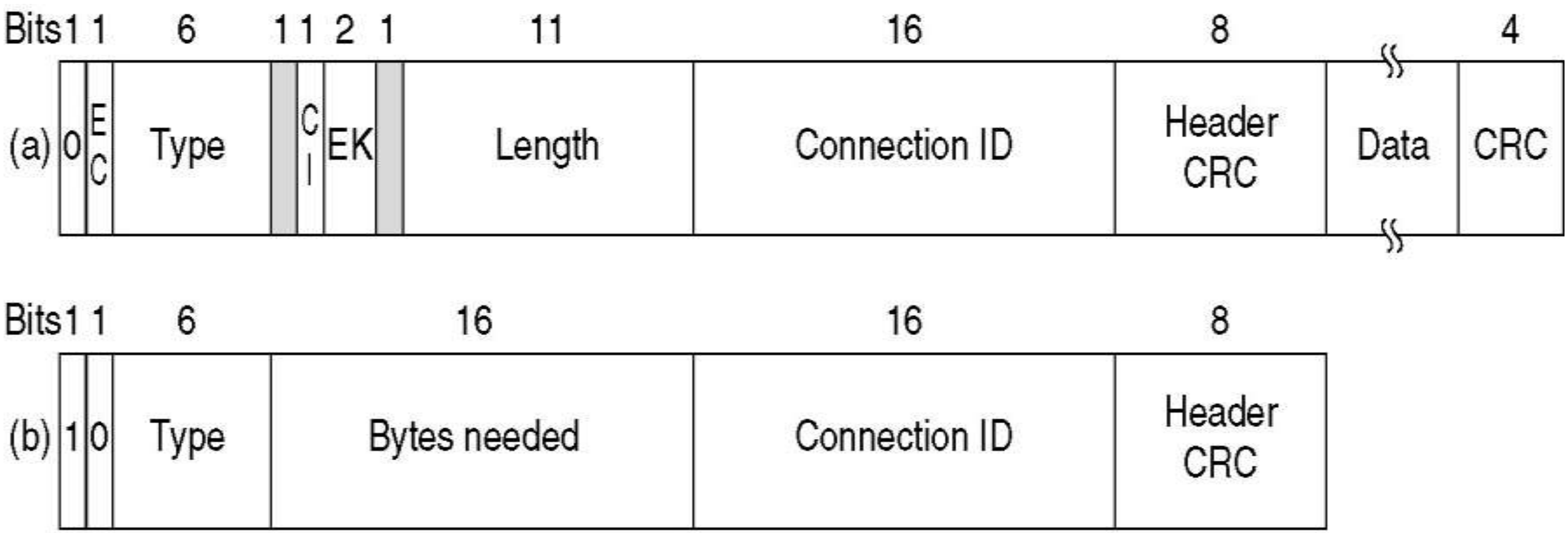


Figure 4-33. (a) A generic frame. (b) A bandwidth request frame.

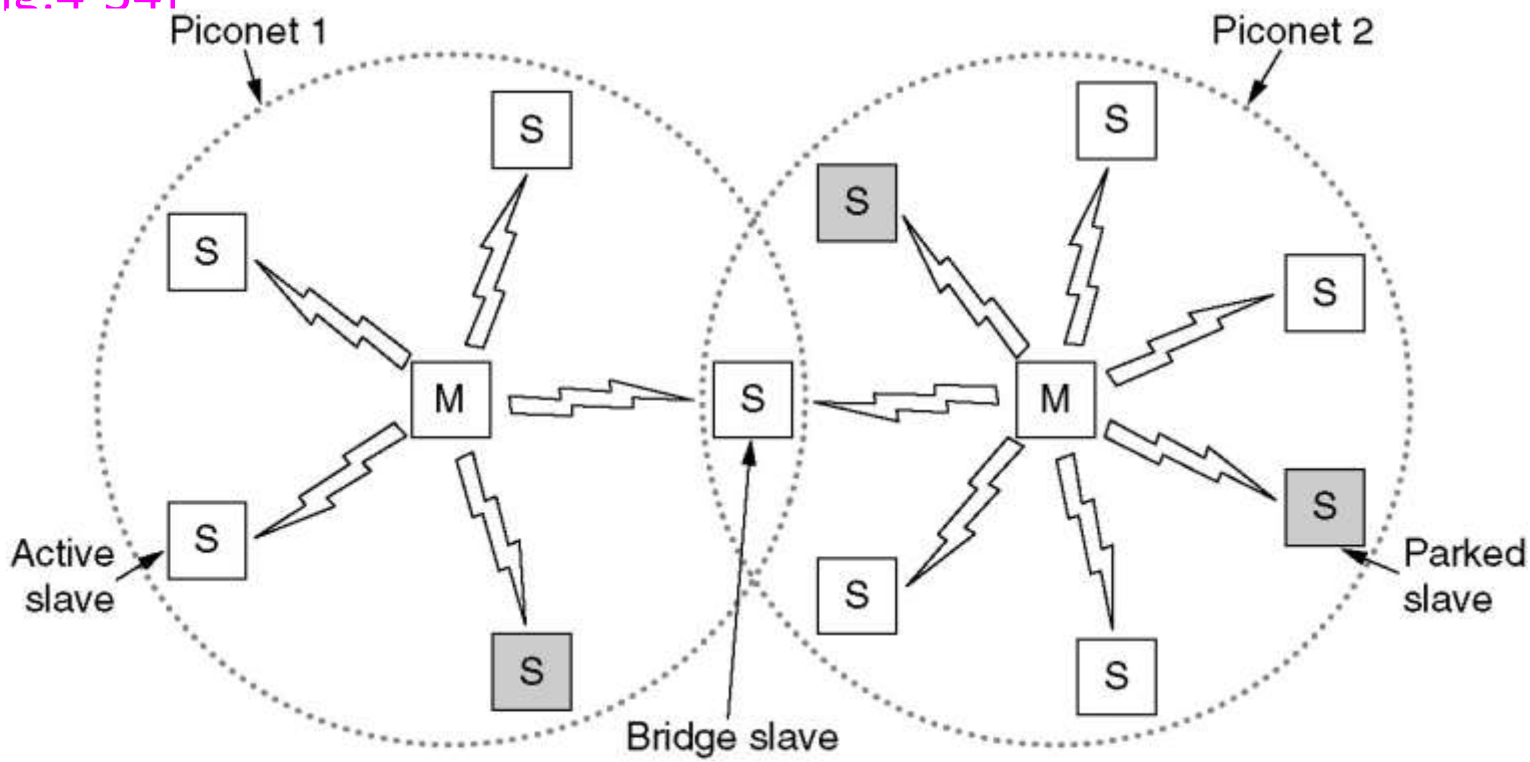
4.6 Bluetooth(*)

- In 1994, L.M.Ericsson company with four other companies(IBM, Intel, Nokia, and Toshiba) formed a SIG
  – to develop a wireless standard for interconnecting computing and communication devices and accessories using short-range, low-power, inexpensive wireless radios
  – named Bluetooth
- SIG and 802.15 (1999)
  – Bluetooth for a complete system
  – 802.15: only physical and data link layers

- Bluetooth Architecture
- Bluetooth Applications
- The Bluetooth Protocol Stack
- The Bluetooth Radio Layer
- The Bluetooth Baseband Layer
- The Bluetooth L2CAP Layer
- The Bluetooth Frame Structure

4.6.1 Bluetooth Architecture

- basic unit : piconet, consists of a master node and up to seven active slave nodes within distance of 10 meters
  - (pico-表示“兆分之一”之义)
- scatternet: interconnected collection of piconets, via bridge node [see Fig.4-34]



22:58:54

Figure 4-34. Two piconets can be connected to form a scatternet.

4.6.1 Bluetooth Architecture

- up to 255 parked nodes in the net
  - In parked state, a divice cannot do anything except respond to an activation or beacon signal from the master
  - two intermediate power states: hold and sniff
- master/slave design:
  - to facilitate the implementation for under \$5
  - the slaves are fairly dumb
  - master-slave communication; no direct slave-slave communication

4.6.2 Bluetooth Application

Name	Description
Generic access	Procedures for link management
Service discovery	Protocol for discovering offered services
Serial port	Replacement for a serial port cable
Generic object exchange	Defines client-server relationship for object movement
LAN access	Protocol between a mobile computer and a fixed LAN
Dial-up networking	Allows a notebook computer to call via a mobile phone
Fax	Allows a mobile fax machine to talk to a mobile phone
Cordless telephony	Connects a handset and its local base station
Intercom	Digital walkie-talkie
Headset	Intended for hands-free voice communication
Object push	Provides a way to exchange simple objects
File transfer	Provides a more general file transfer facility
Synchronization	Permits a PDA to synchronize with another computer

Figure 4-xx. The Bluetooth profiles.

4.6.3 The Bluetooth Protocol Stack

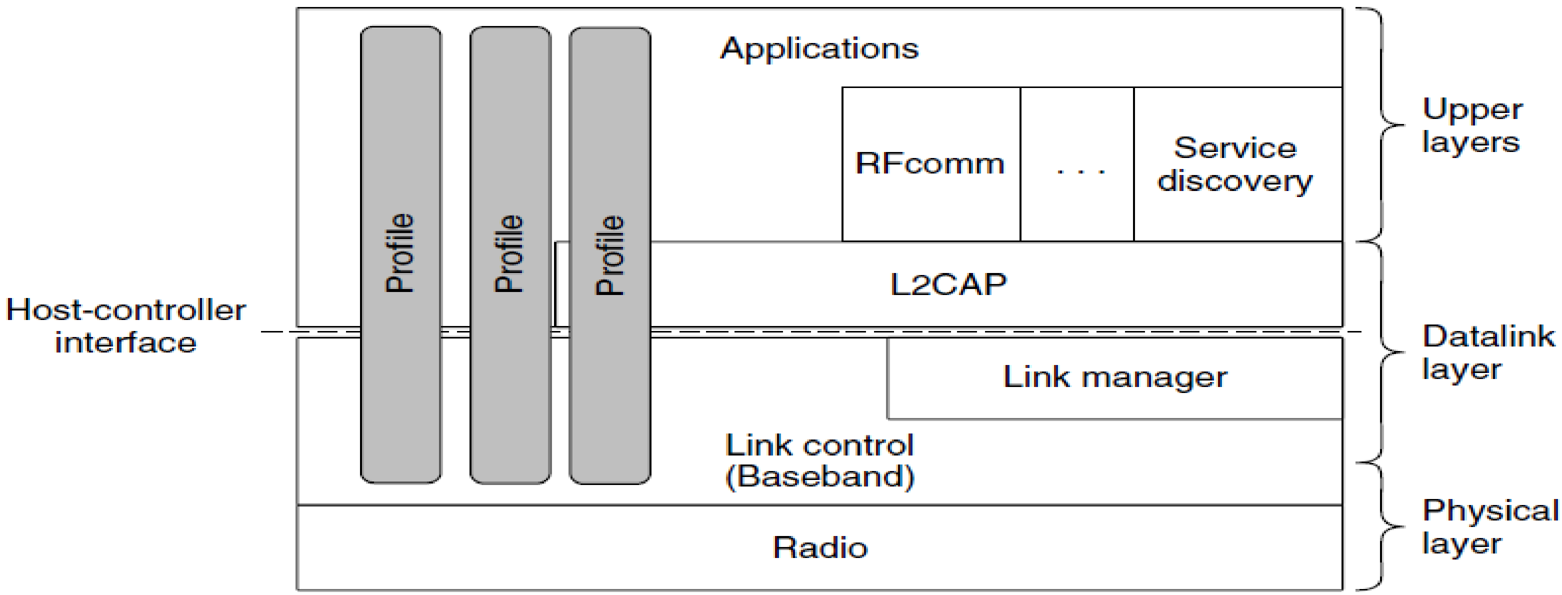


Figure 4-35. The 802.15 version of the Bluetooth protocol architecture.

- Physical radio: deals with radio transmission and modulation.
- Baseband: deals with how the master controls time slots and how these slots are grouped into frames.
- Link manager: handles the establishment of logical channels between devices, including power management, authentication,and QoS

4.6.3 The Bluetooth Protocol Stack

- Logical link control adaptation protocol (L2CAP): shields the upper layers from the details of transmission
- Audio and control: deal with audio and control; application can get at them directly
- 802 LLC was inserted for compatiblility
- Rfcomm: emulates the standard serial port found on PCs
- Telephony: real-time, used for three speech-oriented profiles; also manages call setup and termination
- Service discovery: to locate services within the network
- Top layer: where the application and profiles are located

4.6.4 The Bluetooth Radio Layer

- The radio layer moves the bits from master to slave, or vice versa.
  - Low-power system with a range fo 10 meters operating in the 2.4-GHz ISM band.
  - The band is divided into 79 channels of 1MHz each.
  - Modulation is frequency shift keying, with 1 bit per Hz giving a gross data rate of 1 Mbps, but much is comsumed by overhead
  - To allocate channels fairly, frequency hopping spread spectrum is used with 1600 hops/sec and a dwell time of 625 μsec.
  - All the nodes in a piconet hop simutaneously, with the master dictating the hop the hop sequence
- both 802.11 and Bluetooth operate in the 2.4-GHz ISM band on the same 79 channels, they interfere with each other

4.6.5 The Bluetooth Baseband Layer

- In the simplest form, the master defines a series of 625 μsec time slots, with master starting in even slots while slaves in odd; Frames can be 1, 3, or 5 slots long
- settling time of 250-260 μsec per hop: to allow the radio circuits to become stable.
  - Longer frames are much more efficient than single-slot frames
- Each frame is transmitted over a logical channel, called a link, between the master and a slave
  - ACL(Asynchronous Connection-Less): for packet-switched data available at irregular intervals. Best-effort. Only one ACL link
  - SCO(Synchronous Connection Oriented): for real-time data, such as telephone connections. A fixed slot in each direction; never retransmit, using forward error correction. up to three SCO links

4.6.6 The Bluetooth L2CAP Layer

- The L2CAP layer has three major functions.
  - Accepts packets of up to 64 KB from the upper layers and breaks them into frames for transmission. At the far end, the frames are reassembled into packets again
  - Handles the multiplexing and demultiplexing of multiple packet sources.
  - L2CAP handles the QoS requirements, both when links are established and during normal operation. And the maximum payload size allowed.

4.6.7 The Bluetooth Frame Structure

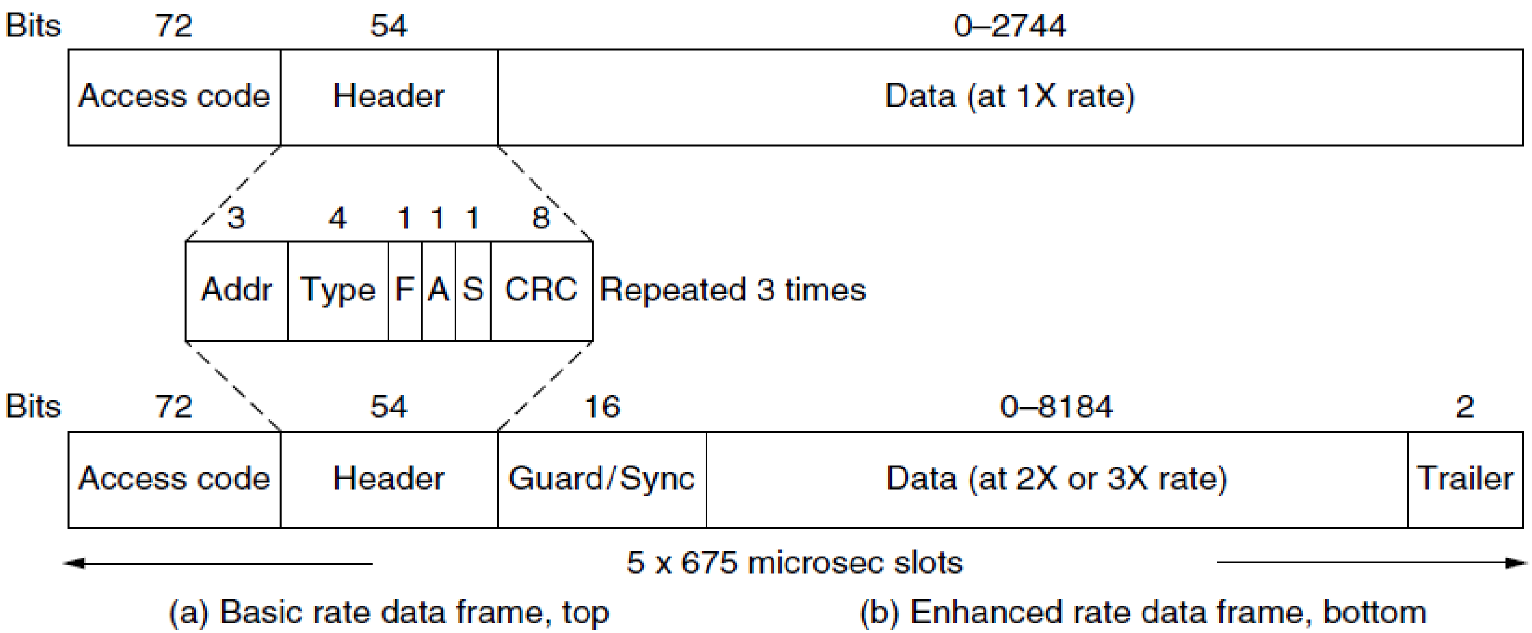


Figure 4-36 Typical Bluetooth data frame at (a) basic, and (b) enhanced, data rates.

- Access code: identifies the master
- Header:
  - Address: identifies which of the eight active divices intended for
  - Type: frame type(ACL, SCO, poll, or null), the type of error correction used in the data field, and how many slots long
  - Flow bit: asserted by a slave when its buffer is full
  - Acknowledgement bit: piggyback an ACK onto a frame

4.6.7 The Bluetooth Frame Structure

- Header:
  - Sequence bit: to number the frames to detect retransmissions, use stop-and-wait protocol, so 1 bit is enough
  - 8-bit header Checksum
  - The entire 18-bit header is repeated 3 times, and examined on the receiving side. Using redundacy for cheap, low-powered (2.5mW) devices with little computing capacity
- Data: up to 2744 bits (five-slot). For single time slot, the format is the same except that the data field is 240 bits
- slave may use only the odd slots, 800slots/sec, channel capacity: 64,000 bps

4.7 RFID（*）

- EPC Gen 2 architecture
- EPC Gen 2 physical layer
- EPC Gen 2 tag identification layer
- Tag identification message formats

4.7.1EPC Gen 2 Architecture

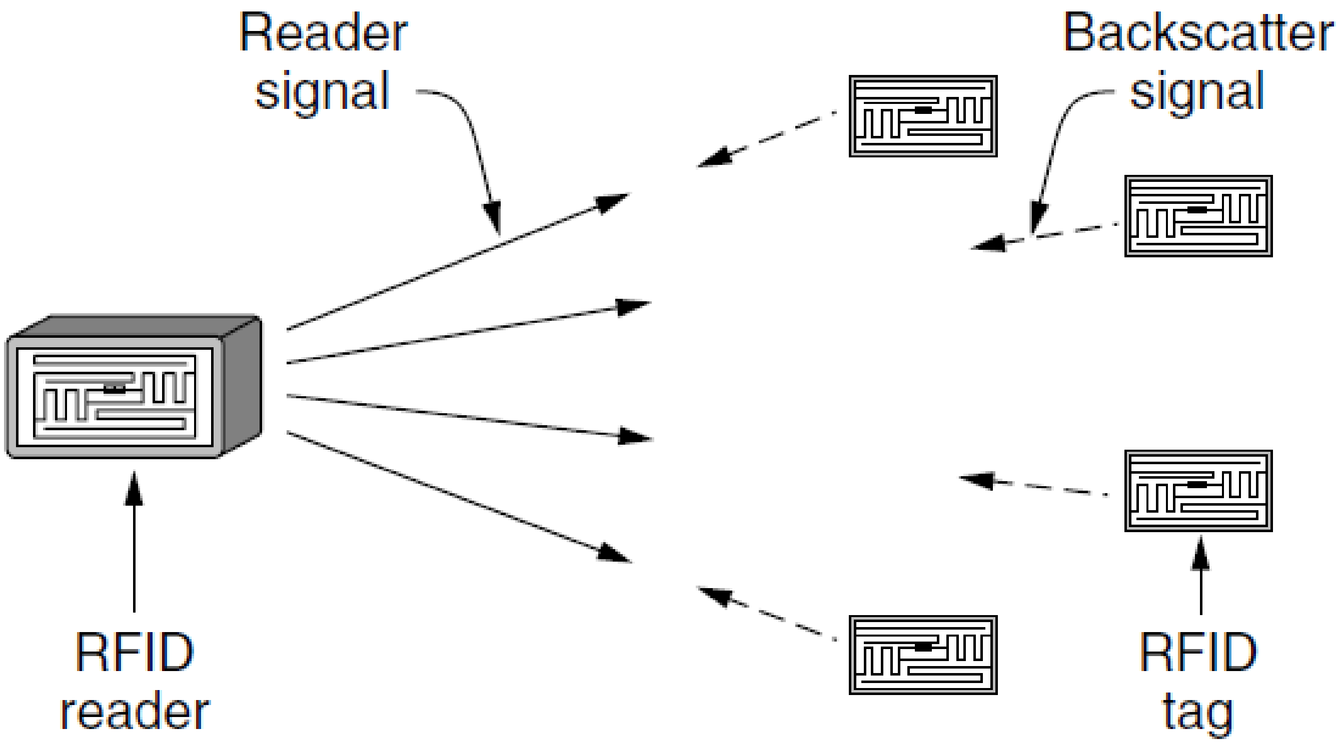


Figure 4-37 RFID architecture.

4.7.2 EPC Gen 2 Physical Layer

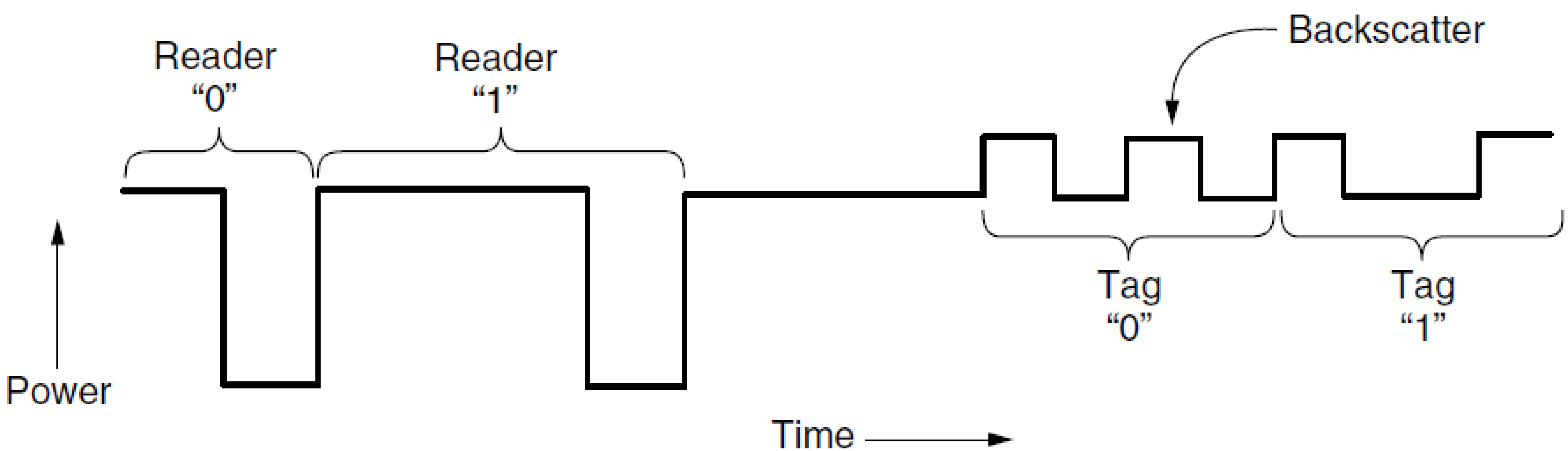


Figure 4-38 Reader and tag backscatter signals.

4.7.3 EPC Gen 2 Tag Identification Layer

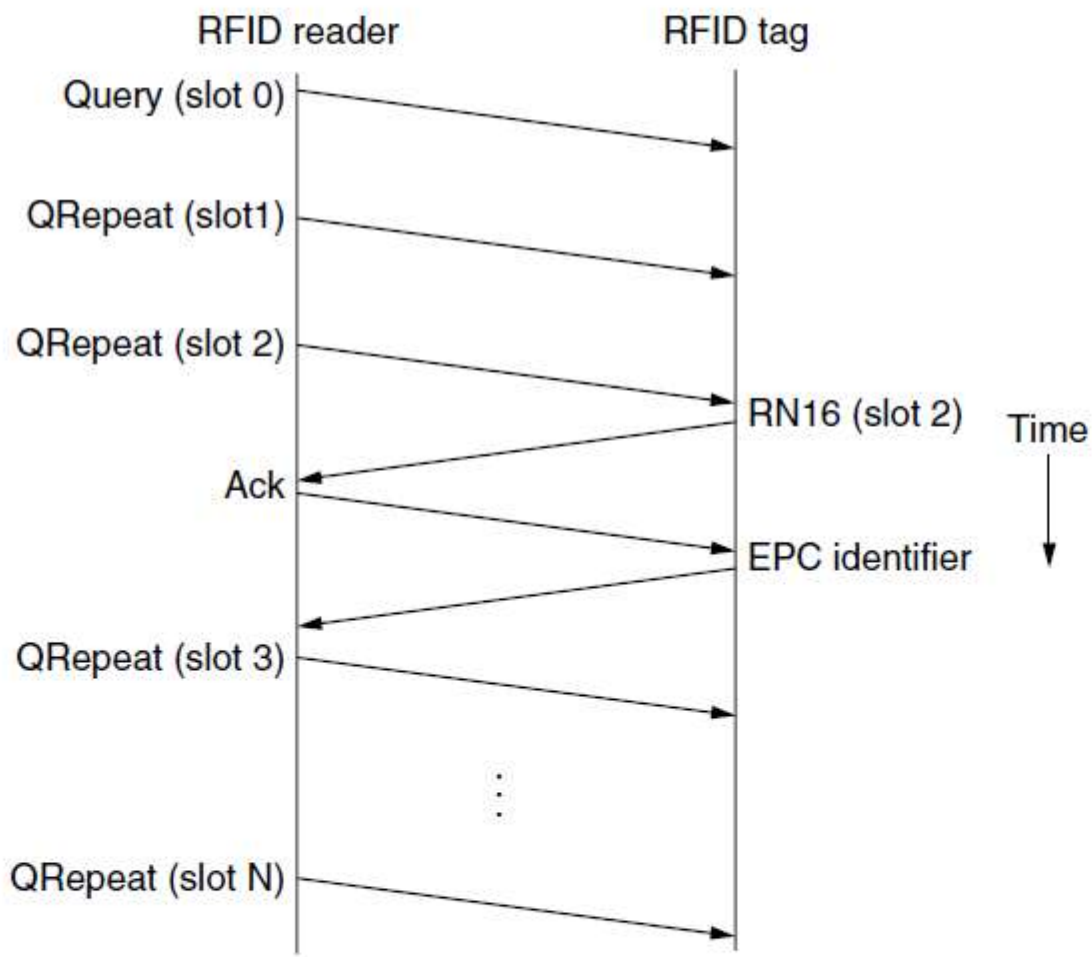


Figure 4-39 Example message exchange to identify a tag.

4.7.4Tag Identification Message Formats

Bits	4	1	2	1	2	2	1	4	5
	Command 1000	DR	M	TR	Sel	Session	Target	Q	CRC
		Physical parameters			Tag selection				

Figure 4-40 Format of the Query message.

4.8 Data Link Layer Switching

- LANs can be connected by devices called **bridges**, which operate in the data link layer
- Bridges examine the data link layer addresses to do routing, can transport IPv4, IPv6, AppleTalk, ATM, etc.

4.8.1 Use of Bridges:

  - goals differ, different departments choose different LANs
  - geographically spead by considerable distances
  - to accommodate the load , most traffic is restricted to a single LAN and does not add load to the backbone
  - physical distance is too great(e.g. more than 2.5 km for Ethernet)
  - reliability: unlike repeaters, Bridges can be inserted to manage which to forward and which not
  - bridges can contribute to security: promiscuous mode

4.8.1 Use of Bridges

Main topics in this sector:

- Bridges from 802.x to 802.y
- Local Internetworking
- Spanning Tree Bridges
- Remote Bridges
- Repeaters, Hubs, Bridges, Switches, Routers, Gateways
- Virtual LANs

4.8.2 Learning Bridges

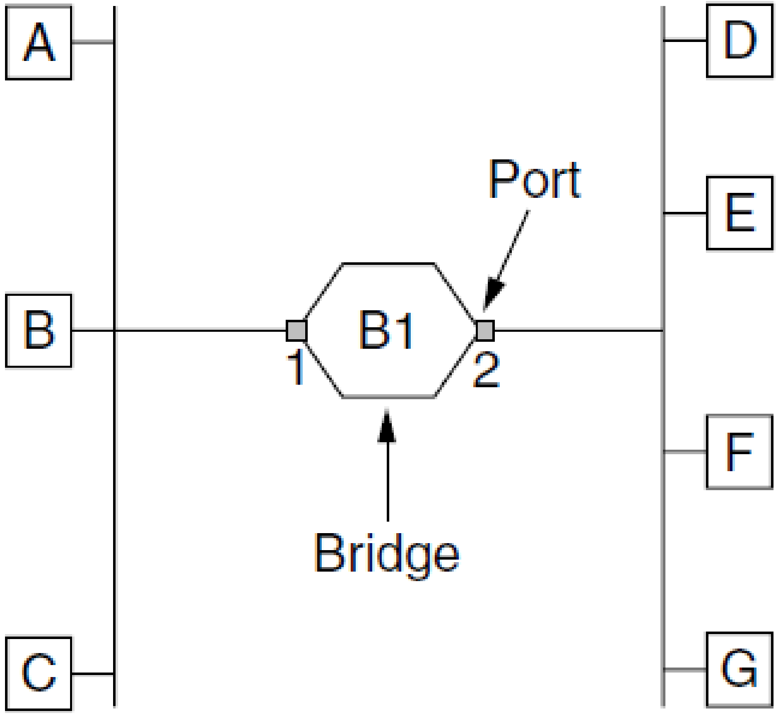


Figure 4-41(a) Bridge connecting two multidrop LANs

4.8.2 Learning Bridges

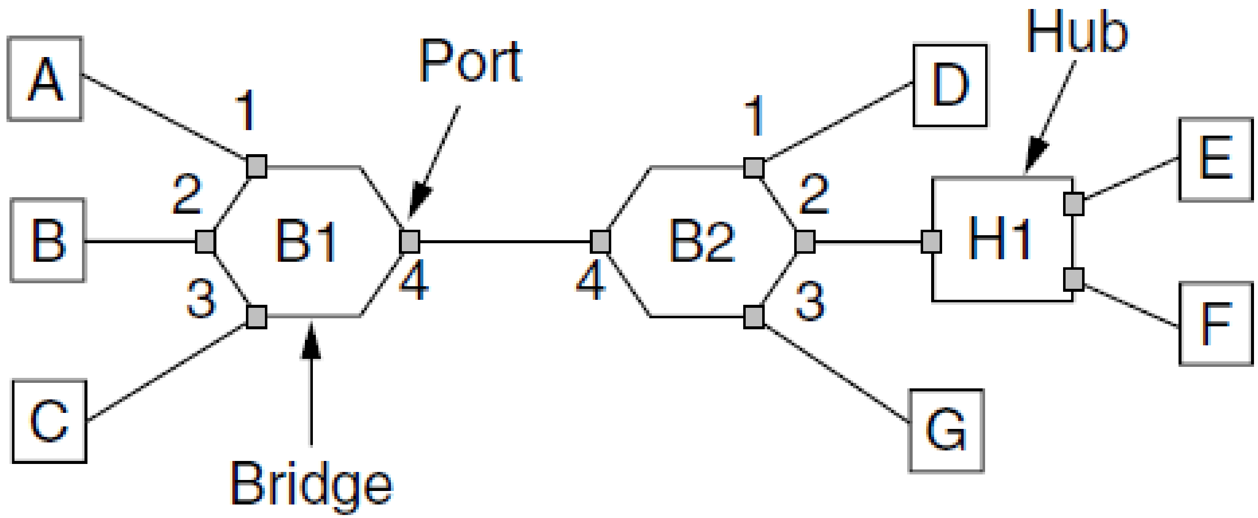


Figure 4-41(b) Bridges (and a hub) connecting seven point-to-point stations.

4.8.2 Learning Bridges

- Operation principle: [see Fig. 4-40]
  - a bridge connecting k different LANs will have k different MAC sublayers and k different physical layers, one for each type

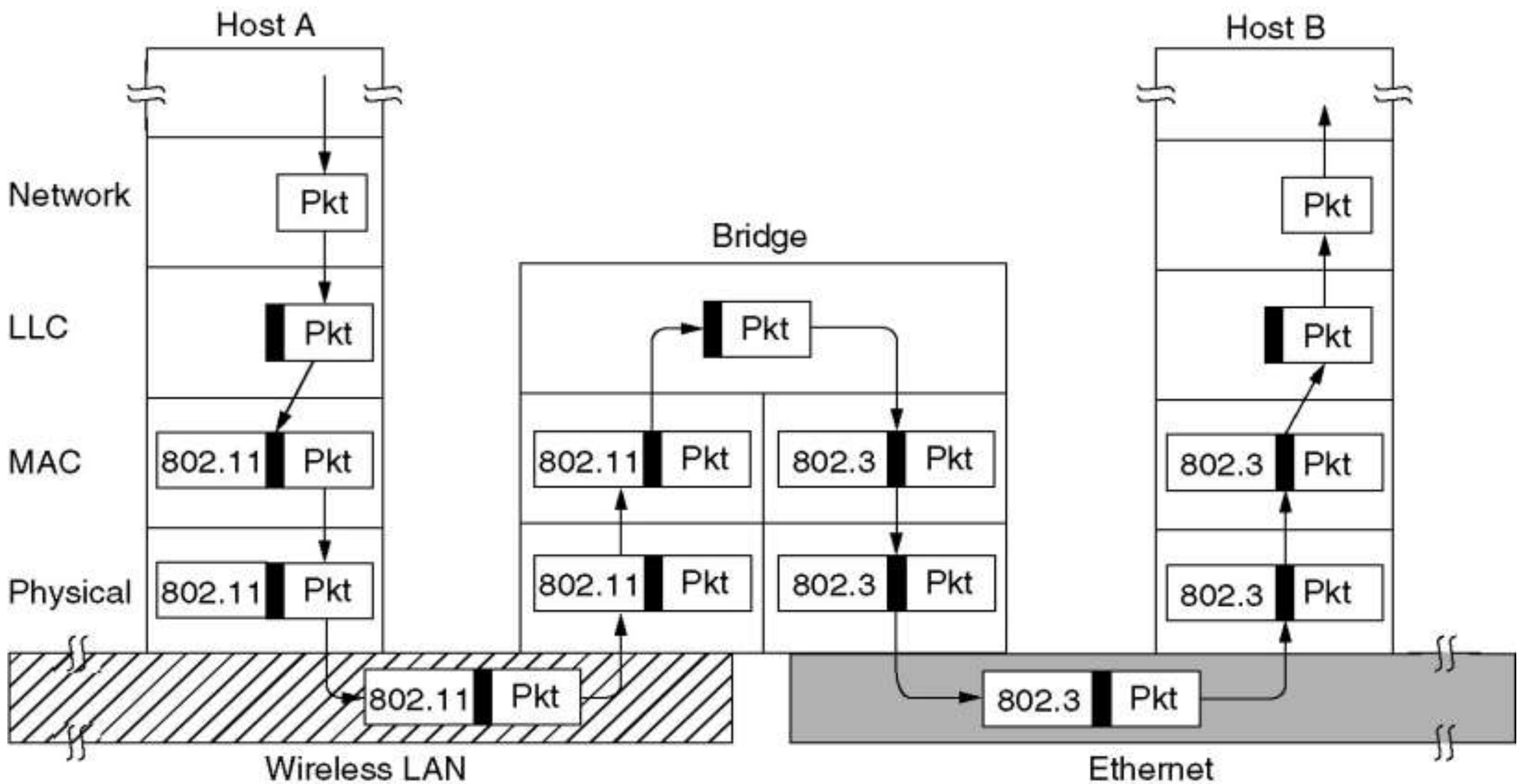


Figure 4-40. Operation of a LAN bridge from 802.11 to 802.3.

4.8.2 Learning Bridges

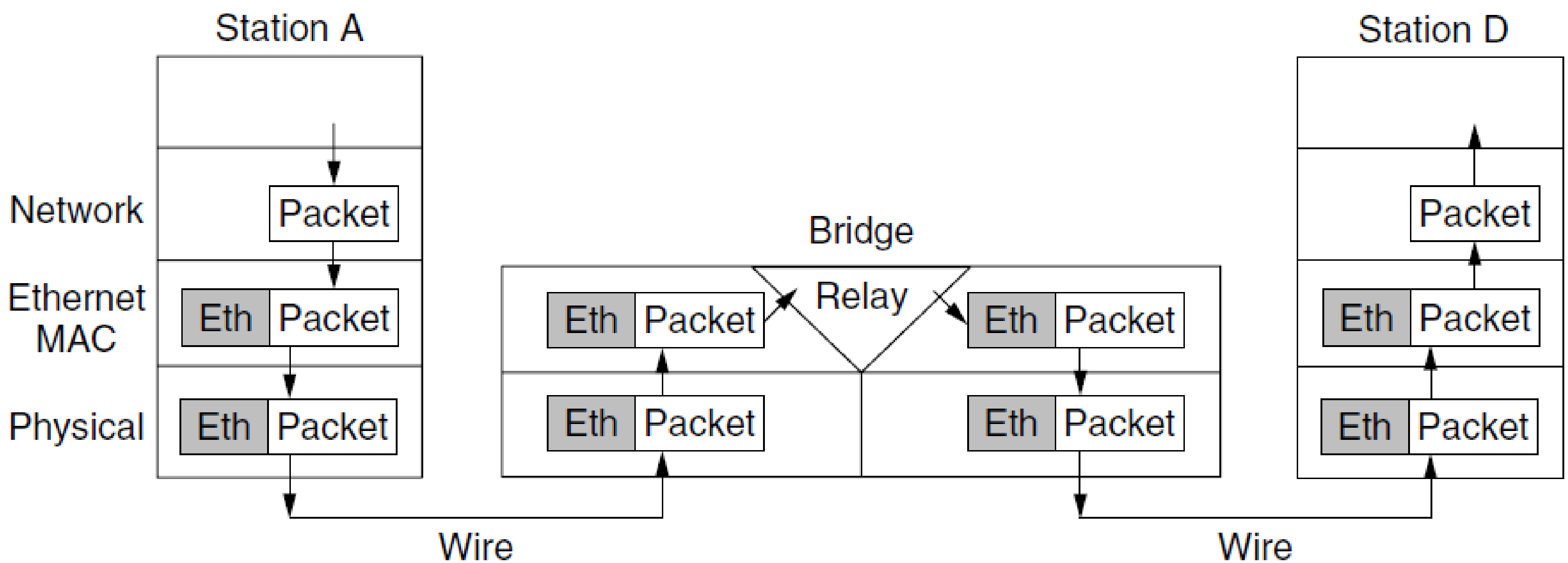


Figure 4-42 Protocol processing at a bridge.

4.8.2 Learning Bridges

- Some difficulties:
  - each of the LANs uses a different frame format
  - interconnected LANs do not necessarily run at the same data rate
  - different 802 LANs have different maximum frame lengths
  - security
  - QoS: 802.11 and 802.16 provide it, while Ethernet not

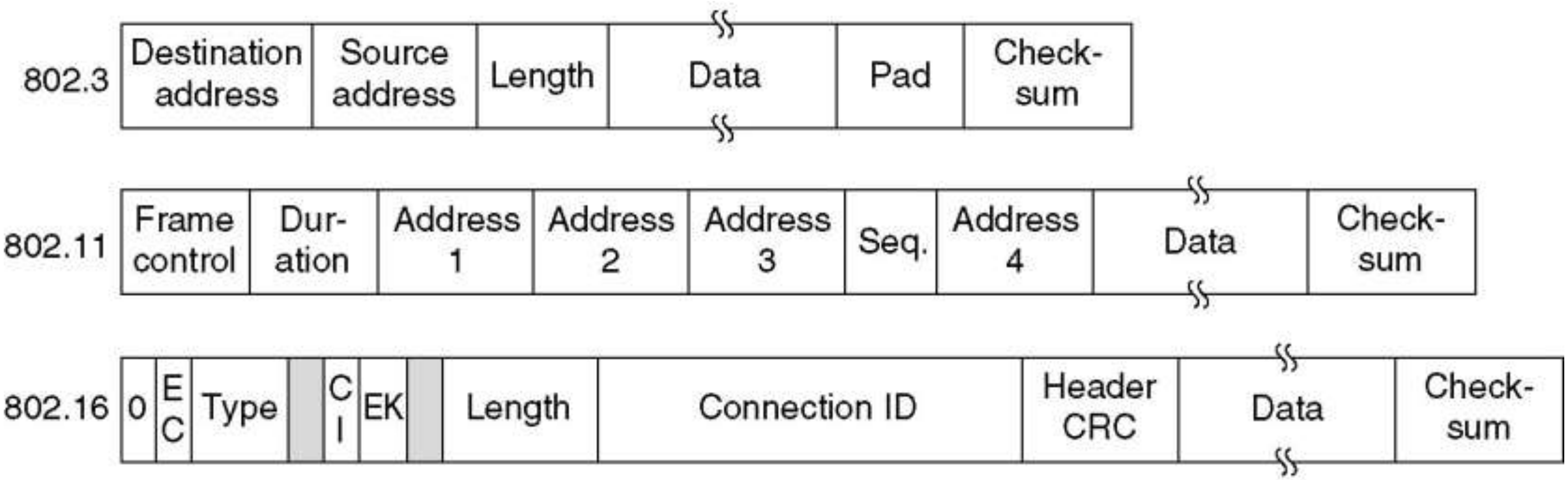


Figure 4-xx. The IEEE 802 frame formats. The drawing is not to scale.

4.8.2 Learning Bridges

- **Transparent bridge** [see Fig. 4-xx]
- hash table, flooding algorithm, **backward learning**, dynamic topologies
- routing procedure for an incoming frame:
  - If destination and source LANs are the same, discard the frame
  - If destination and source LANs are different, forward the frame
  - If the destination LANs is unknown, use flooding
- **Cut-through switching or wormhole routing**

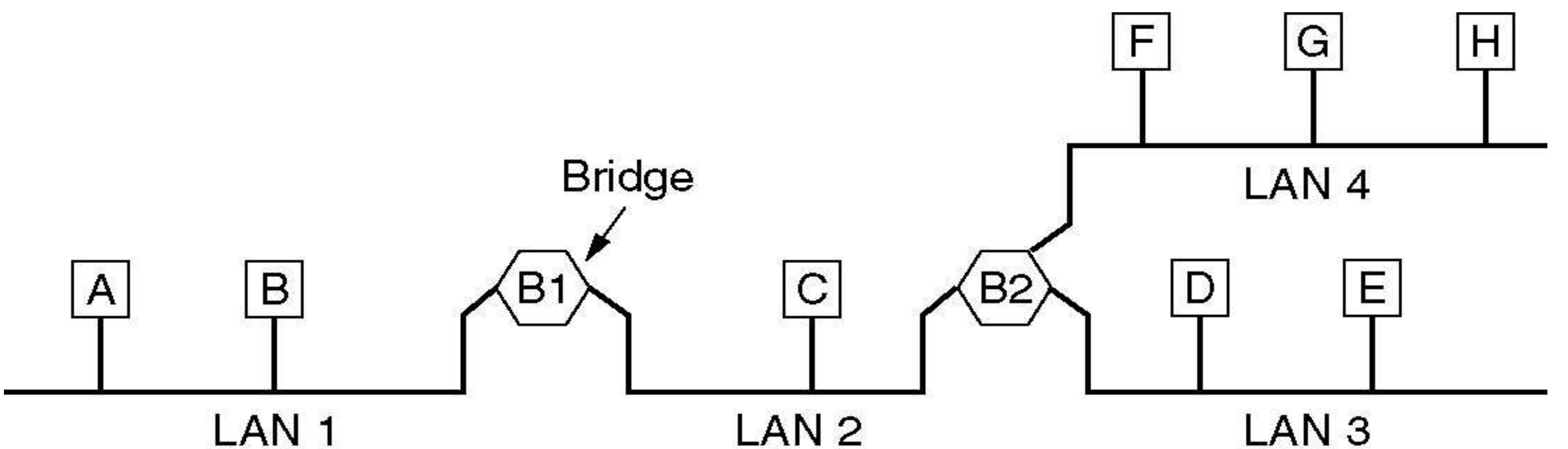


Figure 4-xx. A configuration with four LANs and two bridges.

4.8.3 Spanning Tree Bridges

- **Parallel bridges**: to increase reliablity
  - creates loops in the topology

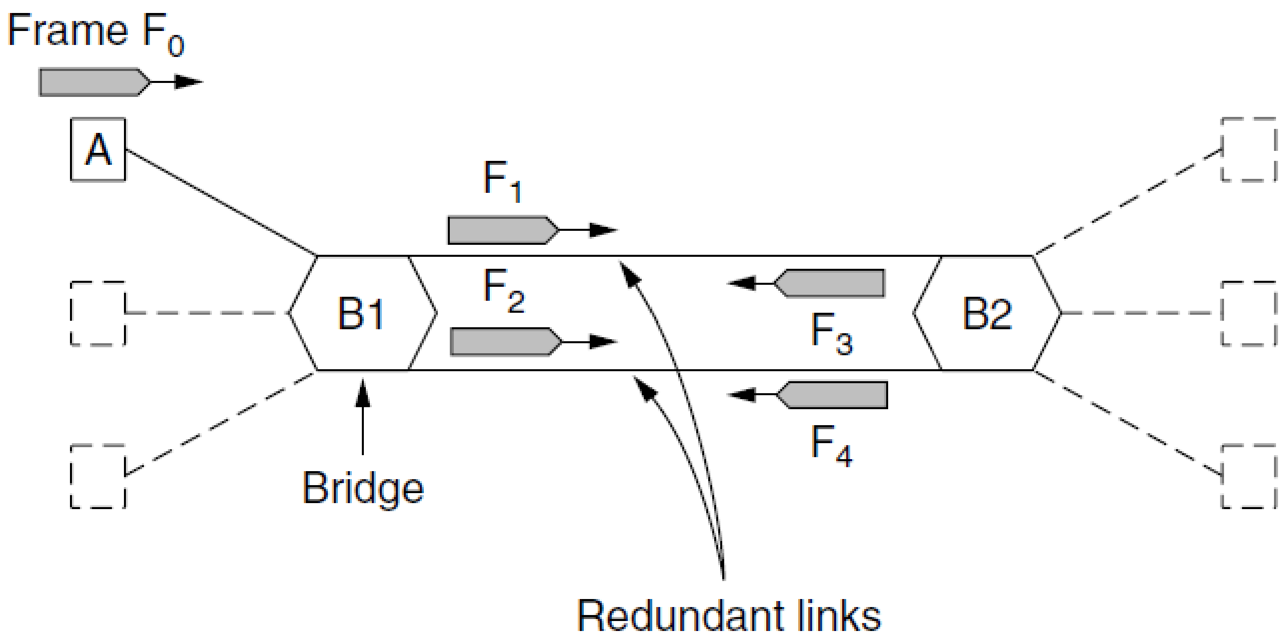
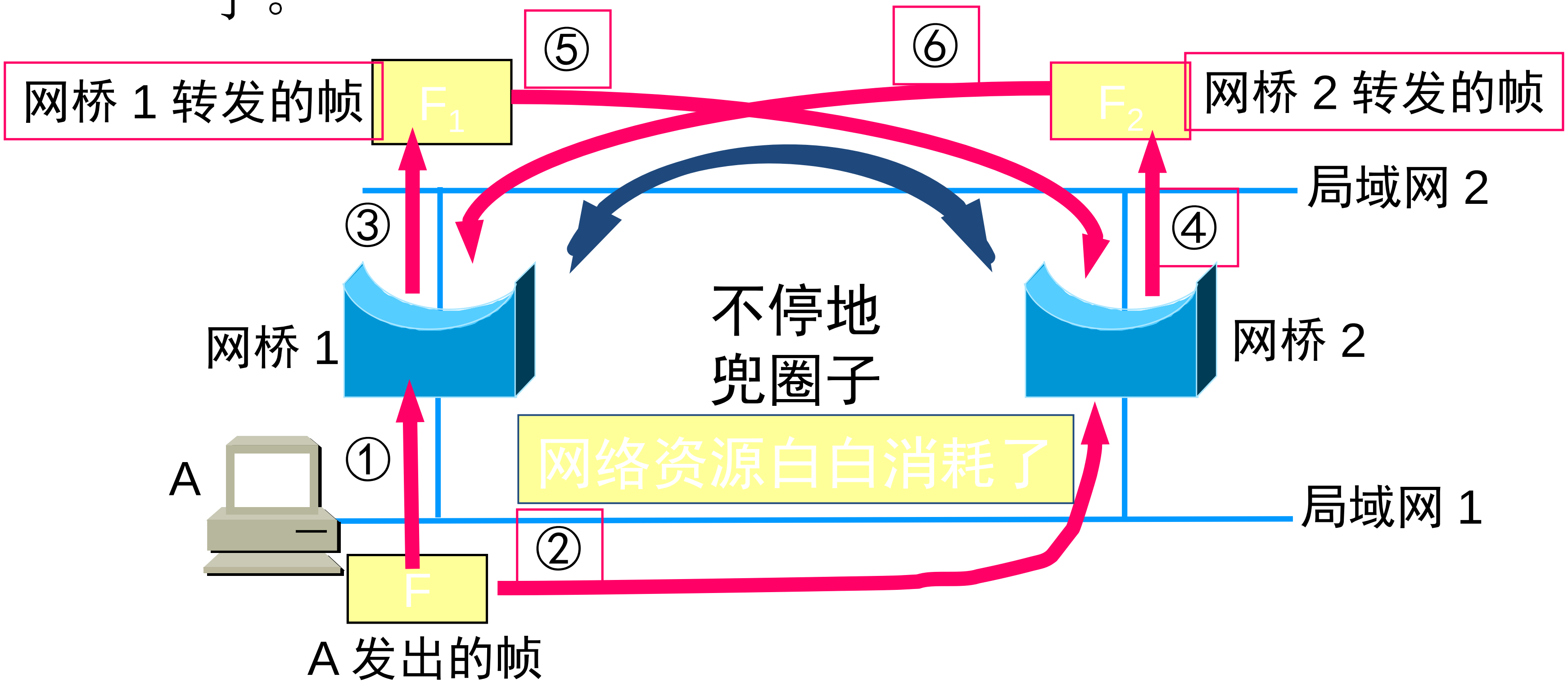


Figure 4-43. Two parallel transparent bridges.

透明网桥使用了生成树算法

- 这是为了避免产生转发的帧在网络中不断地兜圈子。



4.7.3 Spanning Tree Bridges

- **Spanning tree**: loop-free [see Fig. 4-44]
  - choose one bridge to be the root of the tree
  - a tree of shortest paths from the root to every bridge and LAN is constructed
  - if a bridge or LAN fails, a new one is computed

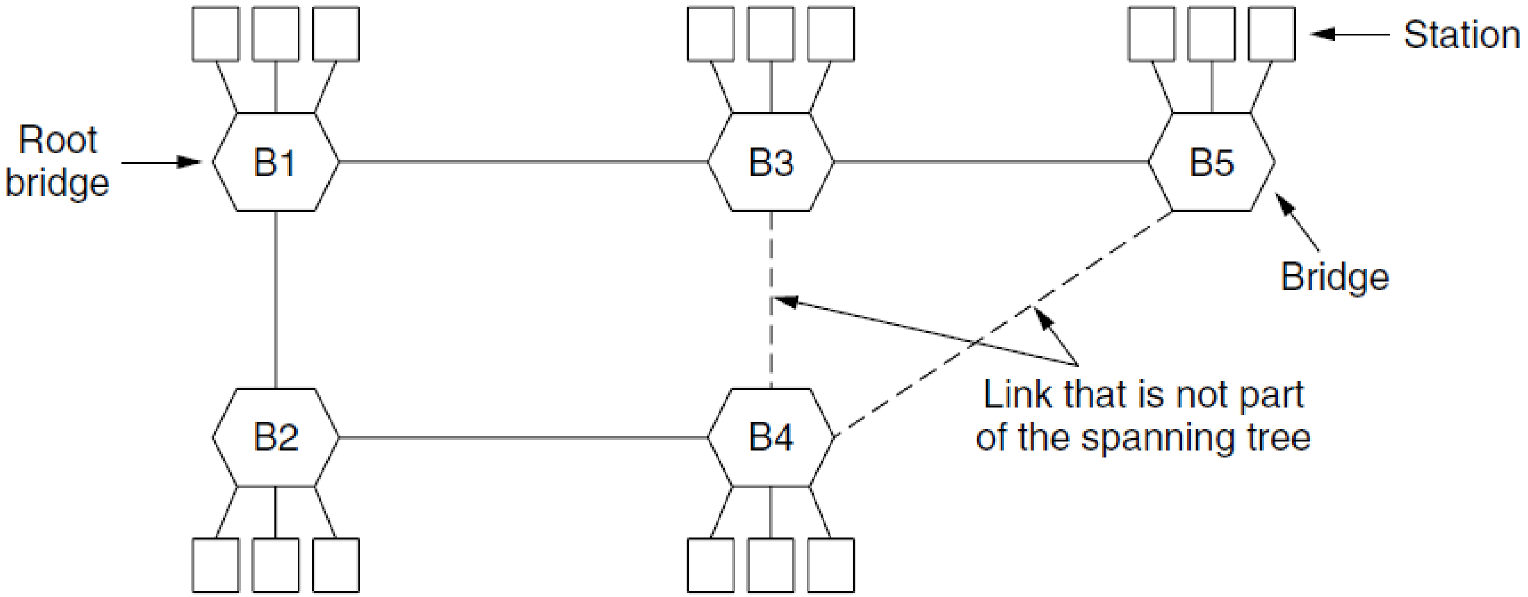


Figure 4-44 A spanning tree connecting five bridges. The dotted lines are links that are not part of the spanning tree.

4.7.4 Repeaters, Hubs, Bridges, Switches, Routers and Gateways

- operate in different layers [see Fig. 4-45]
  - The layer matters because different devices use different pieces of information to decide how to switch

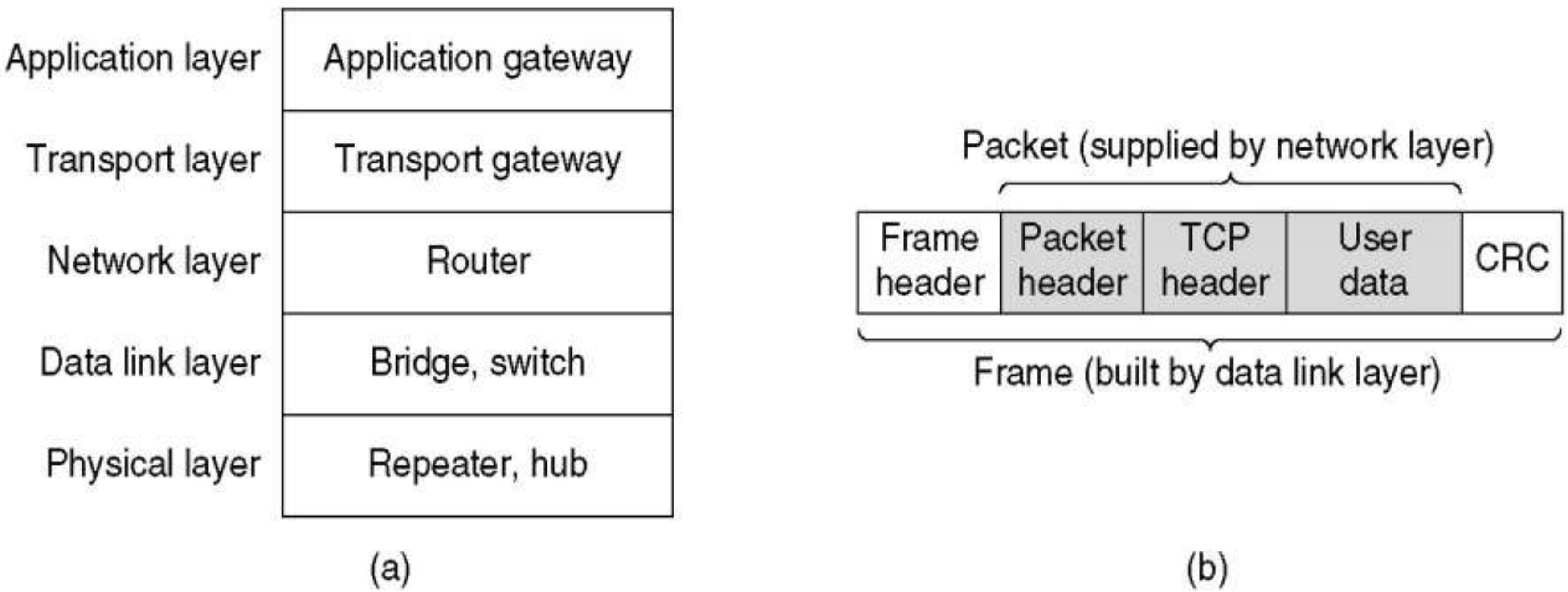


Figure 4-45. (a) Which device is in which layer. (b) Frames, packets, and headers.

4.7.4 Repeaters, Hubs, Bridges, Switches, Routers and Gateways

- **Repeaters**: amplify signal. do not understand frames, packets, or headers, only understand volts
- **Hubs:** not amplify incoming signals, not examine 802 addresses. The entire hub forms a single collision domain [see Fig.4-47(a)]
- **Bridges:** connect LANs, route on frame address, each line is its own collision domain [see Fig.4-47(b)]
- **Switches:** connect individual computers, route on frame address, never lose frames to collisions [see Fig.4-47(c)]
  - cut-through switches
- **Routers:** see chap.5

4.7.4 Repeaters, Hubs, Bridges, Switches, Routers and Gateways

- **transport gateways**: connect two computers that use different connection-oriented transport protocols
- **application gateways:** understand the format and contents of the data and translate messages from one format to another. e.g. e-mail gateway.

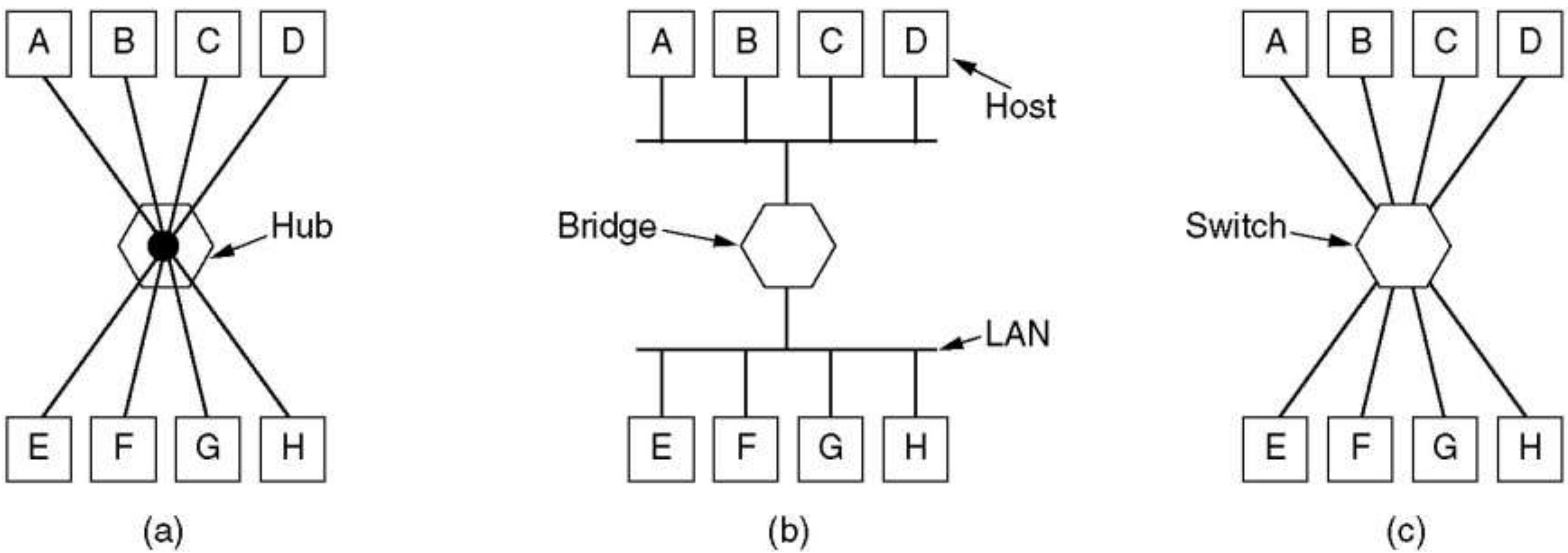


Figure 4-xx. (a) A hub. (b) A bridge. (c) a switch.

4.8.5 Virtual LANs

- A building with centralized wiring using hubs and a switch:

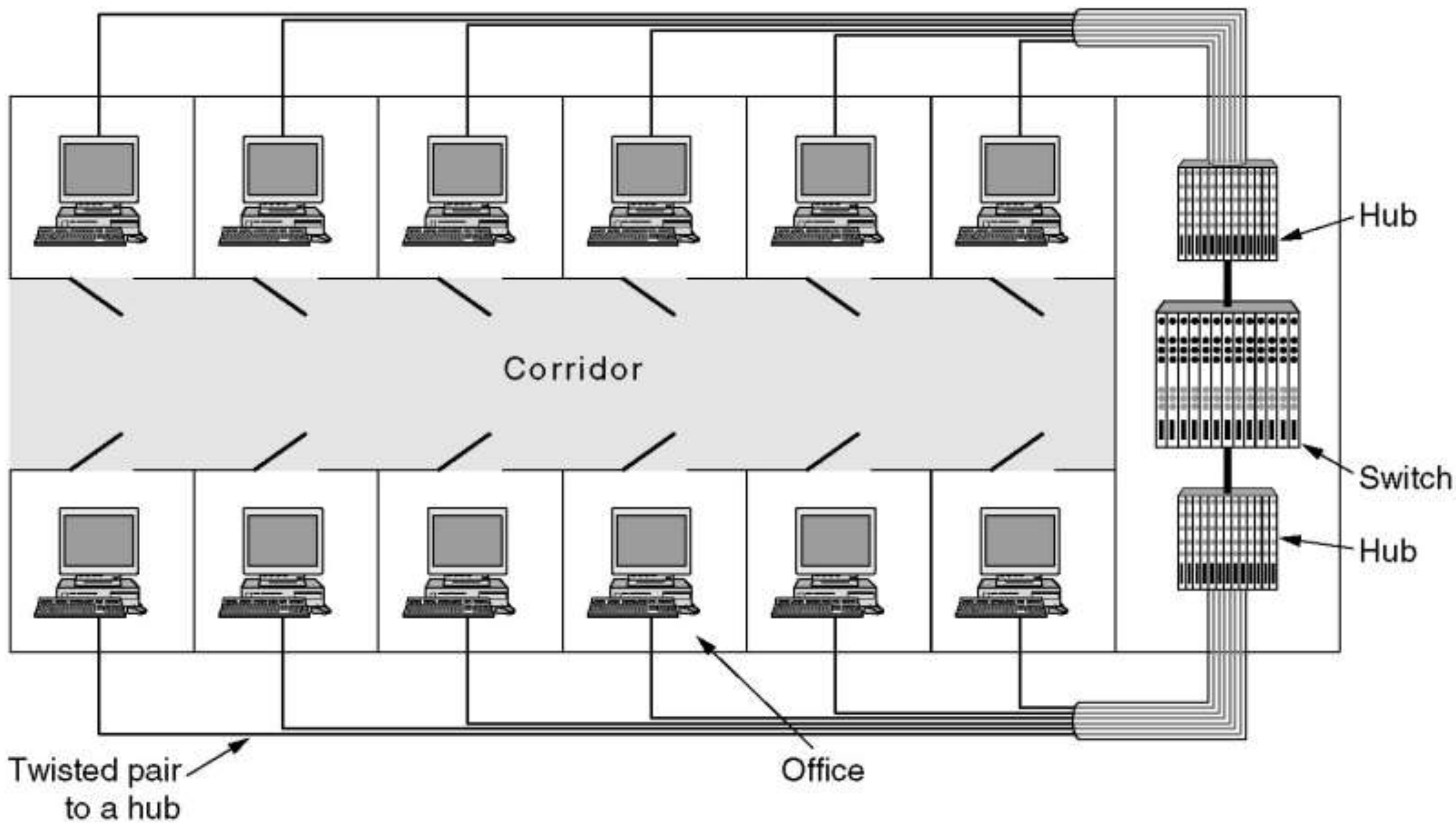


Figure 4-46. A building with centralized wiring using hubs and a switch.

4.8.5 Virtual LANs

- To configure LANs logically rather than physically With hub and switch. Reasons:
  - security
  - load
  - broadcasting: **broadcast storm**
- **VLAN(Virtual LAN)**: based on specially-designed VLAN-aware switches
  - example [see Fig.4-47], Gray VLAN, White VLAN.
  - Configuration tables tell which VLANs are accessible via which ports(lines). When a frame comes in from, say, the gray VLAN, it must be forwarded on all the ports marked G
  - if all machines on LAN 2 and 4 become G, then B2->LAN4, B2->LAN2 become G, and so does B1->B2

4.8.5 Virtual LANs

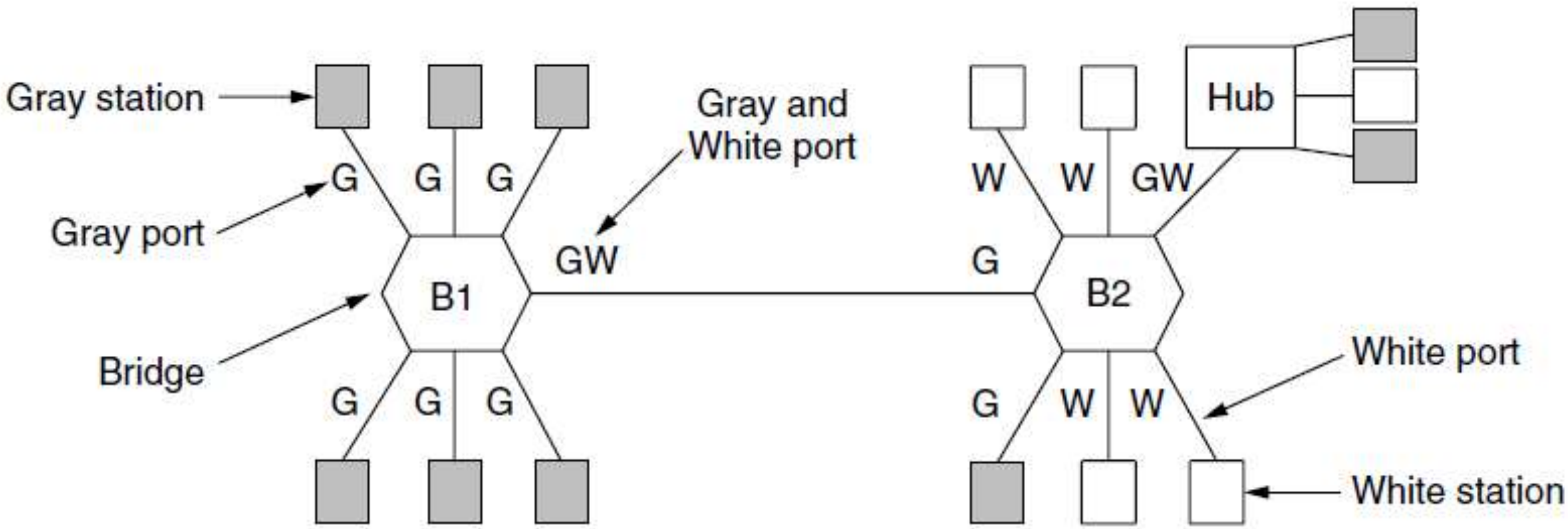


Figure 4-47. Two VLANs, gray and white, on a bridged LAN

Figure 9-1 VLANs and Physical Boundaries

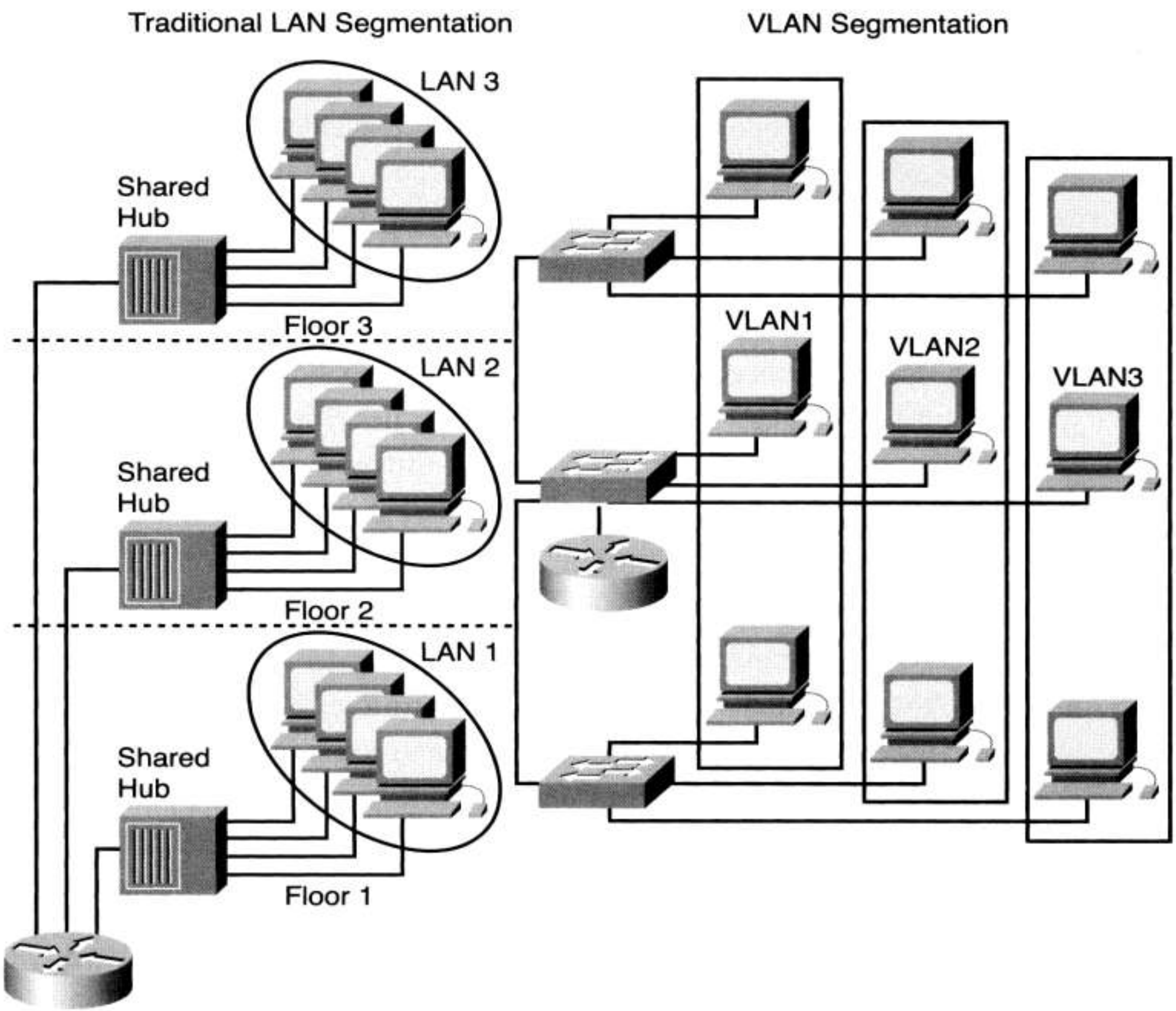


Figure 9-3 VLANs Span Physical Locations

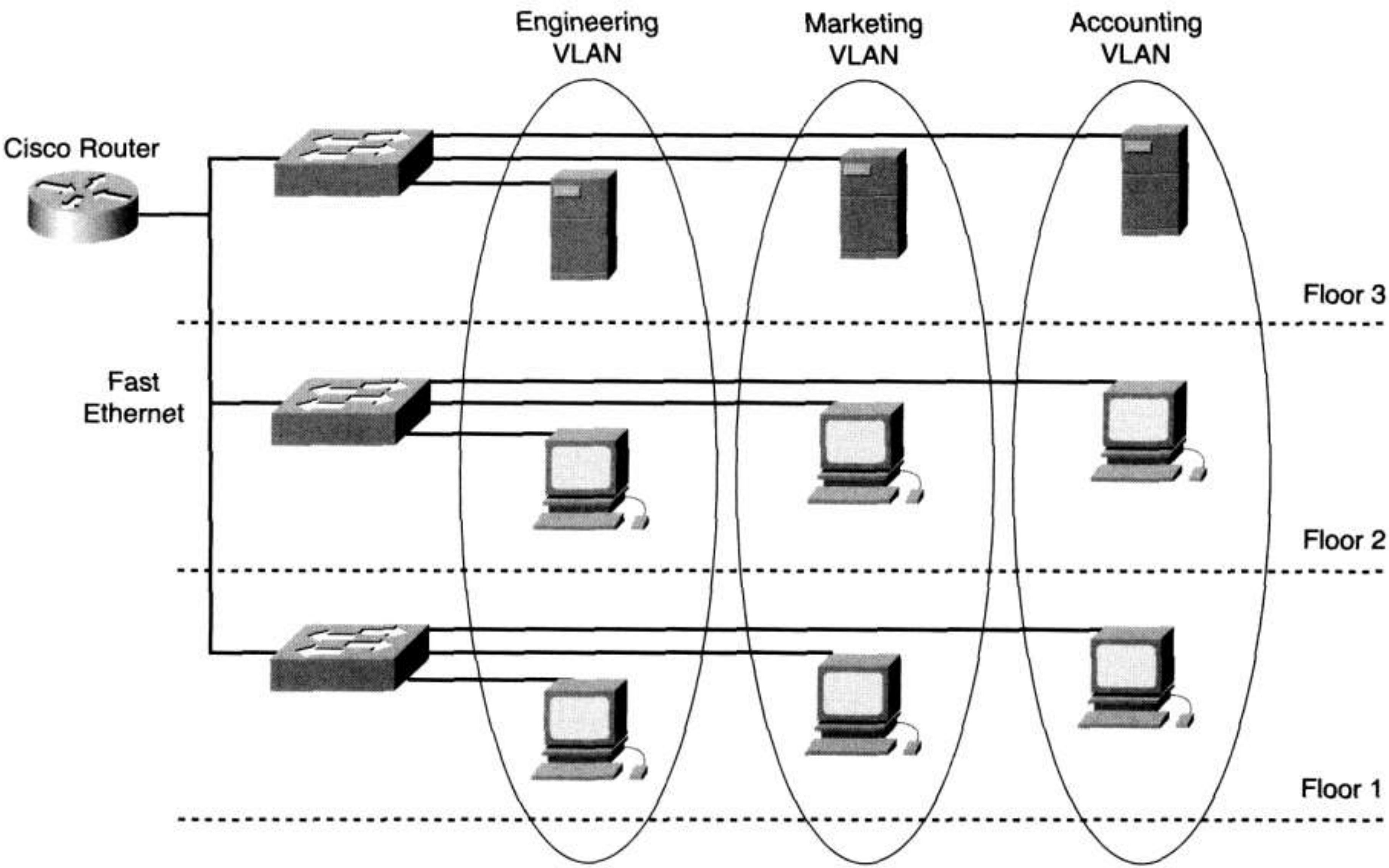
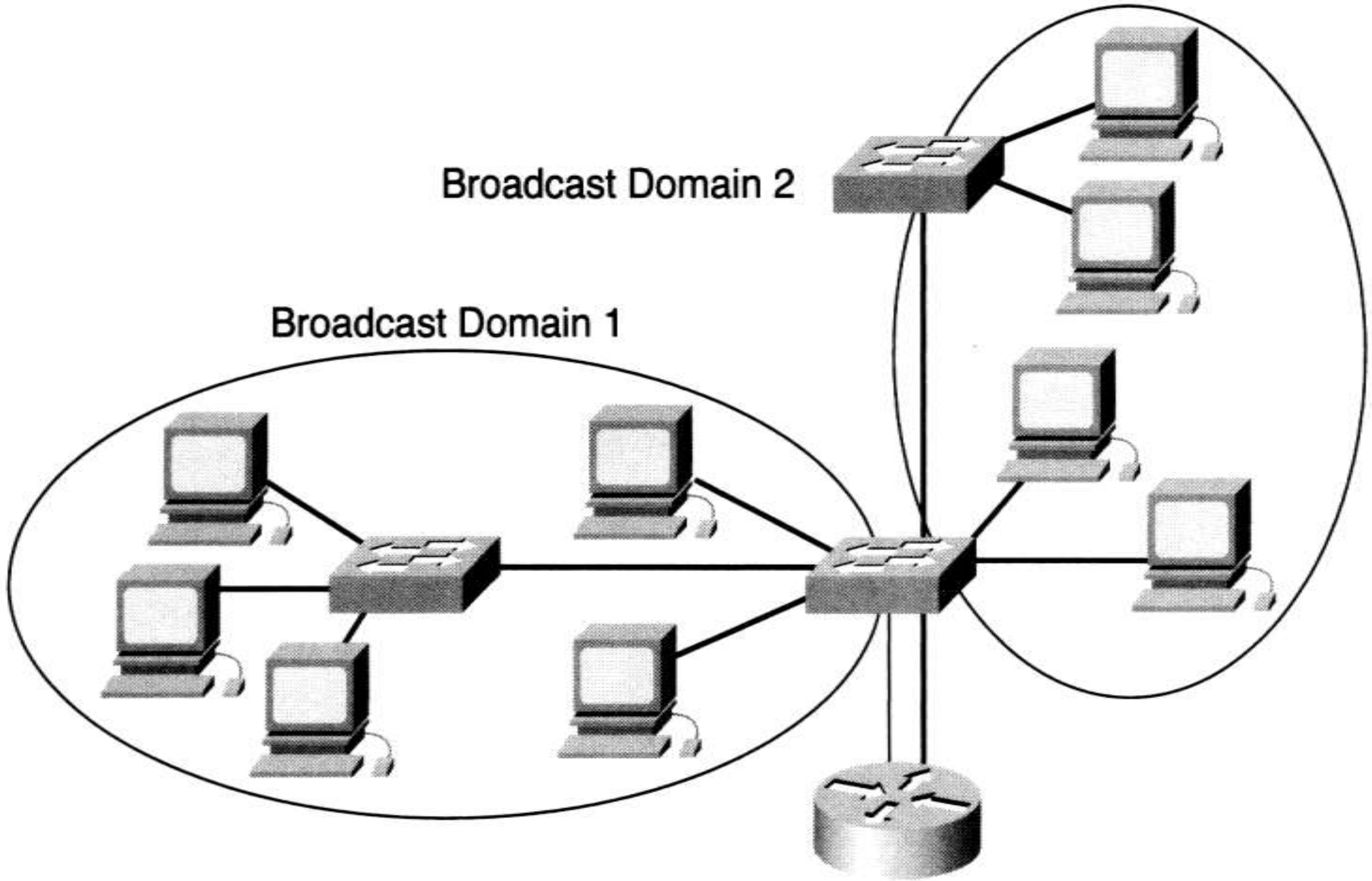


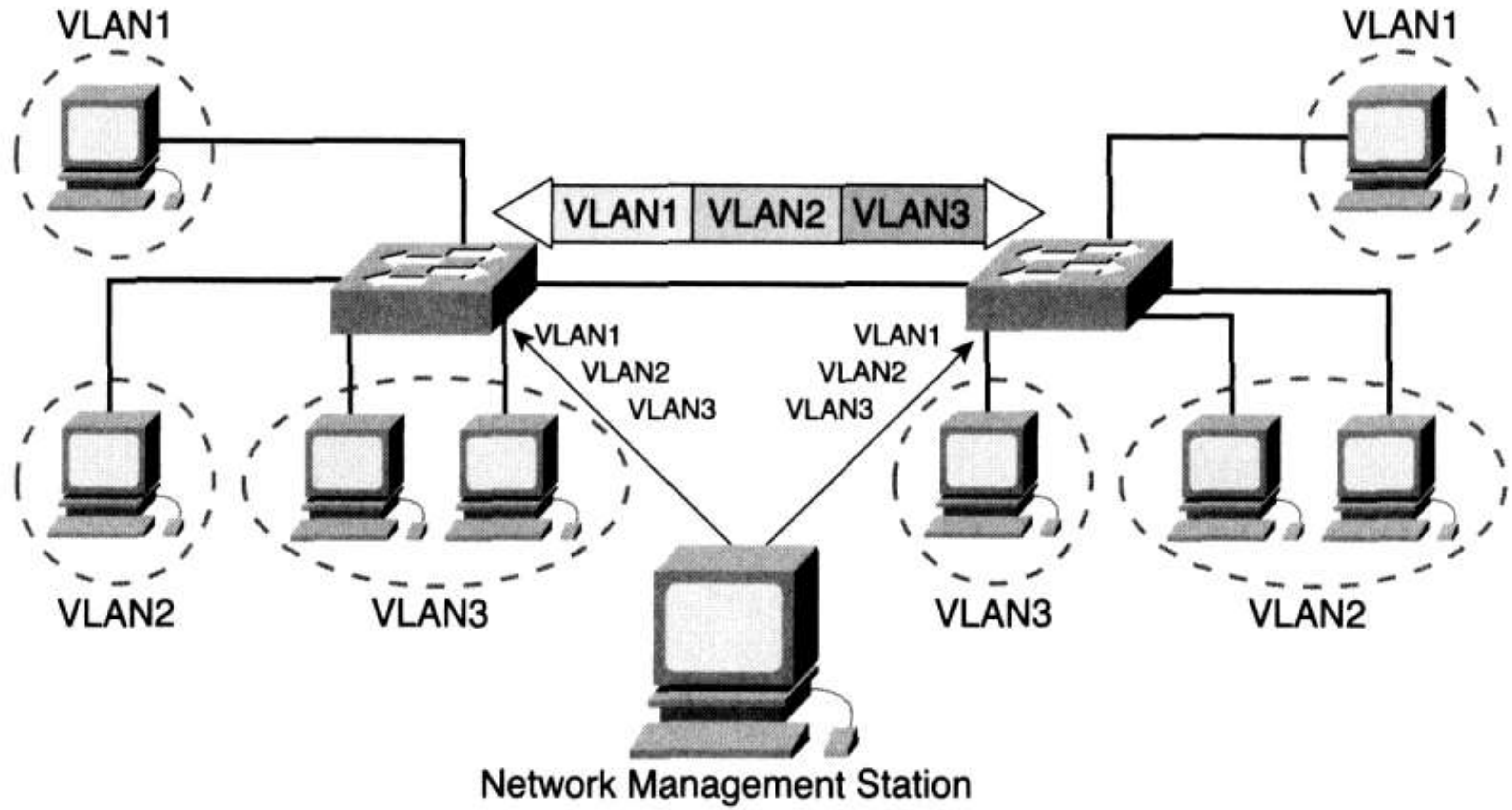
Figure 9-4 VLAN Broadcast Distribution



4.8.5 Virtual LANs

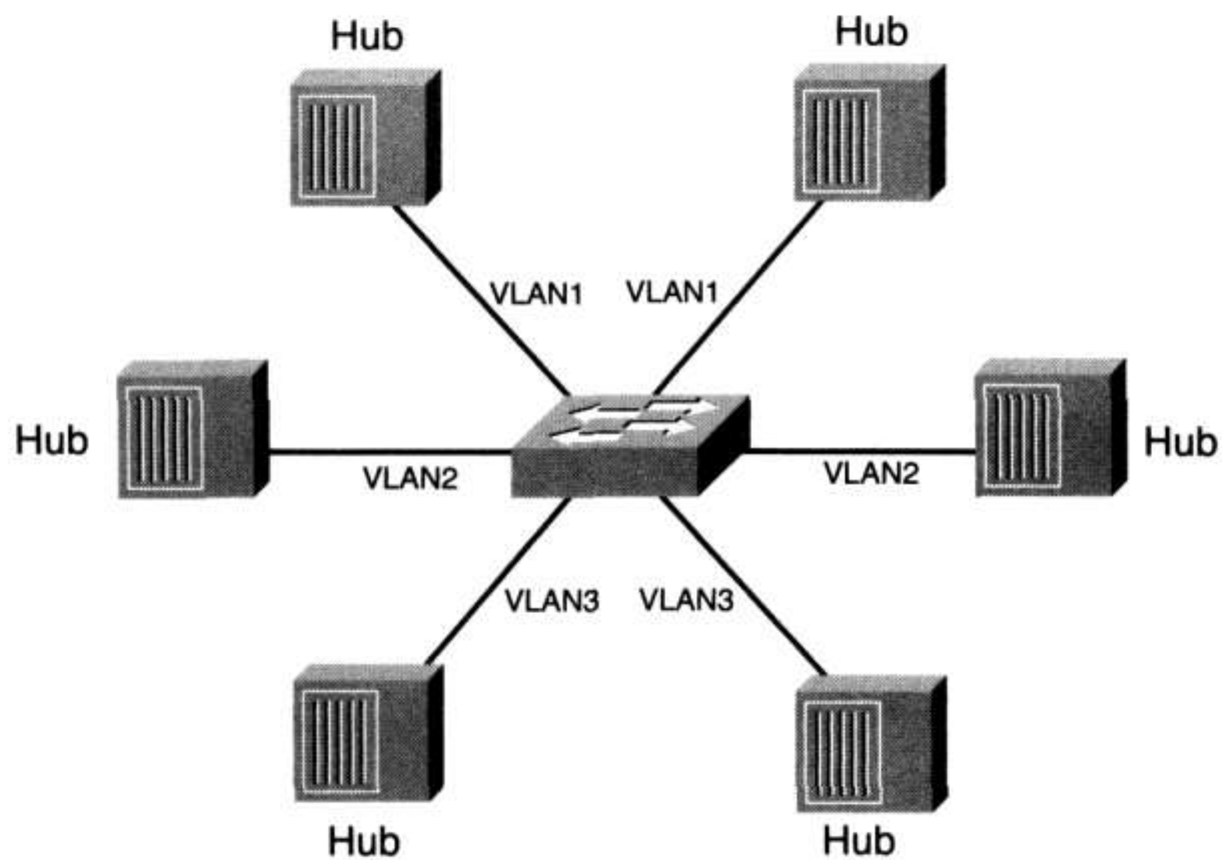
- How do bridges and switches know what color an incoming frame is:
  - **Every port** is assigned a VLAN color
    - only works if all machines on a port belong to the same VLAN
  - **Every MAC address** is assigned a VLAN color
    - has a table listing the 48-bit MAC address of each machine connected to it along with the VLAN that machine is on
  - **Every layer 3 protocol or IP address** is assigned a VLAN color
    - for the bridge or switch to examine the payload field of the frame
    - problem: it violates the most fundamental rule of networking: independence of the layers

Figure 9-5 Static VLANs



Using Hubs with VLANs

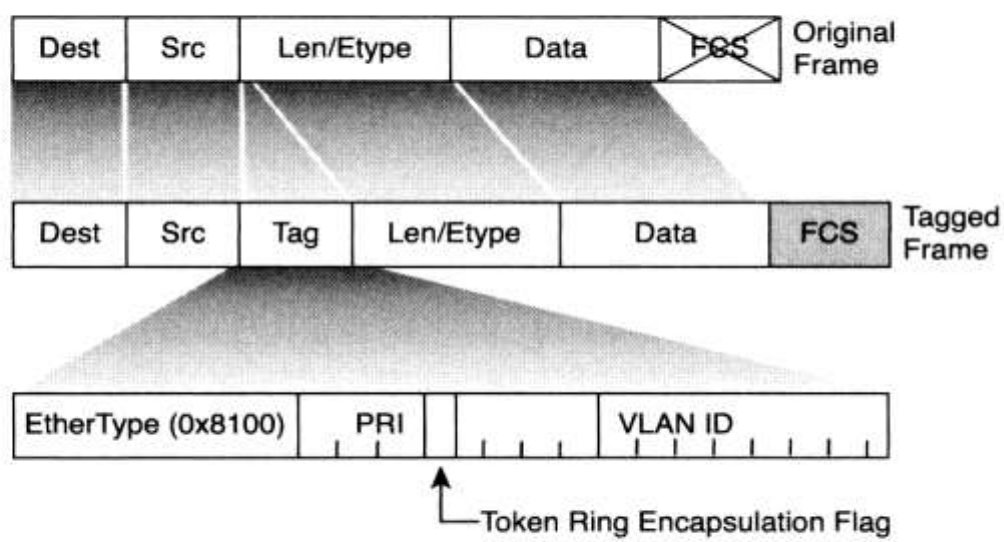
Figure 9-12 Using Existing Hubs in a Switched VLAN Environment



4.7.6 Virtual LANs

- VLAN identification logically identifies:
  - which packets belong to which VLAN group.
- **Multiple trunking methodologies**
  - IEEE 802.1Q
  - ISL
  - 802.10
  - LANE
- IEEE 802.1Q: Frame Tagging

Figure 9-13 802.1Q Frame Format



4.7.6 Virtual LANs

- **The IEEE 802.1Q Standard**
  - VLAN of the frame matters, not VLAN of the sending machine
  - A few questions:
    - Need we throw out several hundred million existing Ethernet cards?
    - If not, who generates the new fields?
    - What happens to frames that are already the maximum size?
  - Key: VLAN fields are only actually used by the bridges and switches and not by the user machines
  - transition situation: [see Fig. 4-48]
  - 802.1Q frame format: [see Fig. 4-49]

The IEEE 802.1Q Standard (1)

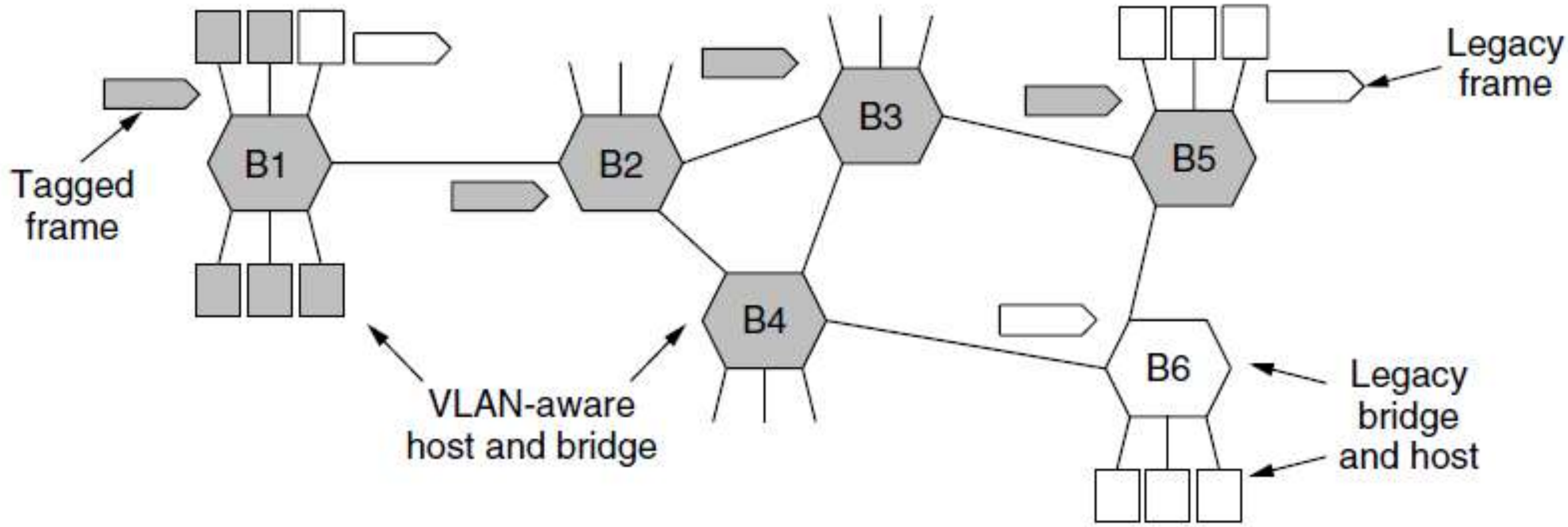
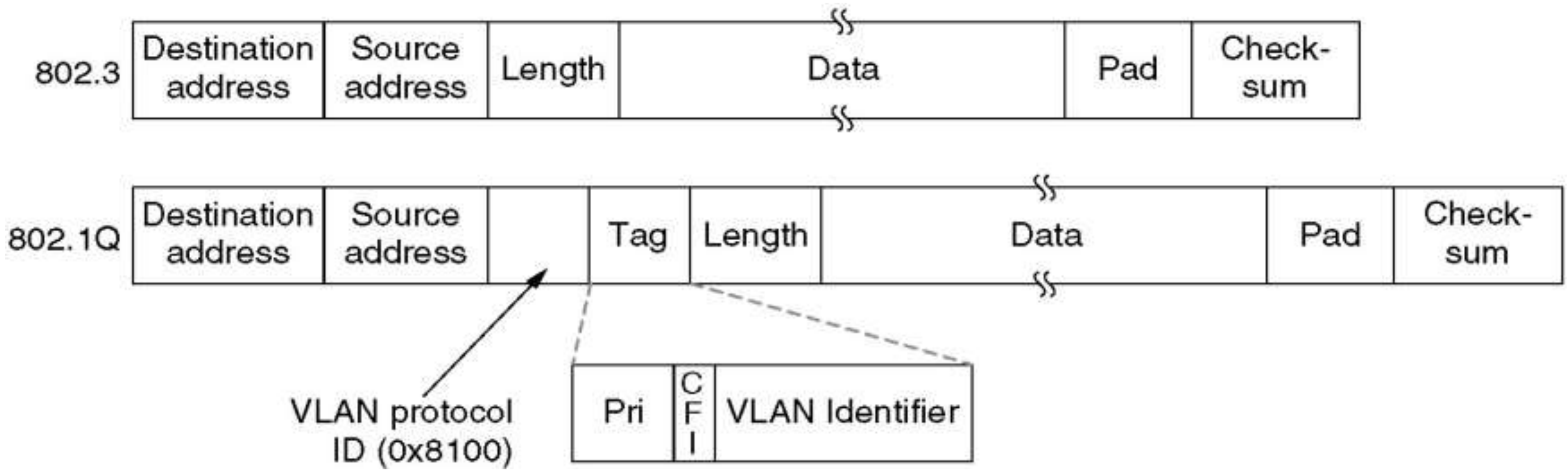


Figure 4-48. Bridged LAN that is only partly VLAN-aware. The shaded symbols are VLAN aware. The empty ones are not.

The IEEE 802.1Q Standard (2)



2 Bytes:

Pri – 3 bit

CFI– 1 bit (Corporate Format Indicator)

VLAN Id – 12 bits (4096)

Figure 4-49. The 802.3 (legacy) and 802.1Q Ethernet frame formats.

Additional Review

- **Collison domain**
  - Ethernet上数据碰撞所影响的范围
  - 总线、Hub、Repeater所连接的设备都在同一个碰撞域中
  - 交换机的每个端口是一个碰撞域
- **Broadcast domain**
  - 数据帧广播所覆盖的范围
  - Hub、Switch都在同一广播域中，但VLAN能划定广播域

4.9 Summary

Method	Description
FDM	Dedicate a frequency band to each station
WDM	A dynamic FDM scheme for fiber
TDM	Dedicate a time slot to each station
Pure ALOHA	Unsynchronized transmission at any instant
Slotted ALOHA	Random transmission in well-defined time slots
1-persistent CSMA	Standard carrier sense multiple access
Nonpersistent CSMA	Random delay when channel is sensed busy
P-persistent CSMA	CSMA, but with a probability of p of persisting
CSMA/CD	CSMA, but abort on detecting a collision
Bit map	Round robin scheduling using a bit map
Binary countdown	Highest numbered ready station goes next
Tree walk	Reduced contention by selective enabling
MACA, MACAW	Wireless LAN protocols
Ethernet	CSMA/CD with binary exponential backoff
FHSS	Frequency hopping spread spectrum
DSSS	Direct sequence spread spectrum
CSMA/CA	Carrier sense multiple access with collision avoidance

Figure 4-xx. Channel allocation methods and systems for a common channel.

Exercises

In 4th Edition:

- 2, 16-17, 21-24, 37,42-43

In 5th Edition:

- 2, 13-14, 16-18, 35-36, 38-39