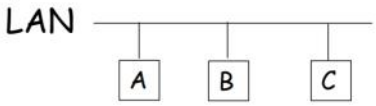
介质访问控制MAC

2019年3月19日　　23:34

- 多路访问链路（广播链路）采用共享介质连接所有站点。发送站点通过广播方式发送数据并占用整个共享介质的带宽。由于每个站点只需要一条线接入网络就可以访问所有站点，这种网络一般安装简单，价格便宜。局域网(Local Area Network, LAN)都是使用这种链路。



- 在多路访问链路中多个站点同时发送数据，则会产生冲突。这种问题是点到点链路没有的，因此，需要重新考虑数据链路层的功能设计。

划分为三种类型：

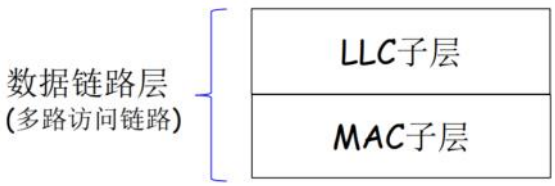
1.信道划分协议

2.随机接入协议

3.轮流协议

- OSI把为解决冲突问题而专门在数据链路层划分出的一个子层，就是介质访问控制子层(Media Access Control，MAC子层)，其功能是控制和协调所有站点对共享介质的访问，以避免或减少冲突。
- 因为MAC子层不提供可靠的数据传输，所以，在MAC子层之上又定义了一个子层，逻辑链路控制子层(Logic Link Control，LLC)，用来为上层协议提供服务：

  (1) LLC1提供无确认无连接服务;
  (2) LLC2提供有确认面向连接的服务;
  (3) LLC3提供有确认无连接的服务。



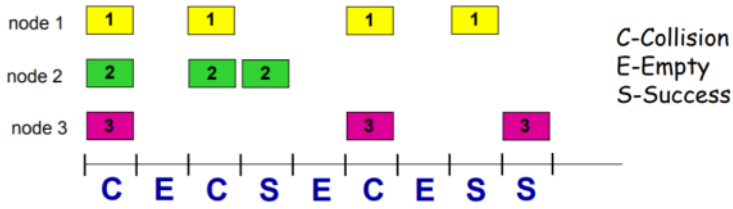
分为：介质访问控制子层（MAC）和逻辑链路控制子层（LLC）

LLC2使用了滑动窗口协议!

随机接入协议:

分槽ALOHA

把时间分为长度相同的时槽(slot)，每个站点只在时槽开始时发送。信道空，立即以概率p发送，以概率1-p延迟一个时间槽；信道忙，延迟一个时间槽。



如果N个站点要发送帧，它们在每个时槽发送的概率为p，则最大效率E为

$N * p * (1-p)^{N-1}$　　最大$E \approx 1/e \approx 36.8\%$

当p为令表达式最大，
N→∞时

当只有一个活跃结点时，时隙 ALOHA 工作出色，但是当有多个活跃结点时效率又将如何呢？这里有两个可能要考虑的效率问题。首先，如在图 5-10 中所示，当有多个活跃结点时，一部分时隙将有碰撞，因此将被“浪费”掉了。第二个考虑是，时隙的另一部分将是空闲的，因为所有活跃结点由于概率传输策略会节制传输。唯一“未浪费的”时隙是那些刚好有一个结点传输的时隙。刚好有一个结点传输的时隙称为一个**成功时隙**（successful slot）。时隙多路访问协议的**效率**（efficiency）定义为：当有大量的活跃结点且每个结点总有大量的帧要发送时，长期运行中成功时隙的份额。注意到如果不使用某种形式的访问控制，而且每个结点都在每次碰撞之后立即重传，这个效率将为零。时隙 ALOHA 显然增加了它的效率，使之大于零，但是效率增加了多少呢？

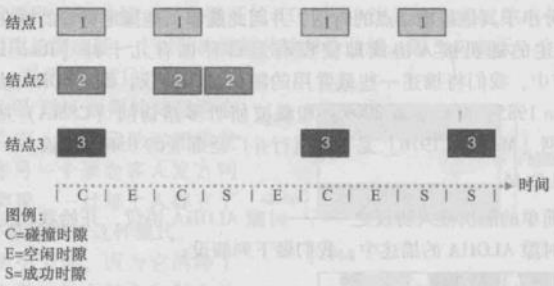


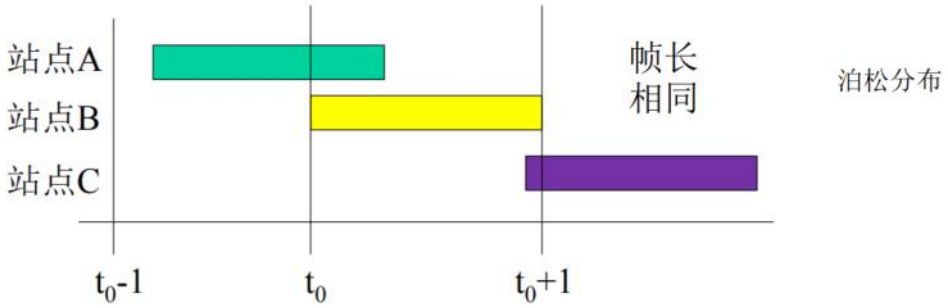
图 5-10　结点 1、2 和 3 在第一个时隙碰撞。结点 2 最终在第 4 个时隙成功，结点 1 在第 8 个时隙成功，结点 3 在第 9 个时隙成功

个结点不传输的概率。一个给定结点传输的概率是 p；剩余结点不传输的概率是 $(1-p)^{N-1}$。因此，一个给定结点成功传送的概率是 $p(1-p)^{N-1}$。因为有 N 个结点，任意一个结点成功传送的概率是 $Np(1-p)^{N-1}$。

因此，当有 N 个活跃结点时，时隙 ALOHA 的效率是 $Np(1-p)^{N-1}$。为了获得 N 个活跃结点的最大效率，我们必须求出使这个表达式最大化的 p^*。（对这个推导的一个大体描述参见课后习题。）而且对于大量活跃结点，为了获得最大效率，当 N 趋于无穷时，我们取 $Np^*(1-p^*)^{N-1}$ 的极限。（同样参见课后习题。）在完成这些计算之后，我们会发现这个协议的最大效率为 $1/e = 0.37$。这就是说，当有大量结点有很多帧要传输时，则（最多）仅有 37% 的时隙做有用的工作。因此该信道有效传输速率不是 R bps，而仅为 $0.37R$ bps！相似的分析还表明 37% 的时隙是空闲的，26% 的时隙有碰撞。试想一个整脚的网络管理员购买了一个 100Mbps 的时隙 ALOHA 系统，希望能够使用网络在大量的用户之间以总计速率如 80Mbps 来传输数据。尽管这个信道能够以信道的全速 100Mbps 传输一个给定的帧，但从长时间范围看，该信道的成功吞吐量将小于 37Mbps。

纯ALOHA

想发送就发送，超时未收到确认则认为发生了冲突。



假设一个站点在任何时刻的发送概率是p，如果有N个站点有很多帧要发送，则最大效率E为：

$$N * p * (1-p)^{N-1} * (1-p)^{N-1}$$

最大$E \approx 1/2e \approx 18.4\%$

该站点在$[t_0,t_0+1]$发送的概率

其它站点在$[t_0-1,t_0]$不发送的概率

其它站点在$[t_0,t_0+1]$不发送的概率

当p为令表达式最大，$N \to \infty$时

纯ALOHA是完全分散的，它的效率仅为分槽ALOHA的一半

- **载波侦听（carrying sensing）多路访问（CSMA）**

CSMA
(Carrier Sense Multiple Access)

发送前先监听信道

信道空，立即发送；信道忙，持续监听。

1-persistent CSMA
(以太网)

信道空，发送；信道忙，延迟一段随机长度的时间。

non-persistent CSMA

信道空，立即以概率p发送，以概率1-p延迟一个时间槽；
信道忙，延迟一个时间槽。

p-persistent CSMA
（分槽 ALOHA）

非持续CSMA（英语：non-persistent CSMA）

当要发送帧的设备侦听到线路忙或发生碰撞时，会随机等待一段时间再进行监听重复操作；此策略可以减少碰撞，但会导致信道利用率降低，以及较长的延迟。在信道比较忙的时候比较省电

1-持续CSMA（英语：1-persistent CSMA）

当要发送帧的设备侦听到线路忙或发生碰撞时，会持续侦听；若发现不忙则立即发送。当传播延迟较长或多个设备同时发送帧的可能性较大时，此策略会导致较多的碰撞，导致性能降低。CSMA/CD采用这种

p-持续CSMA（英语：p-persistent CSMA）

当要发送帧的设备侦听到线路忙或发生碰撞时，会持续侦听；若发现不忙，则根据一个事先指定的概率p来决定是发送帧还是继续侦听（以p的概率发送，1-p的概率继续侦听）如果没有发送则延迟一段时间后，再次监听重复操作；此种策略可以达到一定的平衡，但对于参数p的配置会涉及比较复杂的考量。

正确使用以上策略可以在一定程度上减少碰撞的发生，但无法彻底解决碰撞问题。

- 说话之前先听。如果其他人正在说话，等到他们说完话为止。在网络领域中，这被称为**载波侦听**（carrier sensing），即一个结点在传输前先听信道。如果来自另一个结点的帧正向信道上发送，结点则等待直到检测到一小段时间没有传输，然后开始传输。
- 如果与他人同时开始说话，停止说话。在网络领域中，这被称为**碰撞检测**（collision detection），即当一个传输结点在传输时一直在侦听此信道。如果它检测到另一个结点正在传输干扰帧，它就停止传输，在重复“侦听－当空闲时传输”循环之前等待一段随机时间。

这两个规则包含在**载波侦听多路访问**（Carrier Sense Multiple Access，CSMA）和**具有碰撞检测的CSMA**（CSMA with Collision Detection，CSMA/CD）协议族中［Kleinrock 1975b；Metcalfe 1976；Lam 1980；Rom 1990］。人们已经提出了CSMA和CSMA/CD的许多变种。这里，我们将考虑一些CSMA和CSMA/CD最重要的和基本的特性。

侦听需要持续一段时间才能判断信道为空

- **具有碰撞检测的载波侦听多路访问：CSMA/CD**

以太网的MAC层协议

- 发送帧的方法--CSMA/CD(Carrier Sense Multiple Access With Collision Detection)协议：

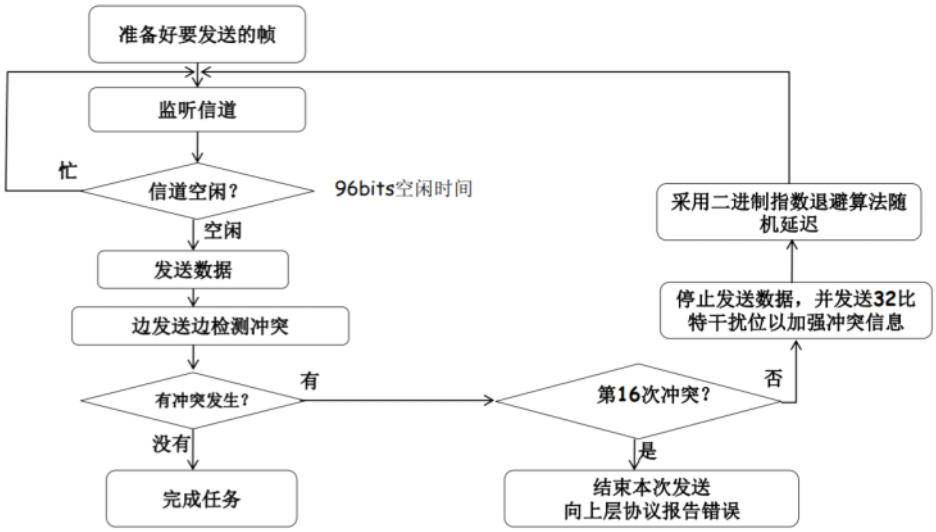
(1) 发送数据帧之前先监听信道。如果信道空闲，立即发送。如果信道忙，则持续监听，直到信道空闲，立即发送。

(2) 边发送边检测冲突。如果发送完毕都没有检测到冲突，则发送成功。

(3) 如果检测到冲突，则停止发送，并发送32位干扰位(jamming signal)以加强冲突信号。采用二进制指数退避算法随机延迟一段时间后，转(1)。

因为是边发送边检测冲突，所以有最短帧的问题！

- CSMA/CD协议的流程图



当到第16次冲突发生，就会自己结束信息传输，并报告错误

帧间距： 96bit空闲时间：检测时间不能太短，也要统一才能防止信道不公平的竞争。因为如果有一个等待时间比较短，他就总是先于其他站点发送。

- **二进制指数退避算法：**

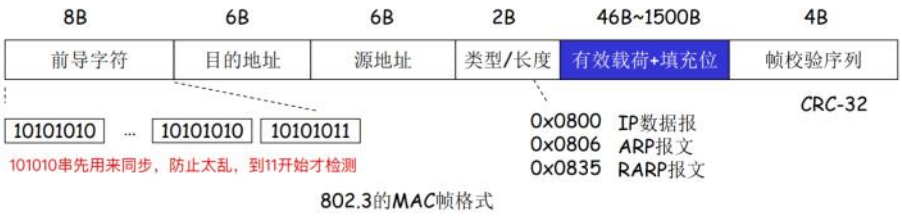
用于以太网以及 DOCSIS 电缆网络多路访问协议［DOCSIS 2011］中的**二进制指数后退**（binary exponential backoff）算法，简练地解决了这个问题。特别是，当传输一个给定帧时，在该帧经历了一连串的 n 次碰撞后，结点随机地从 $\{0, 1, 2, \cdots, 2^n - 1\}$ 中选择一个 K 值。因此，一个帧经历的碰撞越多，K 选择的间隔越大。对于以太网，一个结点等待的实际时间量是 $K \cdot 512$ 比特时间（即发送 512 比特进入以太网所需时间量的 K 倍），n 能够取的最大值在 10 以内。

我们看一个例子。假设一个适配器首次尝试传输一个帧，并在传输中它检测到碰撞。然后该结点以概率 0.5 选择 $K=0$，以概率 0.5 选择 $K=1$。如果该结点选择 $K=0$，则它立即开始侦听信道。如果这个适配器选择 $K=1$，它在开始“侦听－当空闲时传输”。周期前等待 512 比特时间（例如对于 100Mbps 以太网来说为 5.12 毫秒）。在第 2 次碰撞之后，从 $\{0, 1, 2, 3\}$ 中等概率地选择 K。在第 3 次碰撞之后，从 $\{0, 1, 2, 3, 4, 5, 6, 7\}$ 中等概率地选择 K。在 10 次或更多次碰撞之后，从 $\{0, 1, 2, \cdots, 1023\}$ 中等概率地选择 K。因此从中选择 K 的集合长度随着碰撞次数呈指数增长；正是由于这个原因，该算法被称为二进制指数后退。

这里我们还要注意到，每次适配器准备传输一个新的帧时，它要运行 CSMA/CD 算法。不考虑近期过去的时间内可能已经发生的任何碰撞。因此，当几个其他适配器处于指数后退状态时，有可能一个具有新帧的结点能够立刻插入一次成功的传输。

注意：冲突最多到10次之后就不会在增加时间片数量!

802.3的MAC帧格式



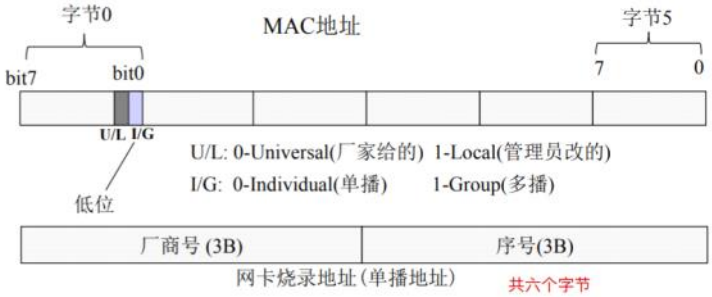
802.3的MAC帧格式

- 前导字符(Preamble)：同步字符(7B)和起始定界符(Start of Frame Delimiter)(1B)。
- 有效载荷(Payload)：用户数据。不足46字节时加入填充字节(任何字节)至46字节。
- 类型/长度字段(Type/Length)：指明上层协议(>1500)或有效载荷的长度(≤1500)。
- 帧校验序列(Frame Check Sequence)：对目的地址、源地址、类型/长度和有效载荷（加填充位）字段进行CRC-32校验。

[类型/长度字段]
DIXv2帧 ——〉 类型。≥1536 （0x0600）
802.3帧（原） ——〉 长度。(SNAP格式)
802.3帧（1997年修订）——〉 类型/长度。

1500是十进制，0X800是16进制，相当于2048 大于1500表示协议

- 源地址和目标地址(6B)
  - 源地址一般为发送者的单播地址。目标地址可以是接收者的单播地址，也可以是多播地址和广播地址。
  - **单播地址**：全球唯一。每个网卡(或接口)一个，最高字节的最低有效位为0。如：06-01-02-01-2C-4B。也称为网卡地址，烧录地址(Burned-In-Address，BIA)，MAC地址，硬件地址，物理地址。
    多播地址的字节0的第0位为1 ，并且地址非全1。如：01-00-5E-20-01-4B。
    广播地址的48位全为1。



IEEE为每个厂商分配的唯一的**厂商号**(Organization Unique Identifier，OUI)。例如，00-00-0C和00-AA-00分别为思科和Intel的厂商号。厂商再为其生产的每个网卡或接口分配**序号**。

从字节0开始发送，每个字节从低位(bit0)开始发送(802.3和802.4),802.5和802.6从高位(bit7)开始发送。

接收帧的方法

（1）以太网站点(网卡)会缓存所有的帧

（2）如果缓存的帧有错 (长度错误，CRC错等)，则丢弃它。

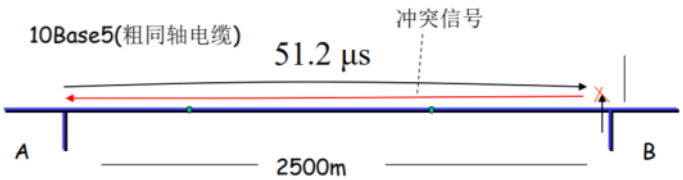
（3）如果缓存的帧的目的地址为**单播地址**并且与接收该帧的网卡的MAC地址一致，则接收它。如果目的地址为**多播地址**并且为网卡预设的多播地址之一，或者**为广播地址**，也接收它。其它情况则丢弃它。

（4）如果把网卡设置为**混杂模式**则会接收所有无错的帧。

如果想要发多播，就需要把分组内的所有设备多播地址设置为相同的多播地址，然后往这个地址发送

最短帧问题

为什么数据长至少要为46字节，否则要加填充位



- 以太网(10M bps)相距最远的两个站点（上图站点A和B)之间的 信号往返时间为51.2 μs。
- 假如站点A发送的数据在快到达站点B时与其发送的数据冲突，因为发送站点只在发送时才检测冲突，为了检测到返回的冲突信号，则要求站点A此时还在发送，故帧长至少为512b(64B)。
- 64B也称为**争用窗口(contention window)长度**。

64个字节不包括前导字节，所以数据段至少要46个字节

以太网(802.3)的物理层(1)

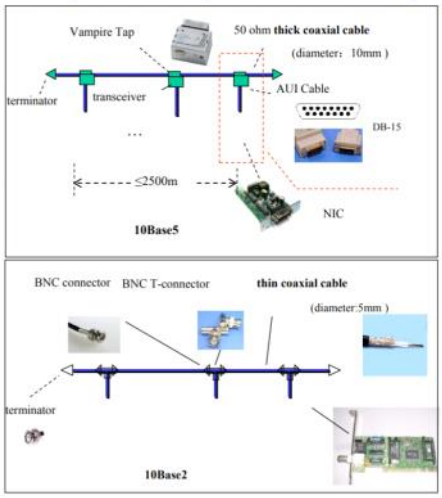
◘ 物理层规范

名称	传输技术	传输介质	网段最大距离	每段最多节点数	IEEE标准及发布时间
10Base5	基带	50欧姆粗同轴电缆	500m	100	802.3，1980
10Base2	基带	50欧姆细同轴电缆	185m	30	802.3a，1985
10BaseT	基带	Cat-3,Cat-5 UTP	100m	1024	802.3i, 1990
10BaseF	基带	光纤， 850nm波长	2000m	1024	802.3j, 1993

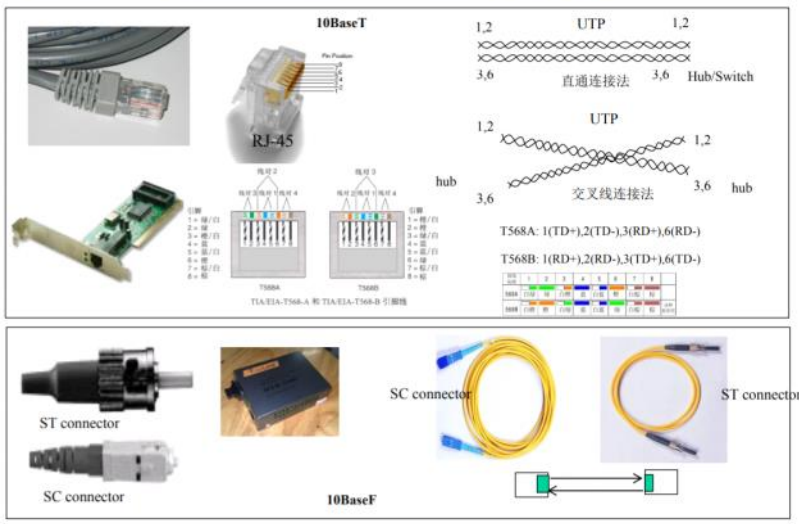
- **传输方法**：均使用异步传输，即信道空闲时以太网设备不任何发送信号。
- **编码方法**：采用曼彻斯特编码。
- **命名规则**：10BaseT ---- 10表示10Mbps，Base表示基带传输，T表示双绞线；10base2的2表示最大距离200m。

早期的以太网为10Broad36

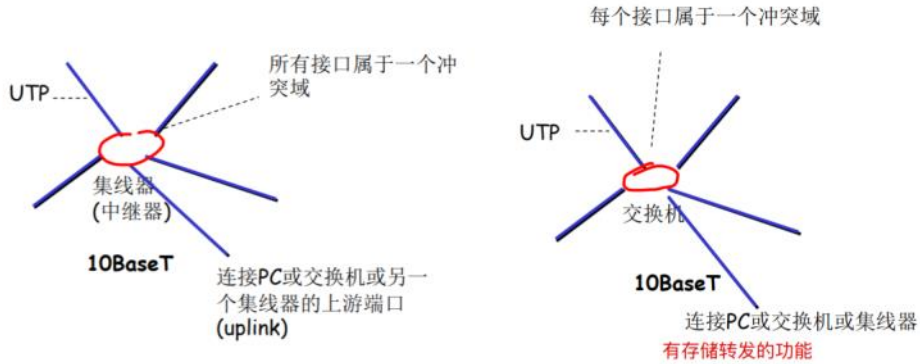
以太网(802.3)的物理层(2)



以太网(802.3)的物理层(3)



以太网(802.3)的物理层(4)



- 如果通过两个接口同时发送数据会产生冲突，则这两个接口属于同一个冲突域(collision domain)。一个广播帧可以到达的所有接口属于同一个广播域。
- 属于同一个冲突域的以太网部分称为网段(segment)。

集线器的英文称为“Hub”。“Hub”是“中心”的意思，集线器的主要功能是对接收到的信号进行再生整形放大，以扩大网络的传输距离，同时把所有节点集中在以它为中心的节点上。它工作于OSI(开放系统互联参考模型)参考模型第一层，即“物理层”。集线器与网卡、网线等传输介质一样，属于局域网中的基础设备，采用CSMA/CD（即带冲突检测的载波监听多路访问技术)介质访问控制机制。集线器每个接口简单的收发比特，收到1就转发1，收到0就转发0，不进行碰撞检测。

集线器（hub） 属于纯硬件网络底层设备，基本上不具有类似于交换机的"智能记忆"能力和"学习"能力。它也不具备交换机所具有的MAC地址表，所以它发送数据时都是没有针对性的，而是采用广播方式发送。也就是说当它要向某节点发送数据时，不是直接把数据发送到目的节点，而是把数据包发送到与集线器相连的所有节点

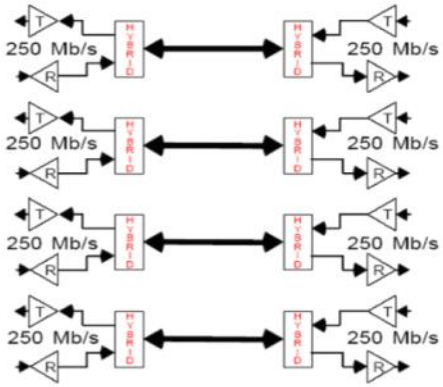
快速以太网概述

- 1995年，IEEE发布了100Mbps的快速以太网的标准IEEE 802.3u。
- 与802.3相比，快速以太网只是把传输速率提高到100Mbps，其它均保持不变：
  1）MAC子层的协议不变：CSMA/CD协议不变，帧格式不变。
  2）最大距离改为100m (10base5的最大距离为2500m)。
  3）帧间空隙隔依然为96b，即0.96 μs。

	电缆	接头	编码方案	距离	传输方向
100Base-TX	Cat 5/Cat 5e UTP(两对) 100-ohm STP(两对)	RJ-45/DB-9	4B/5B MLT-3	100m	全双工
100Base-T4	Cat 3/Cat 4/Cat 5 UTP(四对) (思科不支持)	RJ-45	8B/6T 一种3级编码	100m	半双工
100Base-FX	2个多模光纤	SC或ST	4B/5B NRZI	2000m	全双工

千兆以太网
(802.3ab：1000Base-T)

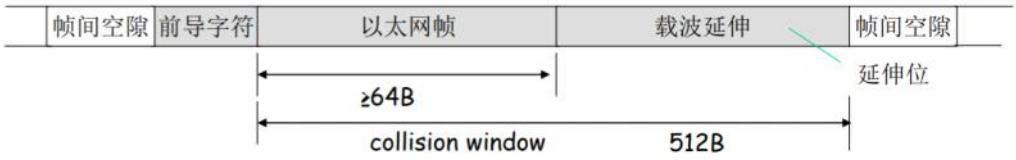
- 使用5类或以上UTP的4对双绞线。每对线每个方向125M波特率和250Mbps。采用了复杂的编码方式8B1Q4和4D-PAM5，并利用混波电路将发送信号和接收信号耦合在同一线缆中传输，使其互不干扰，从而实现了双向传输。
- 可以采用全双工(交换机)或半双工(集线器)传输。



编码和调制方法：
8B1Q4(8-bit 1-Quinary Quarter)
4D-PAM5(4-dimensional 5-level Pulse Amplitude Modulation)。

- 和快速以太网一样，802.3ab除了把传输速率提高1000Mbps，其它不变。由于1000Base-T的速度提高了100倍，故半双工的冲突域也要减少为1/100，即25m。这个距离很难接受，怎么办？可以采用载波延伸技术延长距离到200m。

(1) **载波延伸**(carrier extension)：通过附加填充字节，令帧长至少为512B，网络半径可以延长到200m。填充字节称为延伸位(extension bits)。



(2) **帧突发**(frame bursting)：发送很多短帧时采用载波延伸浪费很大。可以采用帧突发进行改进，即一次传送多个短帧。第一帧小于512B时进行载波延伸，后面的帧直接发出，不用加载波延伸。每一帧之间有一个小的间隔，填入延伸位。

帧突发：https://baike.baidu.com/item/帧突发/10132814?fr=aladdin

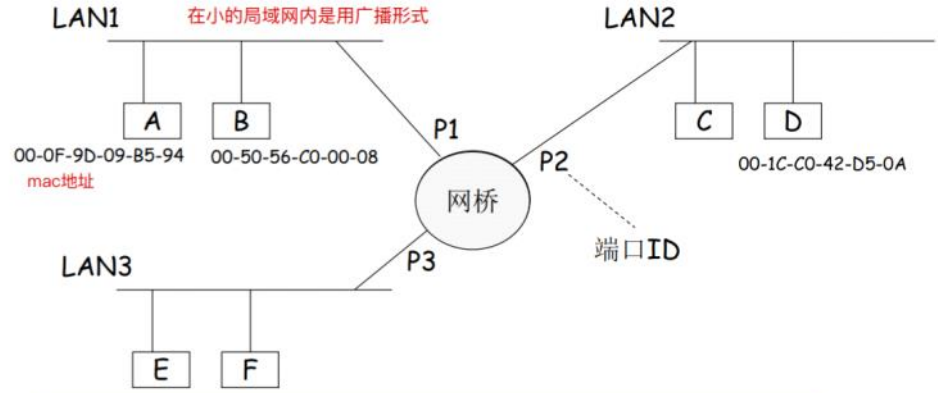
万兆以太网
(10 Gigabit Ethernet)

- 特性

(1) 保持帧格式不变
(2) 光纤或双绞线，全双工
(3) 无冲突，不使用CSMA/CD算法

透明网桥 (1)

- 扩展局域网　三个以太网，用网桥连接形成一个更大的以太网



- 用网桥(bridge)连接若干局域网(LAN)可以建造一个更大的局域网，称为**桥接的局域网**(bridged LAN) 或 **扩展局域网**(extended LAN)。
- 原来的局域网就成为该扩展局域网的一部分，称为该扩展局域网的一个网段(Segment)。

透明网桥 (2)

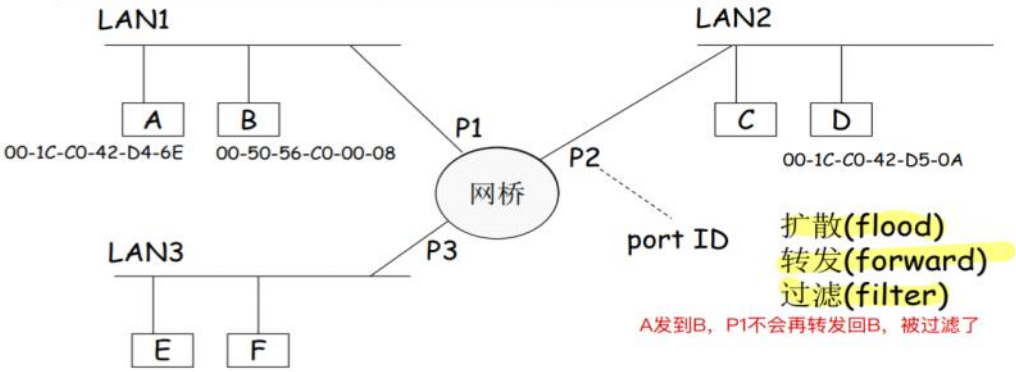
- MAC地址表

Time-To-Live(生存期)

目的MAC 地址	转发端口	TTL(sec)
00-50-56-C0-00-08	P1	60
00-1C-C0-42-D5-0A	P2	120

端口(port)

超时了就会删除这一项



TTL的作用：

1.因为主机有可能被接到其他的端口上，旧的表就无法使用了，所以要不断更新

2.有一些地址因为不活跃没必要记录，节约MAC地址表的空间

透明网桥 (3)

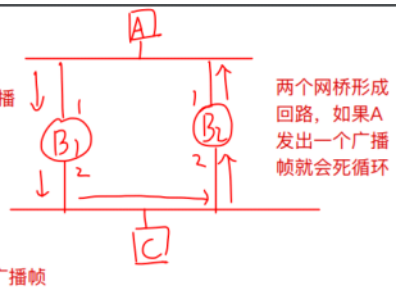
当网桥收到一个单播帧，它会用该帧的目的地址查询MAC地址表

1. 如果没有查到，则扩散(flood)该帧。
2. 如果查到，则看查到的端口是否为收到该帧的端口，
   如果是，则丢弃该帧(filter)，
   否则，把该帧从查到的端口发送出去(forward)。

当网桥收到一多播或广播帧，它会直接扩散(flood)该帧。

扩散(flood)就是网桥把收到的帧转发到除了该帧的接收端口之外的所有其它端口。

透明网桥(4)



如果A给C发一个单播就没事

两个网桥形成回路，如果A发出一个广播帧就会死循环

自学习

通过原地址来学习

- MAC地址表初始为空。 电脑刚连接就会发送一个广播帧
- 网桥从端口接收所有的帧，并把接收到的帧的源地址和接收端口记录到MAC地址表中：如果该源地址在MAC地址表中不存在，则增加一个新记录，并启动超时定时器；如果存在，则更新接口并重置超时定时器。
- 网桥会自动删除超时的记录。

为什么叫透明网桥(Transparent Bridges)?

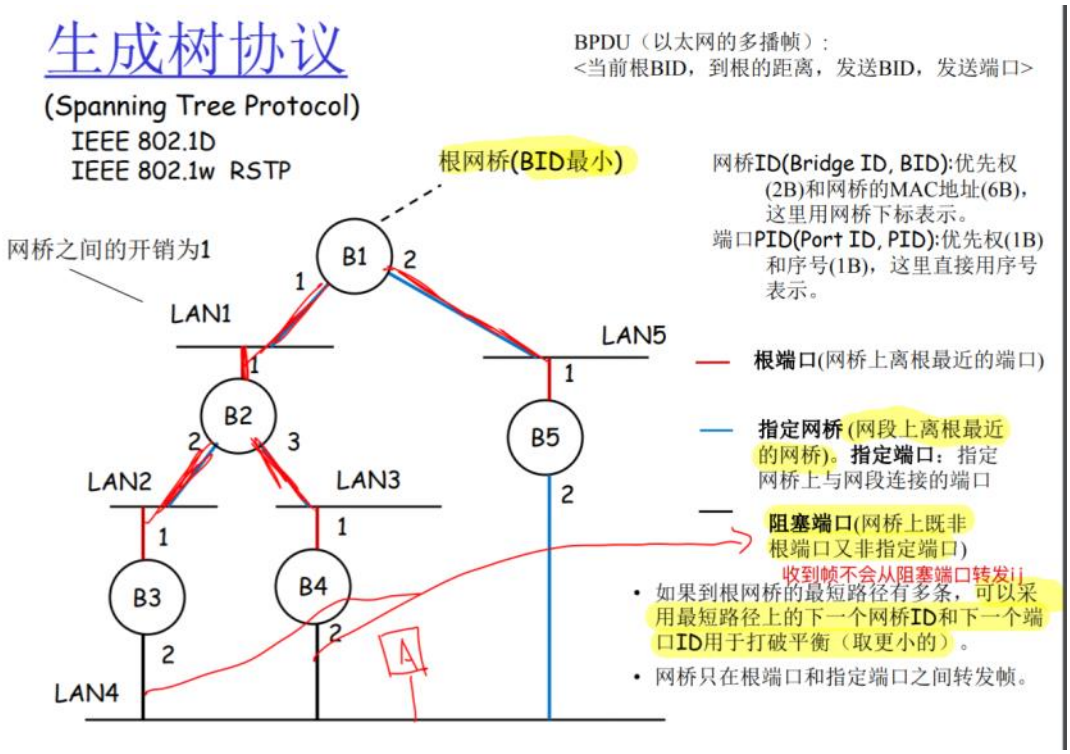
因为不需要任何协议或者软件，只要装上交换机，就能够工作。

为什么叫透明网桥?

1. 以太网上的站点并不知道经过哪几个网桥，
2. 即插即用，只要将网桥接入局域网，不用人工配置转发表，网桥就能工作

透明网桥和交换机关系

1. 联系：风格与交换机都基于帧地址进行路由。
2. 交换机相当于多（高密度）端口的网桥（网桥早期只是连接两个局域网）



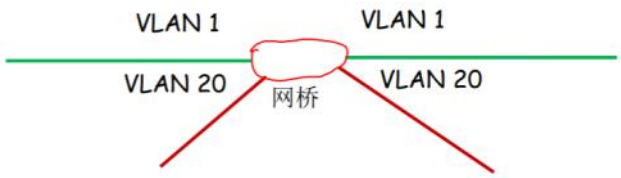
解决广播风暴问题

1.生成树算法：在图上确定根节点，每个节点找一条到根的最短路径，如果有多条只取一条选

2.平衡算法：当有多条可选的时候，选路径上下一个网桥BID最小的

3.选指定网桥：B1发消息，B3B4B5都会知道互相离根的距离，竞选结果离根最小的就是这个网段的指定网桥，同时指定端口也被确定，没选上的连接这个网断的就变成阻塞端口

虚拟局域网(1)



用一台网桥实现多台的效果

如果网桥只在具有相同颜色的端口(Port)之间转发帧，就会把原来的局域网分割成多个相互隔离的局域网，称为虚拟局域网(Virtual LAN，VLAN)。

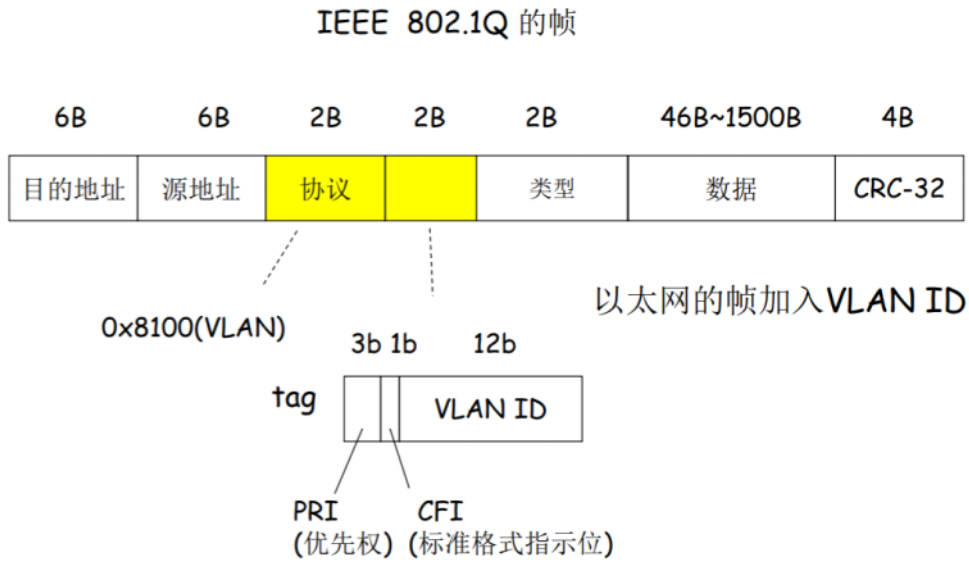
所谓的颜色其实就是VLAN ID，是由管理员为每个端口配置的一个标识。具有相同的VLAN ID的端口处于同一个VLAN，端口的默认VLAN为VLAN 1。

虚拟局域网(2)

一个VLAN的帧只能转发到属于同一个VLAN的端口或者干道(trunk)端口。只有发往干道端口的帧才需要加上VLAN ID。从干道收到的帧中如果没有VLAN ID，则认为是本征VLAN(Native VLAN)，默认为VLAN 1。发往干道的Native VLAN的帧不加VLAN ID。

只会转发到相同颜色的端口和干道

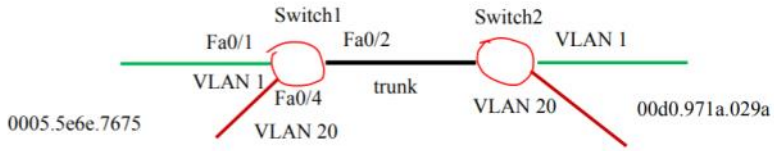
虚拟局域网(3)



比原来的至少64位的帧新增了4个字节（黄色部分）

虚拟局域网(4)

- VLAN 举例



Switch1#show mac-address-table

Vlan	Mac Address	Type	Ports
1	0005.5e6e.7675	DYNAMIC	Fa0/1
1	00d0.971a.029a	DYNAMIC	Fa0/2
20	0002.4a1b.d297	DYNAMIC	Fa0/4
20	000c.cfd7.ac07	DYNAMIC	Fa0/2

左表中的DYNAMIC 是指通过学习得到的而不是手工配置的

虚拟局域网(5)

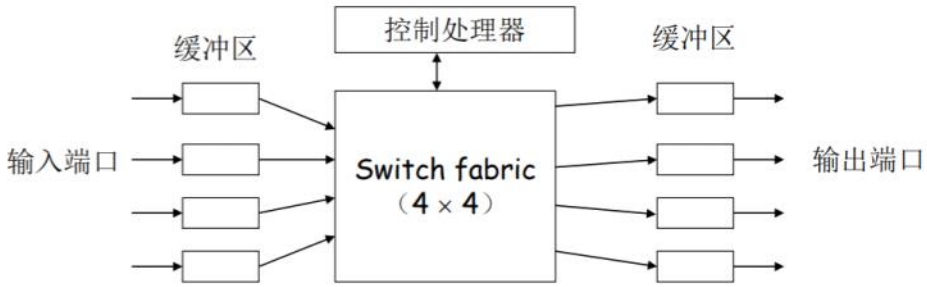
- CST, PVST+ and MSTP
  - IEEE 802.1Q中定义了由所有VLAN共享一棵树的公共生成树 (Common Spanning Tree，CST) 。
  - 具有思科专利的PVST(Per-VLAN Spanning Tree)协议为每个VLAN配置一颗生成树。由于 PVST 只能用于ISL，思科又定义了同时可用于IEEE 802.1Q的PVST+标准。思科的设备现在默认使用PVST+。
  - 多生成树MSTP (Multiple Spanning Tree Protocol)起初单独由IEEE 802.1s定义，后来并入IEEE 802.1Q-2005。它是RSTP的一个扩展，并可以把VLAN分组，每个VLAN组使用一颗生成树。
  - BID：PRIORITY(4b)+VLAN ID(12b)+MAC addr(6B)
    PRIORITY(4b):0,4096,... ,32768(default),..., 61440

虚拟局域网（VLAN）是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样，由此得名虚拟局域网。VLAN是一种比较新的技术，工作在OSI参考模型的第2层和第3层，一个VLAN就是一个广播域，VLAN之间的通信是通过第3层的路由器来完成的。与传统的局域网技术相比较，VLAN技术更加灵活，它具有以下优点： 网络设备的移动、添加和修改的管理开销减少；可以控制广播活动；可提高网络的安全性。

交换机 (1)

❑ 概述

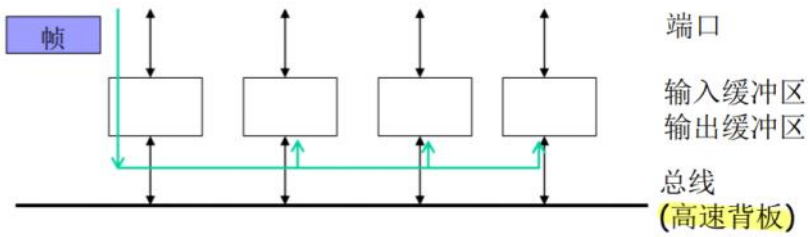
- 交换机(switch)是一个把多个网段连接起来的设备，也称为多端口网桥。



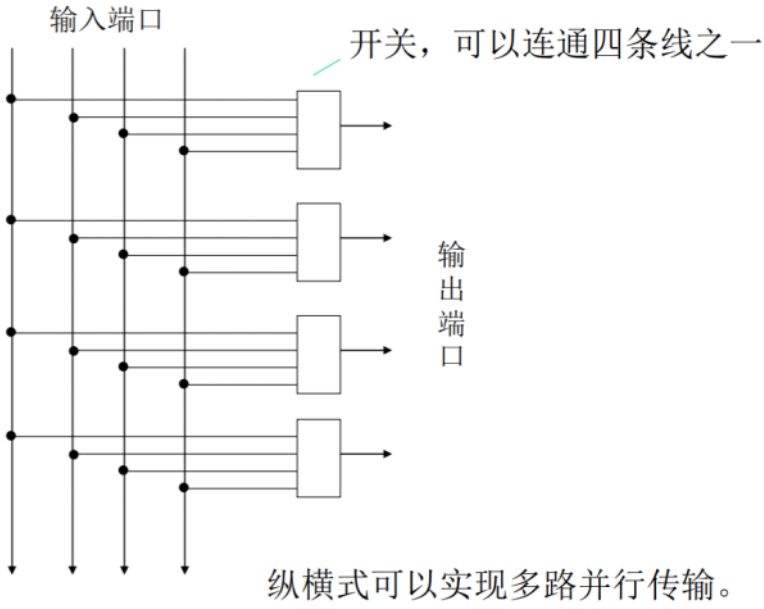
交换机(2)

❑ 交换结构(Fabrics)

- 共享总线式交换机



- **纵横式（crossbar）**



交换机(3)

❑ 转发方法

- **存储转发(Store and forward)**: 交换机接收整个帧后转发它。大部分交换机都采用这种转发模式。
- **直通(Cut through)**: 交换机不用收到整个帧而是收到帧的硬件地址后立即转发它。如果输出(outgoing port)忙，则会转为存储转发。
- **无碎片(Fragment free)**: 交换机不用收到整个帧而是收到帧的前64个字节（冲突窗口）后立即转发它。
- **适应性交换(Adaptive switching)**: 自动在上面三种方式进行选择。

- 直通的方法如果出现冲突就会导致发送一些无用的碎片!

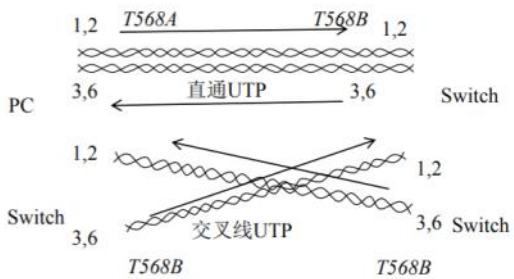
交换机(4)

❑ 全双工模式

交换机可以工作在全双工模式下，因为没有冲突，CSMA/CD算法可以被关闭。

❐ 自动翻转(Auto-MDIX)

大部分交换机可以自动选择连接方式：交叉线或直通线



网线的线序又分为两种：568A与568B。

标准568A线序：1-绿白，2-绿，3-橙白，4-蓝，5-蓝白，6-橙，7-棕白，8-棕；

标准568B线序：1-橙白，2-橙，3-绿白，4-蓝，5-蓝白，6-绿，7-棕白，8-棕；

直连线，同一根网线的两端使用同样的线序；

交叉线，同一根网线的两段使用不同的线序。

即，网线的两端都使用568A或568B的是直连线；网线两端，一端用568A，一端用568B的是交叉线。在实际运用中一般都使用568B，通常认为568B对电磁干扰的屏蔽比较好。

直通线用来连接电脑和交换机（或HUB），路由器和交换机（或HUB）。

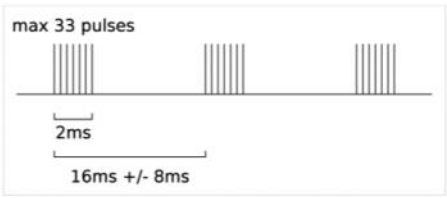
交叉线用来连接电脑和电脑，路由器和路由器。交叉线并不常使用。

这个教你一个简单的办法，就是同种设备用交叉线，异种设备用直连线。

交换机(5)

❑ 自适应(Autonegotiation)

两个站点周期性使用快速链路脉冲(fast link pulse,FLP)选择10M/100M/1000M bps 自适应

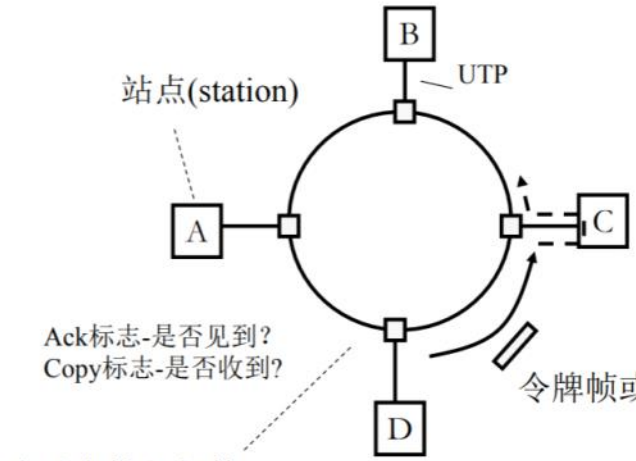


快速以太网

令牌环网(1)

轮流协议

令牌环网(Token Ring)是一个通过在站点之间传递令牌防止冲突并且具有优先权的星形LAN，其标准为IEEE 802.5。现在有千兆令牌环网。



IBM 8228 MSAU

监控站、无主帧

Random Access Protocol
Take Turns Protocol
Centralized Protocol

- **令牌**实际上是一个特殊格式的帧，本身并不包含信息，仅控制信道的使用，确保在同一时刻只有一个节点能够独占信道。当环上节点都空闲时，令牌绕环进行。节点计算机只有取得令牌后才能发送数据帧，因此不会发生碰撞。由于令牌在网环上是按顺序依次传递的，因此对所有入网计算而言，访问权是公平的

  由于每个节点不是随机的争用信道，不会出现冲突，因此称它是一种确定型的介质访问控制方法，而且每个节点发送数据的延迟时间可以确定

  a. 在轻负载时，由于存在等待令牌的时间，效率低
  b. 在重负载时，对各节点公平，且效率高

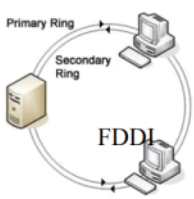
  采用令牌环的局域网还可以对各节点设置不同的优先级，具有高优先级的节点可以发送数据，比如某个节点需要传输实时性的数据，就可以申请高优先级

令牌环网(2)

数据传送过程:

- 令牌(帧)绕环而行。
- 只有截获令牌的站点才可以发送数据帧。
- 发送的数据帧通过所有的活动站点。
- 目的站点拷贝数据帧。
- 只有发送方移除数据帧。
- 当没有数据帧要发送或者持有时间到，当前的发送站点要释放令牌。被释放的令牌继续绕环而行。

光纤分布式数据接口(Fiber Distributed Data Interface, FDDI)是另一种采用了令牌环的局域网，是一种100 Mbps的光纤局域网。



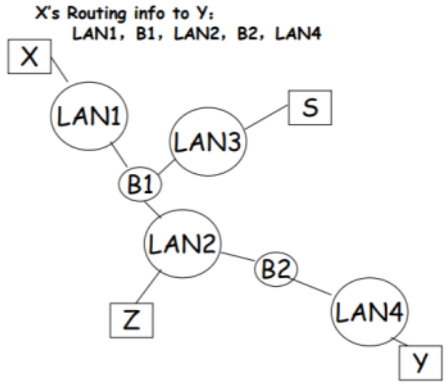
- **工作流程:**

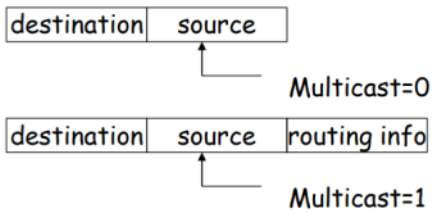
  当环上的一个工作站希望好送帧时，必须首先等待令牌。所谓令牌是一组特殊的比特，专门用来仲裁由哪个工作站访问网环。一旦收到令牌，工作站便可启动发送帧。帧中包括接收站的地址，以标识哪一站应接收此帧。帧在环上传送时，不管帧是否是针对自己工作站的，所有工作站都进行转发，直到待回到帧的始发站，并由该始发站撤消该帧。帧

的意图接收者除转发帧外，应针对自身站的帧维持一个副本，并通过在帧的尾部设置“响应比特”（copy）来指示已收到此副本。当没有帧要发送或时间到，释放令牌。

源路由网桥

- 源路由桥接算法是由IBM开发的用于令牌环网的协议。
- 为了兼容，源路由网桥交换机也必须实现透明网桥的功能。





IEEE 802系列标准