



数据链路层的作用



目录

Contents



学习目标

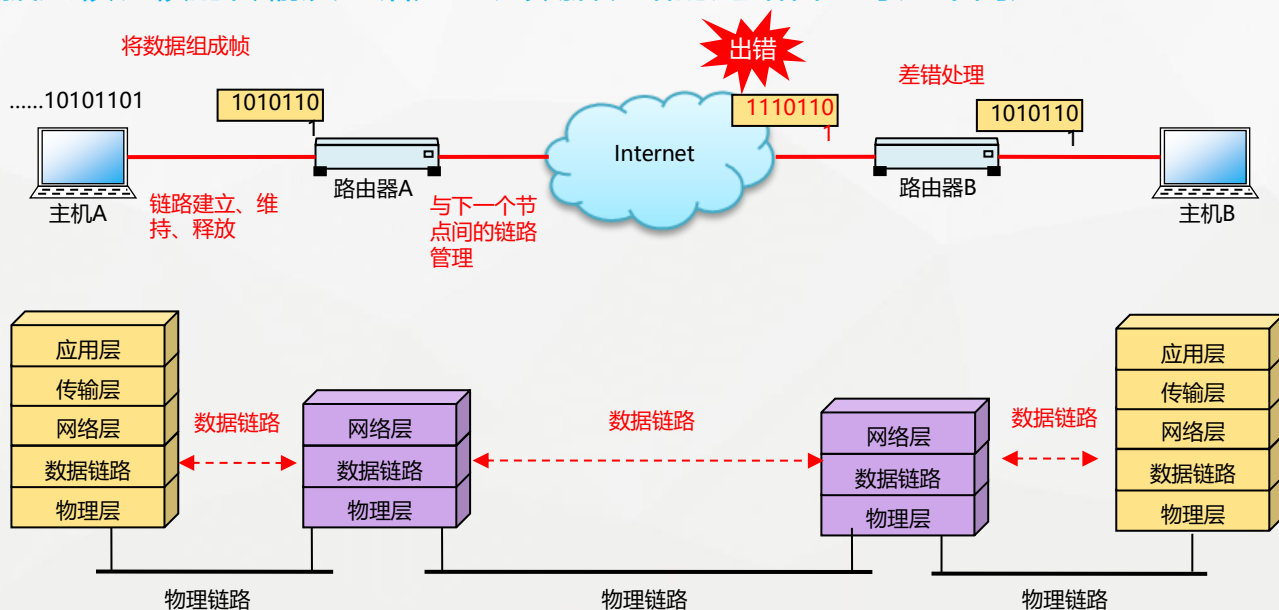
- 理解数据链路层所解决的问题
- 掌握数据链路层的功能

1/ 数据链路层解决的问题

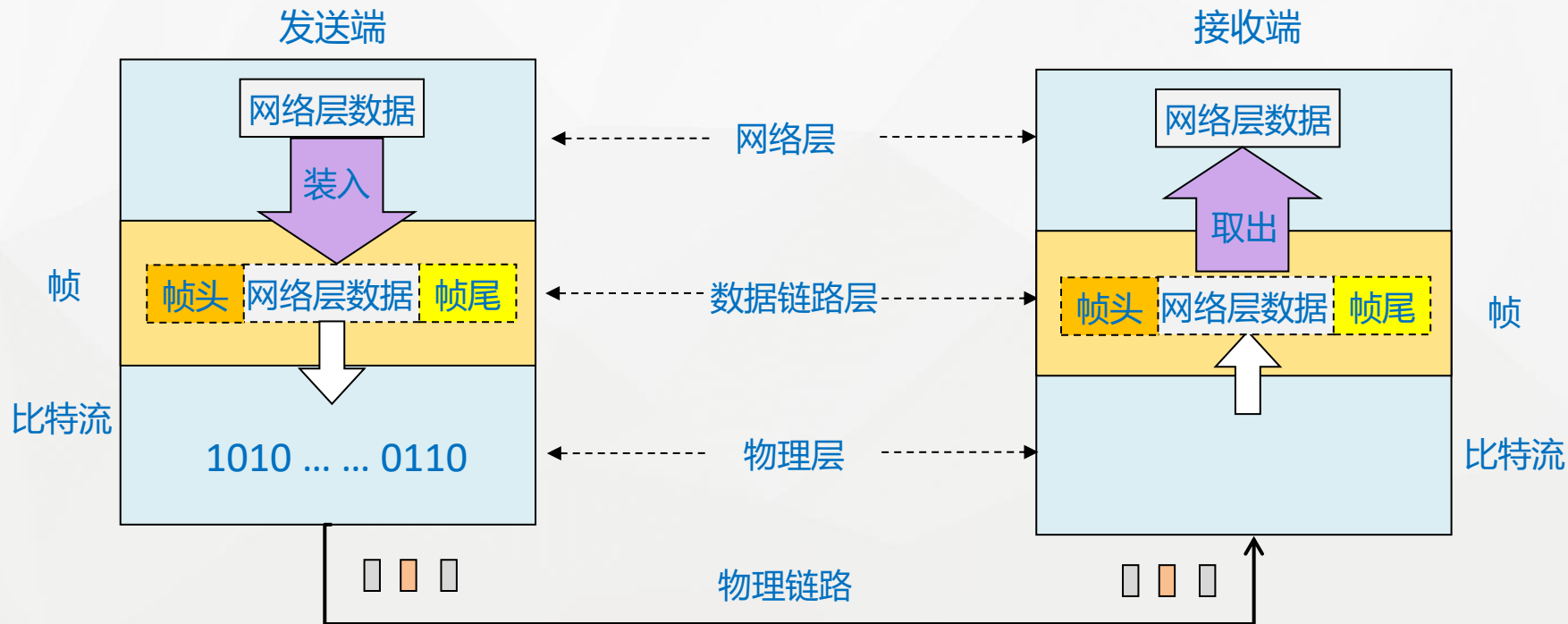
2/ 数据链路层的功能

数据链路层解决的问题

数据链路层在向物理层提供服务的基础上向网络层提供服务，其最基本的服务是将源端网络层来的数据可靠地传输到相邻节点的目标机网络层。为保障数据块的有效传输，数据链路层必须要解决：数据成帧、帧的传输及差错处理、数据链路的通路管理等几个问题。



1、成帧：数据链路层为了实现数据有效的差错控制，以帧的形式传输数据，此时，就必须有相应的帧同步技术，这就是数据链路层的“成帧”（也称为“帧同步”）。

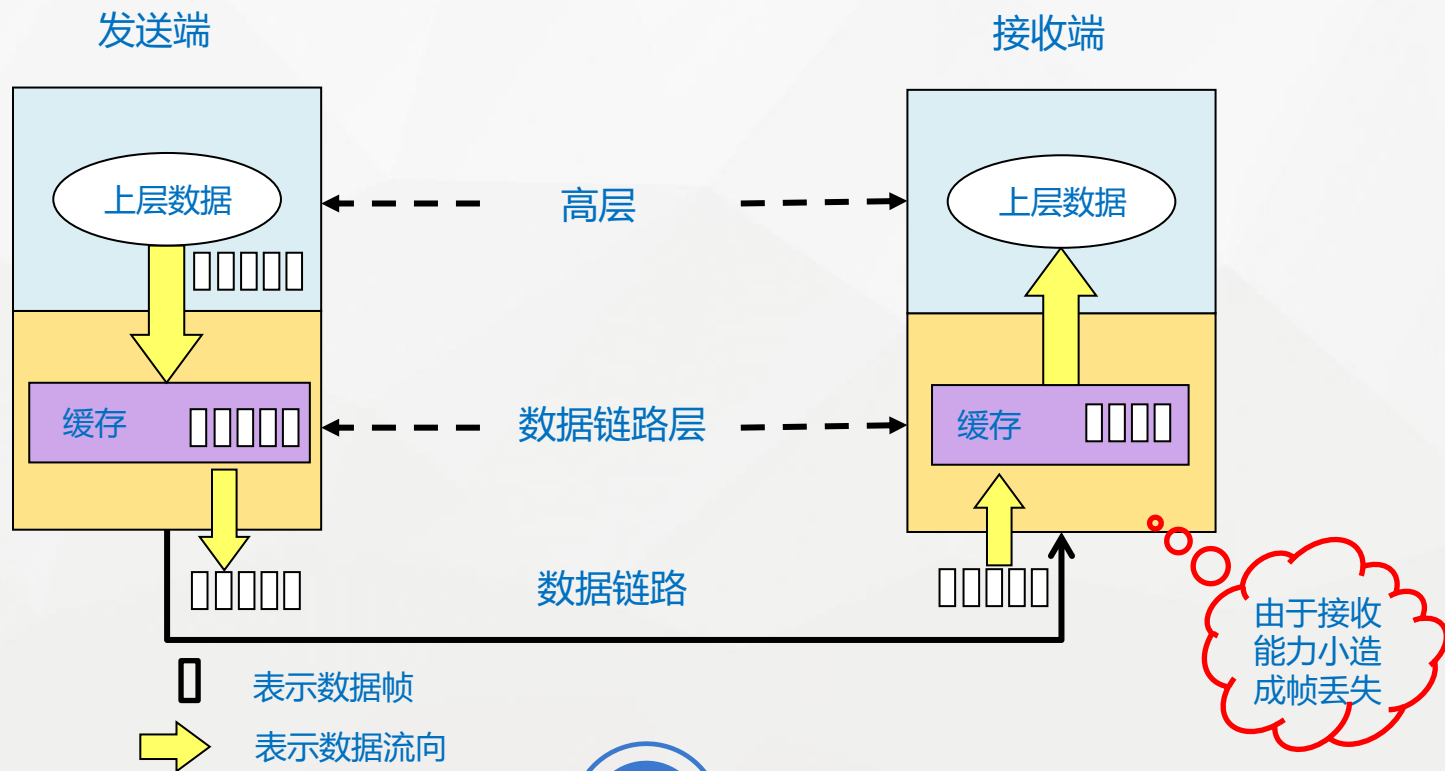


2、差错控制技术：数据链路层的一个重要功能就是分析差错产生的原因与差错类型，研究检查是否产生差错以及如何纠正差错，即差错控制技术。

物理层传输差错的产生过程如下：



3、流量控制：流量控制实际上是对发送方数据流量的控制，使其发送速率不至于超过接收端的处理能力。





4、链路管理：数据链路层的“链路管理”功能包括数据链路的建立、维持和释放三个主要环节。当链路两端的节点要进行通信前，必须首先确认对方已处于就绪状态，并交换一些必要的信息以对帧序号进行初始化，然后才能建立连接，在传输过程中则要能维持该连接。如果出现差错，需要重新初始化，重新自动建立连接，传输完毕后则要释放连接。



奇偶校验码



目录

Contents



学习目标

- 掌握垂直奇偶校验
- 掌握水平奇偶校验
- 掌握水平垂直奇偶校验

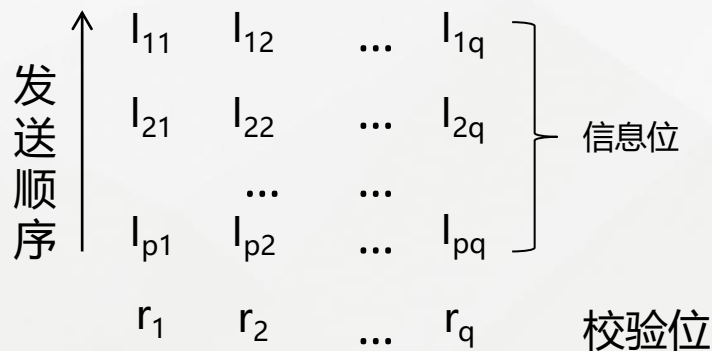
1/ 垂直奇偶校验

2/ 水平奇偶校验

3/ 水平垂直奇偶校验

- 奇偶校验码是一种通过增加冗余位使得码字中“1”的个数为奇数或偶数的编码方法，它是一种检错码。增加的冗余位又叫校验位，一般情况下，校验位是加在原始数据字节的最高位或最低位。
- 把信源编码后的信息数据流分成等长分组，在每一信息分组之后加入一位校验码元作为奇偶校验位，如果总码长 n 中的“1”的个数为偶数，则为偶校验码。否则为奇校验码。
- 奇偶校验只能检测出奇数位错，对偶数位错则无能为力。

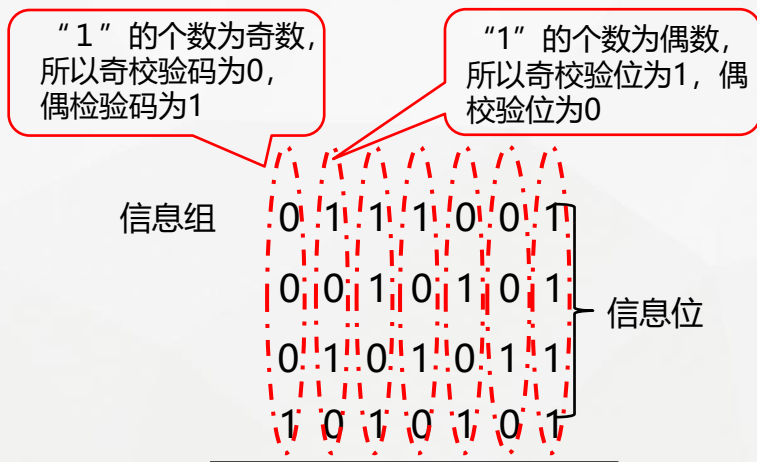
垂直奇偶校验是将整个发送的数据块分为定长 p 位的若干段（比如 q 段），每段后面按“1”的个数为奇或偶数的规律加上一位校验位。组中每行的相同列进行奇/偶校验，最终产生由校验位形成的校验字符（校验行），并附加在信息分组之后传输。



发送方式为按照箭头方向，串行发送：

$l_{11} \ l_{21} \ l_{p1} \ r_1 \ l_{12} \ l_{22} \ \dots \ l_{p2} \ r_2 \ \dots \ l_{1q} \ l_{2q} \ l_{pq} \ r_q$

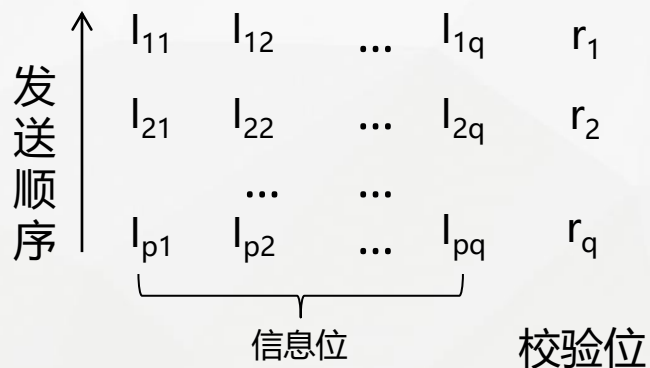
例：4个字符（4行）组成一信息组，其垂直奇/偶校验码为什么？



垂直奇校验 0 1 0 1 1 0 1

垂直偶校验 1 0 1 0 0 1 0

为了降低对突发错误的漏检率，可以采用水平奇偶校验的方法。水平奇偶校验又称横向奇偶校验，它是对各个信息段的相应位横向进行编码，产生一个奇偶校验冗余位。



按照箭头方向发送：

$l_{11} \ l_{21} \ l_{p1} \ l_{12} \ l_{22} \ \dots \ l_{p2} \ \dots \ l_{1q} \ l_{2q} \ l_{pq} \ r_1 \ r_2 \ r_q$

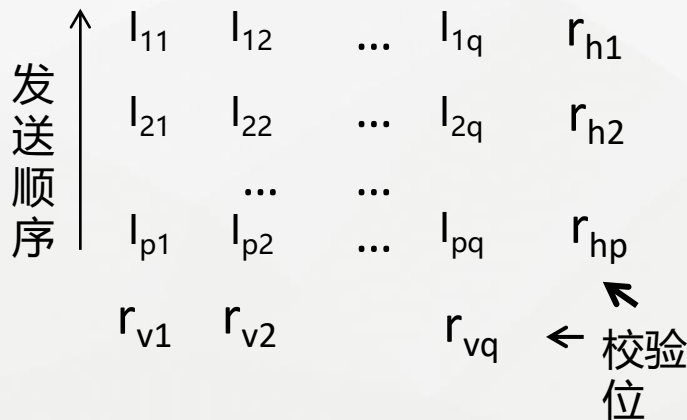
例：4个字符（4行）组成一信息组，其水平奇/偶校验码为什么？

		水平奇校验	水平偶校验
信息组	0 1 1 1 0 0 1	1	0
	0 0 1 0 1 0 1	0	1
	0 1 0 1 0 1 1	1	0
	1 0 1 0 1 0 1	1	0
信息位			

“1”的个数为偶数个，所以奇校验码为1，偶校验码为0

“1”的个数为奇数个，所以奇校验码为0，偶校验码为1

如果同时采用了水平奇偶校验和垂直奇偶校验，既对每个字符作水平校验，同时也对整个字符块作垂直校验，则奇偶校验码的检错能力可以明显提高。这种方式的奇偶校验被称为水平垂直奇偶校验。



例：4个字符（4行）组成一信息组，其水平垂直奇校验码是什么？

信息组	0 1 1 1 0 0 1	1
	0 0 1 0 1 0 1	0
	0 1 0 1 0 1 1	1
	1 0 1 0 1 0 1	1
<hr/>		
	0 1 0 1 1 0 1	校验位

“1” 的个数为偶数个，所以奇校验码为1，偶校验码为0

“1” 的个数为奇数个，所以奇校验码为0，偶校验码为1



CRC循环冗余校验码



目录

Contents

1/ CRC工作原理

2/ CRC循环冗余校验码举例



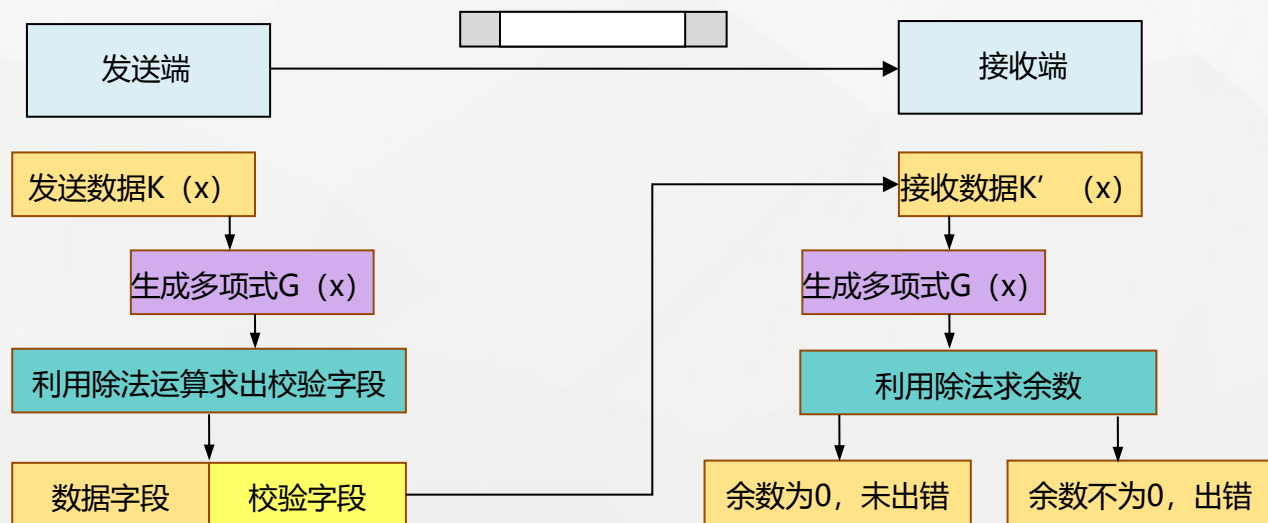
学习目标

- 理解CRC工作原理
- 掌握CRC编码方法

- 循环冗余校验码 (Cycle Redundancy Check, CRC) , 由两部分组成, 前一部分是 $k+1$ 个比特的待发送信息, 后一部分是 r 个比特的冗余码。由于前一部分是实际要传输的内容, 因此是固定不变的, CRC 码的产生关键在于后一部分冗余码的计算。
- CRC计算中主要用到两个多项式: $K(x)$ 和 $G(x)$ 。其中, $K(x)$ 是一个 k 阶多项式, 其系数是待发送的 $k+1$ 个比特序列; $G(x)$ 是一个 r 阶的生成多项式, 由发收双方预先约定。

任何一个待发送的二进制比特流都可以看成是某个一元多项式中各项系数的组合, 如1011011可以看成是一元多项式 $1 \cdot X^6 + 0 \cdot X^5 + 1 \cdot X^4 + 1 \cdot X^3 + 0 \cdot X^2 + 1 \cdot X^1 + 1 \cdot X^0$, 即:
 $X^6 + X^4 + X^3 + X^1 + X^0$, 同理多项式 $X^5 + X^3 + X^2 + X^1 + X^0$ 对应的代码为101111。

CRC工作原理是：将要发送的数据比特序列当做一个多项式 $K(x)$ 的系数，在发送端用收发双方约定的生成多项式 $G(x)$ 去除，求得一个余数多项式，并附加在发送数据多项式之后发送到接收端。接收端收到数据后，除以多项式 $G(x)$ ，如果得到结果为0，则数据传输无差错，若不为0，则传输出错，请求重发。





- (1) 发送方和接收方事先约定一个生成多项式 $G(x)$ 。
- (2) 发送端根据生成多项式 $G(x)$ 去计算要附加在信息帧尾部的冗余位。

计算校验和的算法如下：

- 假设信息帧的比特数为 k 位，对应的多项式为 $K(x)$ ， $G(x)$ 为 r 阶。在信息帧的低位端加上 r 个0，此时信息帧的比特数变为 $k+r$ 位，对应的多项式为 $K(x) \cdot x^r$ 。
 - 按模2除法，用对应于 $G(x)$ 的比特串去除对应于 $x^r K(x)$ 的比特串，从而得到一个小于等于 r 位的余数。这个余数便可作为校验和。
- (3) 将校验和附加在 k 位信息帧尾部，组成一个新的帧，由发送端发送给接收端。



例：CRC实例。假设要发送的信息帧数据比特序列为110011，双方约定的生成多项式为 $G(x) = X^4 + X^3 + X^0$ 。

(1) 发送端发送数据计算方法：

- ① 信息帧的多项式为 $K(x) = X^5 + X^4 + X^1 + X^0$ 。
- ② 由生成多项式 $G(x) = X^4 + X^3 + X^0$ 可知阶数 r 为4，生成多项式的比特序列为11001。
- ③ 此时利用公式 $x^r \cdot K(x)$ ，即信息帧的数据比特序列乘以 x^4 ，则信息帧的多项式变为 $X^9 + X^8 + X^5 + X^4$ ，即信息帧的比特序列变为1100110000。
- ④ 将乘积用多项式比特序列去除，按模2运算，求出余数为：

$$\begin{array}{rcl}
 \text{生成多项式 } G(x) & \longrightarrow & 11001 \quad \int \begin{array}{r} 10001 \\ 1100110000 \\ \hline 11001 \\ \hline 10000 \\ 11001 \\ \hline 1001 \end{array} \longleftarrow K(x) \cdot x^r \\
 & & \longleftarrow \text{余数}
 \end{array}$$

- ⑤ 通过上一步计算可知余数为1001，也就是校验码，将校验码加在信息帧的后面即发送数据为1100111001。

(2) 发送端发送数据计算方法

如果在数据的传输过程中没有发生错误，那么接收端收到的带有CRC校验码的数据比特序列一定能被相同的生成多项式整除，即

$$\begin{array}{rcl}
 \text{生成多项式 } G(x) & \longrightarrow & 11001 \quad \bigg| \quad \begin{array}{r} 100001 \\ 1100111001 \\ 11001 \\ \hline 11001 \\ 11001 \\ \hline 0 \end{array} \\
 & & \longleftarrow K(x) \cdot x^r \qquad \qquad \qquad \longleftarrow \text{余数}
 \end{array}$$



CRC具有较强的检错能力，可以检测出所有的奇数位错、双比特错、小于等于校验和长度的突发错。CRC中生成多项式 $G(x)$ 的选择是非常重要的。

目前广泛使用的生成多项式主要有以下几种：

CRC-16 $G(x) = X^{16} + X^{15} + X^2 + 1$

CRC-CCITT $G(x) = X^{16} + X^{12} + X^5 + 1$

CRC-32 $G(x) = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$



反馈重发机制



目录

Contents



学习目标

- 理解反馈重发机制原理
- 掌握停止等待ARQ协议
- 掌握连续ARQ协议

1/ 反馈重发机制原理

2/ 停止等待ARQ协议

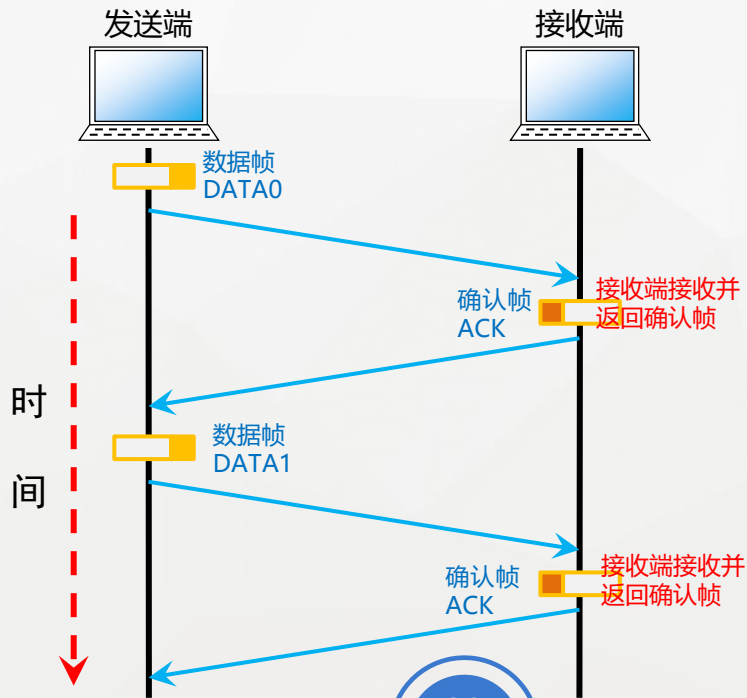
3/ 连续ARQ协议

- 反馈重发的机制：当接收方检出错误的帧时，首先将该帧丢弃，然后接收方给发送方反馈信息请求对方重发相应的帧。反馈重发也被称为自动请求重传（Automatic Repeat Request，简称ARQ）。
- ARQ通过使用确认和超时这两个机制，在不可靠服务的基础上实现可靠的信息传输。如果发送方在发送后一段时间之内没有收到确认帧，它通常会重新发送。
- ARQ包括停止等待ARQ协议和连续ARQ协议。

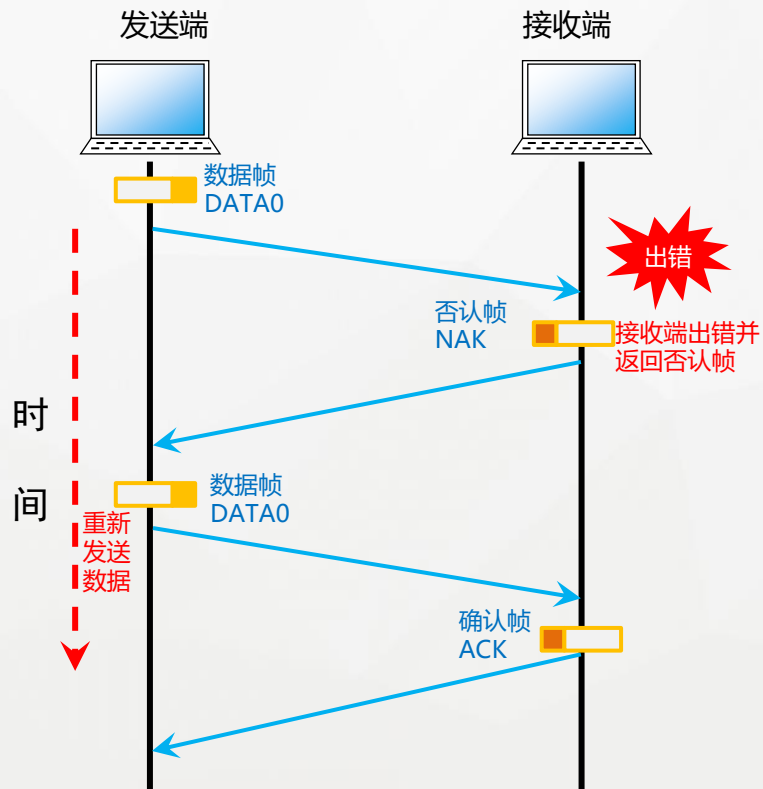
停止等待ARQ协议

在停止-等待方式中，发送方每发送一帧后就等待应答，只有接收到一个应答（ACK）后，才发送下一个帧，直到发送方发送一个传输结束帧。若未收到应答发送方就重发该帧。

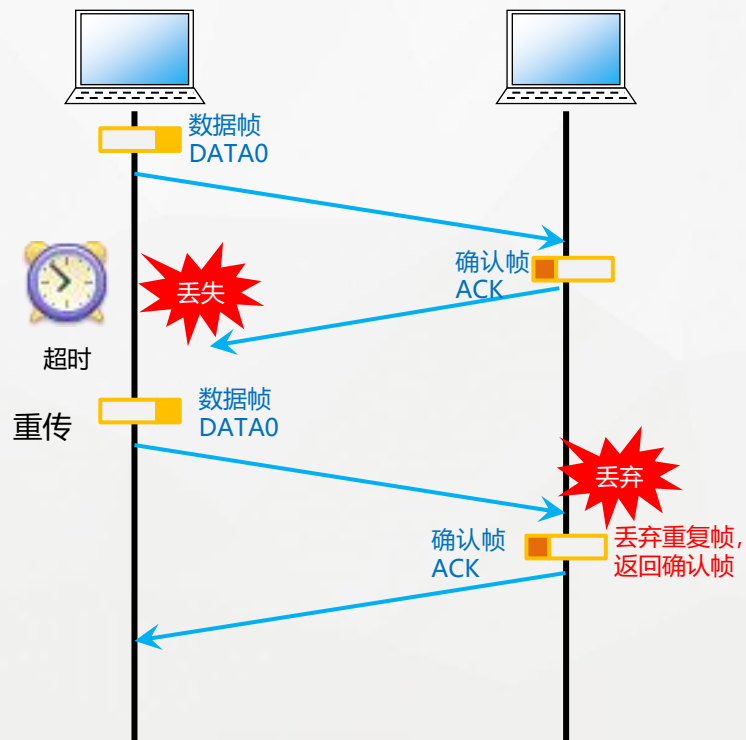
帧传输正常情况



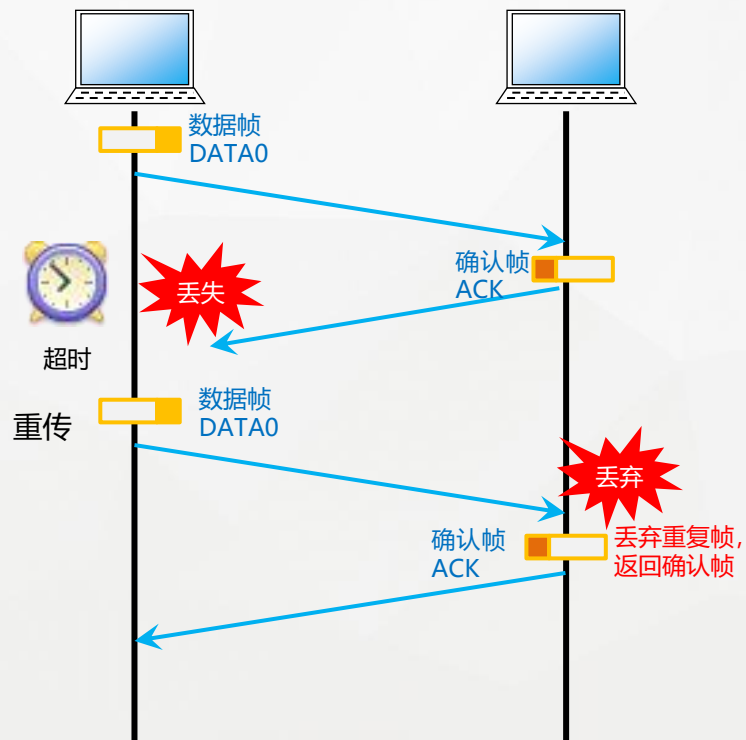
帧破坏造成数据重传



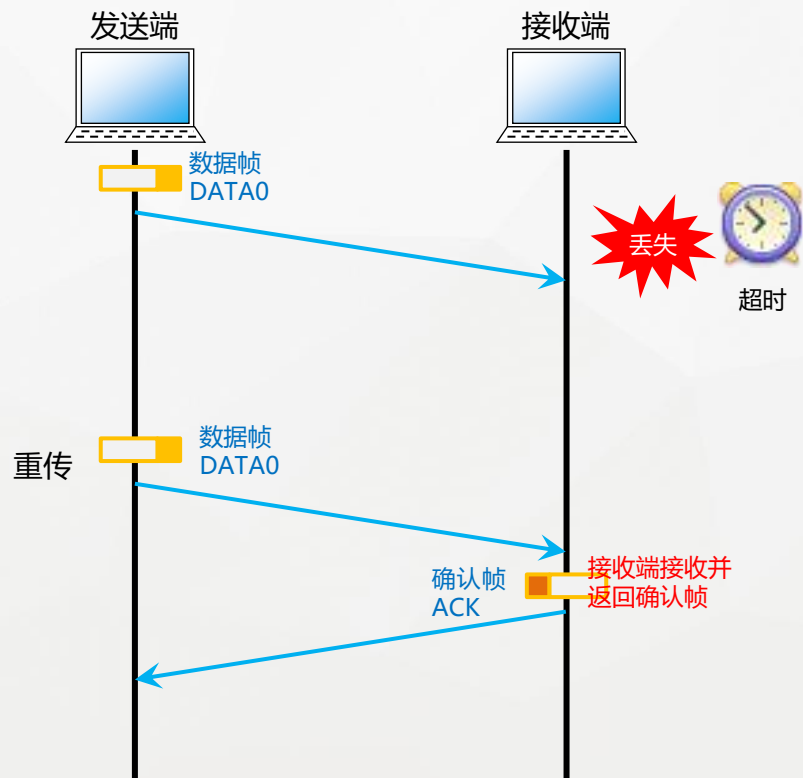
确认帧丢失情况



确认帧丢失情况



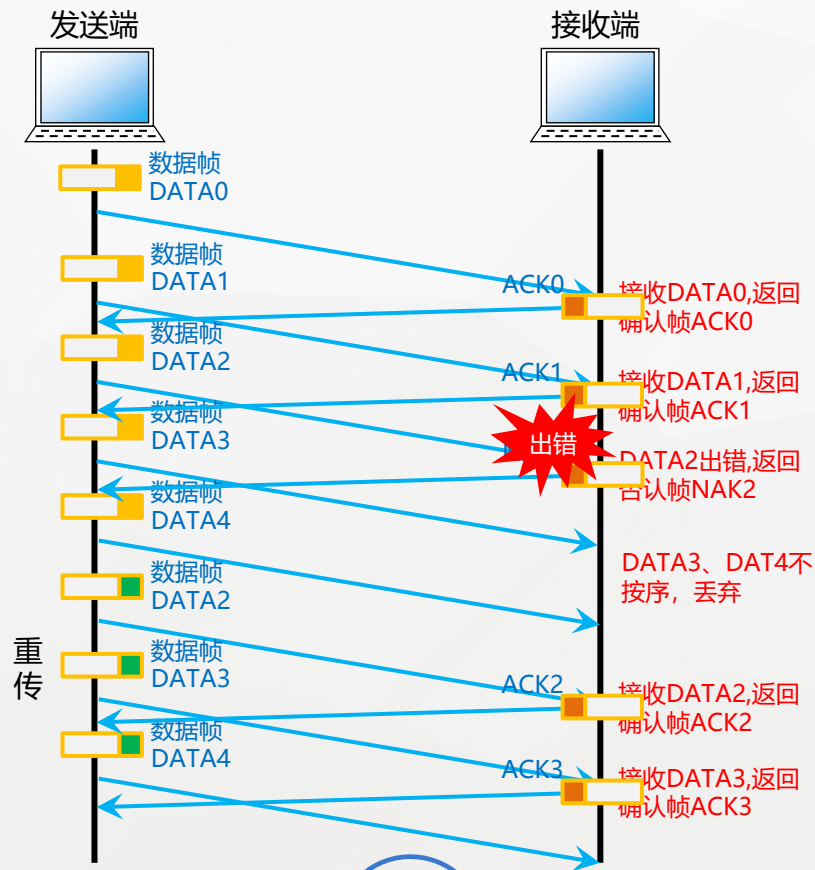
帧丢失情况



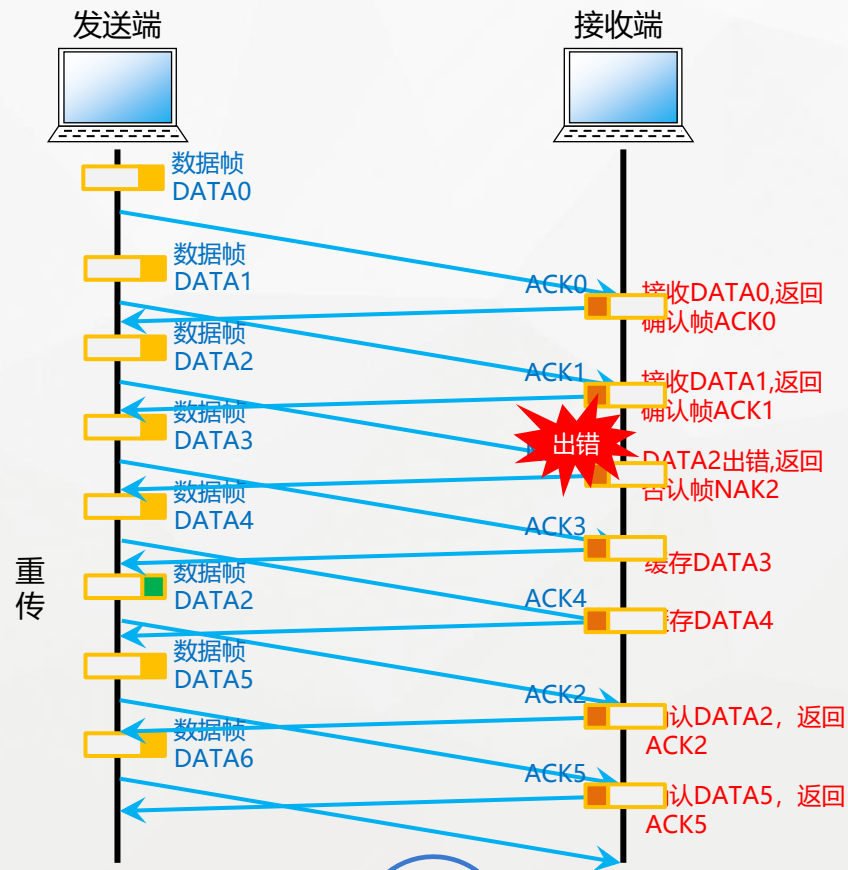


- 连续ARQ协议的特点是发送端在发送一个帧后，不是停下来等待确认帧的到来，而是可以连续再发送多个帧，帧的个数取决于发送方的发送能力和接收端的接收能力。
- 在连续发送的多个帧中，可能会有一个或多个帧出现传输差错。针对这种情况，连续ARQ分别采用了两种不同的处理方式，即拉回方式和选择性重传方式。

拉回方式连续ARQ协议



选择重传连续ARQ协议





局域网体系结构



目录

Contents



学习目标

- 掌握局域网的概念
- 了解IEEE 802系列主要标准
- 掌握局域网体系结构

1/ 局域网基本概念

2/ IEEE 802主要标准

3/ 局域网体系结构

- 局域网，就是在局部地区范围内的网络，它所覆盖的地区范围较小。
- 在网络所涉及的地理距离上一般来说可以是几米至10公里以内。局域网一般位于一个建筑物或一个单位内，不存在寻径问题，不包括网络层的应用。
- 局域网特点是：连接范围窄、用户数少、配置容易、连接速率高。
- 局域网在计算机数量配置上没有太多的限制，少的可以只有两台，多的可达几百台。

局域网标准化委员会（简称IEEE802 委员会）定义了多种主要的LAN网：以太网（Ethernet）、令牌环网（Token Ring）、光纤分布式接口网络（FDDI）、异步传输模式网（ATM）、无线局域网（WLAN）。

IEEE 802局域网系列主要标准

序号	标准	描述
1	IEEE 802.1	描述局域网体系结构以及寻址、网络管理和网络互连（1997）
	◆ IEEE 802.1G	远程MAC 桥接（1998），规定本地MAC 网桥操作远程网桥的方法
	◆ IEEE 802.1H	在局域网中以太网2.0 版MAC 桥接（1997）
	◆ IEEE 802.1Q	虚拟局域网（1998）
2	IEEE 802.2	定义了逻辑链路控制（LLC）子层的功能与服务（1998）

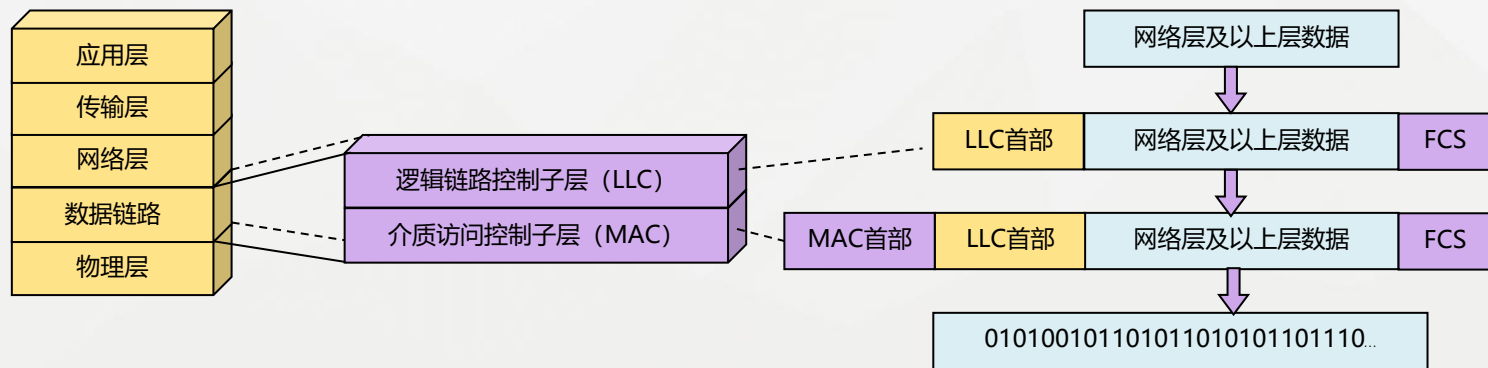
IEEE 802局域网系列主要标准

序号	标准	描述
3	IEEE 802.3	描述带冲突检测的载波监听多路访问（CSMA/CD）的访问方法和物理层规范（1998）
	◆ IEEE 802.3ab	描述1000Base-T 访问控制方法和物理层技术规范（1999）
	◆ IEEE 802.3ac	描述VLAN 的帧扩展（1998）
	◆ IEEE 802.3ad	描述多重链接分段的聚合协议（Aggregation of Multiple Link Segments）（2000）
	◆ IEEE 802.3i	描述10Base-T 访问控制方法和物理层技术规范
	◆ IEEE 802.3u	描述100Base-T 访问控制方法和物理层技术规范
	◆ IEEE 802.3z	描述1000Base-X 访问控制方法和物理层技术规范
	◆ IEEE 802.3ae	描述10GBase-X 访问控制方法和物理层技术规范
4	IEEE 802.4	描述Token-Bus 访问控制方法和物理层技术规范

IEEE 802局域网系列主要标准

序号	标准	描述
5	IEEE 802.5	描述Token-Ring 访问控制方法和物理层技术规范（1997）
	◆ IEEE 802.5t	描述100 Mbps 高速标记环访问方法（2000）
6	IEEE 802.6	描述城域网（MAN）访问控制方法和物理层技术规范（1994）。1995年又附加了MAN 的DQDB 子网上面向连接的服务协议。
7	IEEE 802.7	描述宽带网访问控制方法和物理层技术规范
8	IEEE 802.8	描述FDDI 访问控制方法和物理层技术规范
9	IEEE 802.9	描述综合语音、数据局域网技术（1996）
10	IEEE 802.10	描述局域网网络安全标准（1998）
11	IEEE 802.11	描述无线局域网访问控制方法和物理层技术规范（1999）

- 局域网只涉及OSI的物理层和数据链路层。当不同的局域网需要在网络层实现互连时，可以借助其他已有的通用网络层协议（如IP 协议）实现。
- 局域网的数据链路层分为逻辑链路控制（LLC，Logical Link Control）和介质访问控制（MAC，Medium Access Control）两个功能子层，两个子层都要参与数据的封装和拆封过程。



数据链路层子层与数据封装过程



介质访问控制CSMA/CD



目录

Contents

1/ 共享式以太网数据发送方式

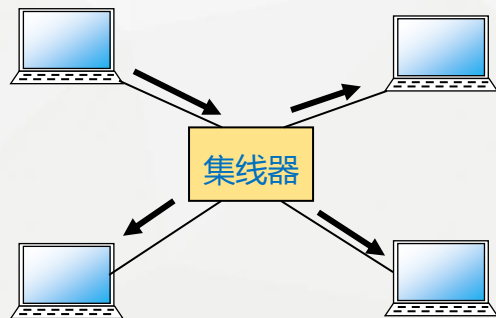
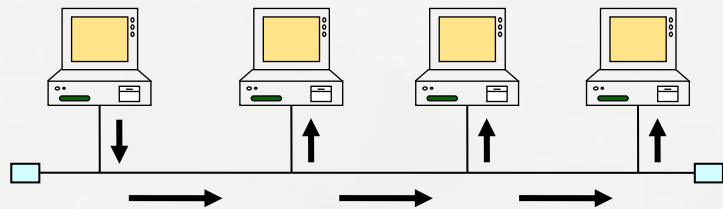
2/ CSMA/CD工作原理



学习目标

- 掌握共享式以太网数据发送方式
- 掌握CSMA/CD 的工作原理

- 从通信介质的使用方法上看，网络可分为共享介质型和非共享介质型。以太网就是介质共享型网络。在这种方式下，设备之间使用同一个载波信道进行发送和接收。
- CSMA/CD (Carrier Sense Multiple Access/Collision Detection) ，即载波监听多路访问/冲突检测，是早期共享式以太网用于解决冲突的协议，即介质访问控制方式。

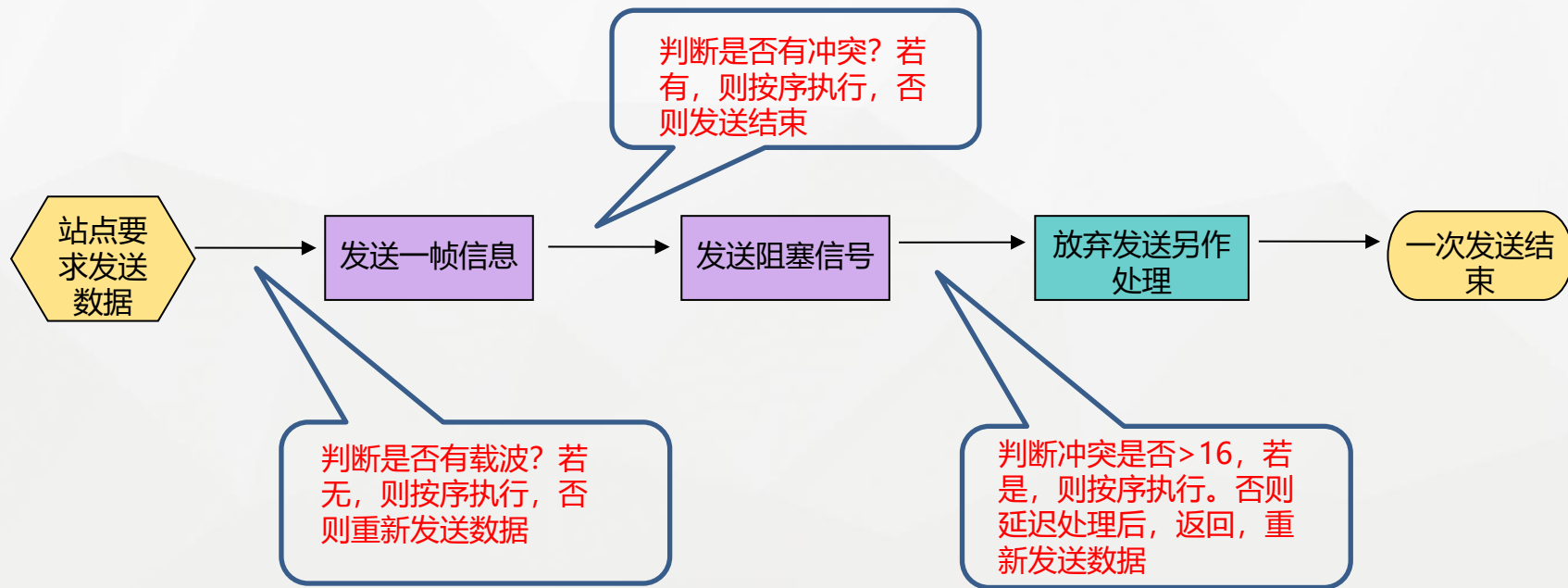


- 共享式以太网采用广播式发送数据，一台终端发送数据，网络中其它主机都将会收到这一数据。
- 若有两台终端同时发送数据，会出现冲突。

CSMA/CD 的工作原

理

- 为解决共享式以太网冲突问题，引入了CSMA/CD工作方式
- CSMA/CD 的工作原理：先听后发，边发边听，冲突停发，随机延迟后重发



优点:

CSMA/CD介质访问控制方法中，每个结点都处于平等的地位去竞争传输介质，网络维护方便，增删结点容易。负载较少时，要发送信息的结点可以立即获得访问控制权限，效率较高。

缺点:

当负载重时，容易出现冲突，使传输效率和有效带宽大为降低。



MAC地址



目录

Contents



学习目标

- 理解MAC地址基础知识
- 掌握MAC地址的结构
- 掌握MAC地址传输方式

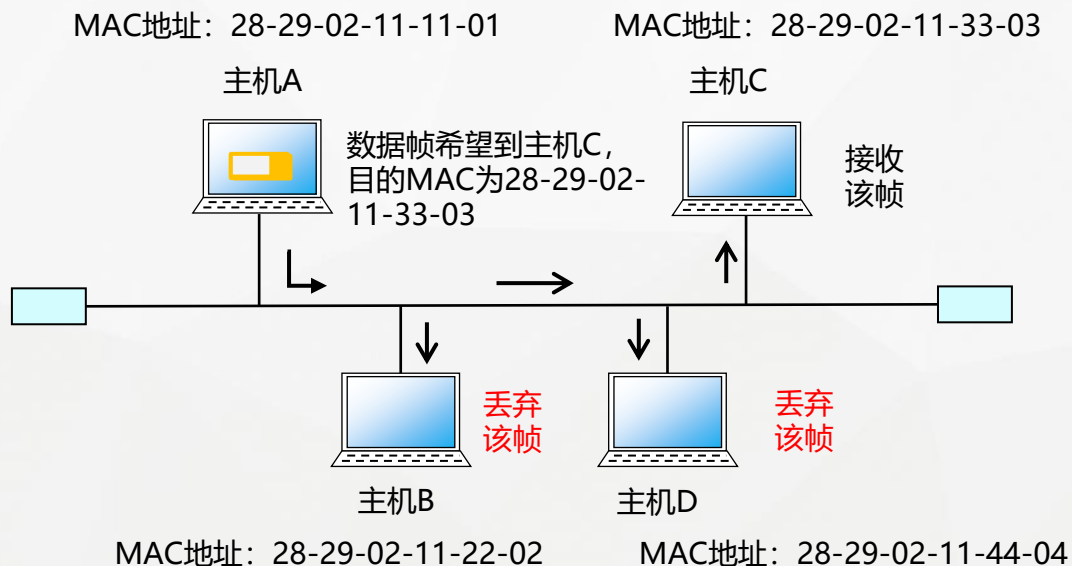
1/ MAC地址基础知识

2/ MAC地址结构

3/ MAC地址传输方式



- 数据链路层分为逻辑链路子层（LLC）和介质访问控制子层（MAC），其中MAC的一个重要功能就是完成局域网中的物理寻址。
- 局域网中各节点之间的通信主要是通过MAC地址完成寻址的。MAC地址又称为物理地址或硬件地址，在以太网中，MAC地址又称以太网地址。
- 网卡的MAC地址一般会被烧入到ROM中，因此，理论上讲任何一个网卡的MAC地址都是唯一的，在全世界都不会有重复。

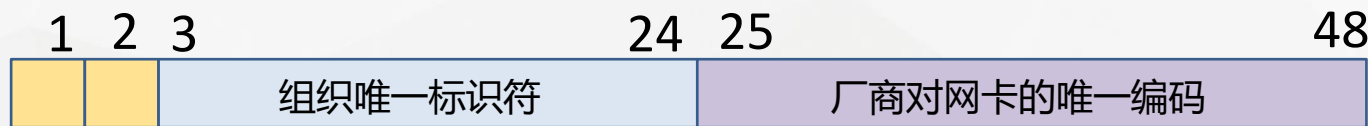


注: 在总线或环型网络中, 主机A发送数据给主机C, 网络中所有主机都将会收到数据, 然后根据自己MAC与数据包中的目的MAC进行匹配, 如果匹配上就接收, 匹配不上就丢弃。

MAC地址长度为48位，即6个字节，通常表示为12个16进制数。如：28-29-02-D1-2A-19，

MAC地址格式：

MM:MM:MM:SS:SS:SS或者MM-MM-MM-SS-SS-SS



第1位：单播地址（0）/多播地址（1）

第2位：全局地址（0）/本地地址（1）

第3~24位：组织唯一标识符

第25~48位：厂商对网卡的唯一编码

MAC地址共有3类：单播、多播和组播。在单播地址中，第1位为0；在多播地址中，第1位为1；而广播地址则是48个1。

MAC地址在传输时是逐字节从左到右发送的，但是对于每一个字节来说，最先发送的是最低位，最后发送的是最高位

01:02:XX:XX:XX:XX

十六进制MAC地址

00000001

00000010

用二进制表示

传输方式

100000000010000000

← 网络中数据传输时的比特序列



以太网帧



目录

Contents



学习目标

- 掌握以太网整体帧结构
- 掌握以太网帧结构

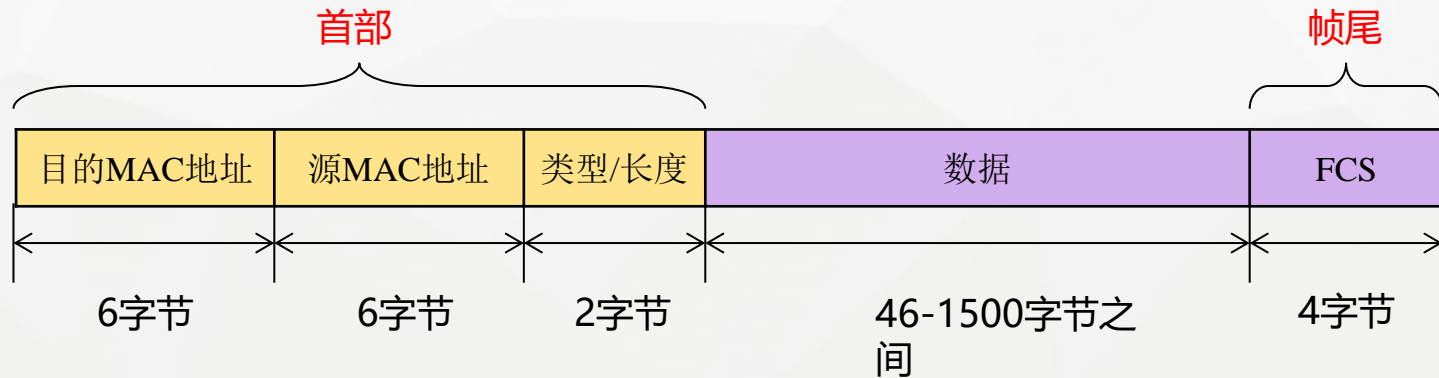
1/ 以太网整体帧结构

2/ 以太网帧结构

网络层的数据包被加上帧头和帧尾，就构成了可由数据链路层识别的以太网数据帧。以太网数据帧的长度变化范围是64-1518字节



常见的以太网帧结构是Ethernet II的格式。以太网帧的前端是以太网的首部，它总共占14个字节。分别是6个字节的目标MAC地址、6个字节的源MAC地址以及2个字节的
上层协议类型



1. **目的MAC地址**: 接收端的MAC地址, 长度为6字节。
2. **源MAC地址**: 发送端的MAC地址, 长度为6字节。
3. **类型/长度**: 该字段长度为2字节, 当字段值大于或等于0x0600时, 表示上层数据使用的协议类型, 当字段值小于0x0600时, 表示以太网用户数据的长度。
4. **数据**: 上层封装下来的数据, 长度在46字节到1500字节之间。
5. **FCS**: 校验码, 长度为4字节, 主要用于错误校验。



以太网类型



目录

Contents



学习目标

- 了解不同以太网类型
- 掌握标准以太网、快速以太网、千兆以太网的结构

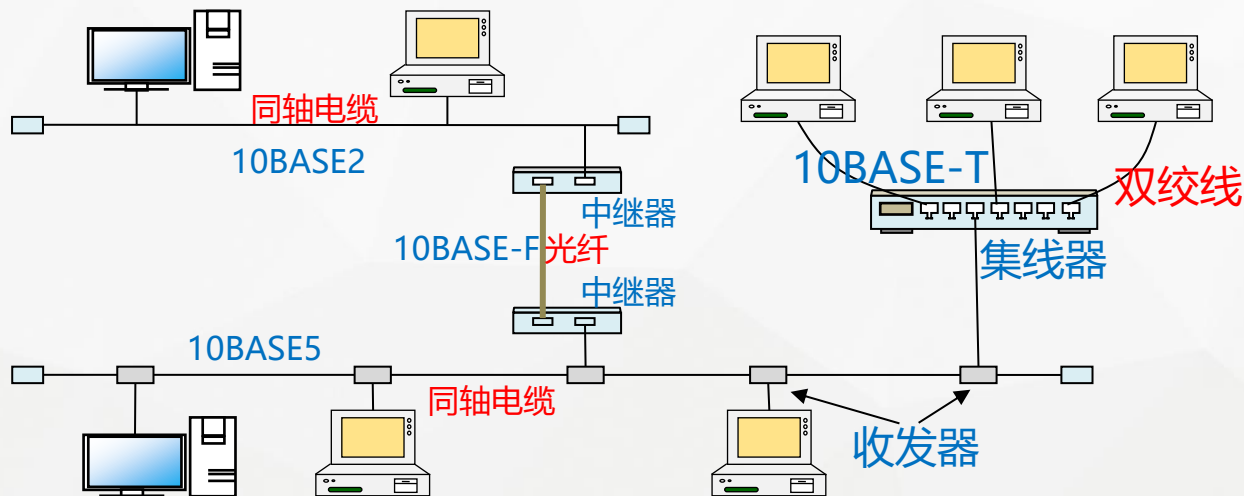
1/ 标准以太网

2/ 快速以太网

3/ 千兆以太网

4/ 万兆以太网

- 在以太网普及之初，以太网只有10Mbps的吞吐量，一般采用多台终端使用同一根同轴电缆的共享介质型连接方式，这种早期的10Mbps以太网也称之为标准以太网。
- 所有的设备采用CSMA/CD的方式使用传输介质，因此在传输过程所有结点共享同一传输介质，这使得数据传输效率和带宽的利用受到了限制。
- 共享式以太网局域网中的网络设备必须保持相同的传输速率，否则一个设备发送的信息，另一个设备不可能收到。单一的共享式以太网不可能提供多种速率的设备支持。
- 早期的10BASE2、10 BASE5、10BASE-T、10BASE-F等标准的以太网就属于共享式以太网，目前共享式以太网已逐渐退出了历史舞台。

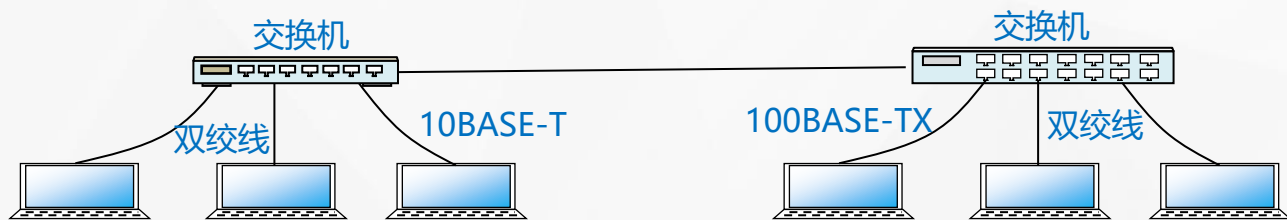


10Base-T 是以太网中最常用的一种标准，与10Base5 和10Base2 相比其特点如下：

- 安装简单、扩展方便；
- 网络的可扩展性强，
- 集线器或交换机具有很好的故障隔离作用



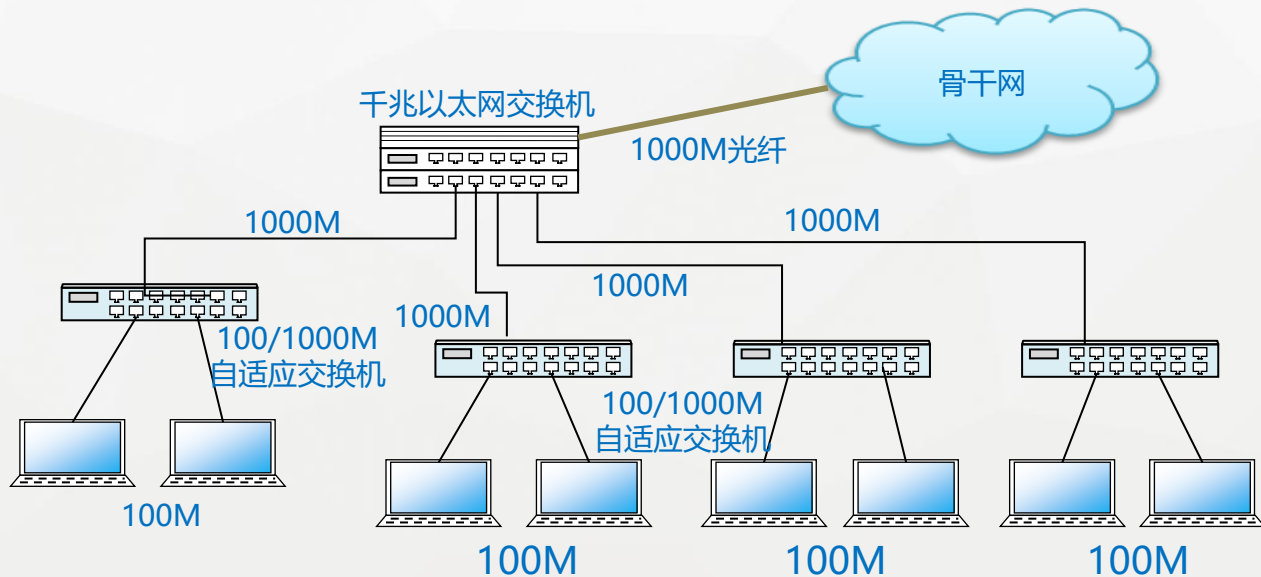
- IEEE在1995年3月推出了802.3u标准，即快速以太网（Fast Ethernet）。它的设计思想非常简单，为了向后兼容以太网，保留了原来的帧格式、接口和过程规则，并和10BASE-T一样使用集线器和交换机作为连接设备。传输介质除了3类双绞线和光纤之外，还增加了5类双绞线。
- 可支持100M的数据传输速率，并且与10BASE-T一样可支持共享式与交换式两种使用环境，在交换式以太网环境中可以实现全双工通信。
- 快速以太网没有采用曼彻斯特编码，而采用效率更高的4B/5B等编码。在传输介质上，快速以太网取消了对同轴电缆的支持。



100M快速以太网标准又分为：100BASE-TX、100BASE-FX、100BASE-T4三个子类。

标准	线缆类型及连接器	线缆对数	最大分段长度	编码方式	主要优点
100BASE-TX	5类UTP/RJ-45接头 1类STP/DB-9接头	2对(1、2对发送数据, 3、6一一对接收数据)	100米	4B/5B	支持全双工通信
100BASE-FX	62.5 μ m/125 μ m多模光纤 8 μ m/125 μ m单模光纤 ST或SC光纤连接器	2芯	多模光纤连接最大距离为550米; 单模光纤连接最大距离为3000米	4B/5B	支持全双工的数据传输。 特别适合于有电气干扰、 较大距离连接、或高保密环境等情况下的适用。
100BASE-T4	3、4、5类无屏蔽双绞线 或屏蔽双绞线	使用4对双绞线(3对用于 数据传输，一对用于 冲突检测)	100米	8B / 6T	用于在3类非屏蔽双绞 线上实现100Mbps数据 速率

千兆以太网标准是对以太网技术的再次扩展，其数据传输率达到1000Mbps即1Gbps，因此也被称为吉比特以太网。千兆以太网向下和以太网与快速以太网完全兼容，从而原有的10M以太网或快速以太网可以方便地升级到千兆以太网。





千兆以太网标准主要包括1000BASE-SX、1000BASE-LX、1000BASE-CX、和1000BASE-T四个协议标准。

标准	线缆类型及连接器	线缆对数	最大分段长度	编码方式	主要优点
1000BASE-SX	芯径为62.5μm和50μm的多模光纤	---	260米 525米	8B/10B	适用于作为大楼网络系统的主干通路
1000BASE-LX	芯径为50 μm 和62.5 μm 的多模光纤 芯径为9 μm 的单模光纤	---	多模：550米 单模：5000米	8B/10B	多模：适用于作为大楼网络系统的主干通路 单模：适用于校园或城域主干网
1000BASE-CX	150 Ω平衡屏蔽双绞线	---	25米	8B/10B	传输速率为1.25 Gbps，适用于集群网络设备的互连，例如机房内连接网络服务器
1000BASE-T	5 类UTP 双绞线	4 对	100米	PAM-5	传输速率为1 Gbps，主要用于结构化布线中同一层建筑的通信，从而可以利用以太网或快速以太网已铺设的UTP 电缆，也可被用做大楼内的网络主干

- IEEE于2002年正式发布802.3ae 10GE标准，即万兆以太网。以太网技术从此开始由局域网领域向城域网领域渗透。2007年，IEEE又提出了802.3ba标准，目标是设计40Gbps或者100Gbps的以太网。
- 为了提供10G的传输速率，802.3ae10GE标准在物理层只支持光纤作为传输介质。在物理拓扑上，万兆以太网既支持星型连接或扩展星型连接，也支持点到点连接以及星型连接与点到点连接的组合。
- 在万兆以太网的MAC子层，已不再采用CSMA/CD机制，其只支持全双工方式。
- IEEE802.3ae10GE标准继承了802.3以太网的帧格式和最大/最小帧长度，从而能充分兼容已有的以太网技术，进而降低了对现有以太网进行万兆位升级的风险。



交换式以太网



目录

Contents

1/ 虚拟局域网起源

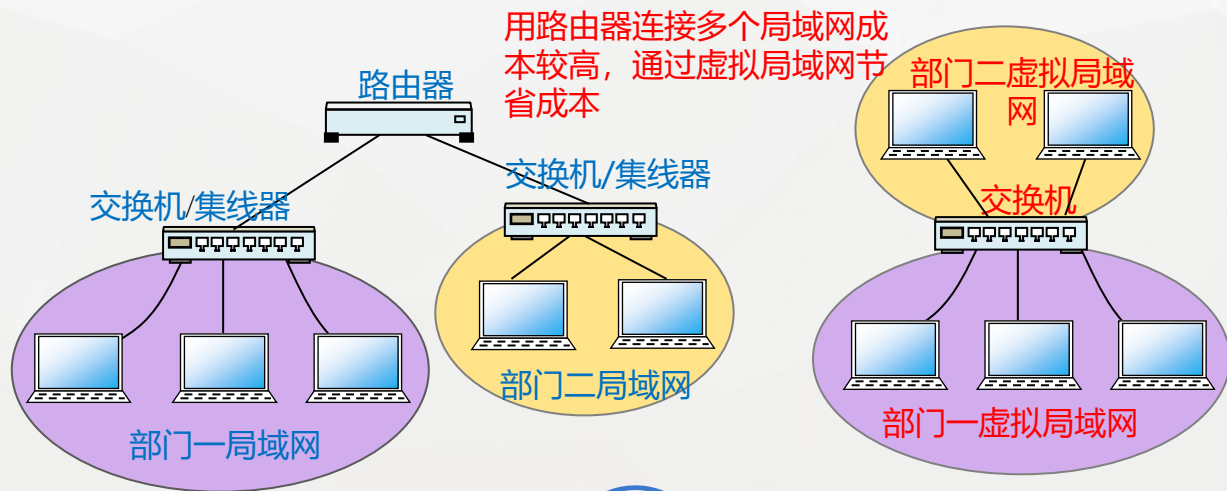
2/ 交换式以太网



学习目标

- 了解虚拟局域网起源
- 掌握交换式以太网工作原理

随着局域网内的主机数量的日益增多，由大量的广播报文带来的带宽浪费、安全等问题变得越来越突出。为了解决这一问题，方法之一是将网络改造成用路由器连接多个子网，但这样会增加网络设备的投入；另一种成本较低又行之有效的方法就是采用虚拟局域网。虚拟局域网的基础是在交换技术上发展起来的，因此需要先了解什么是交换式以太网。



交换式以太网核心就是交换机（Switch）。在这种方式下，网络中的每个站直连交换机，由交换机负责转发数据帧。此方式下，发送端与接收端并不共享通信介质，因此很多情况下采用全双工通信方式。当一台主机希望传送一个以太网帧时，它向交换机送出一个标准帧，交换机收到这个帧后，会查看帧的目的地址，然后将这个帧直接发送到目的地。在这种一对一连接全双工通信的方式下不会发生冲突，因此一般不需要CSMA/CD的机制就可以实现更高效的通信。





冲突域与广播域



目录

Contents

1/ 冲突域

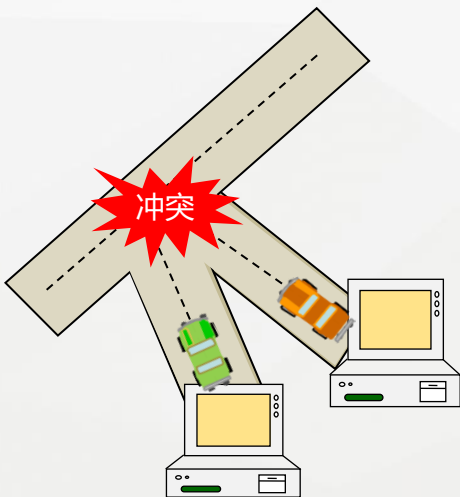
2/ 广播域



学习目标

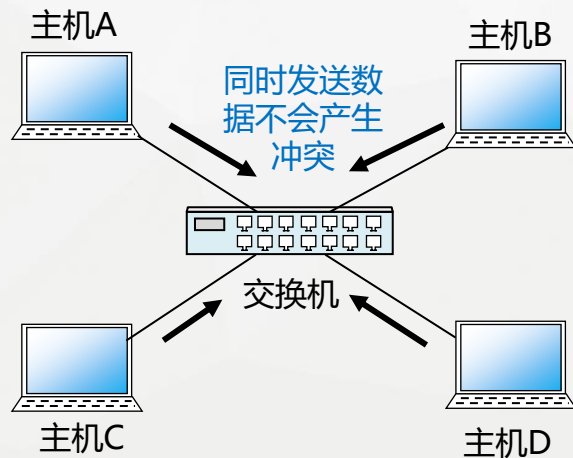
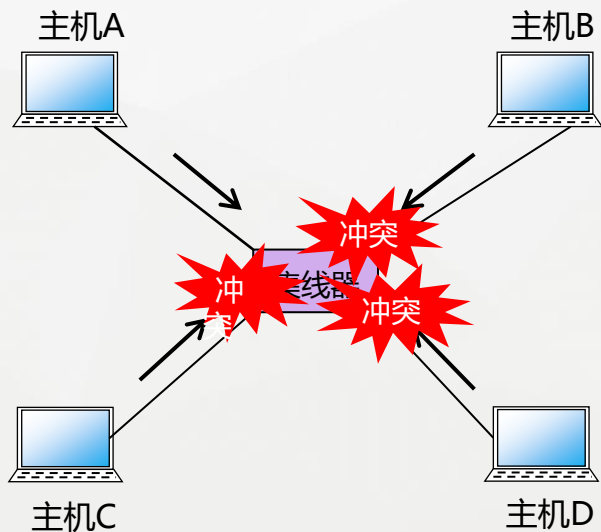
- 理解冲突域的概念
- 理解广播域的概念

在共享链路上，当两个节点同时传输数据时，从两个设备发出的帧在物理介质上相遇，从而发生碰撞，彼此数据都被破坏，即称为冲突。



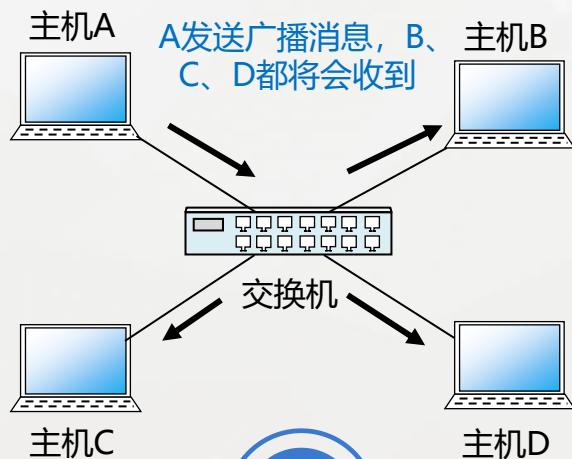
冲突域是指在共享链路上，同时发送数据会产生冲突的计算机所构成的区域。

- 共享式的以太网中，所有结点构成了一个冲突域。
- 交换式以太网中，交换机的每个端口构成了一个冲突域。



在以太网中，如果一个结点发送广播数据包，那么这个局域网网络中的其它结点也会收到这个广播数据包。对于这种能够接收同样广播消息的结点的集合就被称为是一个广播域。

- 同一个共享式以太网中所有结点构成了一个广播域。
- 同一个交换式以太网中的所有结点也构成了一个广播域。





交换机数据转发方式



目录

Contents



学习目标

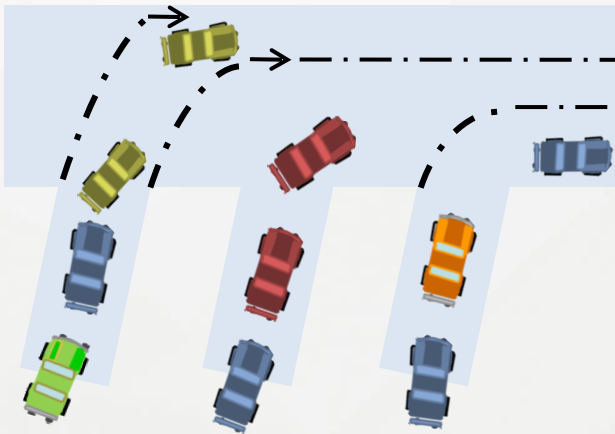
- 理解直通式转发方式
- 理解存储转发方式
- 理解无碎片直通式转发方式

1/ 直通式转发方式

2/ 存储转发方式

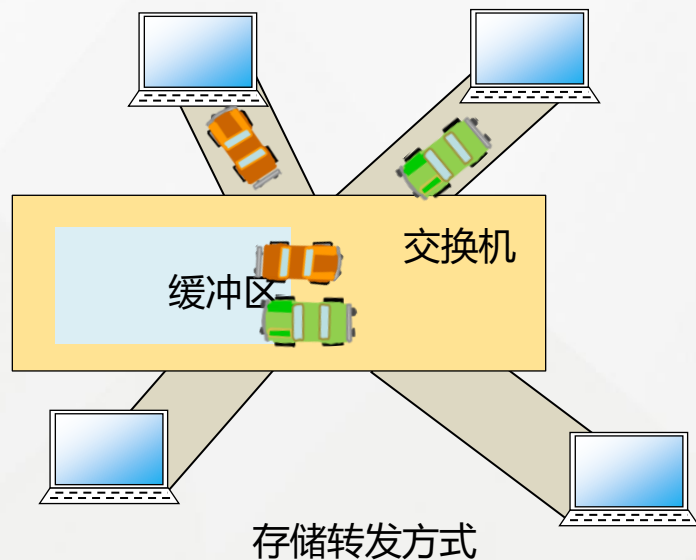
3/ 无碎片直通式转发方式

直通式 (Cut Through) 方式处理过程是在输入端口检测到一个数据包后, 只检查其包头, 取出目的地址, 通过内部的地址表确定相应的输出端口, 然后把数据包转发到输出端口。这样就完成了交换。它的优点是延迟小, 交换速度快。但是不具备检错能力。



注: 交换机之所以同时进行数据转发, 其中重要的一个方面是其具有很宽的总线带宽, 如果有 N 个端口, 每个端口带宽为 M , 则交换机总线的带宽为 $N \times M$, 可以避免冲突的产生

存储转发 (Store and Forward) 处理过程是计算机网络领域使用得最为广泛的技术之一，在这种工作方式下，交换机的控制器先缓存输入到端口的数据包，然后进行CRC校验，滤掉不正确的帧，确认包正确后，取出目的地址，通过内部的地址表确定相应的输出端口，然后把数据包转发到输出端口。对于支持不同速度端口的交换机通常使用这种方式，否则不能保证高速端口（如100Mbps）和低速端口（如10Mbps）间的正常通信。





无碎片直通 (Fragment Free Through) 过程是介于直通式和存储转发式之间的一种解决方案，它检查数据包的长度是否够64 Bytes (512bit) 如果小于64 Bytes，说明该包是碎片（即在信息发送过程中由于冲突而产生的残缺不全的帧），则丢弃该包，如果大于64 Bytes，则发送该包。该方式的数据处理速度比存储转发方式快，但比直通式慢。



交换机工作原理



目录

Contents

交换机工作原理



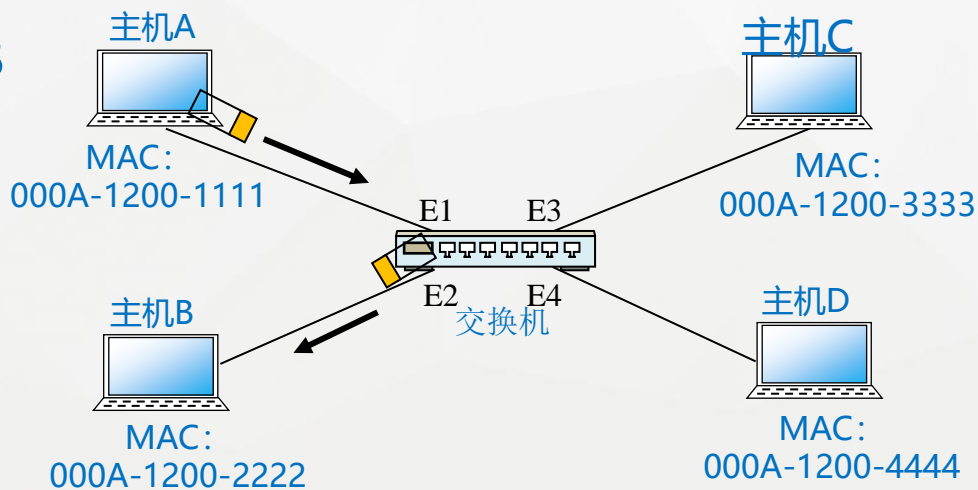
学习目标

- 理解交换机工作原理

在交换机中，维护着一张MAC地址表，表中存放着主机的MAC地址与交换机端口的映射关系。交换机可以通过识别数据包中的MAC地址信息，然后根据MAC地址查询MAC地址表进行数据转发。

例题：分析主机A向主机B
发送数据的过程。

地址表	
端口	物理地址
E1	000A-1200-1111
E2	000A-1200-2222
.....





虚拟局域网简介



目录

Contents

1/ 虚拟局域网概念

2/ VLAN的用途及优势

3/ VLAN的划分方法



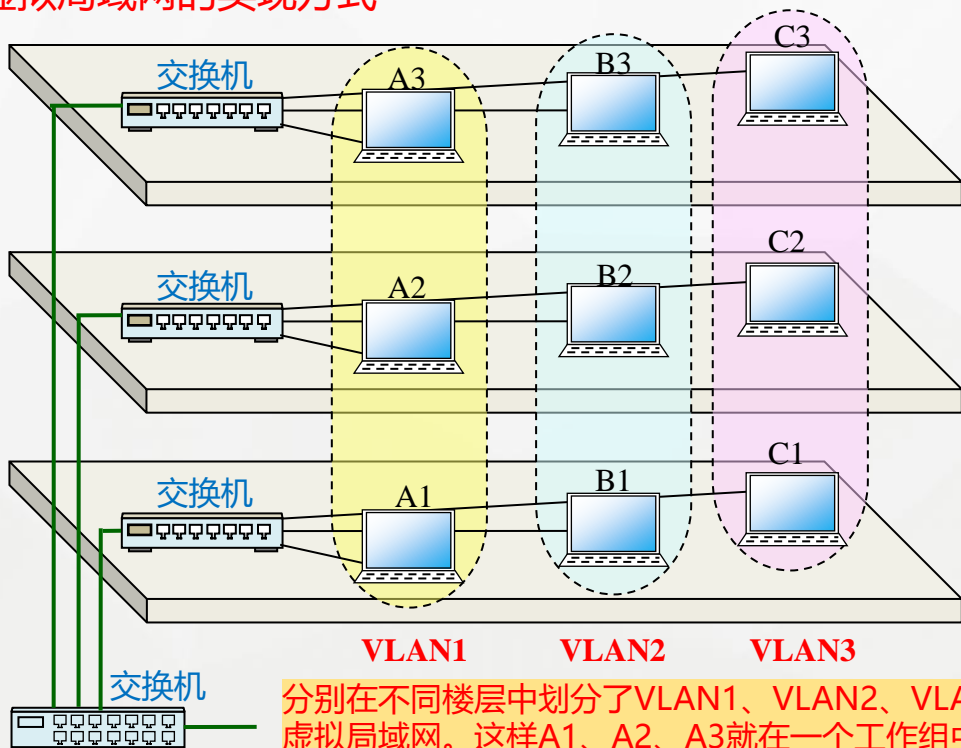
学习目标

- 理解虚拟局域网基本概念
- 了解VLAN的用途及优势
- 掌握VLAN的划分方法



- 虚拟局域网（VLAN，Virtual Local Area Network）是以局域网交换机为基础，通过交换机软件实现根据功能、部门、应用等因素将设备或用户组成虚拟工作组或逻辑网段的技术。其最大的特点是在组成逻辑网时无须考虑用户或设备在网络中的物理位置。
- 数据链路层的单播、广播、单播帧只能在同一个VLAN内转发和扩散，而不会直接进入进入到其它的VLAN之中，VLAN内的各个用户就像是在同一个真实的局域网内一样可以互相访问。
- VLAN可以在一个交换机或者跨交换机实现。同时，若没有路由的话，不同的VLAN之间不可以互相通信。

虚拟局域网的实现方式



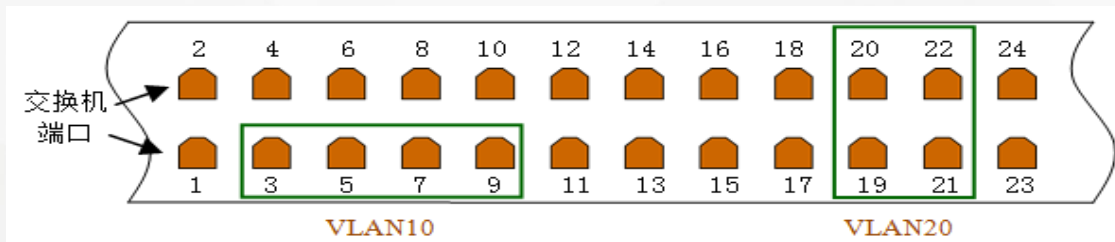
分别在不同楼层中划分了VLAN1、VLAN2、VLAN3三个虚拟局域网。这样A1、A2、A3就在一个工作组中，B1、B2、B3也在一个工作组中

VLAN用途及优势:

- (1) 控制不必要的广播报文的扩散
- (2) 增加了安全性
- (3) 简化了网络管理

划分VLAN的方法有很多种，常见的包括：基于端口的VLAN、基于MAC地址的VLAN、基于网络层的VLAN、基于IP组播的VLAN等。

(1) 基于端口的VLAN



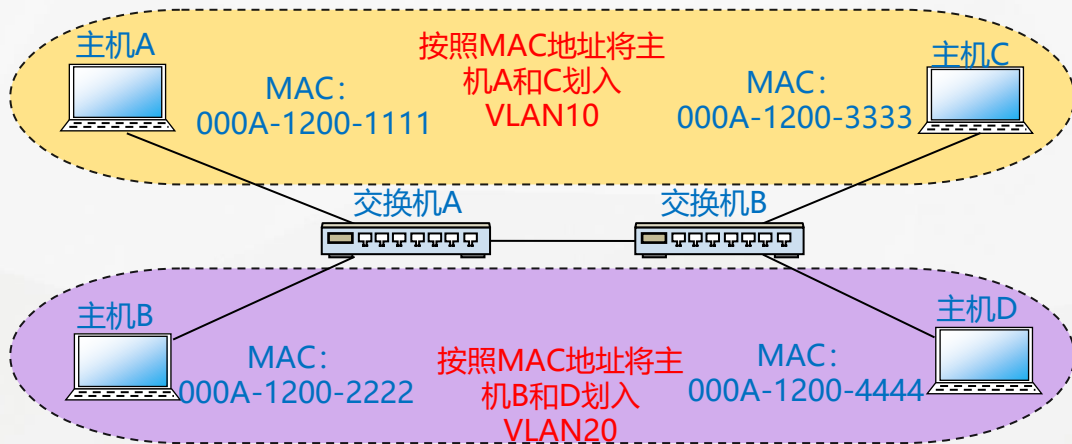
(2) 基于网络层的VLAN

这种划分VLAN的方法是根据每个主机的网络层地址或协议类型（如果支持多协议）划分的。

优点：如果用户的物理位置改变了，不需要重新配置所属的VLAN，而且可以根据协议类型来划分VLAN，还有，不需要附加的帧标签来识别VLAN，这样可以减少网络的通信量。

缺点：是效率低，因为检查每一个数据包的网络层地址是需要消耗处理时间的。

(3) 基于MAC地址的VLAN



(4) 基于IP组播的VLAN

IP组播实际上也是一种VLAN的定义，即认为一个组播就是一个VLAN，这种划分的方法将VLAN扩大到广域网，因此这种方法具有更大的灵活性，而且也容易通过路由器进行扩展，当然这种方法不适合局域网，主要效率不高。



VLAN帧结构



目录

Contents

1/ 普通以太网帧结构

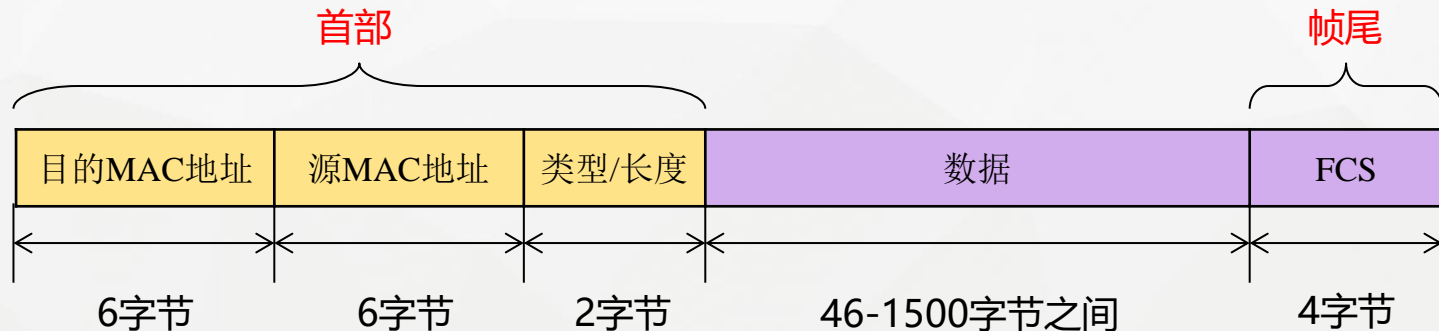
2/ VLAN帧结构



学习目标

- 掌握VLAN帧的结构
- 掌握VLAN帧和普通以太网帧的区别

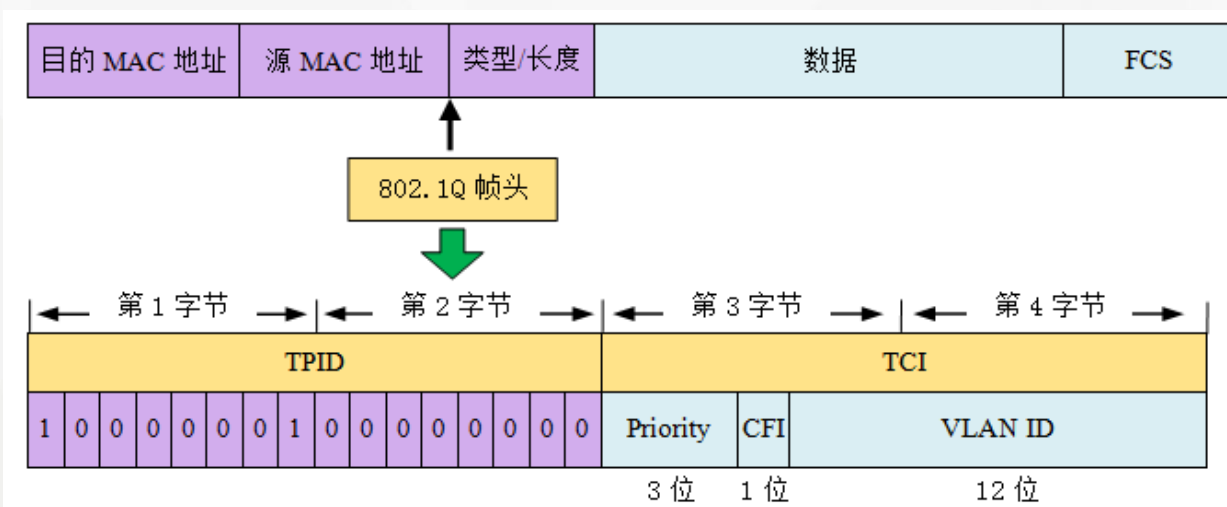
常见的以太网帧结构是Ethernet II的格式。以太网帧的前端是以太网的首部，它总共占14个字节。分别是6个字节的目标MAC地址、6个字节的源MAC地址以及2个字节的
上层协议类型



在交换式以太网中引入VLAN后，不仅在同一台交换机上可存在多个VLAN，同一个VLAN还可以跨越多个交换机。那么交换机如何识别来自不同VLAN的数据，以进行正确的转发呢？

这就需要一种机制来帮助识别不同VLAN的数据，为此，引入了VLAN的帧标记方法。该方法在每个以太网帧的帧头中插入一个惟一的VLAN标识，交换机通过检查这个标识以决定该帧所属的VLAN。

IEEE在1996年3月制定了IEEE802.1Q VLAN标准，给出了IEEE802.1Q的帧格式，它相当于在标准的以太网帧的基础上添加4个字节，两个字节的标记协议标志符（TPID）和两个字节的标签控制信息段（TCI）。



802.1Q帧头放在了标准的以太网帧中“源MAC地址”与“类型/长度”之间，长度为4字节。



TPID: 标签协议标识字段, 值为固定的0x8100, 说明该帧具有802.1Q标签。

TCI: 标签控制信息字段, 包括用户优先级 (User Priority)、规范格式指示器和 VLAN ID三个部分。

- Priority: 共占用3位, 指明帧的优先级。一共有8种优先级, 主要用于当交换机发生拥塞时, 交换机优先发送哪个数据包。
- CFI: 占1位, 为规范格式标识, 用于指示以太网网络和令牌环网络之间的转发, CFI在以太网交换机中总被设置为“0”, 若一个以太网端口接收的帧所具有CFI值为“1”, 表示不对该帧进行转发。
- VLAN ID: 占用12位, 用于标识数据帧所在VLAN的编号。



WLAN概述



目录

Contents

1/ WLAN简介

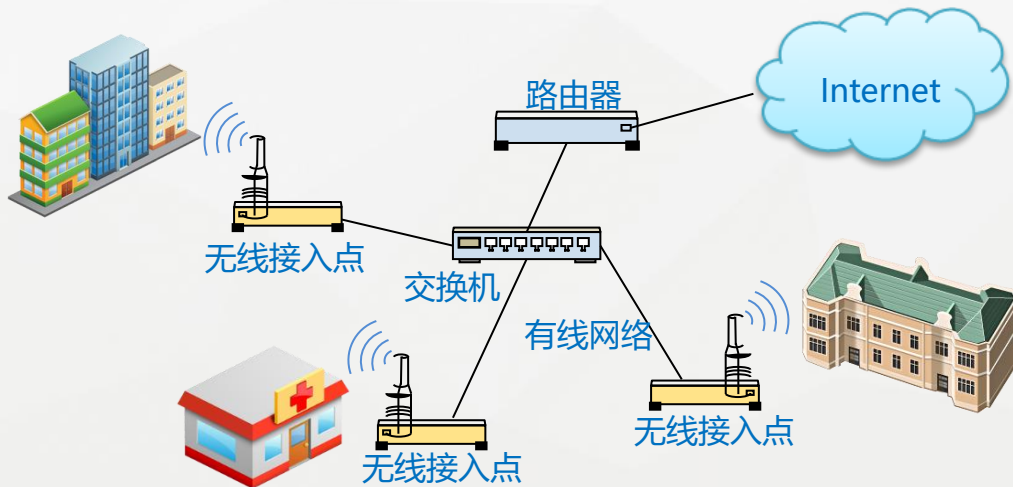
2/ WLAN的优势



学习目标

- 知道什么是WLAN
- 理解无线局域网的优势

无线局域网 (Wireless Local Area Network, 简称WLAN)是指采用无线传输介质的局域网。无线局域网的范围可以是一个房间、一个建筑物内, 也可以是一个校园或者大至几千千米的广大区域。





1. 灵活性和移动性
2. 安装便捷
3. 易于进行网络规划和调整
4. 故障定位容易
5. 易于扩展



WLAN组成结构



目录

Contents



学习目标

- 掌握WLAN的组成和解决方案
- 了解无线传输介质
- 掌握无线局域网的配置方式
- 掌握无线局域网解决方案

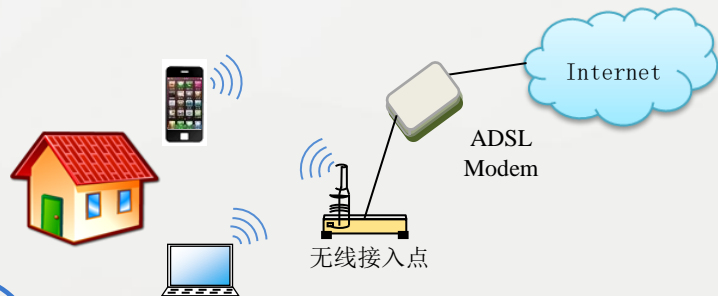
1/ WLAN的组成与解决方案

2/ 无线传输介质

3/ 无线局域网配置方式

4/ 无线局域网解决方案

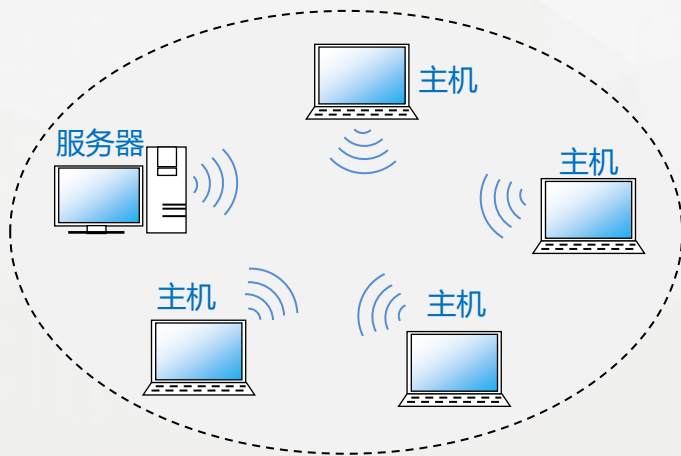
- 无线局域网可独立存在，也可与有线局域网共同存在并进行互连。在WLAN中最常见的组件如下：笔记本电脑和工作站或无线移动终端、无线网卡、无线接入点（AP）、天线等。
- 无线网卡就像标准的网络适配器那样工作，不需要其它特别的无线网络功能。
- AP为Access Point简称，一般翻译为“无线接入点”或“桥接器”。接入点的作用相当于局域网集线器。它在无线局域网和有线网络之间接收、缓冲存储和传输数据，以支持一组无线用户设备。接入点通常是通过标准以太网线连接到有线网络上，并通过天线与无线设备进行通信。在有多个接入点时，用户可以在接入点之间漫游切换。
- 目前常用的AP是无线路由器。



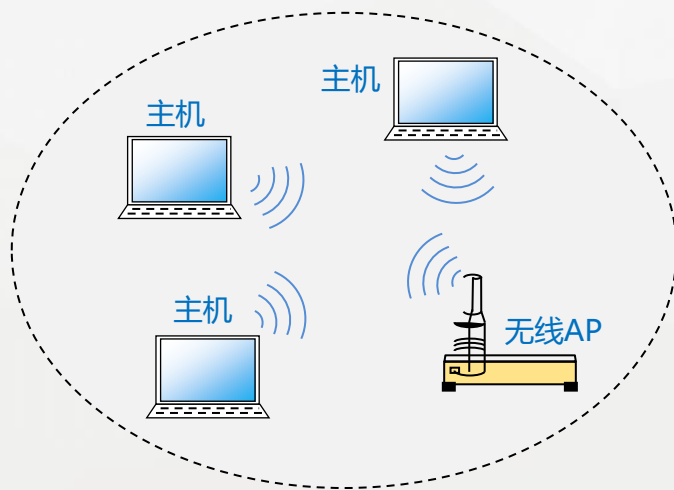
- 无线信号是能够在空气中进行传播的电磁波，无线信号不需要任何物理介质，它在真空环境中也能够传输。无线电波不仅能穿透墙体，还能够覆盖较大的范围，所以成为无线技术组网的一种通用方法。
- WLAN所有的波都以光速传播，所有波都遵循公式：频率×波长=速度。
- 各种电磁波之间的主要区别就是频率。如果电磁波频率低，那么它的波长就长。如果电磁波频率高，那么它的波长就短。

无线局域网配置方式通常有两种：对等模式和基础结构模式。

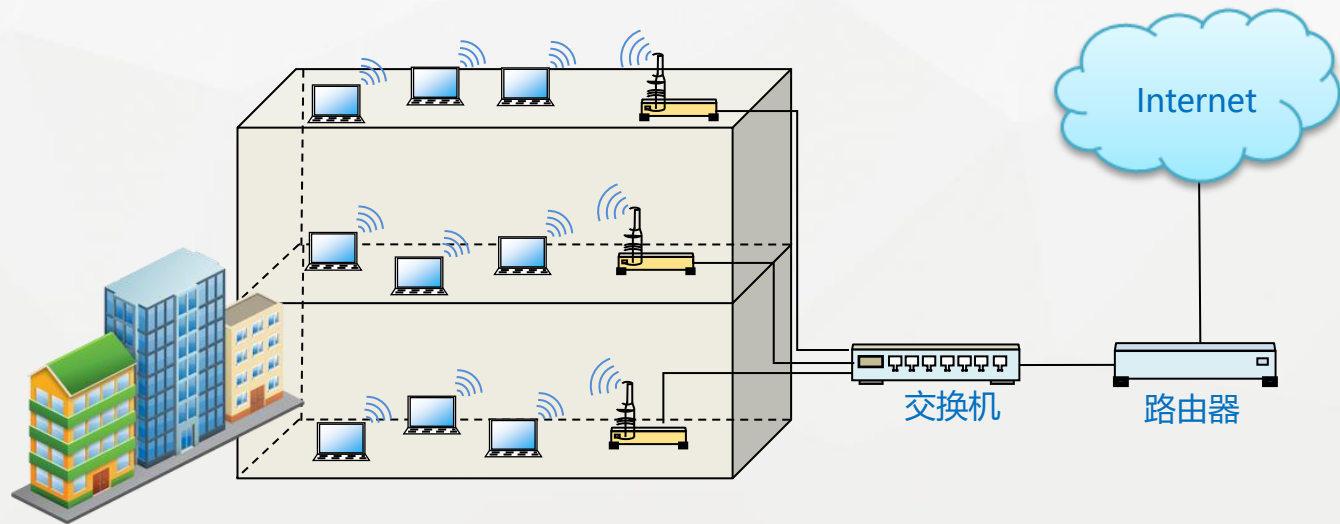
(1) 对等模式： 又称Ad-hoc 模式，是点对点的对等结构。这种应用包含多个无线终端和一个服务器，均配有无线网卡，但不连接到接入点和有线网络，而是通过无线网卡进行相互通信。这种模式主要用在没有基础设施的地方，可以快速而轻松地组建无线局域网。



(2) **基础结构模式**：该模式是目前最常见的一种架构，这种架构包含一个接入点和多个无线终端，接入点通过电缆连线与有线网络连接，通过无线电波与无线终端连接，从而实现无线终端之间、以及无线终端与有线网络之间的通信。通过对这种模式进行复制，可以实现多个接入点相互连接的更大的无线网络。



基础结构模式的WLAN不仅可以应用于独立的无线局域网中，如小型办公室无线网络，也可以以它为基础网络单元组建成庞大的WLAN系统。下图是一家宾馆的无线网络方案，宾馆中各层楼的无线用户通过接入该楼层，并与有线网络相连接的AP实现与Internet的连接。





WLAN冲突检测技术

CSMA/CA



目录

Contents



学习目标

- 了解IEEE 802.11标准
- 掌握CSMA/CA技术原理

1/ IEEE802.11标准

2/ CSMA/CA技术



- IEEE802.11定义了无线LAN协议中物理层与数据链路层的一部分(MAC层)。IEEE802.11这个编号有时指众多标准的统称，有时也专指无线局域网的一种通信方式。
- MAC层中物理地址与以太网相同，都使用MAC地址，介质访问控制使用CSMA/CA方式。

802.11标准与无线技术

无线技术与标准	802.11	802.11a	802.11b	802.11g	802.11n	802.11ac
工作频段	2.4GHz	5GHz	2.4GHz	2.4GHz	2.4GHz和5GHz	5GHz
最高传输速率	2Mbps	54Mbps	11Mbps	54Mbps	108Mbps以上	1Gbps以上
实际传输速率	低于2Mbps	31Mbps	6Mbps	20Mbps	大于30Mbps	300Mbps以上
传输距离	100m	80m	100m	150m以上	100Mm以上	--
主要业务	数据	数据、图像、语音	数据、图像	数据、图像、语音	数据、高清图像、语音	数据、高清图像、语音
成本	高	低	低	低	低	低

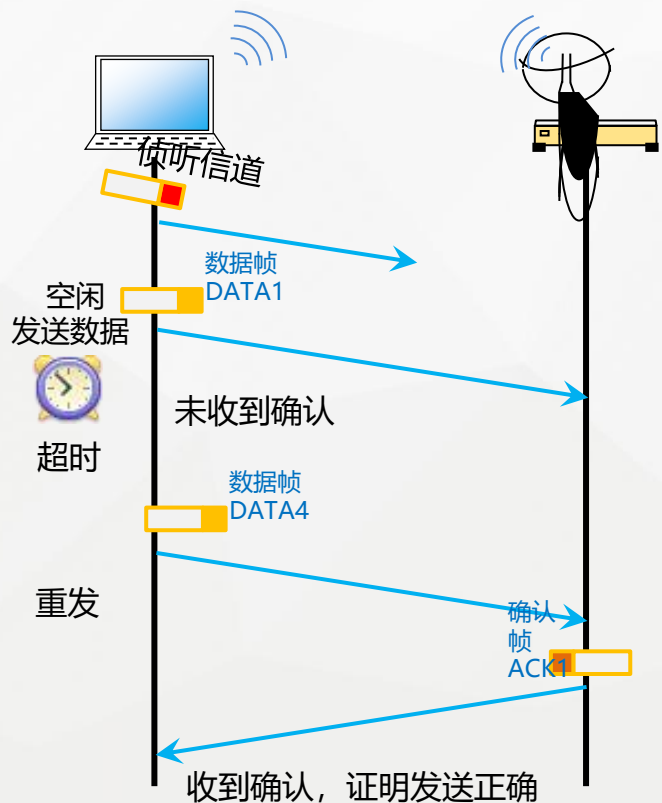


- IEEE 802.11规范覆盖了无线局域网的物理层和MAC子层。
- 无线局域网标准802.11的MAC和802.3协议的MAC非常相似，都是在一个共享媒体之上支持多个用户共享资源，由发送者在发送数据前先进行网络的可用性检测。
- CSMA/CA利用ACK信号来避免冲突的发生，也就是说，只有当客户端收到网络上返回的ACK信号后才确认送出的数据已经正确到达目的地址。CSMA/CA没有CSMA/CD的冲突检测机制，因此各发送站点要等待一个帧间隔（interframe space ,IFS）时间，还必须执行二进制指数退避算法以进一步减少冲突。

(1) 首先检测信道是否有使用，如果检测出信道空闲，则等待一段随机时间后，才送出数据。

(2) 接收端如果正确收到此帧，则经过一段时间间隔后，向发送端发送确认帧ACK。

(3) 发送端收到ACK帧，确定数据正确传输。如果在规定的时间内没有收到确认，表明出现冲突，发送失败，执行退避算法，重发此帧。





PPP协议概述



目录

Contents



学习目标

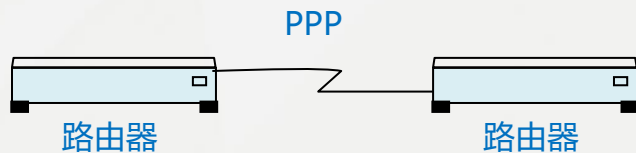
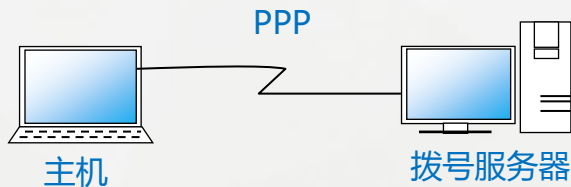
- 了解PPP协议的应用
- 理解PPP协议的特点
- 掌握PPP协议体系结构

1/ PPP协议的应用

2/ PPP协议的特点

3/ PPP协议体系结构

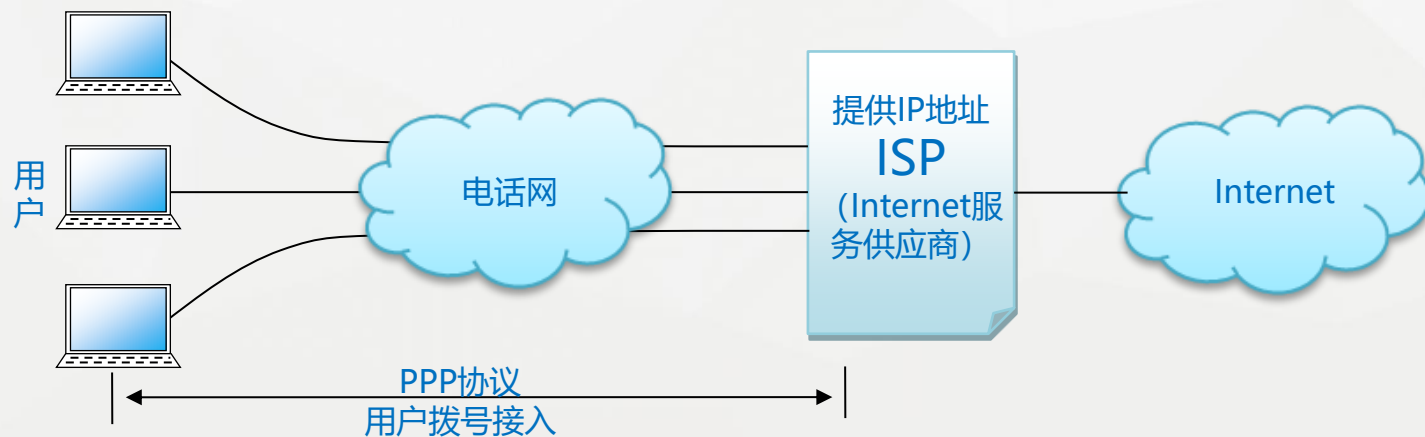
- PPP 是点对点协议 (Point-to-Point Protocol) 的简称, 它是一个工作于数据链路层的广域网协议, 它通常用在两节点间创建直接的连接, 并可以提供连接认证、传输加密等。
- PPP 由IETF (Internet Engineering Task Force) 开发, 目前已被广泛使用并成为国际标准。无论是同步电路还是异步电路, PPP协议都能够建立路由器之间或者主机到网络之间的连接。PPP属于纯粹的数据链路层, 与物理层没有任何关系。换句话说, 仅有PPP无法实现通信, 还需要有物理层的支持。



PPP可以使用电话线或ISDN、专线、ATM线路等接入

PPP协议的应用案例

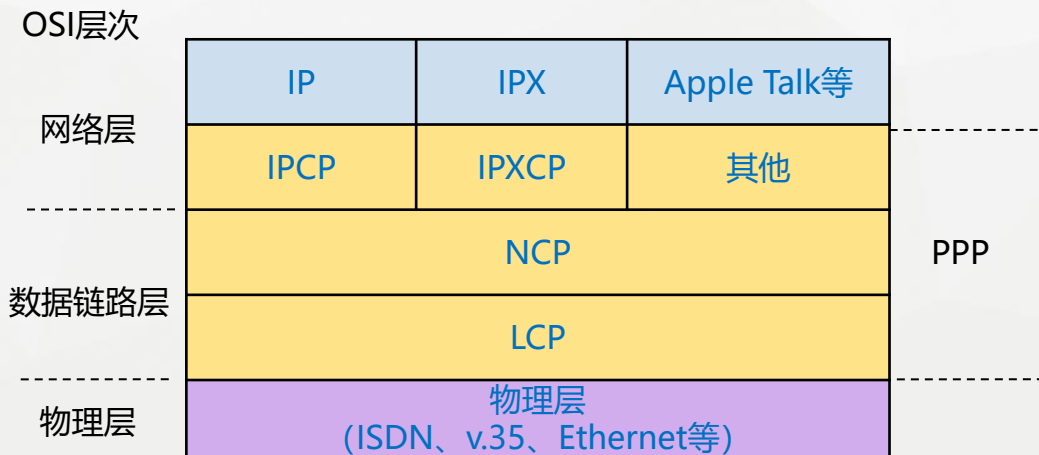
在ADSL上网的方式中，每一个ISP（Internet 服务提供商）都已经从因特网的管理机构或更大的ISP申请到一批IP地址，ISP通过高速通信专线与Internet相连。用户在申请后，就可以通过拨号方式利用Modem、电话线接入到该ISP。用户在接通ISP后就分配给他一个临时IP地址，然后用户就可以实现与Internet的连接。用户接入ISP的方式主要通过PPP协议实现。当用户断开连接后，ISP收回IP地址，以便再分配给其他用户使用。



- 能够控制数据链路的建立。
- PPP具有动态分配IP地址的能力，可以为接入的终端自动分配IP地址，在链路释放后可以收回IP地址。
- PPP支持多种网络协议，能够支持IP、IPX等网络协议，允许在一条链路上同时传输多种网络协议报文。
- 能够进行错误检测，PPP的错误检测机制使得进程能够识别错误的情形。
- 支持身份验证，用来确保接入者的合法身份，另外PPP还具有授权、计费等功能。
- 有协商选项，能够对网络层的地址和数据压缩等进行协商，通过压缩可缩小数据的长度，从而提高数据的吞吐量。

PPP协议使用了OSI分层体系结构中的3层。在PPP的主要功能中包括两个协议：一个是不依赖上层的LCP协议(Link Control Protocol)，另一个是依赖上层的NCP协议(Network Control Protocol)。如果上层为IP，此时的NCP也叫做IPCP(IP Control Protocol)。

PPP体系结构与OSI结构关系：





- ① LCP (Link Control Protocol, 链路控制协议)主要用于数据链路连接的建立、拆除和监控、参数的协商等。
- ② NCP (Network Control Protocol, 网络层控制协议族)主要用于协商在该链路上所传输的数据包的格式与类型, 建立和配置不同网络层协议; 目前, NCP有IPCP和IPXCP两种。
- ③ 通过PPP连接时, 有两种验证方式, 分别为PAP和CHAP。

PAP是PPP连接建立时, 通过两次握手进行用户名和密码验证, 其中密码以明文方式传输。CHAP采用密文验证方式, 此外, 在建立连接后还可以进行定期的密码交换, 用来检验对端是否中途被替换。



PPP工作过程



目录

Contents

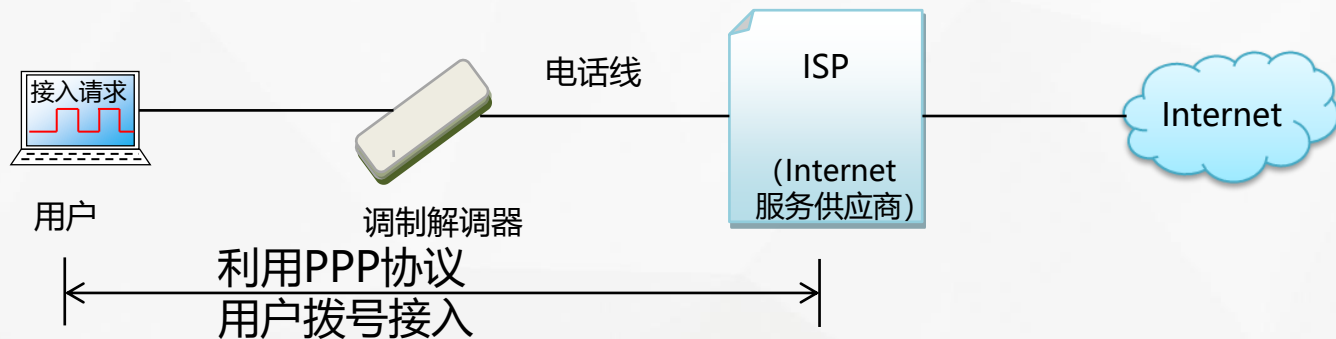
1/ ADSL模式中PPP协议的应用

2/ PPP协议工作过程

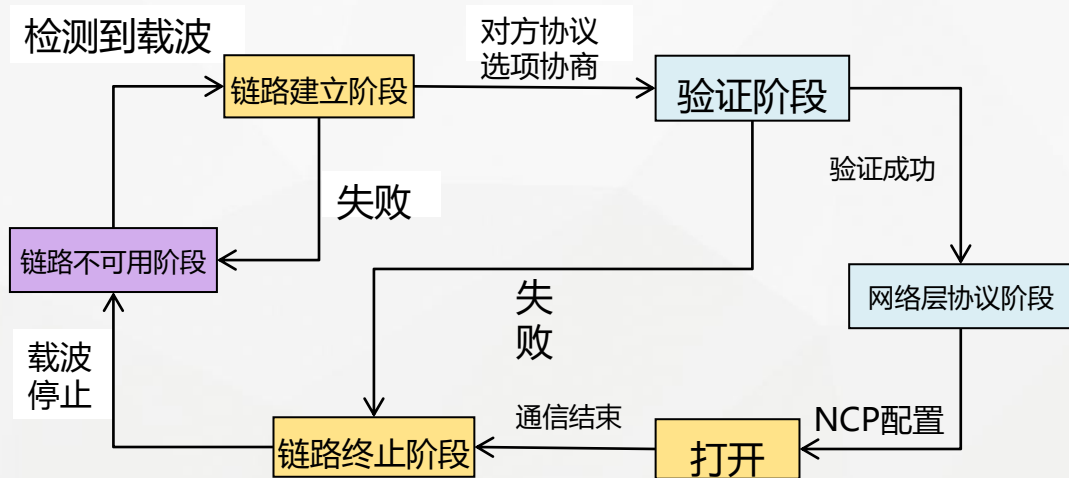


学习目标

- 掌握ADSL模式中PPP协议的应用
- 理解PPP协议工作过程



当用户拨号接入ISP时，路由器的调制解调器对拨号做出应答，并建立物理层连接后，线路就进入建立状态。这时PC机向路由器发送一系列的LCP分组（封装成多个PPP帧）。这时LCP开始协商一些选项，协商结束后就进入验证状态。若通信的双方验证身份成功，则进入网络层协议协商阶段。NCP给新接入的PC机分配一个临时的IP地址，这样PC机就成为Internet上一个主机了。当用户通信完毕时，NCP释放网络层连接，收回原来分配出去的IP地址。接着LCP释放数据链路层连接，最后释放的是物理层的连接。





PPP协议帧格式



目录

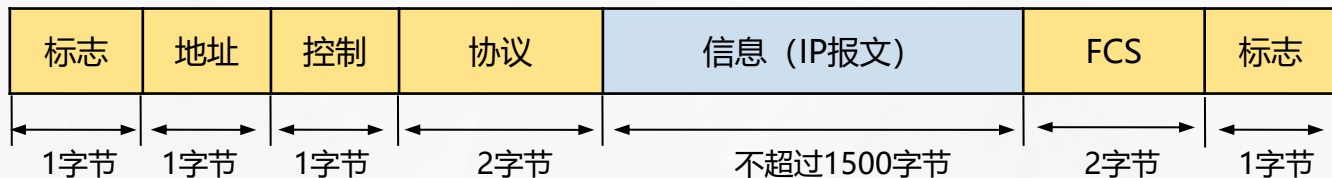
Contents

PPP协议帧格式



学习目标

- 掌握PPP协议帧的格式



标志字段：用来区分每个帧。这一点与HDLC协议非常相似，因为PPP本身就是基于HDLC制定出来的一种协议。所有的PPP帧是以标准的HDLC标志字节（01111110）开始的，如果是用在信息字段上，就是所填充的字符。

地址字段：总是设成二进制值11111111，表明主从端的状态都为接收状态。

控制字段：其缺省值为00000011，此值表明是一个无序号帧。换言之，缺省情况下，PPP没有采用序列号和确认来进行可靠传输。在有噪声的环境中，如无线网络，则使用编号方式进行可靠的传输，

协议字段：是告知在信息字段中使用的是哪类分组，针对LCP、NCP、IP、IPX、AppleTalk及其它协议，定义了相应的代码。

信息字段：是变长的，最多可达到所商定的最大值。缺省长度1500字节。如果需要的话，在有效



PPPoE简介



目录

Contents

1/ PPPoE的概念

2/ PPPoE的典型应用

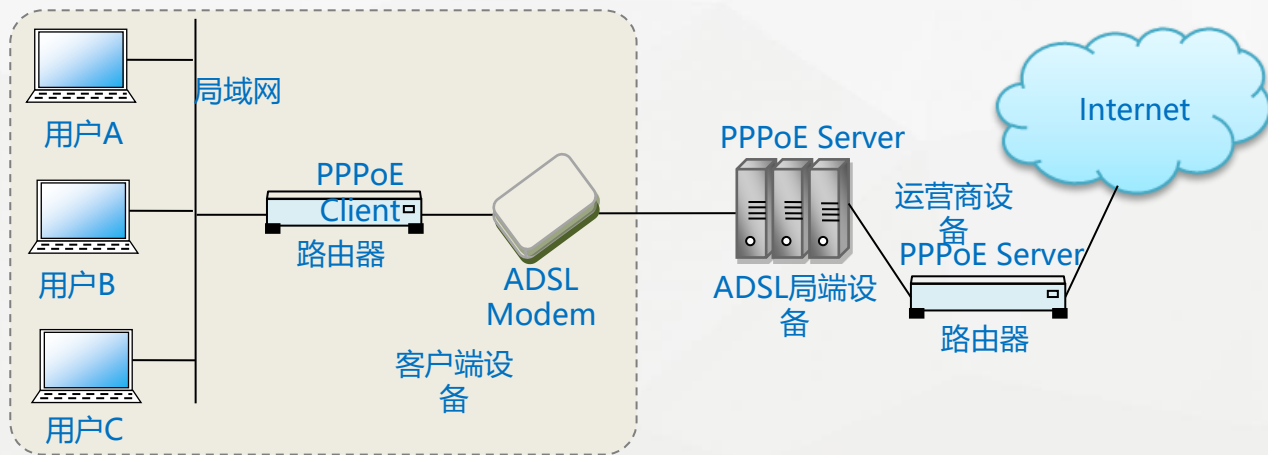


学习目标

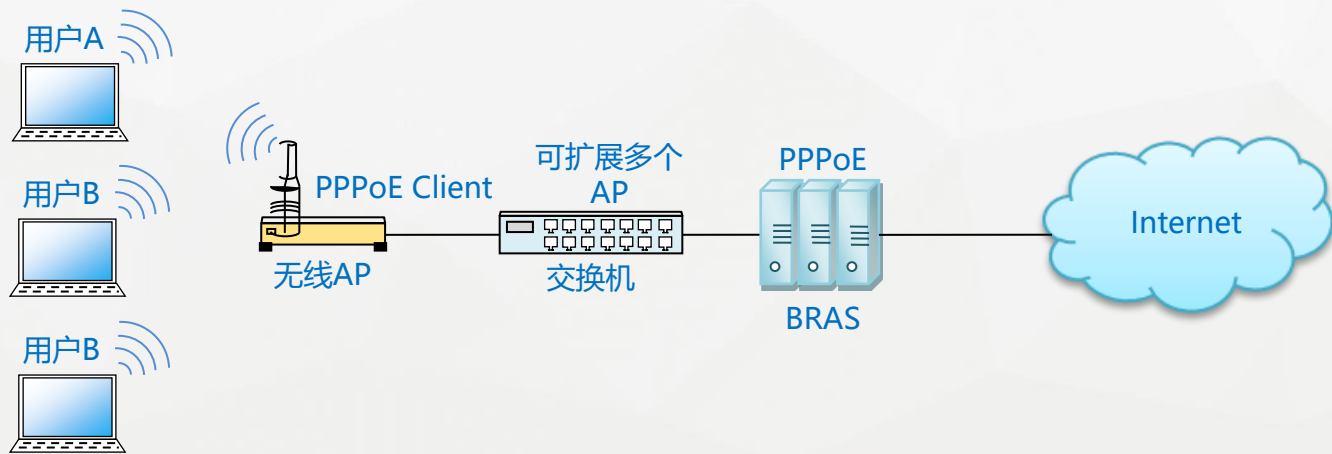
- 掌握PPPoE的概念
- 了解PPPoE的典型应用

- PPPoE (Point to Point Protocol over Ethernet, 以太网上的点对点协议), 简单地说, 就是将以太网和PPP协议结合后的协议, 目前广泛应用在ADSL接入方式中。通过PPPoE技术和宽带调制解调器 (比如ADSL Modem), 就可以实现高速宽带网的个人身份验证访问, 为每个用户创建虚拟拨号连接, 这样就可以高速连接到Internet。
- 单纯的以太网没有验证功能, 也没有建立和断开连接的处理, 因此无法按时计费。而如果采用PPPoE管理以太网连接, 就可以利用PPP的验证等功能使各家ISP可以有效地管理终端用户的使用。
- PPPoE使用Client/Server模型, PPPoE的客户端为PPPoE Client, PPPoE的服务器端为PPPoE Server。PPPoE Client向PPPoE Server发起连接请求, 两者之间会话协商通过后, PPPoE Server向PPPoE Client提供接入控制、认证等功能。

根据PPP会话的起止点所在位置的不同，有两种组网结构：一种是利用通信设备之间建立连接，如企业中有众多用户，希望通过局域网的方式实现网络连接。另一种是主机与通信设备的连接，主要是个人通过拨号连接到Internet的方式。



在无线网络中，AP设备可以作为PPPoE Client，宽带远程接入服务器（BRAS）作为PPPoE Server，终端用户可以直接通过无线网络访问Internet。





谢谢

Thanks!