Http学习

# 网络通讯简介

学习地址https://www.bilibili.com/video/BV1h5411a79A/?p=9&spm\_id\_from=pageDriver&vd\_source=e1c95be592bf4b86f4e2917a7a40bae9

## 1、网络技术

为了达到服务通信目的，而所需要的技术手段

## 2、通信网络

通信网络=通信设备（PC,手机，平板，打印机--终端设备；路由器，交换机，防火墙、网络传输设备）+传输介质（同轴电缆、双绞线、光纤等）

1. 双绞线线序



现在是自适应的。

3)光纤

光电转换器：就是光锚，pc的电信号传给光锚，光锚再将光信号转为电信号

光纤

光锚

Pc

光锚

Pc

## 3、以太网数据传输

以太网数据传输遵循IEEE 802.3标准来管理和控制数据帧。

## 4、网络通信协议

定义：决定数据的格式和传输的一组规则或者一组惯例。

# 二、网络分层模型

## 1、分层模型-OSI

1. 七层设计理念：主要目的是解决异种网络连接时遇到的兼容性问题

最大的优点：将服务、接口、和协议这三个概念明确的区分开来。

服务：某一层为上一层提供一些什么功能。

接口：上一层如何使用下层的服务。

协议：如何实现本层的服务。



## 2、分层模型-TCP/IP



应用层处理过的数据称之为：PDU。（protocol data unit）

传输层处理后的数据称之为：Segment（数据段）

网络层处理后的数据称之为：Packet(数据包)

数据链路层处理后的数据称之为：Frame（数据帧）

物理层处理完的数据称之为：Bit（比特流）



网络传输设备只处理到网络层。（交换机，路由器）

# 三、终端通信

## 1、终端之间的通信

帧：

Ethernet\_II帧格式type值>=1536;数据帧的长度在64-1518字节之间。

type标识上层数据采用的协议，type=0x0800代表IP协议。0x0806代表ARP协议

6B 6B 2B 46-1500B 4B



这里的DATA包含IP头，TCP/UDP头，客户端输入数据。

## 2、冲突域

以对讲机为例：在一个共享网络中，只能一个人说话，其他人不能说话。

以太网的最小包长和最大包长：最小64字节，最大无限

为什么要有最小字节：经过实践证明当发送字节>64的时候，如果有冲突的话就会在64字节之前检测到。如果小于64字节的话，则有可能检测不到冲突。

## 3、双工模式

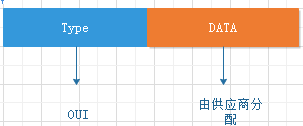
半双工：对讲机--只能一个人发消息。

全双工：电话--双方可以同时发送消息，不冲突。目前的网络中全是全双工。

## 4、数据帧传输

数据链路层基于MAC地址进行帧的传输。

MAC地址的组成：



OUI:唯一组织标识符。由IEEE管理和分配。

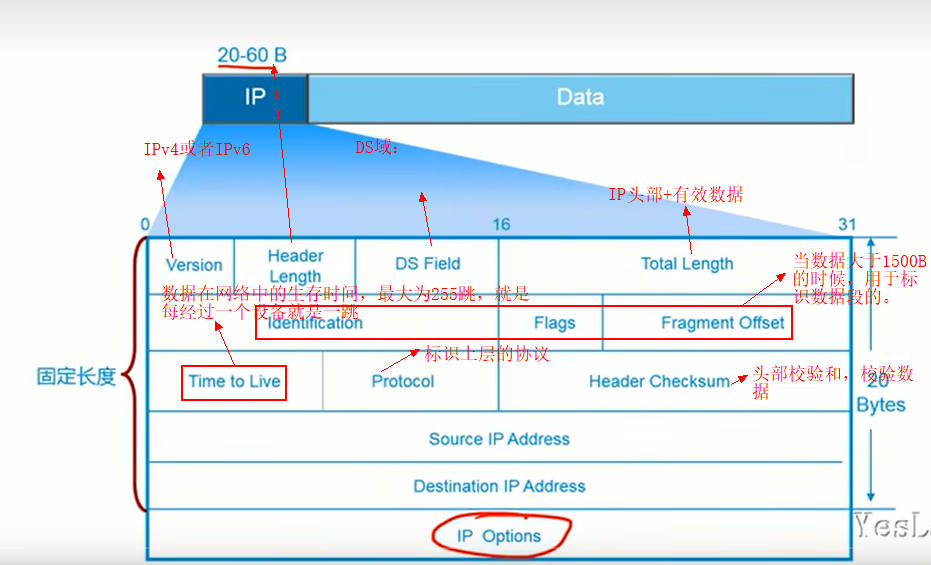
## 5、数据的类型

1. 单播：只限于两个终端之间。比如邮件。MAC地址的第八个bit如果为0则为单播。
2. 广播：目的MAC地址如果是全部F则为广播
3. 组播：MAC地址的第八个bit为1.比如腾讯会议。

# 四、IP协议（internet protocol）

## 1、ip报文

ip头报文长度为20-60字节不等。

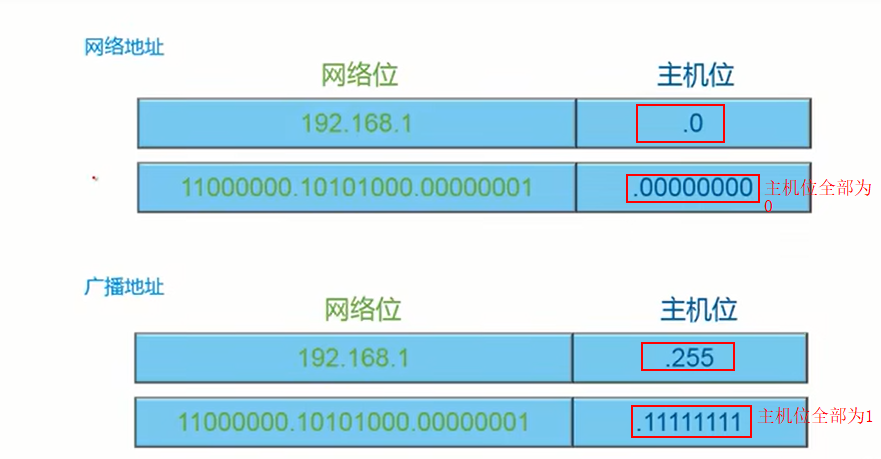


## 2、ip地址构成

IP地址分为网络部分和主机部分。

IP地址由32个二进制位组成，通常由点分十进制形式表示。单指Ipv4地址。





网络地址和广播地址有特殊作用，不可用于分配，其他的都可以用来分配。

## 3、IP地址的分类

按照IANA组织的分类：



## 4、公网地址和私网地址

公网地址也就是internet网络地址，私网地址是内网地址，不可以连接外网，如果想连接外网需要出口设备，出口设备实现了技术NAT---网络地址转换。

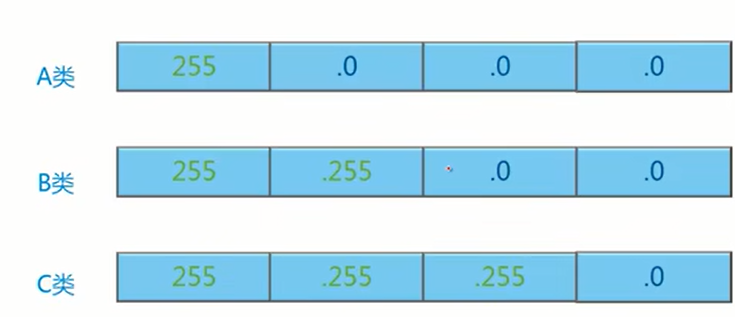
有的公司的地址是公网地址？其实公网地址是可以用在内网的，只不过这个IP如果想访问外网的话还是需要用NAT转换一下，转换后的公网地址和私网中的公网IP不是一个。

## 5、子网掩码

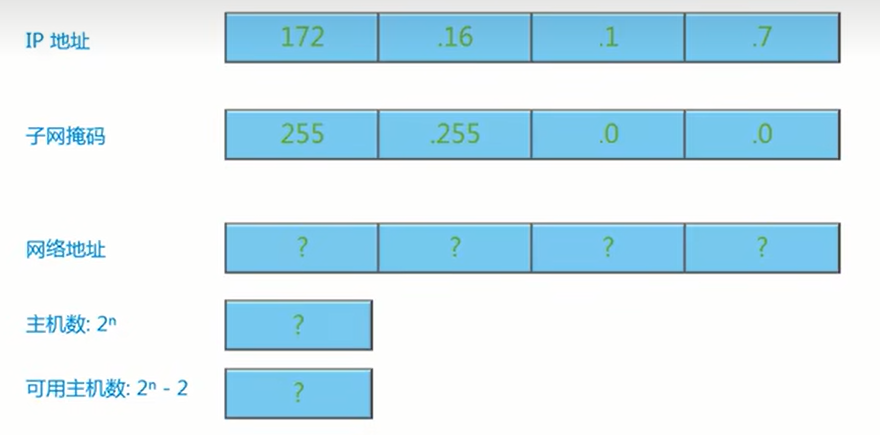
1）子网掩码用来告诉某台设备哪部分是网络位，哪一部分是主机位。

2）子网掩码的网络地址全是1，主机位全是0.

针对A，B,C类IP的子网掩码分别为：



## 6、举例说明



如上图中网络地址为172.16.0.0 （由子网掩码可以知道主机位为16bit,网络位也是16bit）广播地址为172.16.255.255

主机数：2的16次方。

可使用的主机数：2的16次方减去2（2代表不可用来分配的在网络地址和广播地址）

## 7、同一个网段

何为同一个网段：就是网络地址是一样的。

比如：192.168.1.2 子网掩码：255.255.255.0和192.168.1.1 子网掩码：255.255.255.0是在一个网段。

但是：192.168.1.2子网掩码：255.255.0.0和192.168.1.1子网掩码：255.255.255.0就不是在一个网段。因为192.168.1.2子网掩码：255.255.0.0的网络地址是192.168.0.0而192.168.1.1子网掩码：255.255.255.0的网络地址是192.168.1.0

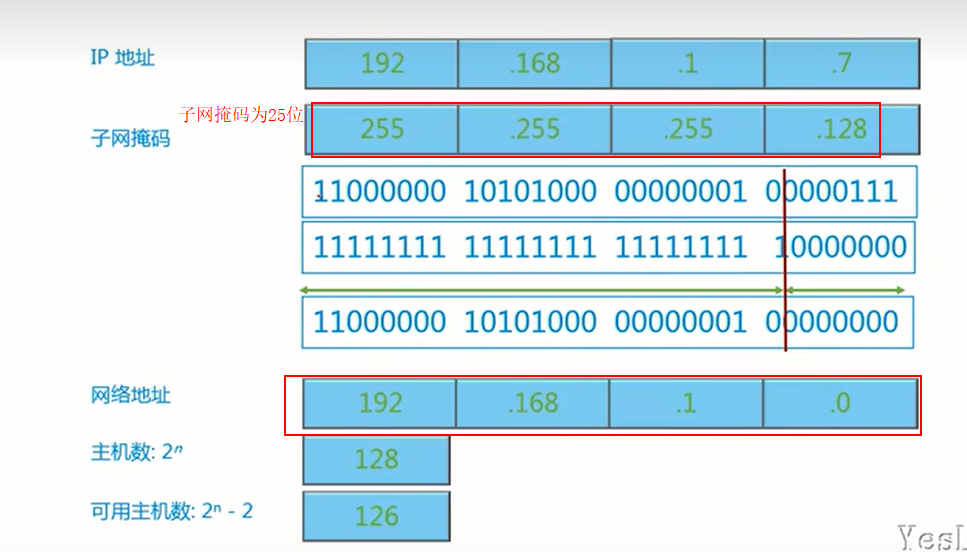
## 8、有类IP编址

1）概念：就是按照A.B.C类划分的缺省的子网掩码地址。

2）这样的缺陷：容易造成地址的浪费。比如以C类IP地址为例，如果只有30台主机，但是使用缺省的子网掩码的话计算出可以拥有2的8次方减2个（254）地址可以分配，这样就会有224个地址浪费掉了。

3）如何解决上面的问题呢？------变长子网掩码（就是将子网掩码的位数变长，比如由原来的24位变为25位）--则可使用的主机地址就是2的7次方减2个。

这样子网掩码的地址就变为了255.255.255.128（128是因为网络位借了1位主机位，借完以后主机位就剩下2的7次方可用，所以2的8次方减去2的7次方就是128）如下图：



## 9、192.168.1.0/24

24代表的是子网掩码是24个一，也就是255.255.255.0

## 10、可变长的子网划分（VLSM）重要

1）核心的思想：就是“借用”主机位来“制造”新的“网络”。

2）网络增多，同一个网段的主机减少。

3）这样做的好处是？

缩减网络流量--可分配的主机IP少了，网络流量减少。

优化网络性能--

简化管理，更为灵活的形成大覆盖范围的网络。

最本质的作用就是合理的分配IP地址

。

## 11、子网数目、主机数目

1）子网的数目=2的x次方（x代表的是子网的位数）

以A类IP地址为例：网络位为8bit，且必须以0开头，则网段数目就是2的7次方，也就是。假如我借了主机3个bit，则子网的数目就是2的3次方。

## 12、变长子网掩码划分举例

以C类网络地址段192.168.10.0/24为例：划分出三个子网。

第一种方法：三个子网的话，需要2的2次方，所以需要借用两个主机位就可以了。主机位就是2的6次方减去2.

划分的子网如下：

192.168.10.0/26 也就是借来的两位都为0，

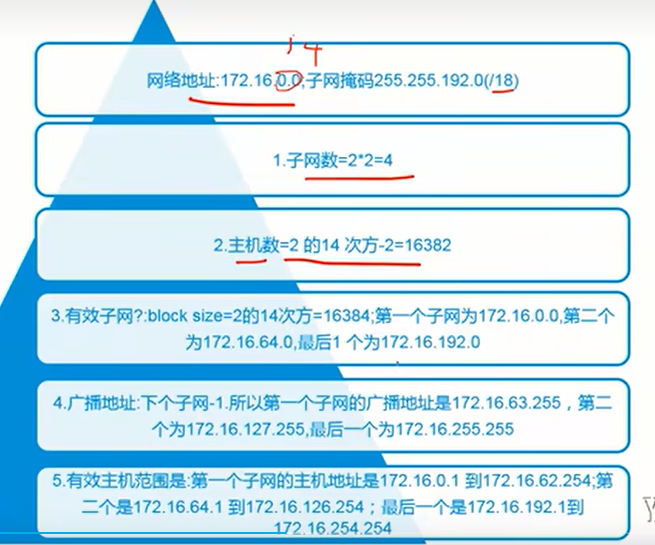
192.168.10.64/26，借来的两位为01

192.168.10.128/26，借来的两位为10

192.168.10.192/26，借来的两位为11

这种方法划分，浪费IP地址。

B类的



第二种方法：先确定主机的个数，再划分子网。

VLSM（）的好处：节约IP地址。

注意点：使用VLSM时，所采用的路由协议必须支持它，这些路由协议包括：

RIPv2 OSPF,BGP

# 五、ICMP协议

Internet control message protocol(Internet 控制消息协议)

## 1、概念

1)也是网络层协议：用于在网络设备间传递各种差错和控制信息，并对于收集各种网络信息、诊断和排除各种网络故障等方面起着重要的作用。

## 2、作用

用来传递差错、控制、查询等信息。例如重定向就属于控制信息。

## 3、报文格式类型

ICMP Redirect：重定向报文

ICMP Echo request(type 8)

ICMP Echo reply(type 0)

## 4、ping

1）用来检测客户端到目的主机的网络是否畅通

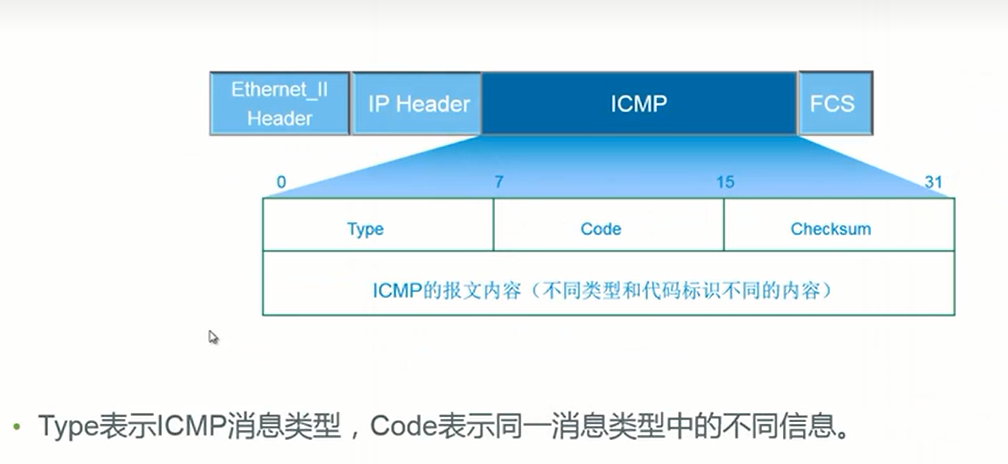
2）遇到的问题种类：

Ping 某台服务器的时候，如果是找不到目的服务器，就会返回ICMP目的不可达。

## 5、抓包工具

Wireshark

## 6、报文格式结构





## 7、tracert

用来查看到目的主机所经过的设备。

# 六、ARP协议

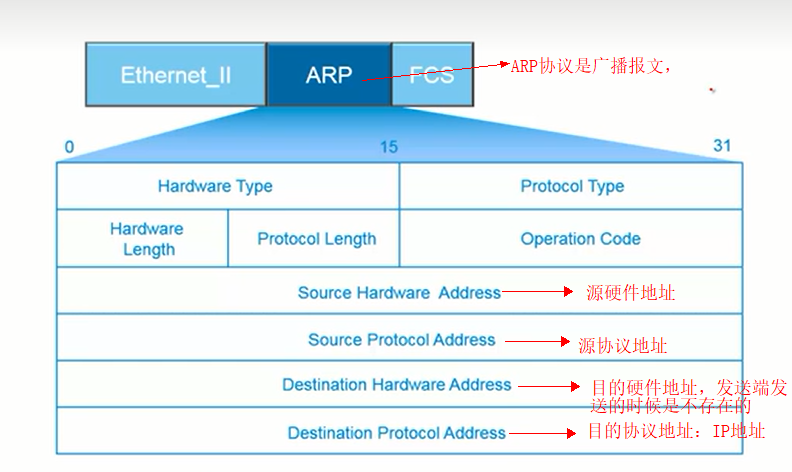
## 1、ARP协议是啥

数据链路层在对数据进行封装的时候，需要目的MAC地址，这个地址如何获取到呢？这个时候需要提前得到目的MAC地址，这个时候就需要ARP协议了.

ARP协议：地址解析协议。主要是解析目的IP地址所对应的MAC地址。ARP也是网络层协议

## 2、报文格式结构

1）请求报文



ARP协议请求报文是广播报文，并且报文是不能经过路由器的。路由器可以收到，连在交换机上的设备可以收到。

请求的时候，Ehernet\_ii的目的MAC地址是FF-FF-FF-FF-FF-FF

ARP中的目的MAC地址为00-00-00-00-00-00（也有可能是全F）表示不知道目的MAC地址

ARP操作类型为Request

2)响应报文为

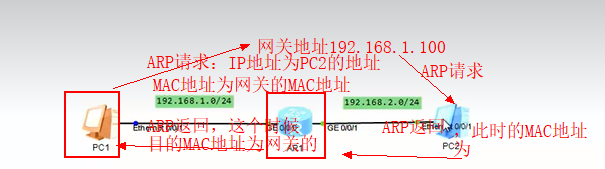
响应报文为响应报文。因为目的主机经过请求报文的中IP地址拆分匹配之后，将发送主机的IP地址和MAC地址记录了下来。

操作类型为Reply,响应报文的目的就是告诉发送主机我的MAC地址。

1. 发送方主机接到响应报文以后，就可以给目的主机发送单播报文了。

注：同一网段、不同物理网络上的计算机之间、可以通过ARP代理实现相互通信。

## 3、不同的网段之间通信---使用网关



PC1 ping 192.168.2.0的时候，APR请求是发给了网关，ip地址是网关的地址，返回的MAC地址是网关的地址。

网关进行数据转发的时候，将进行ARP请求报文转发，此时的源MAC地址为网关的MAC地址，源IP地址为网关的IP地址？。

PC2进行响应的时候，源MAC地址为PC2的地址，目的MAC地址为网关的MAC地址。

PC1只能解析网关的MAC地址，而且PC1知道是解析的网关的MAC地址。

## 4、不同网段之间的通信---使用ARP代理

两台主机之间不设置网关，直接通信。

主机A10.1.0.1/8 主机B10.2.0.1/8必须这样设置，这样A和B会被认为是在一个网段（虽然不是，因为经过路由器了。路由器需要开启ARP的代理）

此时A进行ARP request的请求10.2.0.1的MAC地址，实际上是请求的路由的MAC地址，ip地址是主机B的地址。但是A不知道，误以为MAC地址就是B的地址。

## 5、免费ARP用来探测IP地址冲突’

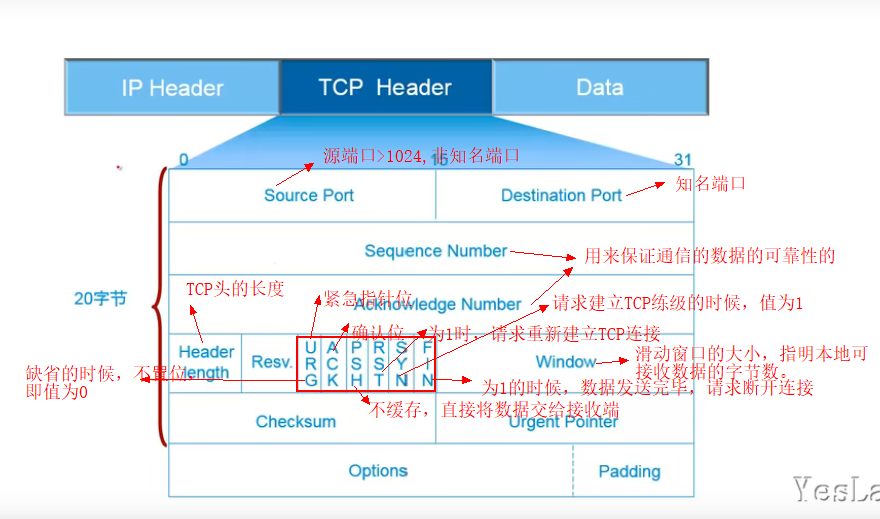
原理就是当给主机配置完ip的时候，就会用配置的IP地址作为目标地址，往同一个网段发送arp请求，如果收到响应，就证明有冲突。

# 七、TCP协议

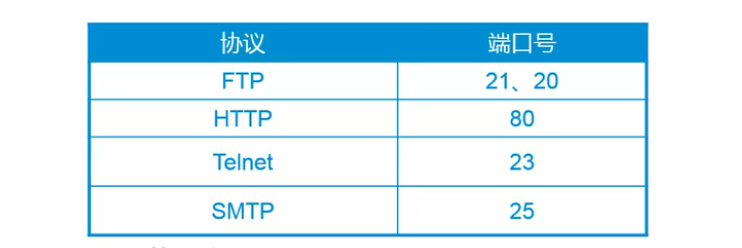
## 1、简介

TCP协议（Transmission Control Protocol）：传输控制协议，属于传输层的协议。

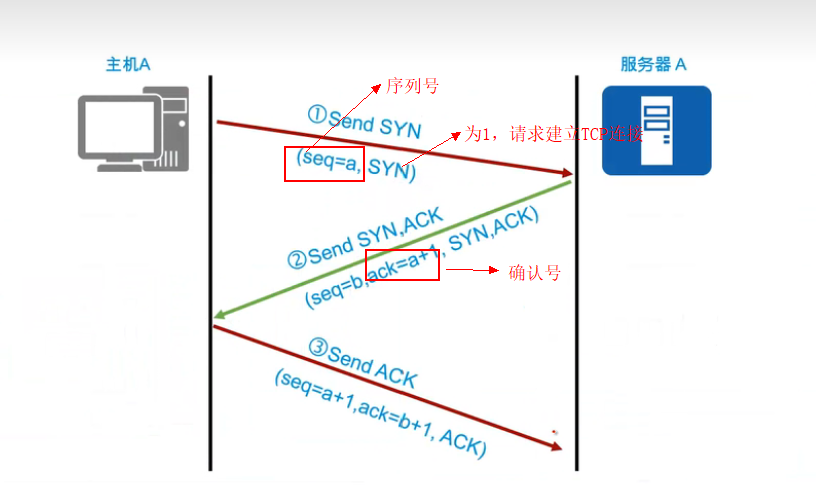
## 2、TCP报文



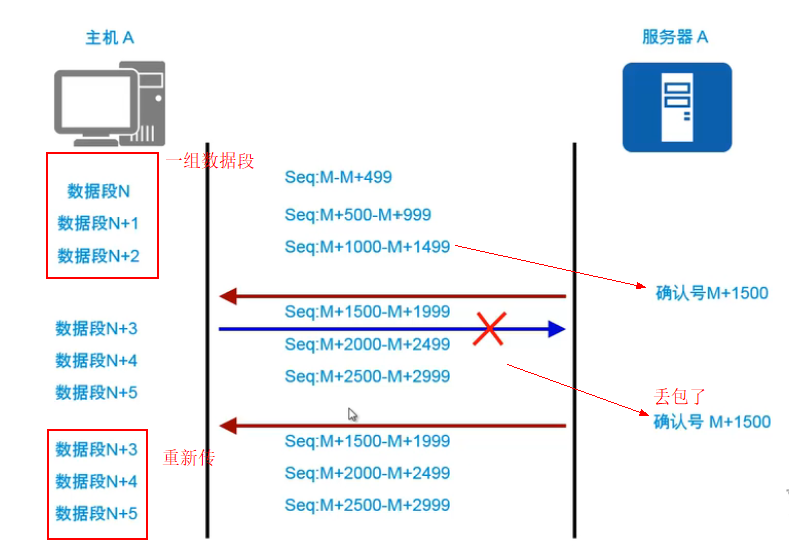
## 3、常用协议的端口



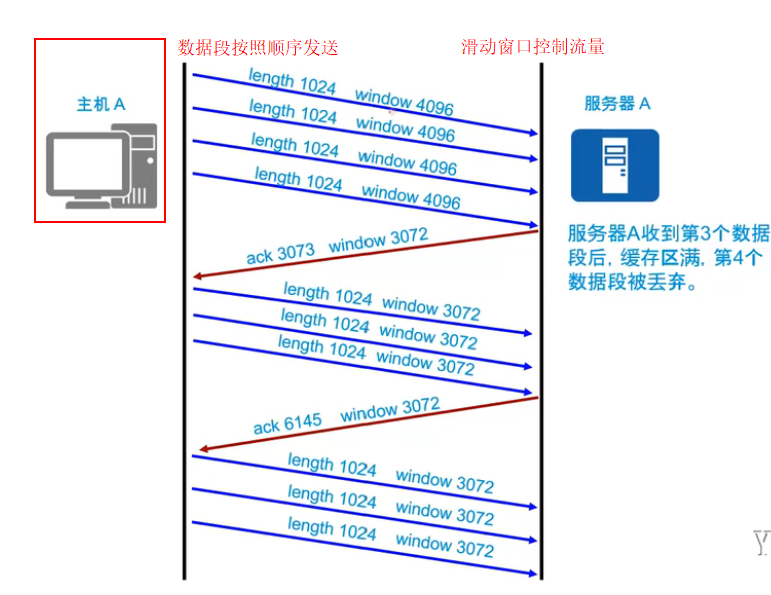
## 4、建立TCP连接的过程



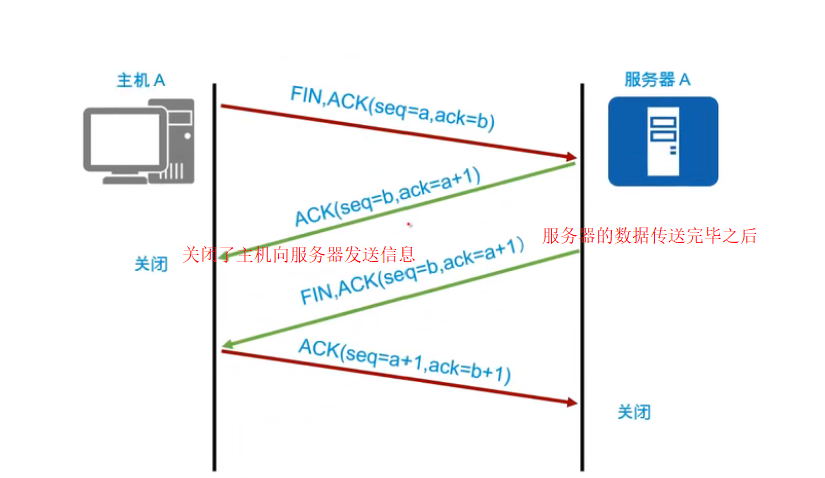
## 5、数据传输的过程



## 6、流量控制



## 7、关闭连接--四次挥手



# 八、UDP协议

## 1、简介

用户数据包协议UDP（User Datagram Protocol），属于面向无连接的传输层协议，传输可靠性没有保证。

## 2、UPD报文

