计算机网络概述

网络安全设备

包括计算机、服务器、集线器（用来将信号整形放大，把所有节点集中到以它为中心的节点上，在物理层）、交换机（比集线器智能，依据MAC地址选择性发送数据，在数据链路层）、路由器（连接不同网络）、（光）调制解调器（用于信号转换）、防火墙（控制数据）、入侵检测/防御系统（IDS/IPS）

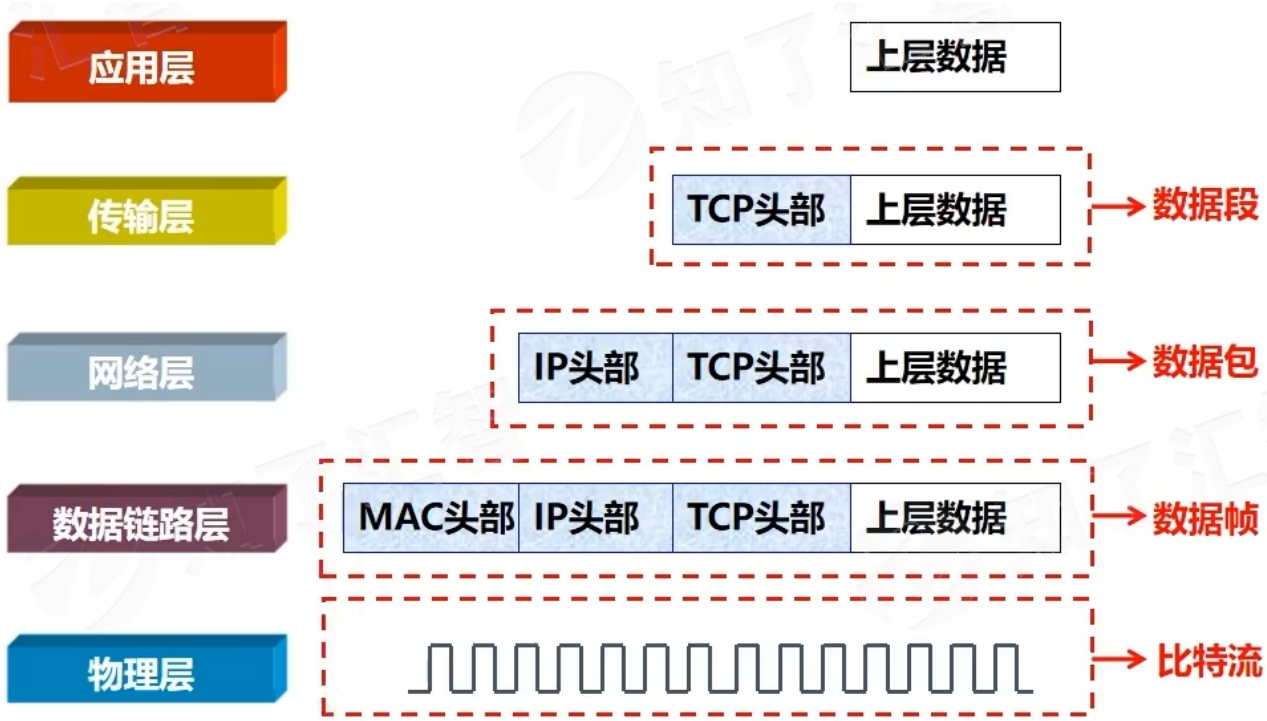
网络参考模型

OSI模型（七层）

- 应用层---为应用程序提供网络服务
- 表示层---数据格式化、加密、解密
- 会话层---建立、维护、管理会话连接
- 传输层---建立、维护、管理端到端连接
- 网络层---IP寻址和路由选择
- 数据链路层---Mac地址寻址
- 物理层---如何利用物理讯号表示0 和1，比特流传输

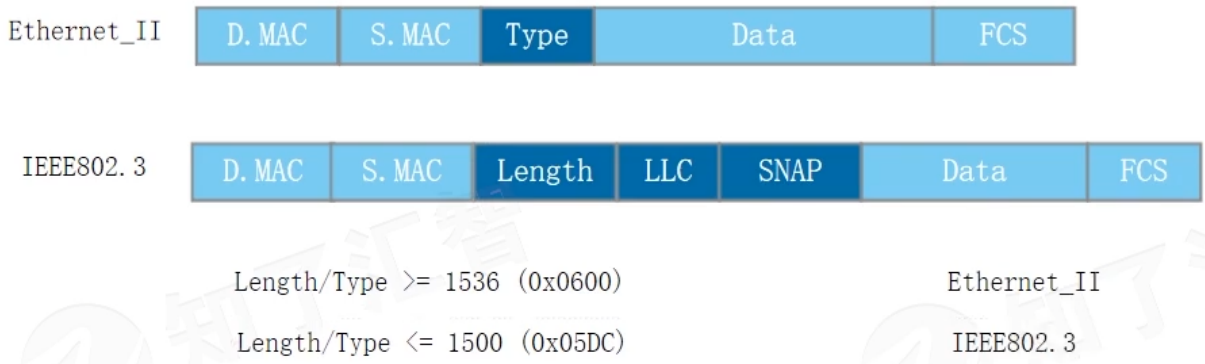
TCP/IP协议簇

- 应用层：HTTP、FTP、TFTP、SMTP、SNMO、DNS
- 传输层TCP、UDP
- 网络层ICMP、IGMP、IP、ARP、RARP
- 数据链路层、物理层：RJ45、PPP、HDLC、IEEE、VLAN



以太网的帧格式

有两种格式：



D.MAC是目标MAC地址，C.MAC是原主机MAC地址.
以太网II的类型值大于1536，IEEE小于1500

计算机的**通信方式**有：

- 广播：d.MAC地址为ff-ff-ff-ff-ff-ff，作用于当前网络范围
- 单播：d.MAC地址的第八位为0，效率最高且最安全
- 组播：d.MAC地址的第八位为1，只有采用相同协议的软件才能收到

网络传输介质

线缆

1. 双绞线
   Cat5(10~100Mbps)、Cat 5e(1000Mbps)、Cat6(1000Mbps)、Cat7(10Gbps)
2. 光纤

单模光纤	多模光纤
用于高速度、长距离	用于低速度、短距离
成本高	成本低
端接较难	端接较易
窄芯线，需要激光源	宽芯线，聚光好，光源可采用激光或发光二极管
一般为黄色	橘黄色、灰色
纤芯为9.0μm，大约在1mm的百分之一	50.0μm、62.0μm
耗散极小，高效	耗散大，低效

接口

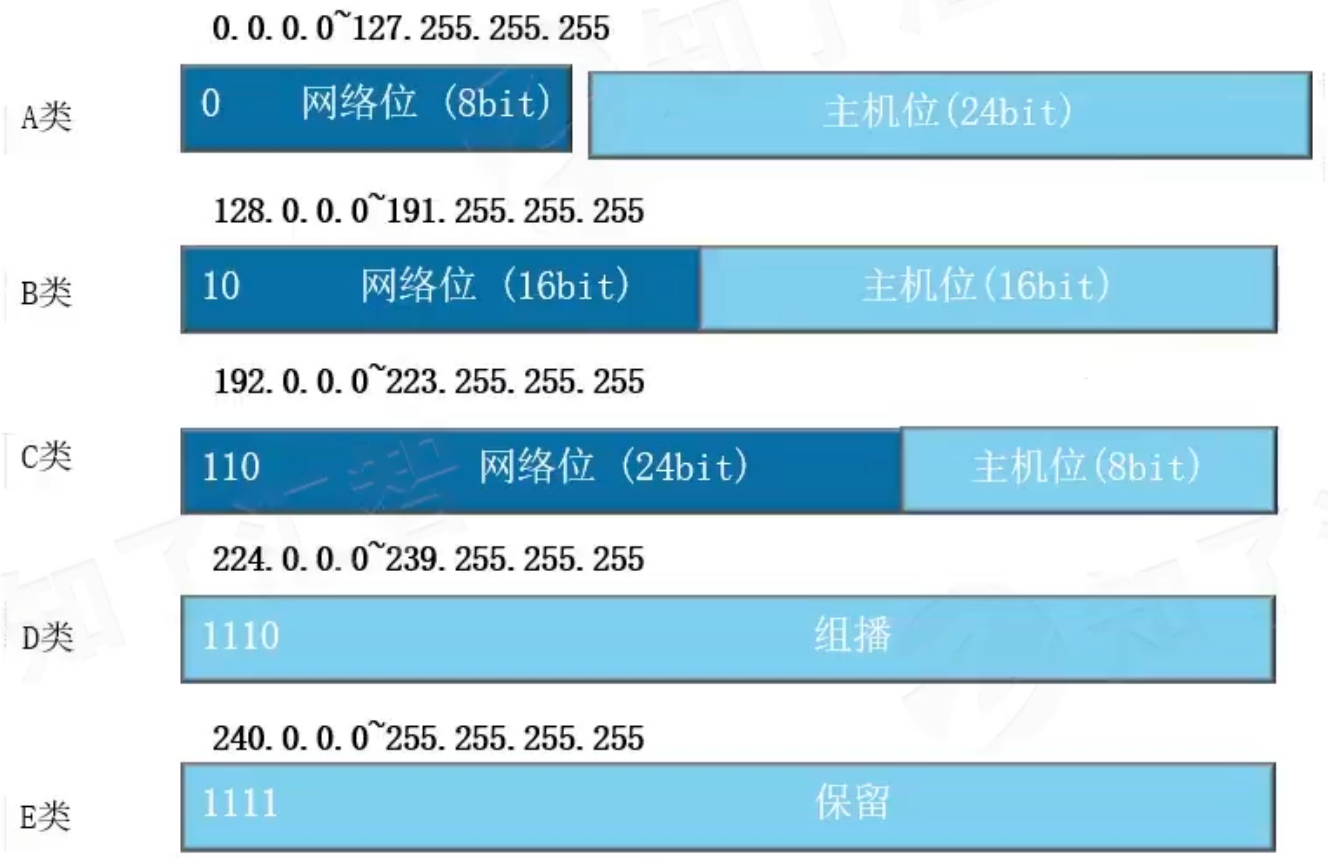
RJ45接口 光纤接口：

- FC 圆形带螺纹
- ST 卡接式圆形
- SC 方形
- LC 窄体方形
- MT-RJ收发一体方形 光模块 信息插座

网络层

IP地址介绍

组成：网络部分和主机部分



- A类：10.X.X.X是私有地址，127.X.X.X是保留地址，用作循环测试用（127.0.0.1，测试本机TCP/IP是否安装正确）
- B类：172.16.0.0~172.31.255.255是私有地址，169.254.X.X是保留地址（如果IP地址是自动获取IP地址，而在网络上没找到可用DHCP服务器，则会得到一个可用的该保留地址），191.255.255.255是广播地址
- C类：192.168.X.X是私有地址

子网掩码：网络位都为1，主机位都为0
DHCP:自动分配IP地址等参数的协议/服务

无类IP

无类IP指的是子网掩码不是标准的8/16/24位的IP。

好处：可以减少IP地址的浪费、满足不同网络对IP地址的需求、实现网络的层次性

实现方式：子网划分

子网划分含义：将一个大的网段分为小的网段（切割网络位）

超网：使用一个子网掩码将多个有类地址聚合成单个网络地址（与划分相反）

windows常用命令

- ipconfig：
  - /all 显示所有
- ping X.X.X.X：
  - -t 一直进行
  - -n 2 指定发送包的数量

- -l 100 指定要发送的字节数
- -S 1.1.1.1 从本地的1.1.1.1为原地址ping

IP数据包格式

- 版本：IPV4/IPV6
- TTL：生成周期
- 标识符、标志、段偏移量：用于标注、划分、排序包中的内容（用于描述包中的数据关系）
- 协议号：指是哪个协议

ARP协议（Address Resolusion Protocal）

作用：将已知IP地址解析成MAC地址
ARP代理：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
免费ARP：用来探测IP地址是否冲突
windows主机ARP相关命令：
arp -a：查看arp缓存表
arp -d：清除arp缓存
arp -s：arp绑定

vrp系统的ARP命令:
dis arp all：查看arp缓存表
reset arp dynamic：清除arp缓存
arp static 192.168.1.100 1111.1111.1111：arp绑定

arp报文通信过程：

```
25 53.110000    HuaweiTe_bc:63:bc    Broadcast            ARP     60 Who has 192.168.1.2? Tell 192.168.1.1
26 53.141000    HuaweiTe_4b:7a:28    HuaweiTe_bc:63:bc    ARP     60 192.168.1.2 is at 54:89:98:4b:7a:28
27 53.156000    192.168.1.1          192.168.1.2          ICMP    74 Echo (ping) request  id=0xc50d, seq=1/256, ttl=128 (reply in 28)
28 53.203000    192.168.1.2          192.168.1.1          ICMP    74 Echo (ping) reply    id=0xc50d, seq=1/256, ttl=128 (request in 27)
```

ICMP协议

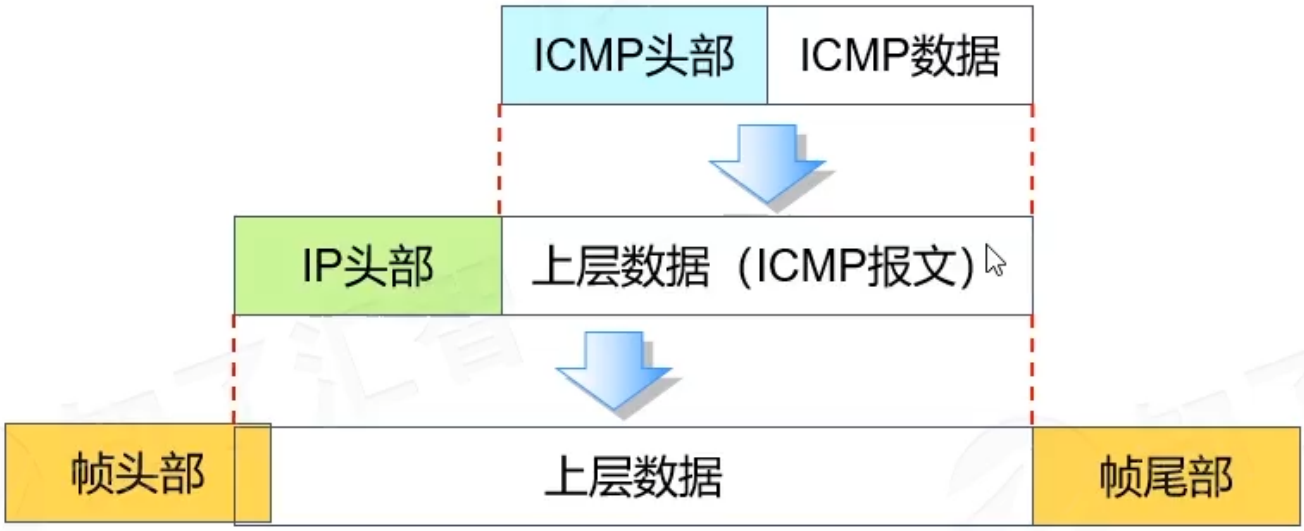
ICMP协议作用：用来确认两个主机是否能够通信
ICMP报文格式：

8位的类型字段标识了该ICMP报文的具体类型，
8位的代码字段进一步指出产生这种类型ICMP报文的原因，
每种类型报文的产生的原因都可能有多个，就拿目的站不可达报文来说，
产生的原因可能有主机不可达、协议不可达、端口不可达等；
16位校验和字段包括整个ICMP报文，即包括ICMP首部和数据区域。
首部中的剩余4个字节在每种类型的报文中有特殊的定义

ICMP主要功能：

- 差错检查：查询和相应某些信息
- 错误报告：ICMP目的不可达（无法访问目标网络）

ICMP协议的封装：



传输层

TCP协议

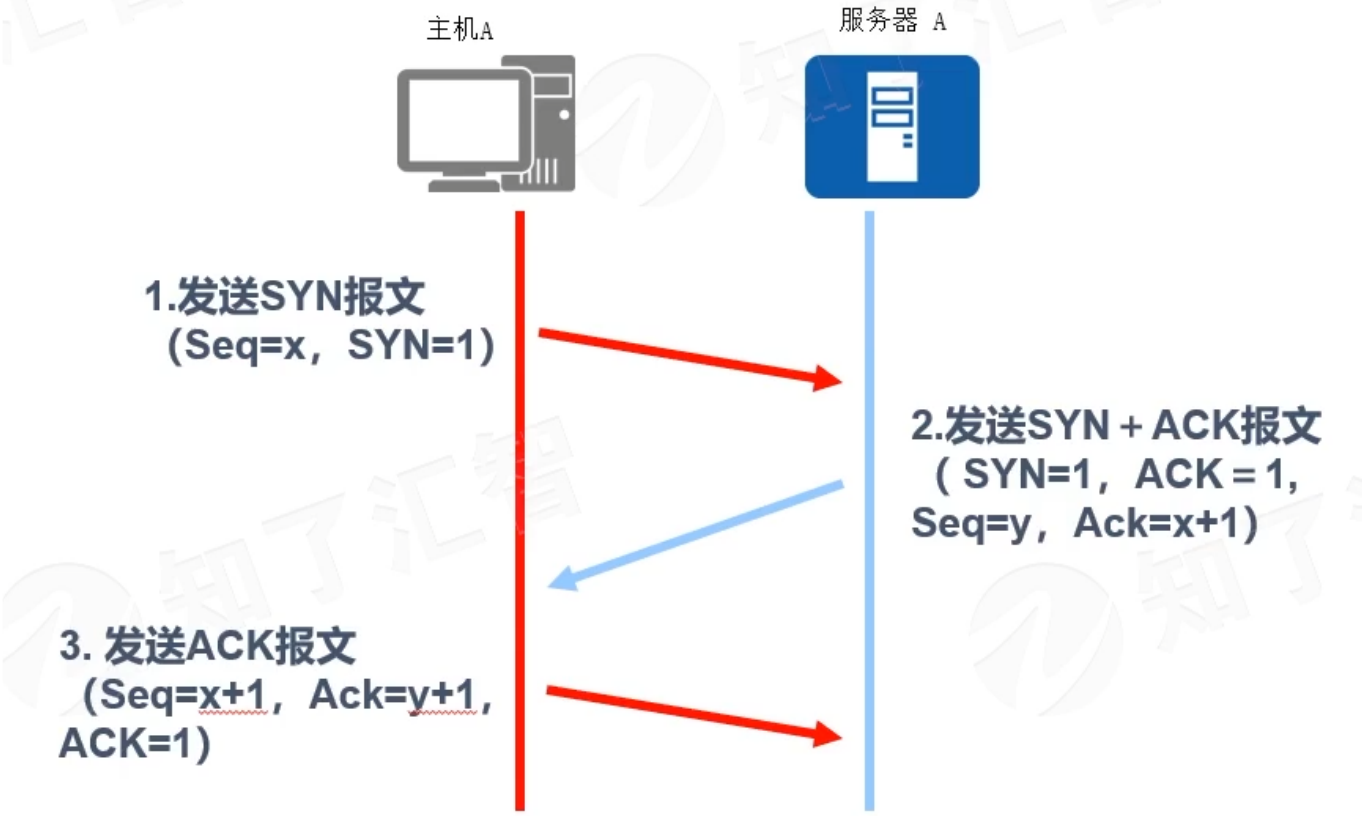
TCP报文段：

<table>
<tr><td colspan="8">源端口号（16）49152-65535</td><td colspan="8">目标端口号（16）0-1023</td></tr>
<tr><td colspan="16">序号（32）</td></tr>
<tr><td colspan="16">确认号（32）</td></tr>
<tr><td colspan="4">首部长度（4）</td><td colspan="2">保留（6）</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td colspan="4">窗口大小（16）</td></tr>
<tr><td colspan="8">校验和（16）</td><td colspan="8">紧急指针（16）</td></tr>
<tr><td colspan="16">选项</td></tr>
</table>

- 端口：传输层与应用层的服务接口
- 序号Seq：发送端为每个字节进行编号，便于接收端正确重组
- 确认号Ack：用于确认发送端的信息
- 首部长度：确定首部数据结构的字节长度
- 保留：目前未被使用，用于今后拓展
- 窗口大小：用来控制本地可接受数据段的数目，此值大小可变化，流量控制机制依靠此属性大小实现
- 紧急比特URB：当URB=1有效，告诉此报文段有紧急数据，尽快发送
- 确认比特ACK：当ACK=1有效，用于确认发送方的数据
- 推送比特PSH：接收到PSH=1的报文则尽快交付给应用程序，而非等到缓存填满再交付
- 复位比特RST：RST=1时表明TCP出现严重差错（如主机崩溃等），必须释放连接，重新建立连接
- 同步比特SYN：SYN=1表明这是一个连接请求或连接接受报文（建立连接）
- 终止比特FIN：FIN=1用于释放一个连接，表明发送端数据发送完毕（终止连接） TCP端口号与常用网络服务关系

协议	端口号
FTP	21、20
HTTP	80
SSH	22
Telnet	23
SMTP	25

TCP的建立连接过程需要进行“三次握手”：




```
12 23.844000    1.1.1.1    1.1.1.2    TCP    58 2049 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
13 23.860000    1.1.1.2    1.1.1.1    TCP    58 80 → 2049 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
14 23.860000    1.1.1.1    1.1.1.2    TCP    54 2049 → 80 [ACK] Seq=1 Ack=1 Win=8192 Len=0
```