协议总览

ARP 地址解析协议（Address Resolution Protocol）：基本功能：知道目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。它是 IPv4 中网络层必不可少的协议，不过在 IPv6 中已不再适用，并被邻居发现协议（NDP）所替代。

ICMP（Internet Control Message Protocol）互联网控制报文协议：通过下发指令来感知和控制网络环境,配合 IP(包括 IPv4 和 IPv6)协议来工作的。
它的主要功能是传输网络诊断信息，信息主要包括两类:

(1)查询类报文 ：主要用于信息的查询和采集，比如采集传输路径上的每个路由器都是谁，本次传输的报文是否达到目的地等等。

(2)错诊断类报文 ：主要用于诊断网络故障，比如传输报文被丢弃的原因是什么等等。

UDP(User Datagram Protocol):无连接，不可靠，面向数据报

TCP(Transmission Control Protocol):能够确保连接的建立和数据包的发送，支持错误重传机制，拥塞控制，流量控制

DNS(Domain Name System)**域名解析系统**:根据域名查出对应的 IP 地址。

HTTP(HypertextTransferProtocol)超文本传输协议：协议以普通文本、超文本、音频、视频等格式传输数据,HTTP 在公认端口 80 上使用 TCP 服务。

FTP(FileTransferProtocol)文件传输协议 :FTP 是基于 TCP 的文件传输协议，用于在两台异构的主机间传输文件，可靠性由 TCP 保障。主要功能是减少或消除不同操作系统下处理文件的不兼容性。有两种类型：匿名、非匿名

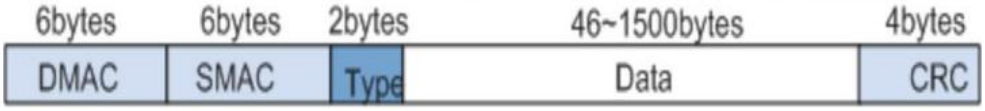
DHCP（DynamicHostConfigurationProtocol ）动态主机配置协议：它提供了一种动态指定 IP 地址和配置参数的机制，用于简化主机 IP 配置管理。

简单邮件传输协议 SMTP(SimpleMailTransferProtocol) ：使用客户服务器模式，负责发送邮件的 SMTP 进程是 SMTP 客户，负责接受邮件的 SMTP 进程是 SMTP 服务器。服务进程端口号：TCP25 号端口

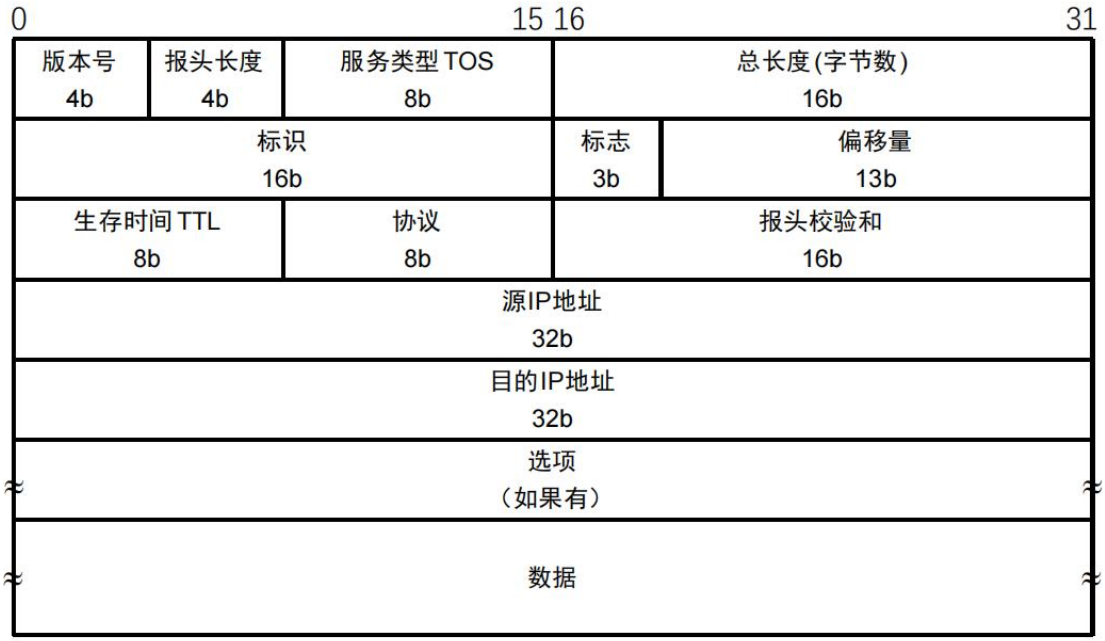
POP(PostOfficeProtocol)接收邮件协议:POP 使用客户服务器模式，接收邮件的计算机运行 POP 客户程序，其 ISP 的邮件服务器中运行 POP 服务程序，服务进程端口号：110（TCP)

以太网帧、IPV4、IPV6 报文

以太网帧格式:



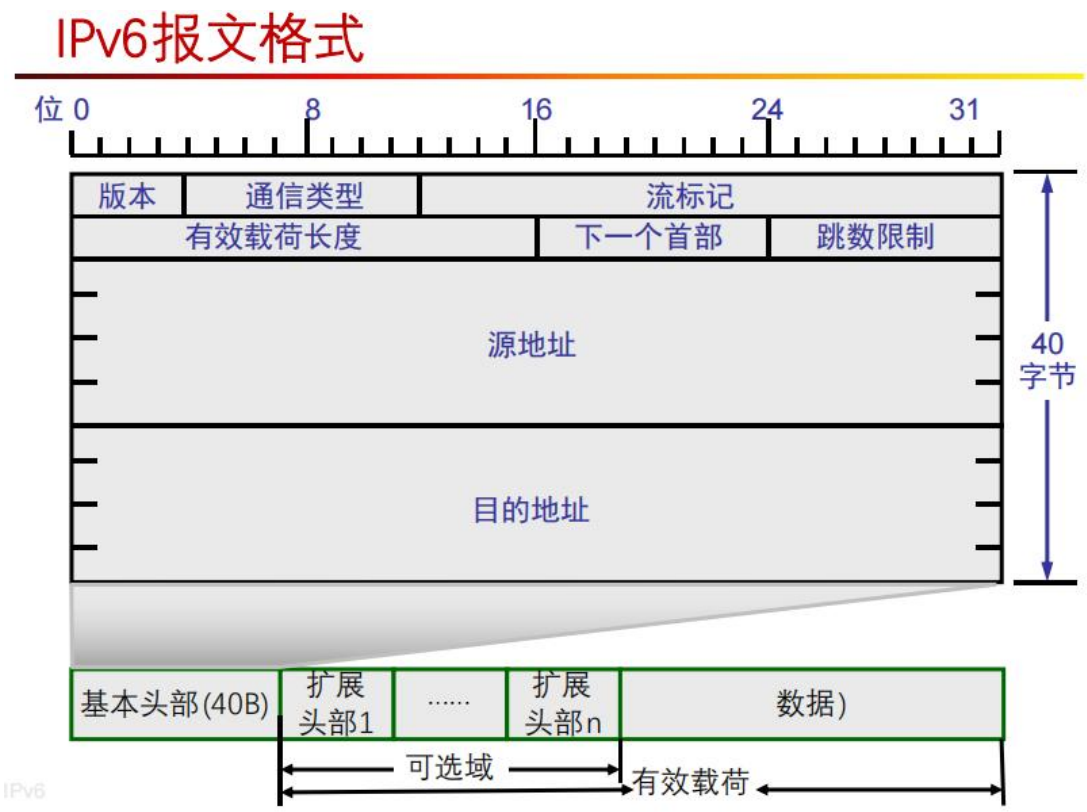
IPv4报文格式



■协议字段 (8)： IP数据报的上层携带的协议。

常用协议字段值

协议名	ICMP	IGMP	TCP	EGP	IGP	UDP	IPv6	OSPF
协议字段值	1	2	6	8	9	17	41	89



IPv6 的 128 位地址是以 16 位为一分组，每 16 位分组写成 4 个十六进制数，中间用冒号分隔，称为冒号分十六进制格式

DNS 循环域名体

反向域 IP地址的反向域名循环体 进行IP反向解析 域名循环体：包括7块
34.0.16.172.in-addr.arpa.（空）7个部分

DNS 查询报文 UDP 包里的目的端口号是 53

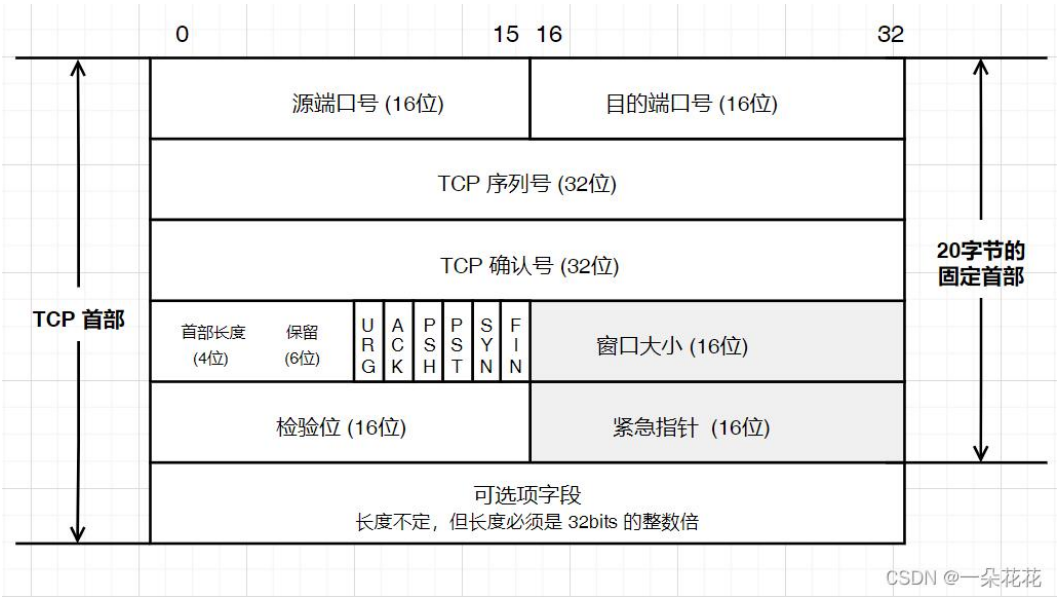
DNS 的应答报文中源端口是 53

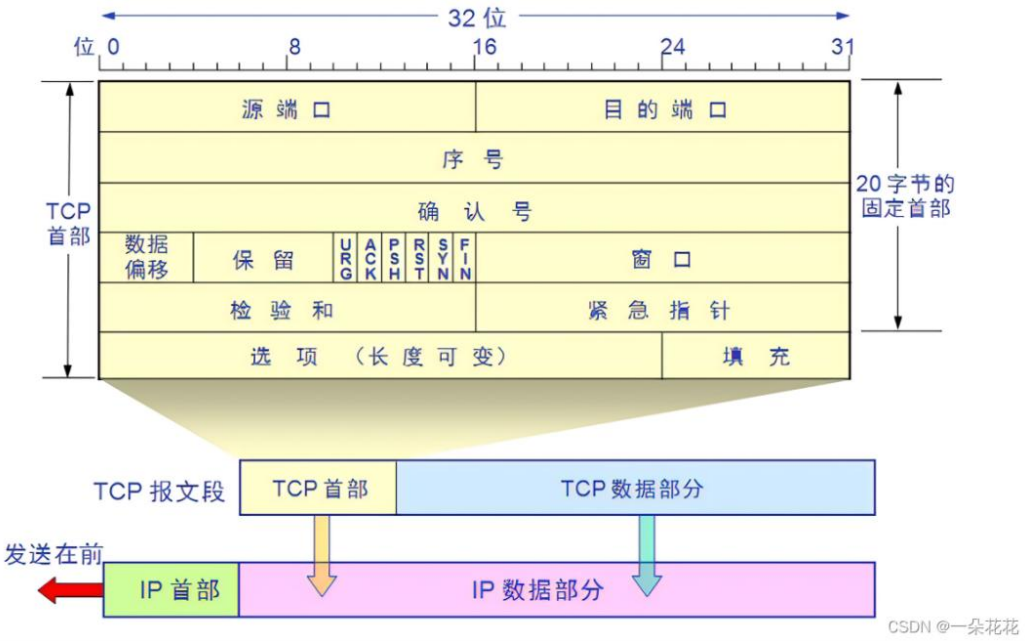
IP 协议报文

IP 报文中包含 ：

（1） 4 位版本号，如果是 IPv4，版本号就是 4。
（2） 4 位首部长度，用于确定报头长度，假如是“1111”，则报头长度为 4x15=60。
（3） 8 位服务类型，其中 4 位 TOS 字段类型：最小延迟，最大吞吐量，最高可靠性，最小成本（4 种只能选其一）。
（4） 16 位总长度，报文长度，结合首部长度获得的报头长度可将报文和报文分离。
（5）16 位标识，如 tcp 中的序号，区分各个报文，确定是那个报文，保证唯一性。
（6） 3 位标志，第一位保留(保留的意思是现在不用, 但是还没想好说不定以后要用到). 第二位置为 1 表示禁止分片, 这时候如果报文长度超过 MTU, IP 模块就会丢弃报文，第三位表示更多分片，1 标识后续还有报文 ，0 标识没有报文，后面没有分片了。
（7）13 位片偏移，是分片相对于原始 IP 报文开始处的偏移. 其实就是在表示当前分片在原报文中处在哪个位置. 实际偏移的字节数是这个值 * 8 得到的. 因此, 除了最后一个报文之外, 其他报文的长度必须是 8 的整数倍(否则报文就不连续了)。
（8） 16 位校验和，校验数据是否有错。
（9） 32 位源地址和目的 IP，确定从哪来到哪去。
（10） 8 位生存时间，经过一个节点生存时间–，减完丢弃。
（11） 8 位协议，上层协议种类。

TCP 协议报文





URG：表示本报文段中发送的数据是否包含紧急数据：URG=1 时表示有紧急数据。当 URG=1 时，后面的紧急指针字段才有效

ACK ：表示前面的确认号字段是否有效：ACK=1 时表示有效；只有当 ACK=1 时，前面的确认号字段才有效；TCP 规定，连接建立后，ACK 必须为 1

PSH：告诉对方收到该报文段后是否立即把数据推送给上层。如果值

为 1，表示应当立即把数据提交给上层，而不是缓存起来

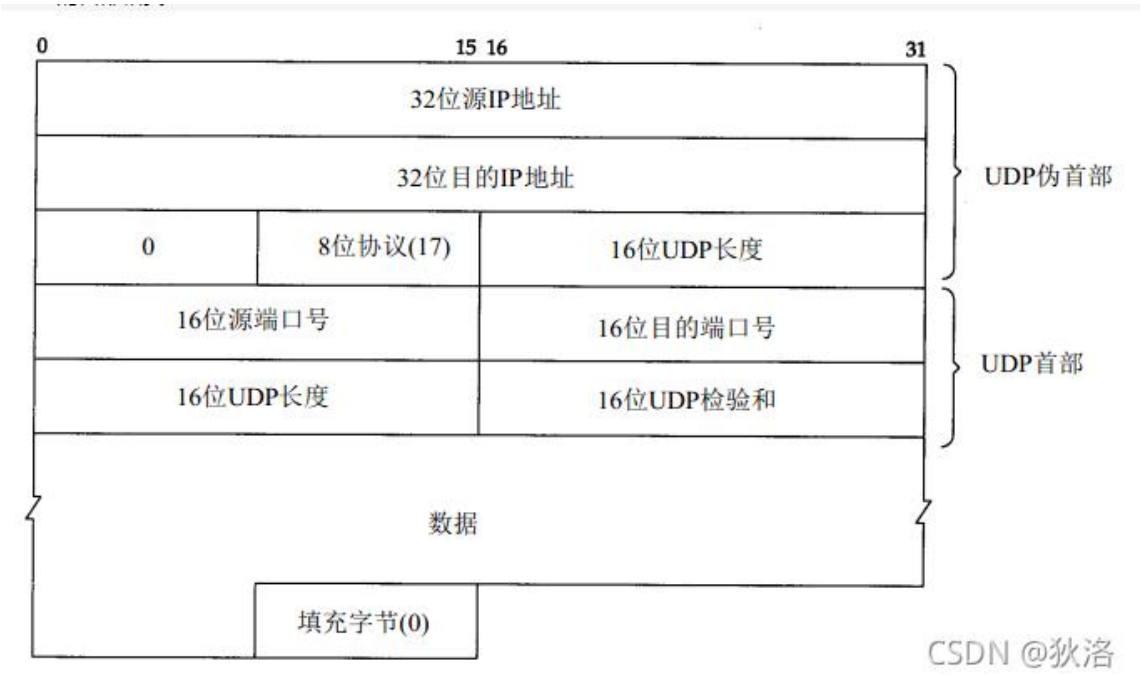
RST：表示是否重置连接：若 RST=1，说明 TCP 连接出现了严重错误（如主机崩溃），必须释放连接，然后再重新建立连接

SYN ：在建立连接时使用，用来同步序号：当 SYN=1，ACK=0 时，表示这是一个请求建立连接的报文段；当 SYN=1，ACK=1 时，表示对方同意建立连接；SYN=1 时，说明这是一个请求建立连接或同意建立连接的报文；只有在前两次握手中 SYN 才为 1

FIIN:标记数据是否发送完毕：若 FIN=1，表示数据已经发送完成，可以释放连接

窗口大小(Window Size)：占 16 位；它表示从 Ack Number 开始还可以接收多少字节的数据量，也表示当前接收端的接收窗口还有多少剩余空间。该字段可以用于 TCP 的流量控制。

UDP 协议报文



伪头部：只是为了提取 IP 数据报中的源 IP，目的 IP 信息并加上协议等字段构造的数据。在实际传输中并不会发送，仅起到校验和计算使用，因此称之为伪首部。

源端口号、目的端口:端口号范围是 0 ~ 65535,0~ 1023 为知名端口号。

UDP 长度：是指整个 UDP 数据报的长度 ， 包括 报头 + 载荷，

UDP 校验和：用于检查数据在传输中是否出错，是否出现 bit 反转的问题，当进行校验时，需要在 UDP 数据报之前增加临时的 伪首部。

协议类型：IP 协议号 0x0800

ARP 协议报文

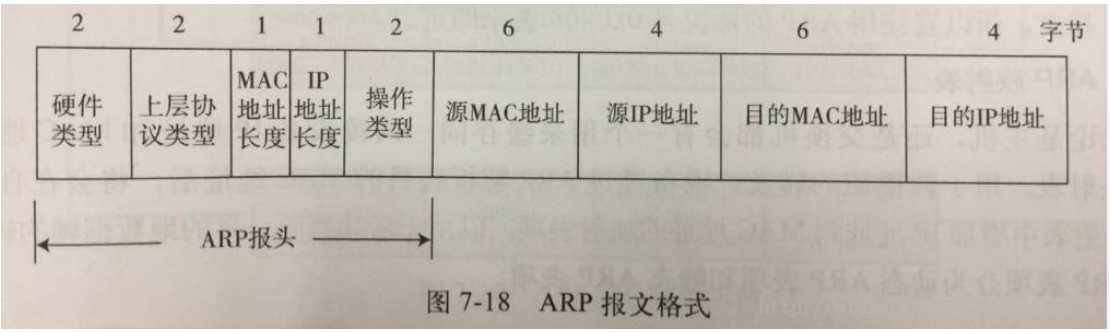


图 7-18 ARP 报文格式

硬件类型：占两字节，表示 ARP 报文可以在哪种类型的网络上传输，值为 1 时表示为以太网地址。

上层协议类型：占两字节，表示硬件地址要映射的协议地址类型，映射 IP 地址时的值为 0x0800。

MAC 地址长度：占一字节，标识 MAC 地址长度，以字节为单位，此处为 6。

IP 协议地址长度：占一字节，标识 IP 得知长度，以字节为单位，此处为 4。

操作类型：占 2 字节，指定本次 ARP 报文类型。1 标识 ARP 请求报文，2 标识 ARP 应答报文。

源 MAC 地址：占 6 字节，标识发送设备的硬件地址。

源 IP 地址：占 4 字节，标识发送方设备的 IP 地址。

目的 MAC 地址：占 6 字节，表示接收方设备的硬件地址，在请求报文中该字段值全为 0，即 00-00-00-00-00-00，表示任意地址，因为现在不知道这个 MAC 地址。

目的 IP 地址：占 4 字节，表示接受方的 IP 地址。

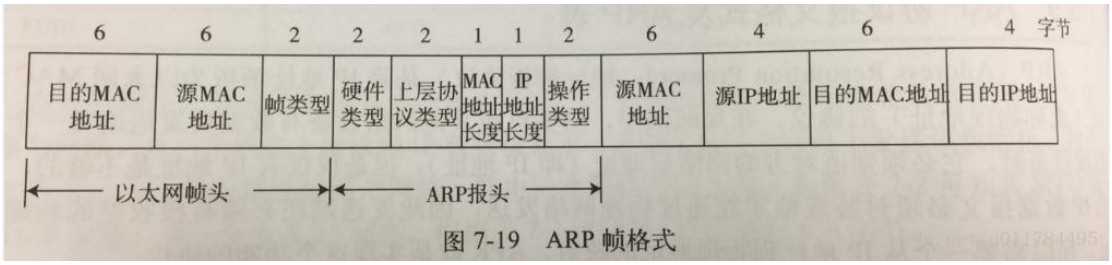


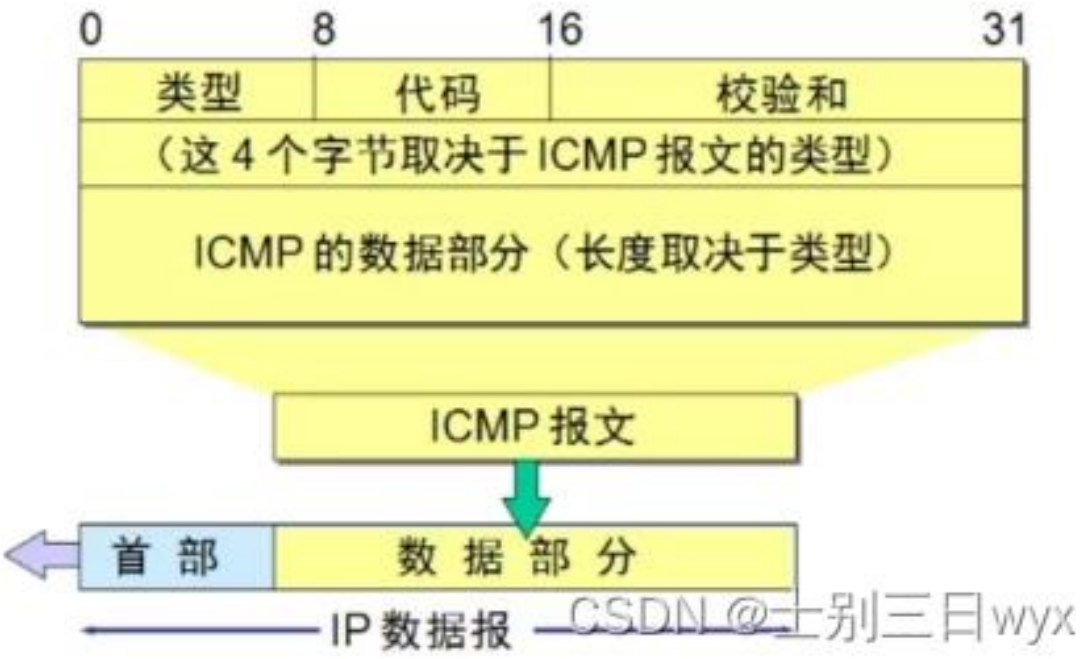
图 7-19 ARP 帧格式

目的 MAC 地址：占 6 字节，如果是 ARP 请求帧，因为它是一个广播帧，所以要填上广播 MAC 地址（FF-FF-FF-FF-FF-FF），其目标主机是网络上的所有主机。

源 MAC 地址：占 6 字节，这是发送 ARP 帧的节点 MAC 地址。

帧类型：占两字节，这里用来标识帧封装的上层协议，因为本帧的数据部分是 ARP 报文，所以直接用 ARP 的协议号 0x0806 表示就可以了。

ICMP 协议报文



ICMP报文的主要类型

类型	代码	描述	查询	差错
0	0	回显应答(Ping应答)	√	
3	0 1 2 3	目的不可达 网络不可达 主机不可达 协议不可达 端口不可达		√ √ √
5	0 1	对网络重定向 对主机重定向		√
8	0	请求回显（Ping请求）	√	
9 10	0 0	路由器通告 路由器请求	√ √	
12	0	坏的IP首部（包括各种差错）		√
13 14	0 0	时间戳请求 时间戳应答	√ √	
17 18	0 0	地址掩码请求 地址掩码应答	√ √	

FTP

- 端口 21 用于控制连接，如用户标识、操作命令
- 端口 20 用于数据连接（在 PORT 模式中）

HTTP

4种主要的HTTP请求类型

- GET：请求一个文档
  - 服务器响应：发送状态信息，紧接着发送该文档的一个副本
- HEAD：请求状态信息
  - 服务器响应：发送状态信息，但不发送文档副本
- POST：发送数据给服务器
  - 服务器将该数据添加到指定的项上
- PUT：发送数据给服务器
  - 服务器用该数据完全替代指定项

DHCP

- DHCP使用UDP协议，**服务器端使用67号端口，客户端使用UDP的68号端口**。
- DHCP支持3种IP地址分配机制：
  - 自动分配—DHCP服务器为DHCP客户分配一个永久IP地址
  - 动态分配—DHCP服务器为DHCP客户分配一个有租赁期的临时IP地址
  - 人工分配—DHCP客户的IP地址有管理员分配好，DHCP只负责传达