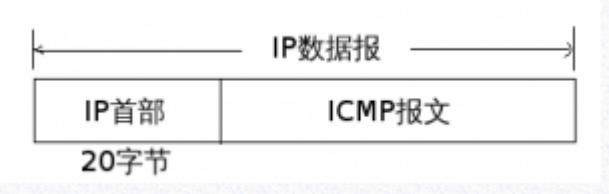
第五讲 网络扫描技术

测试点 5-1

1. 主机扫描技术是利用 ICMP 协议来实现，请查阅相关资料，了解 ICMP 协议的工作原理，并简要说明 Ping 功能的实现原理。

ICMP：Internet 控制报文协议。由于 IP 协议并不是一个可靠的协议，它不保证数据被成功送达，那么，如何才能保证数据的可靠送达呢？ 这里就需要使用到一个重要的协议模块 ICMP(网络控制报文)协议。它传递差错报文以及其他需要注意的信息，经常供 IP 层或更高层协议（TCP 或 UDP）使用。所以它经常被认为是 IP 层的一个组成部分。它在 IP 数据报文中的封装如下：



ICMP 的数据报文格式如下所示。所有报文的前 4 个字节都是一样的，其他的因报文类型不同而不一样。类型字段可以有 15 个不同的值，用以描述不同的 ICMP 报文。校验和字段覆盖整个 ICMP 报文，使用了和 IP 首部检验和一样的算法。

ICMP 协议大致分为两类，一种是查询报文，一种是差错报文。查询报文是用一对请求和应答定义的，它通常有以下几种用途:

ping 查询

子网掩码查询（用于无盘工作站在初始化自身的时候初始化子网掩码）

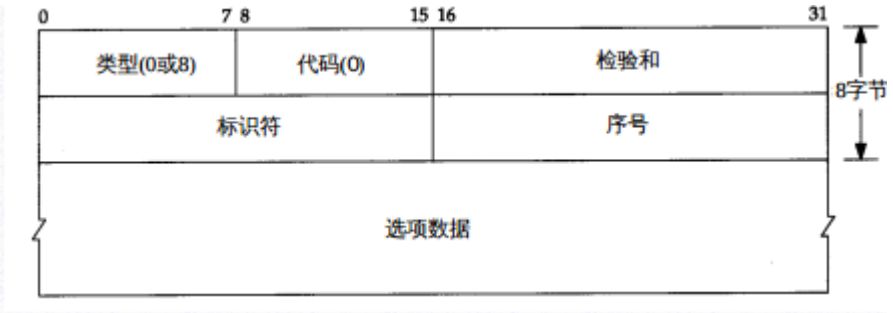
时间戳查询（可以用来同步时间）

而差错报文通常包含了引起错误的 IP 数据报的第一个分片的 IP 首部(和选项)，加上该分片数据部分的前 8 个字节。RFC 792 规范中定义的这 8 个字节中包含了该分组运输层首部的所有分用信息，这样运输层协议就可以向正确的进程提交 ICMP 差错报文。

ping 程序原理分析

ping 程序是由 Mike Muuss 编写，目的是为了测试另一 台主机是否可达，现在已经成为一个常用的网络状态检查工具。该程序发送一份 ICMP 回显请求报文给远程主机，并等待返回 ICMP 回显应答。利用 ping 这种原理，已经出现了许多基于 ping 的网络扫描器，比如 nmap、arping、fping、hping3 等。所以随着 Internet 安全意识的增强，现在有些提供访问控制策略的路由器和防火墙已经可以设置过滤特定 ICMP 报文请求。因此并不能通过简单的 ping 命令判断远程主机是否在线。

ping 使用的是 ICMP 协议，它发送 icmp 回送请求消息给目的主机。ICMP 协议规定：目的主机必须返回 ICMP 回送应答消息给源主机。如果源主机在一定时间内收到应答，则认为主机可达。大多数的 TCP/IP 实现都在内核中直接支持 Ping 服务器，ICMP 回显请求和回显应答报文如下图所示



ping 的原理是用类型码为 0 的 ICMP 发请 求，受到请求的主机则用类型码为 8 的 ICMP 回应。通过计算 ICMP 应答报文数量和与接受与发送报文之间的时间差，判断当前的网络状态。这个往返时间的计算方法是：ping 命令在发送 ICMP 报文时将当前的时间值存储在 ICMP 报文中发出，当应答报文返回时，使用当前时间值减去存放在 ICMP 报文数据中存放发送请求的时间值来计算往返时间。ping 返回接受到的数据报文字节大小、TTL 值以及往返时间。

Unix 系统在实现 ping 程序时是把 ICMP 报文中的标识符字段置成发送进程的 ID 号。这样 即使在同一台主机上同时运行了多个 ping 程序实例，ping 程序也可以识别出返回的信息。

测试点 5-2

1. 思考题：编制一个端口扫描程序，可以实现对指定 IP 或指定 IP 段的主机进行端口扫描。（该思考题为课程实验内容之一，不需要在作业中提交，请查阅资料进行相关的技术准备）