第7讲讲ICMP与ping：投石问路的侦察兵

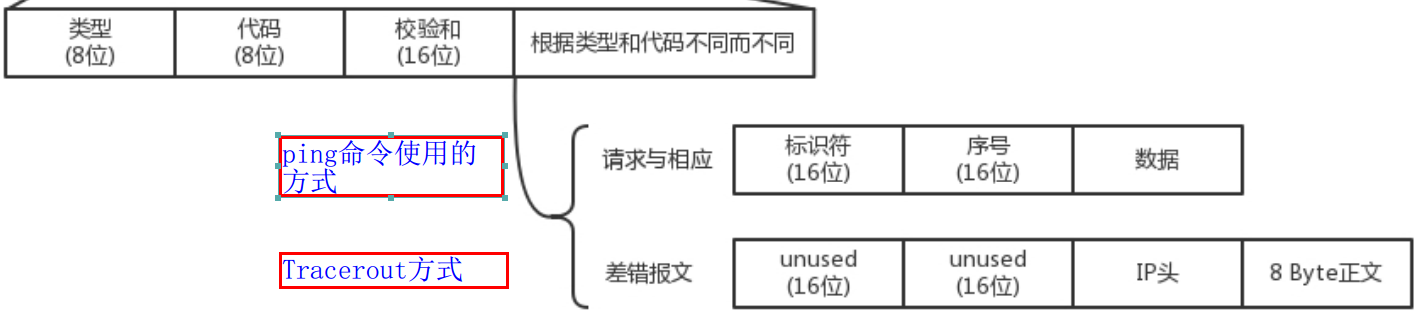
**ICMP**全称**Internet Control Message Protocol**，就是**互联网控制报文协议**。封装在IP包里面。

常用的ping是基于ICMP协议工作的。

IP包格式如下：



ICMP报文：



ICMP报文有很多的类型，**最常用的类型是主动请求为8，主动请求的应答为0**。

查询报文类型

ping就是查询报文，是一种主动请求，并且获得主动应答的ICMP协议。

主动请求： ICMP ECHO REQUEST。

主动请求回复：ICMP ECHO REPLY

标识符：分类别

序号：连续发出的包的序号区分

请求的时间值:用来计算往返时间，说明路程长短

**实战中使用：**

使用ping的时候，应该要清楚地知道一个网络包从源地址到目标地址都需要经过哪些设备，然后逐个ping中间的这些设备或者机器。如果可能的话，在这些关键点，通过tcpdump -i eth0 icmp。查看包有没有到达某个点，回复的包到达了哪个点。

经常会遇到一个问题，如果不在我们的控制范围内，很多中间设备都是禁止ping的，但是ping不通不代表网络不通。这个时候就要使用telnet，通过其他协议来测试网络是否通

差错报文类型

使用ICMP的规则，故意制造一些能够产生错误的场景。

**Traceroute的第一个作用就是故意设置特殊的TTL，来追踪去往目的地时沿途经过的路由器**。

中间的路由器不止一个， 将TTL设置成1，也就是说一旦遇到一个路由器或者一个关卡，就表示它“牺牲”了。于是，返回一个ICMP包，也就是网络差错包，类型是时间超时。

接下来，将TTL设置为2。第一关过了，第二关就“牺牲”了，那我就知道第二关有多远。如此反复，直到到达目的主机。这样， Traceroute 就拿到了所有的路由器IP。

当然，有的路由器压根不会回这个ICMP。

**怎样知道UDP是否到达主机？**

Traceroute 程序会发送一份UDP数据报给目的主机，但它会选择一个不可能的值作为UDP端口号（大于30000）。当该数据报到达时，将使目的主机的 UDP模块产生一份“端口不可达”错误ICMP报文。如果数据报没有到达，则可能是超时。

为什么要设置这样的差错？

因为如果没有差错得不到任何回应的话，无法区别判断半路到底是丢包了还是被主机接受了，只有反馈回差错才会得到相应的消息。

**Traceroute还通过故意设置不分片，从而确定路径的MTU（Maximum Transmission Unit）。**要做的工作首先是发送分组，并设置“不分片”标志。发送的第一个分组的长度正好与出口MTU相等。如果中间遇到窄的关口会被卡住，会发送ICMP网络差错包，类型为“需要进行分片但设置了不分片位”。

**错误报文类型：**

**终点不可达为3，源抑制为4，超时为11，重定向为5**。

**第一种是终点不可达**。小兵：报告主公，您让把粮草送到张将军那里，结果没有送到。

网络不可达代码为0，具体场景是，网络不可达：主公，找不到地方呀？

主机不可达代码为1，具体场景是，主机不可达：主公，找到地方没这个人呀？

协议不可达代码为2，具体场景是，协议不可达：主公，找到地方，找到人，口号没对上，人家天王盖地虎，我说12345！

端口不可达代码为3，具体场景是，端口不可达：主公，找到地方，找到人，对了口号，事儿没对上，我去送粮草，人家说他们在等救兵。

需要进行分片但设置了不分片位代码为4，具体场景是，需要进行分片但设置了不分片位：主公，走到一半，山路狭窄，想换小车，但是您的将令，严禁换小车，就没办法送到了。

**第二种是源站抑制**，也就是让源站放慢发送速度。小兵：报告主公，您粮草送的太多了吃不完。

**第三种是时间超时**，也就是超过网络包的生存时间还是没到。小兵：报告主公，送粮草的人，自己把粮草吃完了，还没找到地方，已经饿死啦。

**第四种是路由重定向**，也就是让下次发给另一个路由器。小兵：报告主公，上次送粮草的人本来只要走一站地铁，非得从五环绕，下次别这样了啊。