Echo requset 回显请求 Echo reply 回显响应 Date \*\*字节 为ping包内容长度

icmp要经过ip协议的封装后，再发送给数据链路层，然后层层封装到数据帧，在通过物理层发送出去

Windows系统默认防火墙不可让其他物理机来ping自己，Linux则没有限制，用wf.msc可打开防火墙设置，已进行配置可ping操作

Windows默认情况下，ping命令会发出四个包，通的话会返回四个包，也就是wireshark的8条记录。而Linux默认情况下，是会一直发出数据包，按Ctrl + C 强制停止。

Linux默认情况下，发出的ping包为64个字节，而Windows默认ping包为32字节。

TTL （Time To Live），意为生存时间，数据包允许被路由转发的最大次数，每转发一次则减1。TTL是在IP头部封装的信息之一。

TTL Linux系统的初始值为64，Windows系统的初始值为128。可通过此项值简单判断对方服务器系统，但初始值可更改，并不绝对准确。

Tracert命令，跃点跟踪，可看出经过了多少次路由转发。TTL值从1开始递增，意为可让中间所经过的每一个路由发送回显相应。Tracert每次会发出三个数据包，\* 号代表数据包丢失。

Tracert在Linux系统中为traceroute命令

ICMP的类型：Type

8：回显请求

0：回显响应（回显应答）

3：目标不可达

4：源抑制

11：超时

源抑制为网络拥塞，路由器无法处理大量报文，因此丢掉，并向源主机发送源抑制控制消息

超时为TTL值已为0，则由路由器向源主机发送超时控制消息