网络检测

一、PING

1. Ping 网络检测原理：利用网络上机器 IP 地址的唯一性，给目标 IP 地址发送一个数据包，再要求对方返回一个同样大小的数据包来确定两台网络机器是否连接相通，时延是多少

2. Ping 工作流程

(1) Ping 同一网段 IP：检测目的 IP 是否与自己处于同一局域网，并通过 ARP 表得出目的 mac 地址，然后发送 ping 的数据包，目的主机收到报文后返回应答报文

(2) Ping 外网 IP：发现 ping 的目的 IP 不在同一网段内，就将数据包发送给路由器（目的 IP 为 ping 的 IP 地址，目的 mac 为路由器 LAN MAC）

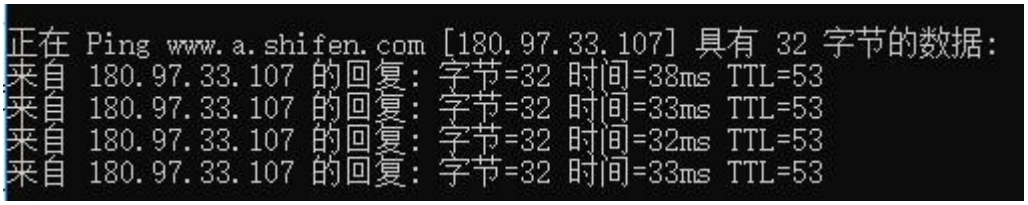
(3) Ping 域名：先解析域名得到 IP 地址，然后向该 IP 地址发送 ping 包

3. Ping 参数解读

(1) 字节：ping 包大小

(2) 时间：报文发出到接收的时间差

(3) TTL：指定数据报被路由器丢弃之前允许通过的网段数量（通常起始值都为 64，128，255 并且跳转数一般小于 30，TTL 的值会因不同的操作系统而变化）



二、Traceroute

1. Traceroute 原理：首先它发送一份 TTL 字段为 1 的 IP 数据包给目的主机，处理这个数据包的第一个路由器将 TTL 值减 1，然后丢弃该数据报，并给源主机发送一个 ICMP 报文（“超时”信息，这个报文包含了路由器的 IP 地址，这样就得到了第一个路由器的地址），然后 traceroute 发送一个 TTL 为 2 的数据报来得到第二个路由器的 IP 地址，继续这个过程，直至这个数据报到达目的主机

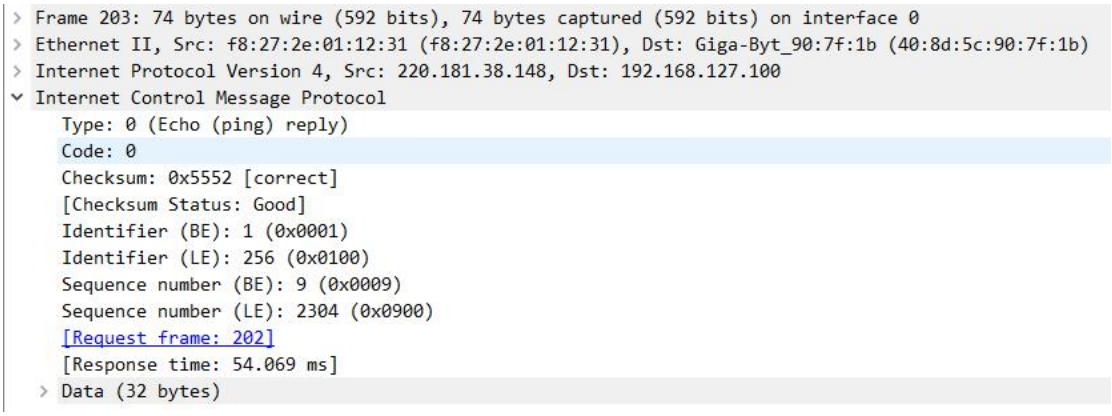
2. Traceroute 路径：根据路由表确定下一跳的网关地址

三、ICMP 报文解析

1. 请求报文

Type 和 code：通过 type 和 code 判断次报文是请求还是回应以及定义错误类型
校验和：判断数据是否没有错误
标志号（码）：可以理解为端口，当路由器收到返回后才知道返给那一台主机
系列标志号（码）：每次发出请求时的值不一样，返回的报文需要和请求的一致

2. 回答报文



Type 和 code：（0 0）代表回答报文

四、Nslookup

1. 原理：通过 DNS 解析域名的 IP，达到检查域名解析是否正常的目的
2. Nslooup 会同时查询域名的 ipv4 和 ipv6 的地址，但是只默认显示 ipv4 的地址

```
DNS         69 Standard query 0x0002 A baidu.com
DNS        101 Standard query response 0x0002 A baidu.com A 123.125.114.144 A 220.181.38.148
DNS         69 Standard query 0x0003 AAAA baidu.com
DNS        112 Standard query response 0x0003 AAAA baidu.com SOA dns.baidu.com
```