第八章Traceroute程序

8.1 Traceroute和IP路径记录选项比较

选择Traceroute而不选择IP路径记录选项的原因：

(1)并不是所有的路由器都支持记录路由选项(traceroute不许要中间路由器具备任何特殊的或可选的功能)

(2)Ping –r 记录下来的IP地址翻了一番(traceroute程序只需要目的端运行一个UDP模块，其他不需要特殊的服务器应用程序)

(3)IP首部中留给选项的空间有限，不能存放大量路径。

8.2 Traceroute程序的操作

(1)Traceroute程序使用ICMP报文和IP首部中的TTL字段(生存周期)。TTL一般为64，老系统为15或32。ICMP中常设置为255。

(2)TTL本质跳站计数器

(3)如果TTL为0或1，则路由器不转发数据报，路由器会丢弃并给源机发送一份ICMP超时信息。

(4)Traceroute给目的主机发送端口大于30000的UDP数据报，使得目的主机产生端口不可达的错误的ICMP报文，Traceroute区分ICMP是端口不可达还是超时就行。

试验一：window下tracert

|  |
| --- |
|  |
| （a）tracert百度域名 |
|  |
| （b）捕捉报 |
|  |
| （c）本机->百度(ping,TTL=1) |
|  |
| （d）途径路由器(第TTL个路由器)->本机(ICMP,类型11,代码0) |

(a-b)tracert [www.baidu.com](http://www.baidu.com)以及数据包

(c)window下tracert是发送ping协议给百度地址(110.242.68.3)，发送三次，但是TTL=1

(d)TTL=1，路由器丢包，向源地址发送ICMP(超时，类型11，代码0)

最后到了110.242.68.3后，110.242.68.3向本机发送ICMP数据报(类型0，代码0)

实验二：centos下

8.3 IP源站选路选项

发送者指定路由，可以采取以下两种形式：

(1)严格的源站路由。发送端指明一个数据经过的IP地址清单，如果一个路由器发现源路由所指定的下一个路由器不在其直连网络，那么他就会返回一个“源站路由失败”的ICMP差错报文。

(2)宽松的源站路由。发送端指明一个数据经过的IP地址清单，但是数据报在清单上指明的任意两个地址之间可以通过其他路由器。



格式如上所示，相比记录路由选项格式基本一致。源站选路必须在发送IP数据报前填充IP地址清单。对于宽松的源站选路来说，code字段的值是0x83；而对于严格的源站选路，其值为0x89。len和ptr字段与之前描述一致。

8.4 IP源站选路的操作机制

发送主机从应用程序接收源站路由清单，将第一个表项去掉(它是数据报的最终目的地址)，将剩余的项移到一个项中，并将原来的目的地址作为清单的最后一项。指针仍然指向清单的第一项。

如果该路由器是最终目的，且指针不大于路径长度，那么(1)由ptr所指定的清单中的下一个地址就是数据报的最终地址；(2)由外出接口相对应的IP地址取代刚才使用的源地址；(3)指针加4。

新的源站路由将取代旧的源站路由。