TTL是 Time To Live的缩写。简单的说就是“生存时间”的意思。是指定TTL值在对方的系统里所停留的时间，单位为“毫秒”。

IP规范规定：

TTL应该被设置为60 (尽管ping 信息包的TTL是255)。这样做主要是为了让一个信息包不要永远在网络中存在。但该信息对我们来说有特殊的含义。我们可以使用TTL大致确定该信息包经过了多少个路由器过渡段。

用255减去N，N是返回的回送答复的TTL。如果TTL值在连续几个ping中发生变化，这说明返回的信息包经过了不同的路由器。

TTL每经过一个ip子层就减少1，那么，相关TTL值对应的操作系统其实是有一定联系的，整理了如下：

ICMP 回显应答的 TTL 字段值为 64

- LINUX Kernel 2.2.x & 2.4.x

ICMP 回显应答的 TTL 字段值为 255

- FreeBSD 4.1, 4.0, 3.4
- Sun Solaris 2.5.1, 2.6, 2.7, 2.8
- OpenBSD 2.6, 2.7,
- NetBSD
- HP UX 10.20

ICMP 回显应答的 TTL 字段值为 32

- Windows 95/98/98SE
- Windows ME

ICMP 回显应答的 TTL 字段值为 128

- Windows NT4 WRKS
- Windows NT4 Server
- Windows 2000

总结：

UNIX 及类 UNIX 操作系统 ICMP 回显应答的 TTL 字段值为 255

Compaq Tru64 5.0 ICMP 回显应答的 TTL 字段值为 64

微软 Windows NT/2K操作系统 ICMP 回显应答的 TTL 字段值为 128

微软 Windows 95 操作系统 ICMP 回显应答的 TTL 字段值为 32

当然，可能存在有些情况下有所特殊。

这样，我们就可以通过TTL辅助这种方法来辨别操作系统，当然，了解一下就行，你完全也可以使用类似nmap类的刺探工具。