

C 实现ping

Subtitle

2022/10/05

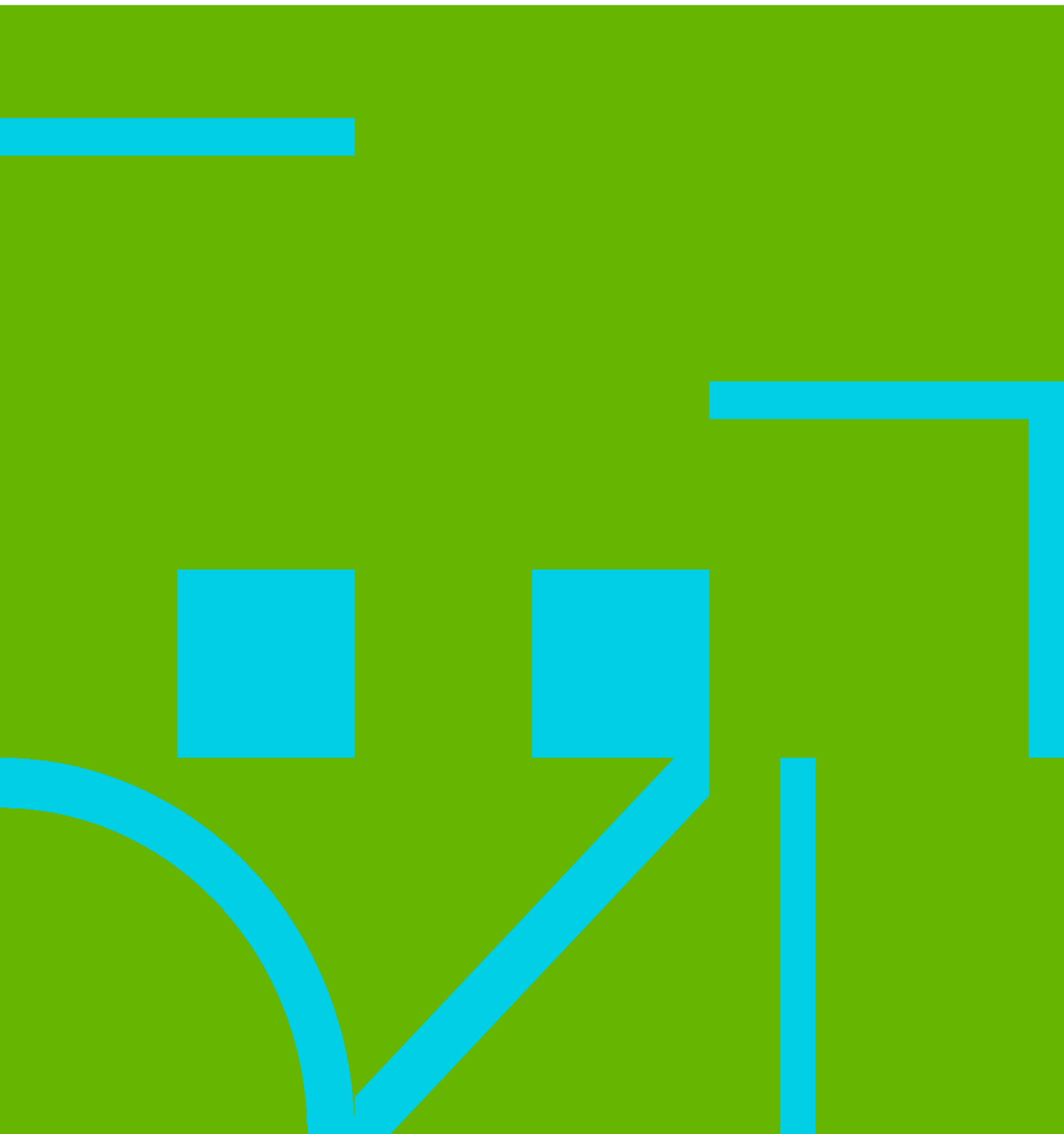


Table of Contents


C++实现ping 1

ping的工作原理 1

参考资料 2

C++实现ping

ping的工作原理

在windows下执行  ping 命令：

```
$ ping baidu.com
```

正在 Ping baidu.com [220.181.111.85] 具有 32 字节的数据:

来自 220.181.111.85 的回复: 字节=32 时间=30ms TTL=53

来自 220.181.111.85 的回复: 字节=32 时间=29ms TTL=53

来自 220.181.111.85 的回复: 字节=32 时间=29ms TTL=53

来自 220.181.111.85 的回复: 字节=32 时间=30ms TTL=53

220.181.111.85 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),

往返行程的估计时间(以毫秒为单位):

最短 = 29ms, 最长 = 30ms, 平均 = 29ms

TTL的含义 首先、TTL 是 echo 包在网络上的生存时间

当我们对网络上的主机进行ping操作的时候、我们本地机器会发出一个数据包

数据包经过一定数量的路由器传送到目的主机，但是由于很多的原因，一些数据包不能正常传送到目的主机

那如果不给这些数据包一个生存时间的话，这些数据包会一直在网络上传送，导致网络开销的增大

当数据包传送到一个路由器之后，TTL就自动减1，如果减到0了还是没有传送到目的主机，那么就自动丢失

其次、TTL 字段值可以帮助我们识别操作系统类型

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

WINXP-32bit 回显应答的 TTL 字段值为 64

微软 Windows NT/2K/2003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，返回的TTL值是相同的

但有些情况下有所特殊：

LINUX Kernel 2.2.x & 2.4.x ICMP 回显应答的 TTL 字段值为 64

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 255

Windows 95/98/98SE

Windows ME

ICMP 回显应答的 TTL 字段值为 32

Windows NT4 WRKS

Windows NT4 Server

Windows 2000

Windows XP

ICMP 回显应答的 TTL 字段值为 128

这样，我们就可以通过这种方法来辨别操作系统

TTL值的注册表位置HKEYLOCALMACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
其中有个DefaultTTL的DWORD值，其数据就是默认的TTL值了，我们可以修改，但不能大于十进制的255

参考资料

<http://blog.csdn.net/yum2006/article/details/7721694>

<http://blog.csdn.net/zhuhuihy/article/details/6788881>

http://blog.csdn.net/yaopeng_2005/article/details/7062927

<http://blog.csdn.net/jaylong35/article/details/6165306>

Printed on: 2022/10/05 21:46

Convert to img Failed!