基于跟踪的路由信息系统的开发和应用

The Development & Application Of Routine Information System Based On Tracing

杨宗长 徐继生（武汉大学电信学院 430072）

摘要：在很多实际应用问题中，常常需要了解网络的路由信息情况。文中较详细地介绍了如何使用 IP/ICMP 协议及套接字通过路由跟踪实现的路由信息系统。并给出了必要的 VC++6.0 的程序代码。

关键词：路由信息 IP/ICMP 套接字 Visual C++6.0

路由就是指通过相互连接的网络把信息从源地点移动到目标地点的活动。而路由器则是进行这种活动所必不可少的网络设备。一般通过路由器连接不同的网络。路由器工作在网络层，主要工作就是为经过路由器的每个数据帧寻找一条最佳传输路径。在很多实际应用中，比如多播通信和路由问题决策中，路由信息显得尤为珍贵。

1 IP 及 ICMP 协议

1.1 IP 协议

IP (Internet Protocol 网际互联协议)是一种具有不可靠、无连接交付机制的协议，是 TCP/IP 互联网设计中最基本的部分。IP 数据报分为首部和数据区，首部分为固定部分和可变部分。IPv4 表示 IP 协议的 4.0 版本，以下的讨论中 IP 将指 IPv4。

表 1 IP 数据报

首部	数据区

表 2 IP 报文首部格式

32

0	4	8	16	31
版本	首部长度	服务类型	总长度	
标识			标志	片偏移量
寿命		协议	首部校验和	
源站 IP 地址				
目的站 IP 地址				
长度可变的任选字段				填充
数据……				

如表 2 所示，IP 数据报的首部包含了 IP 的版本、首部长度、服务类型、协议、源地址和目的地址以及一些其他首部信息，而数据区则存放了要发送的具体内容。

1.2 ICMP 协议

ICMP(Internet Control Message Protocol)是为了让互联网中的路由器报告错误或提供有关意外情况的信息而设计的一个特殊报文机制。它是 IP 协议的附属协议，是封装在 IP 数据报内部传送的。

表 3 ICMP 封装在 IP 数据报内部

IP 首部	IP 数据区(ICMP 报文)

表 4 ICMP 报文格式

ICMP 类型(8 位)	ICMP 代码(8 位)	ICMP 校验和(16 位)
ICMP 报文具体内容(不同类型不同代码有不同内容)		

尽管每个 ICMP 报文都有自己的格式，但它们开始的三个字段都是一样的：一个 8 位的报文类型(type)用来标识报文，一个 8 位的代码(code)用来提供有关类型的进一步信息，一个 16 位的校验和(checksum)。(ICMP 采用和 IP 相同的校验和算法，但 ICMP 校验和只覆盖 ICMP 报文)；这里我们给出 ICMP 报文首部的数据结构：

1.2.1 ICMP 首部数据结构

```
struct ICMPHEADER
{ BYTE i_type; //类型
  BYTE i_code; //代码
  USHORT i_cksum; //首部校验和
  USHORT i_id; //标识
  USHORT i_seq; //序列号
  ULONG timestamp; //时间戳(选用)
};
```

1.2.2 常用的 ICMP 报文格式

下面只介绍回显请求和应答 ICMP 报文格式

回显请求和应答报文格式:通常用来判断目的主机是否可以通过网络访问到;本地机向目的主机发送 ECHO 请求的 ICMP 报文,当数据报到达目的主机以后,目的主机会发回一个 ECHO 回应。

表 5　回应、请求和应答报文格式

类型(8 或 0)	代码(0)	校验和
标识符		序号
可选项		

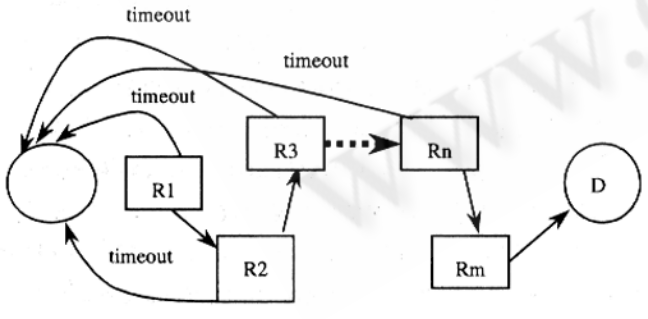
2　路由器跟踪系统的实现

2.1　路由器跟踪的原理

记录数据报所经过的路由器可以有很多办法。可以通过设置 IP 数据报首部的记录路由器选项来记录数据报发送过程中所经过的路由器,常用的方法如下。

IP 数据首部中有一项为寿命(TTL time to live),它规定了数据报在网络中"存活"的时间。每当数据报经过一个节点的时候,寿命就减 1,当寿命为 0 的时候该报文就被丢弃。同时向源主机发送一个超时的 ICMP 报文。这是为了防止迷失的报文在网络上"游荡"而设计的。我们可以通过向目的主机发送 TTL 寿命递增的 ICMP 报文,让沿途的路由器顺次的发回超时报文,收集这些报文并且提取了地址以后就可以知道报文发送途中所经过的路由器的地址。

这样通过向目的主机发送寿命递增的 ECHO 请求的 ICMP 报文,当数据报到达目的主机以后,目的主机会发回一个 ECHO 回应,这时跟踪就完成了。



S——源端主机　D——目的主机　Rn——途径的第 n 个路由器

图 1　实现原理示意图

2.2　网络应用程序接口:套接字

原始套接字(Raw Socket)可以让我们对底层的传输协议加以控制。我们可以用 socket()或 WSASocket()来创建。在创建原始套接字的时候可以选用 ICMP 协议、UDP 协议、IGMP 协议、IP 或原始 IP。它们的标志分别是 IPPROTO_ICMP、IPPROTO_UDP、IPPROTO_IGMP、IPPROTO_IP 和 IPPROTO_RAW。这里给出 ICMP 协议的原始套接字的创建例子:

```
//原始套接字的创建
SOCKET s=WSASocket(AF_INET,SOCK_RAW,IPPROTO_ICMP,NULL,0,
    WSA_FLAG_OVERLAPPED);
//或者 s=socket(AF_INET,SOCK_RAW,IPROTO_ICMP);
if(s==INVALID_SOCKET){//创建失败}
```

需要注意的是由于原始套接字可以对底层的协议加以控制,所以在 Windows NT/2000 中必须以管理员身份(Administrator)或者拥有同等权限的用户身份登陆才可以创建原始套接字。

2.3　路由信息的生成

2.3.1　树控制(CTree Control)

树控制用于显示具有一定层次结构的数据项。很多应用程序都使用该控件,例如资源管理器中的磁盘目录等。树控制中有根数据项(root item),根数据项下包含各个子数据项(child item)。根数据项是所有子数据项的父亲,而这些子数据项是根数据项的孩子。所有子数据项互为兄妹(sibling)关系。每个数据项包括数据项名称(文本字符串)和用于表示该数据项的图像,每个数据项下还可以包含子项,整个结构就象一棵树,使得整个视图清晰,结构明了。

2.3.2　树的遍历算法(略)

2.3.3　树结构视图的生成算法(略)

3　系统界面及演示

下面的例子,就是通过路由跟踪建立一个树状结构的路由信息图如图 2。

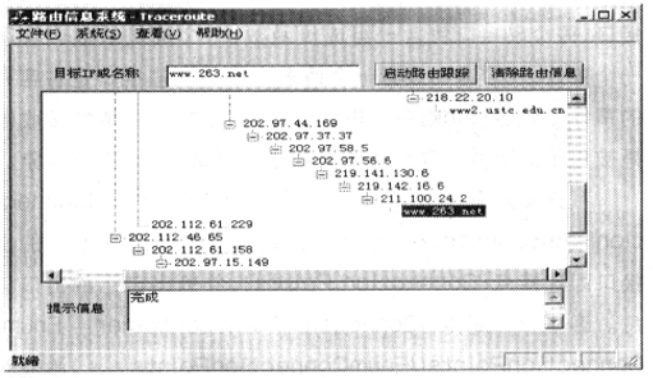


图 2　系统界面及演示

它们分别为:www.whu.edu.cn、www.236.net、www.163.net、www2.Ustc.edu.cn　(下转第 62 页)

(上接第 43 页)

当然跟踪的站点或主机越多,路由信息也就越完善。

参考文献

1 《计算机网络》,谢希仁编著,电子工业出版社,1994。

2 Microsoft Windows 网络编程(第二版),[美]Anthony Jones, Jim Ohlund 编著,杨合庆译,清华大学出版社,2002 年 10 月。

3 Visual C++ 开发指南 [美] Nabajgoti Barkakati ,电子工业出版社,2002 年 1 月。