基于 ICMP 协议的 Ping 主机探测①

Probing of Host IP by Ping Class Based on ICMP Protocol

杜树杰　(中国海洋大学 计算中心 山东 青岛 266003)

摘　要： 给出了使用基于 ICMP 协议的远程主机探测方法，通过对 ICMP 回响报文的格式分析，定义了相应的数据类型。并通过 Ping 类的设计，实现了采用预测补偿技术开发测试控制算法来实时测量远程主机的响应延迟的方法。

关键词： ICMP Ping 主机 IP 探测

1　引言

CMP 协议同 IP 协议一样工作在 ISO 模型的网络层，它的全称是 Internet Control Message Protocal. 其在网络中的主要作用是主机探测、路由维护、路由选择和流量控制。

对于主机探测来说有很多方法，例如某些论坛服务器中的 BANNER，以及像 NetStumbler、NMAP 这样的网络扫描与嗅觉探测专用工具。在 WEB 上也有 www.netcraft.com 等专业网站来估测主机。它们所基于的原理都是使用 ICMP 协议来探测主机，以下主要通过对 ICMP 数据报文的响应来分析 ICMP 协议的执行过程，并通过构建 ICMP 报文的数据结构实现主机地址探测。

2　主机探测用到的ICMP报文

在基于 IP 数据报的网络体系中，网关必须自己处理数据报的传输工作，而 IP 协议自身没有内在机制来获取差错信息并处理。为了处理这些错误，TCP/IP 设计了 ICMP 协议，当某个网关发现传输错误时，立即向信源主机发送 ICMP 报文，报告出错信息，让信源主机采取相应处理措施，它是一种差错和控制报文协议，不仅用于传输差错报文，还传输控制报文。

ICMP 报文包含在 IP 数据报中，属于 IP 的一个用户，IP 头部就在 ICMP 报文的前面，所以一个 ICMP 报文包括 IP 头部、ICMP 头部和 ICMP 报文。IP 头部的 Protocol 值为 1 就说明这是一个 ICMP 报文，ICMP 头部中的类型域用于说明 ICMP 报文的作用及格式，此外还有一个代码域用于详细说明某种 ICMP 报文的类型，所有数据都在 ICMP 头部后面。其数据类型定义如下：

```
Public Type ICMP_OPTIONS
Ttl             As Byte
Tos             As Byte
Flags           As Byte
OptionsSize     As Byte
OptionsData     As Long
End Type
```

RFC 定义了 13 种 ICMP 报文格式，下面是三种常见的 ICMP 报文格式。

2.1 回送或回送响应

在主机没有被配置为过滤 ICMP 形式的情况下，使用 ICMP ECHO 数据包来探测主机地址是否存活。通过简单的发送一个 ICMP ECHO-REQUEST(Type 8)数据包到目标主机，如果接收到 ICMP ECHO-REPLY (ICMP Type 0)数据包，说明主机是存活状态。如果没有就认为主机没有在线或者使用了某些过滤设备过滤了 ICMP 的 REPLY[1]。这种机制就是 Ping 命令来检测目标主机的实现过程。若要形成一个回送响应消息，应该将源和目的地址交换，将类型代码更改为 0，并重新计算机校验码。下面是这个报文的格式：

① 收稿时间:2009-03-23

表 1　ICMP 回送请求和应答报文头部格式

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31		
IP 头部（20 字节）		
类型（0、8）	代码（0）	校验码
标识符		序列号
选项（若有）		

其中，类型 8 代表回送消息 ECHO-REQUEST；0 代表回送响应消息 ECHO-REPLY。代码段回送请求并应答报文。校验码是 16 位数据(从 ICMP 类型开始)的反码和再取反而得。为计算校验码，校验码域应该为零。这些零在以后会被校验码取代。对于标识符部分，如果代码为 0，帮助匹配回送和回送响应的代码可以为 0。序列码字节，如果代码为 0，帮助匹配回送和回送响应的序列码可以为 0。

回送消息中接收到的消息应该在回送响应消息中返回。标识符和序列码由回送发送者使用帮助匹配回送请求的响应。代码段从主机或网关接收 0。

2.2 超时报文

表 2　ICMP 超时报文头部格式

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31		
IP 头部（20 字节）		
类型（11）	代码（0、1）	校验码
未定义（全 0）		
IP 头部（包括选项）+原始 IP 数据报中数据的前 8 字节		

ICMP 超时报文返回类型是 11。返回代码为 0 = 传送超时，为 1 = 分段级装超时。Internet 包头 64 位源数据报数据是由 Internet 包头加上源数据的头 64 位而得。此数据用于主机匹配信息到相应的进程。如果高层协议使用端口号，应该假设其在源数据的头 64 个字节之中。

如果网关在处理数据报时发现生存周期域为零，此数据报必须抛弃。网关同时必须通过超时信息通知源主机。如果主机在组装分段的数据报时因为丢失段未能在规定时间内组装数据，此数据报必须抛弃。网关发送超时信息。代码 0 由网关发送，代码 1 由主机发送。

2.3 目标主机不可达报文

表 3　ICMP 目标不可达报文头部格式

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31		
IP 头部（20 字节）		
类型（3）	代码	校验码
未定义（全 0）		
IP 头部（包括选项）+原始 IP 数据报中数据的前 8 字节		

该种情况报文返回类型是 3。对于代码段，返回值代表以下情况：

- 0 = 网络不可达；
- 1 = 主机不可达；
- 2 = 协议不可用；
- 3 = 端口不可达；
- 4 = 需要段和 DF 设置；
- 5 = 源路由失败；

Internet 包头源数据报是由 Internet 包头加上源数据的头 64 位而得。此数据用于主机匹配信息到相应的进程。如果高层协议使用端口号，应该假设其在源数据的头 64 个字节之中。相应于网关的路由表，如果在目的域中指定的网络不可达，如网络距离为无限远，网关会向发送源数据的主机发送目的不可达消息。而且，在一些网络中，网关有能力决定目的主机是否可达。如果目的地不可达，它将向发送源数据的主机发送不可达信息。在目的主机，如果 IP 模块因为指定的协议模块和进程端口不可用而不能提交数据报，目的主机将向发送源数据的主机发送不可达信息。另外一种情况是当数据报必须被分段传送，而“不可分段”位被置 1，在这种情况下，网关必须抛弃此数据报，并向发送源数据的主机发送不可达信息[2]。

基于上述几种报文格式，可以将 ICMP 报文回送响应的数据定义如下：

```
Public Type ICMP_ECHO_REPLY
    Address          As Long
    status           As Long
    RoundTripTime    As Long
    DataSize         As Integer
    Reserved         As Integer
    DataPointer      As Long
    Options          As ICMP_OPTIONS
    Data             As String * 250
End Type
```

3 基于ICMP的Ping类结构

在 Windows 平台编程中，我们通过调用 ICMP.DLL，使用 Raw Winsock 库函数，对 IP 数据包进行分析，测试网络延迟及丢包率的情况，以实现主机通路状态的探测，下面是核心 Ping 类方法的主要框架及说明。

```
Public Function Ping(szAddress As String, ECHO As ICMP_ECHO_REPLY) As Long
    Dim hPort As Long
    Dim dwAddress As Long
    Dim sDataToSend As String
    Dim iOpt As Long
    sDataToSend = "Echo This"
    dwAddress=AddressStringToLong(szAddress)
    Call SocketsInitialize
    hPort = IcmpCreateFile()
    If IcmpSendEcho (hPort, dwAddress, sDataToSend, Len(sDataToSend), 0, ECHO, Len(ECHO), PING_TIMEOUT) Then
        'ping 成功，status 为 0;
        '.Echo.RoundTrip 保留 Ping 的时间
        Ping = ECHO.RoundTripTime
    Else
        Ping = ECHO.status * -1
    End If
    Call IcmpCloseHandle(hPort)
    Call SocketsCleanup
End Function
```

通过 Ping 类的实现，可以获取远程主机的即时响应速度，然后在远程对象的控制命令中加入对时间延迟的处理，得到对控制对象较好的控制，较好解决了不确定时延带来的问题[3]。

4 结论

ICMP 协议主要是用来进行错误信息和控制信息的传递，本文提供了一个利用 ICMP 协议中的 ECHO request 报文进行网络中主机状态响应探测的方法。并给出了相应的 ICMP Ping 类的实现方法。该算法适用于 Intranet 的 IP 网络的拓扑自动发现，以及正确获取远程主机的响应速度，通过加入适时延迟实施有效控制的方法。

参考文献

1 Conta A, Deering S. Internet control massage protocol (ICMPv6) for the Internet protocol version6(IP6) specification. RFC2463. 2006,12:101－106.

2 Joyo M, Quisquater JJ. On the importance of securing your bins:the garbage man in the middle attack. In;4th ACMCorf Computer Comm Security. 2007.135－141.

3 Nikander P, Kempf J, Nordmark E. IPv6 neighbor discovery (ND) trust models and threats. RFC3756, Internet Engineering Task Force, 2004.92－99.