**第六章 ICMP:Internet控制报文协议**

6.1 ICMP介绍





ICMP介绍：由于IP协议是不可靠协议，他不能保证数据送达，自然的，保证数据送达应该由其他模块完成。ICMP将差错报文(封包)以及需要注意的信息返回用户进程。

类型字段：可以有15个不同的值，以描述特定类型的ICMP报文。

代码字段：用来进一步描述特定类不同的条件。

ICMP检验：必需校验后面所有的。

下面几种情况都不会导致ICMP差错报文：

1. ICMP差错报文(除ICMP查询报文可能产生ICMP报文)、
2. 目的地址是广播地址或多播地址的IP数据报。
3. 作为数据链路层广播的数据报。
4. 不是IP分片的第一片。
5. 源地址不是单个主机的数据报。这就是说，源地址不能为零地址、换回地址、广播地址或多播地址。

ICMP报文的类型(续)

(1)不同类型由报文中的类型字段和代码字段来共同决定。

(2)最后两列表示ICMP报文是一份查询报文还是一份差错报文。

(3)当发送一份ICMP差错报文时，报文始终包含IP的首部和超生ICMP差错报文的IP数据包的前8个字节。这样，接收ICMP差错报文的模块就会把它与某个特定的协议(根据IP数据报首部中的协议字段来判断)和用户进程(根据包括含在IPS数据报前8 个字节中的TCP或UDP报文首部中的TCP或UDP端口号)联系起来。

6.2 ICMP试验

试验一：PC0向server发送tftp邮件(server的tftp端口关闭)

|  |  |
| --- | --- |
|  |  |
| （a）关闭server的TFTP端口 | （b）PC0创建TFTP邮件 |
|  |  |
| （c）PC0->server(UDP) | （d）server->pc0(ICMP) |
|  |  |
|  | |
| 1PC和1server(ICMP) | |

过程：

(1)关闭server的tftp端口;

(2)创建PC0->server的tftp邮件。

(3)PC0发送端口号为69的UDP协议(tftp)到server

(4)因为server的tftp端口未开启，向PC0发送类型为3代码为3(33为端口不可达差错)的ICMP协议，ICMP数据报中包含IP首部和UDP前8个字节

实验二：wireshark端口不可达(ftp [www.baidu.com](http://www.baidu.com))

|  |
| --- |
|  |
| （a）ftp百度域名 |
|  |
| （b）wireshark抓包 |

过程：

(1)cmd中ftp [www.baidu.com](http://www.baidu.com)

(2)wireshark抓ICMP包，可以看到类型为3代码为3(端口不可达)，包括了IP首部,和UDP前8字节数据。(DNS暂时不管)