第 5 章 ICMP 协议

因为 IP 协议是提供不可靠传输服务的，因此源地址发出的 IP 数据包很可能无法到达目标地址。发生这种情况的原因是很多的，可能是目标主机根本不存在，也可能是传输途中的某个链路中断等。那么在 IP 数据包无法传送到目标地址时，发送方怎样才能知道是什么原因造成的呢？ICMP 协议就是用来探测并报告 IP 数据包传输中产生的各种错误的。在本章中，我们将介绍 ICMP 协议。

5.1 ICMP 协议的作用与原理

ICMP 是 Internet Control Message Protocol(互联网控制消息协议)的缩写。ICMP 协议就是用来探测并报告 IP 数据包传输中产生的各种错误的。

我们都知道 IP 协议的工作原理，IP 数据包在网络上的传输是通过路由器对数据包的转发来完成的。如果在 IP 数据包的传输过程中，某个路由器因为某种原因无法转发收到的数据包时，数据包就会被丢弃。但这时数据包的发送站无法得知传输出错，更不知道出错的具体原因。而一个有效的错误检查与报告机制对 TCP/IP 协议是非常重要的，因为它可以使我们在网络发生故障时知道故障的具体原因与位置。

ICMP 协议就是这样一种能让我们对网络进行调试的报错机制，它能让发现错误的路由器向数据包的源站发送一个出错消息，报告出

错原因。这样源站就可以根据不同的错误采取相应的措施进行处理。

需要指出的是，ICMP 的错误报告只能通知出错数据包的源主机，而无法通知从源主机到出错路由器途中的所有路由器。例如：在图 5.1 中主机 H_1 向 H_2 发送一个 IP 数据包，路由器 R_C 发现无法将该数据包转发到 H_2。我们看看通过 R_C 接收到的数据包能提取哪些信息。R_C 能知道数据包的源地址和目标地址，但它无法知道该数据包到达本路由器时途中经过了哪些其他的路由器。因此 R_C 只能将出错消息发送给数据包的源地址 H_1。

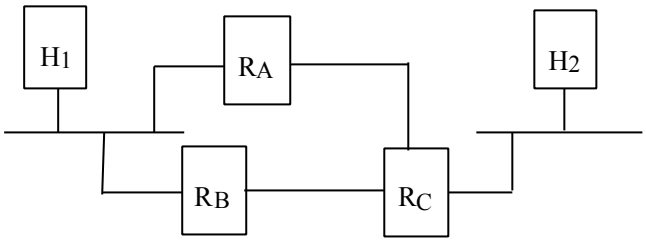

图 5.1 IP 数据包出错示例

从图 5.1 中还可以看出 ICMP 数据包应该如何传输。如果 R_C 要向 H_1 发送一个 ICMP 数据包，那么该数据包必须通过路由器 R_A 或 R_B，即要由它们之中的一个将数据包转发给主机 H_1。但路由器只会转发 IP 数据包，所以应该将 ICMP 数据包封装在 IP 数据包中才能将它传输到目的地。事实上 ICMP 数据包确实是封装在 IP 数据包中的，如图 5.2 所示。

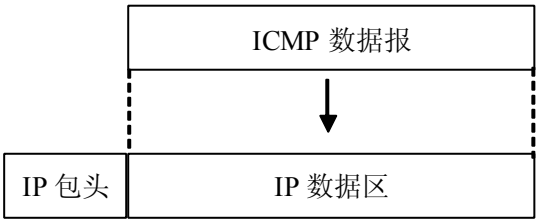

图 5.2 ICMP 数据包的封装

因为 ICMP 数据包是封装在 IP 数据包中的，因此 ICMP 数据包的传输也有可能会出错。这时就需要为这个 ICMP 数据包产生另一个 ICMP 数据包，并将它发送给源 ICMP 数据包的源路由器。在一个已经很繁忙的网络中，IP 数据包的出错率是比较高的，也即发送的 ICMP 数据包比较多，如果再为这些 ICMP 数据包产生新的 ICMP 数据包，就会加重网络负载，使得本已阻塞的网络阻塞得更严重。因此 ICMP 协议规定，如果传输 ICMP 数据包的 IP 数据包出错，不能为该数据包产生新的 ICMP 数据包。

5.2 ICMP 数据包的格式

因为传输错误的种类多种多样，ICMP 协议要报告这些错误就必须根据不同的错误采用不同的格式。但各种 ICMP 数据包都有一个共同的 ICMP 头部。图 5.3 说明了 ICMP 数据包的头部格式。

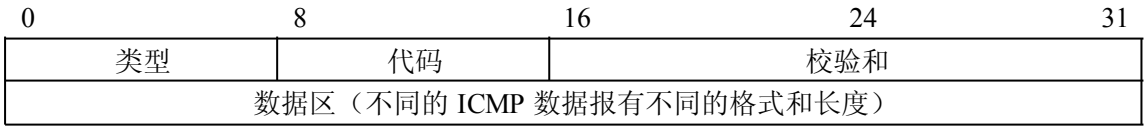

图 5.3 ICMP 数据包格式

类型字段定义了各种不同的 ICMP 数据包，不同的 ICMP 数据包起到不同的作用，也有不同的格式。表 5.1 是已定义的各种 ICMP 类型。

表 5.1 ICMP 数据包类型

类型字段值	描述
0	反射应答
3	目标不可达
4	源端关闭

类型字段值	描述
5	重定向
8	反射请求
9	路由器通告
10	路由器请求
11	超时
12	数据包参数错误
13	时间戳请求
14	时间戳应答
15	信息请求（作废）
16	信息应答（作废）
17	地址掩码请求
18	地址掩码应答

虽然大多数的 ICMP 数据包都是用来报错的，但有的是用作探测和获取信息的。代码字段是用来说明错误的具体原因的，将在 5.3 节具体介绍各种 ICMP 数据包时详细说明。

5.3 各种 ICMP 数据包

由于 ICMP 数据包的种类较多，在本节将按照各种 ICMP 数据包的不同功能分小节对其中常见的几种进行详细说明。

5.3.1 反射请求与应答

反射请求和应答数据包用来测试从发送主机到接收主机的网络链路是否完好以及目标主机的 TCP/IP 协议是否工作正常。图 5.4 是反射请求与应答数据包的格式。

图 5.4 ICMP 反射请求与应答数据包格式

反射请求与应答数据包的代码字段都必须设为 0。可选数据字段是一个变长的字段，发送方可以用任何数据填充该字段，当然，该字段的长度也可以为 0。标识和序列号字段是发送方用来匹配请求数据包和应答数据包的。反射请求与应答的工作过程如下：发送方构造一个反射请求数据包，它可以设置任意长度的可选数据字段，其中可以随意填写数据。目标主机收到该数据包后将类型字段由 8 改为 0，再发送给请求数据包的发送方。一旦请求发送方接收到请求数据包的应答数据包，它能肯定两个问题：首先，从发送方到接收方的网络通路工作正常；第二，目标主机的 TCP/IP 协议工作正常。

5.3.2 目标不可达错误

当一个路由器无法将一个 IP 数据包转发到目的地时，它会将该数据包丢弃，但同时它会向该数据包的源主机发送一个目标不可达的 ICMP 数据包，该数据包起到了报错的作用。ICMP 目标不可达数据包的格式如图 5.5 所示。

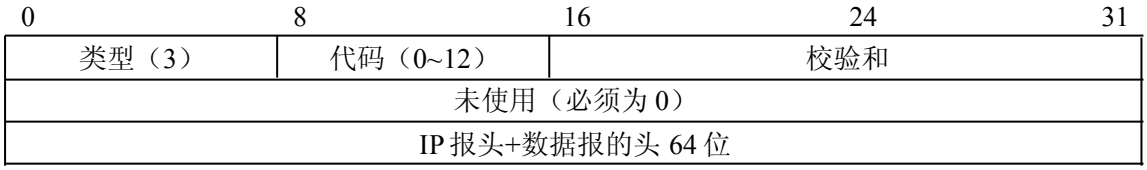

图 5.5 ICMP 目标不可达数据包格式

类型字段为 3，标识这是一个 ICMP 目标不可达数据包。代码字段的值进一步说明了出错的具体原因，其取值范围为 0-12。各值的含义如表 5.2 所示。

表 5.2 ICMP 目标不可达数据包代码字段值

代码值	描述
0	网络不可达

代码值	描述
1	主机不可达
2	协议不可达
3	端口不可达
4	需要分片，但设置了 DF（不分段）位
5	源路由失败
6	未知的目标网络
7	未知的目标主机
8	源主机孤立
9	禁止与目标网络通信
10	禁止与目标主机通信
11	指定服务类型的网络不可达
12	指定服务类型的主机不可达

另外我们注意到 ICMP 目标不可达数据包中最后一个字段，该字段包含了出错 IP 数据包的 lP 头部和 IP 数据包数据部分的头 64 位。之所以要包含这个字段是为了能让 IP 数据包的发送者知道是哪个数据包出错。

5.3.3 源端关闭

路由器转发 IP 数据包时是仅仅根据单个数据包的信息进行转发的，因此它无法为某个数据包预留一定的资源。由于路由器的资源（内存，计算时间等）是有限的，在网络数据流量比较大时，路由器为了转发数据包可能会耗尽其所有资源，这种情况称为阻塞。出现阻塞就是路由器能力有限，无法转发所有需要转发的数据包。这时路由器会选择丢弃一些数据包。但仅仅这样做还是无法减轻网络阻塞的情况，因为发送端在发出数据包后如果无法收到响应往往会发送更多的数据包到网络上，使得网络更加拥挤，使网络的阻塞更加严重。因此路由器在丢弃数据包时会发送一个信息到数据包的发送方，通知它网络已阻塞，请缓发数据包。用来发送这个通知的就是 ICMP 源端关闭数

据包。该数据包格式如图 5.6 所示。

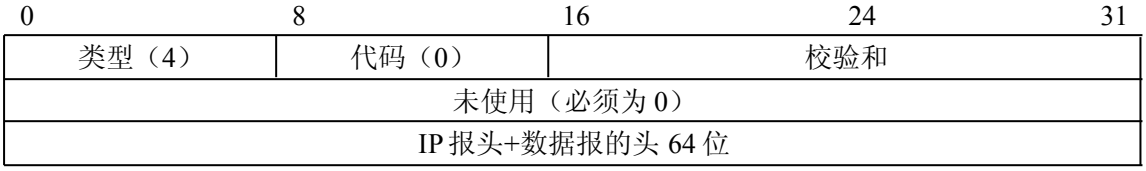

图 5.6 ICMP 源端关闭数据包格式

从图中可以看出，ICMP 源端关闭数据包的格式和目标不可达数据包格式相同，只是类型和代码字段的值不同。ICMP 源端关闭数据包也在最后一个字段包含了被丢弃的 IP 数据包的 IP 头部和数据部分的头 64 位。

5.3.4 超时错误

在 IP 数据包中有个 TTL 字段。IP 数据包每被路由器转发一次该字段的值就至少减 l。当该字段的值减少到 0 时，路由器会将该数据包丢弃。但这种情况是很少发生的，因为 IP 数据包都会将该字段的值设置的足够大，使得该数据包被转发到目标主机时该字段的值仍然大于 0。但有时也会发生这种清况，例如几个路由器组成一个环，而且路由器中的路由表有错误，这时在其中转发的数据包可能一直在这个环中直到 TTL 字段减为 0。在将 TTL 为 0 的数据包丢弃之前，路由器需要通知数据包的源主机数据包转发超时了。

由于一个 IP 数据包在转发到目标主机的过程中可能被分成了多个段，而这些分段是单独路由的。因此很有可能一个 IP 数据包的多个分段只有部分能到达目标主机而其他的可能丢失了。目标主机在对一个 IP 数据包的多个分段进行重组时，如果等待一定的时间后剩下的分段还没有到达，目标主机就认为这些分段不会到达，并将已收到

的分段丢弃。在丢弃这些分段之前，目标主机会通知源主机 IP 数据包的分段在进行重组时超时了。

不管是上述两种情况的哪一种，路由器和目标主机都是通过向源主机发送一个ICMP超时数据包来通知它的。该数据包的格式如图5.7所示。

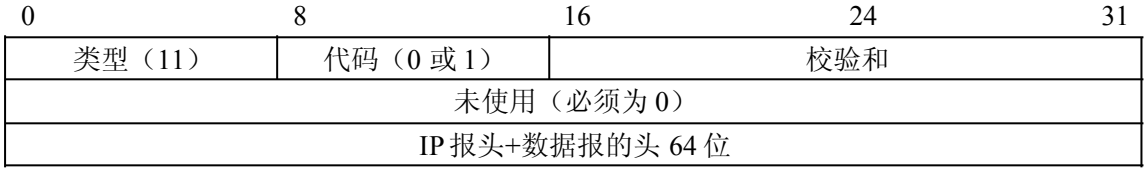

图 5.7 ICMP 超时数据包格式

其中代码字段说明了超时的具体原因。“0”标识 TTL 值减为 0，而“1”表示分段重组超时了。

5.3.5 数据包参数问题

如果路由器或主机发现一个收到的IP数据包的格式不符合要求，它就会向源主机发送一个报错，并指出数据包中的什么字段格式或值不正确。这就是 ICMP 参数错误数据包的作用，该数据包的格式如图5.8 所示。

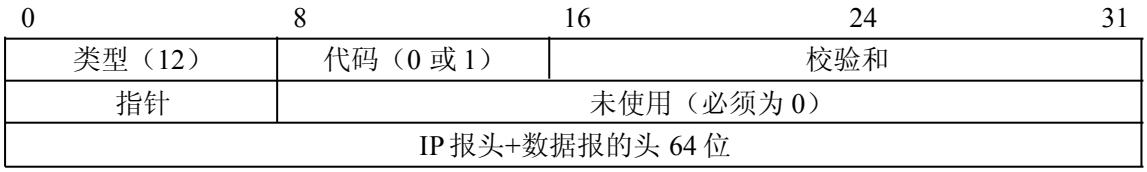

图 5.8 ICMP 参数错误数据包

在 ICMP 参数错误数据包中，代码字段的值表示了 IP 数据包格式错误的类型。“0”表示 IP 数据包中头部某个字段的值设置错误，这时指针字段的值就表示是 IP 头部的哪个八位字的值出错了。代码

“1”表示 IP 头部需要设置某个选项但没有设置，这时指针字段没有意义。

5.3.6 获取子网掩码

关于子网掩码的作用与原理在第 3 章已经详细讲述过。现在的问题是一个使用了子网掩码技术的网络中，主机要与该网络中的其他主机或者与该网络外面的主机通信必须知道该网络的网络掩码。在常见的系统中，这个掩码是可以人为设置的，但这就要求系统管理人员知道该网络的掩码。ICMP 可以自动获取网络使用的子网掩码，这是通过发送子网掩码请求数据包并接收响应数据包实现的。这两种数据包的格式如图 5.9 所示。

图 5.9 ICMP 子网掩码请求与响应数据包

请求主机可以向路由器或者直接广播该数据包，路由器会将网络的子网掩码通知给该主机。