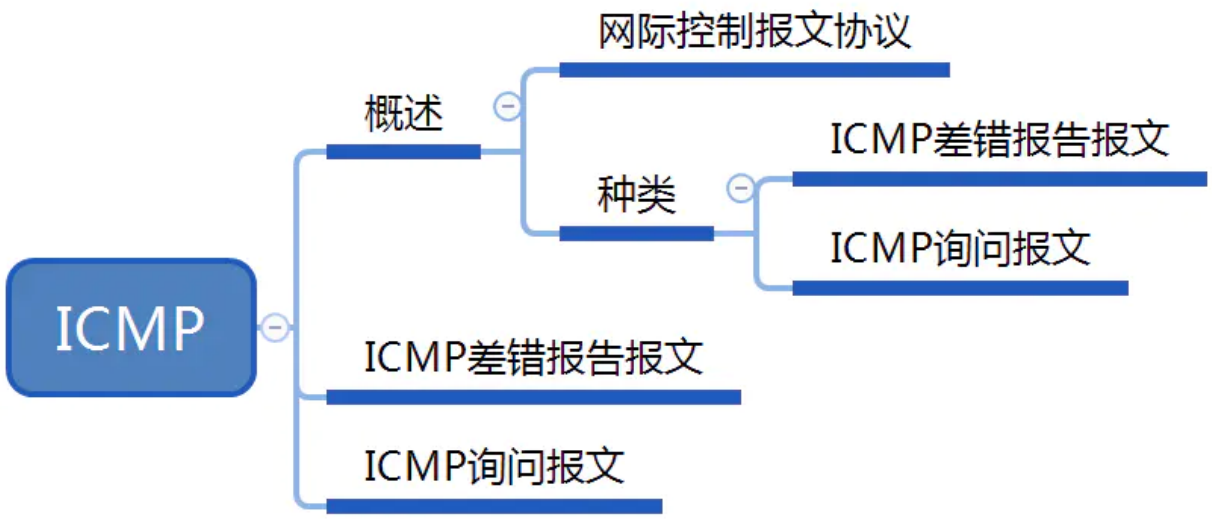
ICMP协议

内容总览



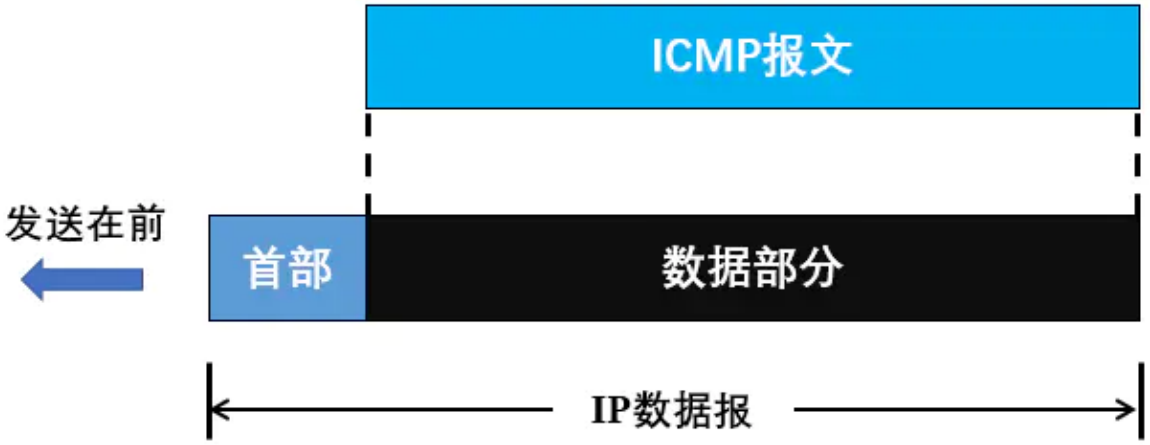
1.ICMP协议

网际控制报文协议ICMP（Internet Control Message Protocol），ICMP允许主机或路由器报告差错情况和提供有关异常情况的报告。

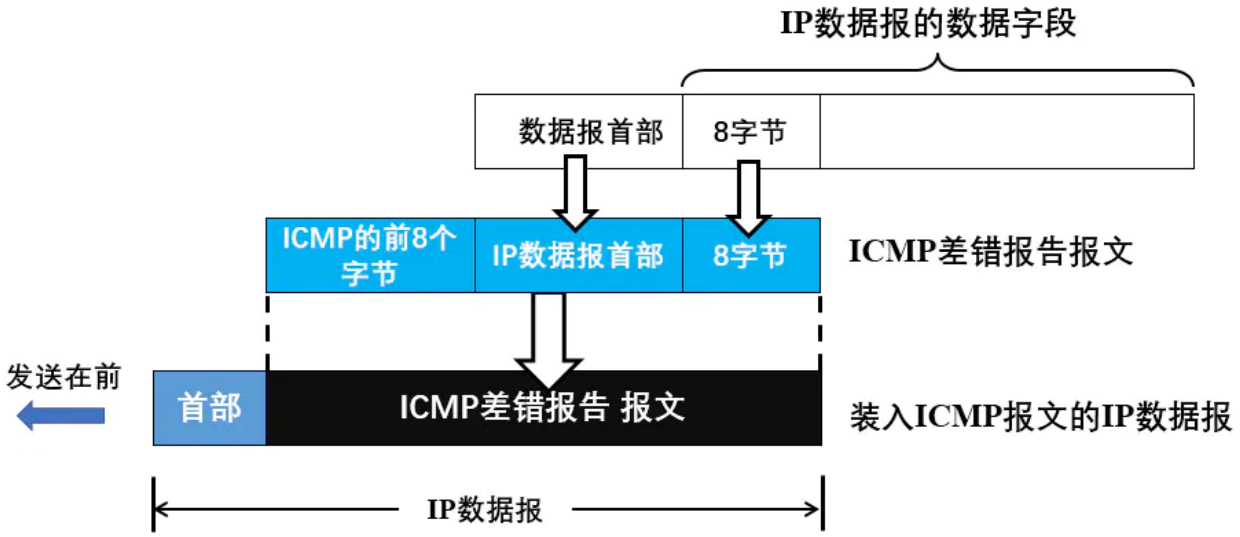
> IP数据报在传输的过程中难免出错，对于出错的报文最典型的就是丢弃，同时允许路由器或主机发送ICMP报文报告发送IP数据报的源主机。

ICMP协议的两个作用：**差错报告和网络探寻。**对应这两个功能，ICMP报文分为：**ICMP差错报告报文和ICMP询问报文。**

2.ICMP报文格式



ICMP报文作为IP层数据报的数据，加上IP数据报首部发送出去。ICMP协议是网络层协议。



ICMP 差错报告报文的组成：

> (1) 需要进行差错报告的IP数据报首部和数据字段的前8个字节。
> (2) ICMP报文的前8个字节。

3.ICMP差错报告报文

差错报告报文共有4种：

(1) 终点不可达报文——无法交付

> 当数据报到达路由器或主机但是不能交付时，数据报就会被丢弃，同时向源点发送终点不可达报文。

(2) 时间超过报文——TTL值为0

> 1. 当路由器收到生存时间为零的数据报时，除丢弃该数据报外，还要向源点发送时间超过报文。

> 2. 当终点在规定的时间内不能收到一个数据报全部数据报片时，就把已收到的数据报片全部丢弃，并向源点发送时间超过报文。

(3) 参数问题报文——首部字段有问题

> 当路由器或目的主机收到的数据报的首部中有的字段值不正确时，就丢弃该数据报，并向源点发送参数问题报文。

(4) 改变路由（重定向）报文——路由不好

> 互联网中的主机也要有一个路由表，当主机要发送数据时，首先是查找自己的路由表，看应当从哪个接口把数据报发送出去。在刚开始工作时，一般都在路由表中设置一个默认路由器的IP地址（默认网关）。不管数据报发送到哪个目的地址，都一律先把这个数据报传送给这个路由器，而这个默认路由器知道到每一个目的网络的最佳路由（通过和其他路由器交换信息）。如果默认路由器发现主机发往某个目的地址的数据报的最佳路径由应当经过网络上的另一个路由器R时，就用改变路由报文把这一情况告知主机。于是，主机就在其路由表增加一个项目：到某某目的地址应经过的路由器R（而不是默认路由器）。

(5) 源点抑制报文——拥塞丢数据

> 这种报文已经不使用了。用于流量控制，当路由器或主机由于拥塞而丢弃数据时，就向源点发送源点抑制报文。告知源点将数据报的发送速率放慢。

4种特殊情况下不会发送差错报文：

(1) **对ICMP差错报告报文**，不再发送ICMP差错报告报文。

> 前面已经直到，整个ICMP报文封装在IP数据报的数据部分作为IP数据报发送给源点，其本身也是一个IP数据报，如果这个IP数据报也发生了差错，那么将不会再发送差错报文了。

(2) **对第一分片的数据报片的所有后续数据报片，都不发送ICMP差错报告报文。**

> 如果一个数据报被分片为多个数据报片，如果数据报片发生差错，那么只会对第一个分片发送ICMP差错报告报文，其余的均不发送。

(3) **对于多播地址的数据报，都不发送ICMP差错报告报文。**

(4) **对具有特殊地址（如127.0.0.0或0.0.0.0）的数据报，不发送ICMP差错报告报文。**

4.ICMP询问报文

(1) **回送请求和回答报文**

> ICMP回送请求报文是由主机或路由器向同一个特定的目的主机发出询问。收到此报文的主机必须给源主机或路由器发送ICMP回送回答报文。

这种报文用来**测试目的站是否可达**以及**了解其有关状态。**

(2) **时间戳请求和回答报文**

> 这种报文是请求某台主机或路由器回答当前的日期和时间。

用于时钟同步和时间测量。

(3) **子网掩码请求和应答报文**及**路由器询问和通告报文**这两个报文也不再使用了。

5.ICMP的应用

(1)**PING**

ICMP的一个重要应用就是分组网间探测PING（Packet InterNet Groper），用来测试两台主机的连通性。PING使用了回送请求和回答报文。

> 例如，在Windows命名提示符窗口键入 ping www.baidu.com 用来测试本机和百度服务器的连通性测试结果。

(2) **Traceroute**

Traceroute是跟踪一个分组从源点到终点的路径，使用了**ICMP时间超过差错报告报文。**

Traceroute工作原理：
源主机会发送多组生存时间TTL连续的IP数据报，每组3个，数据报中封装的是无法交付的UDP数据报。

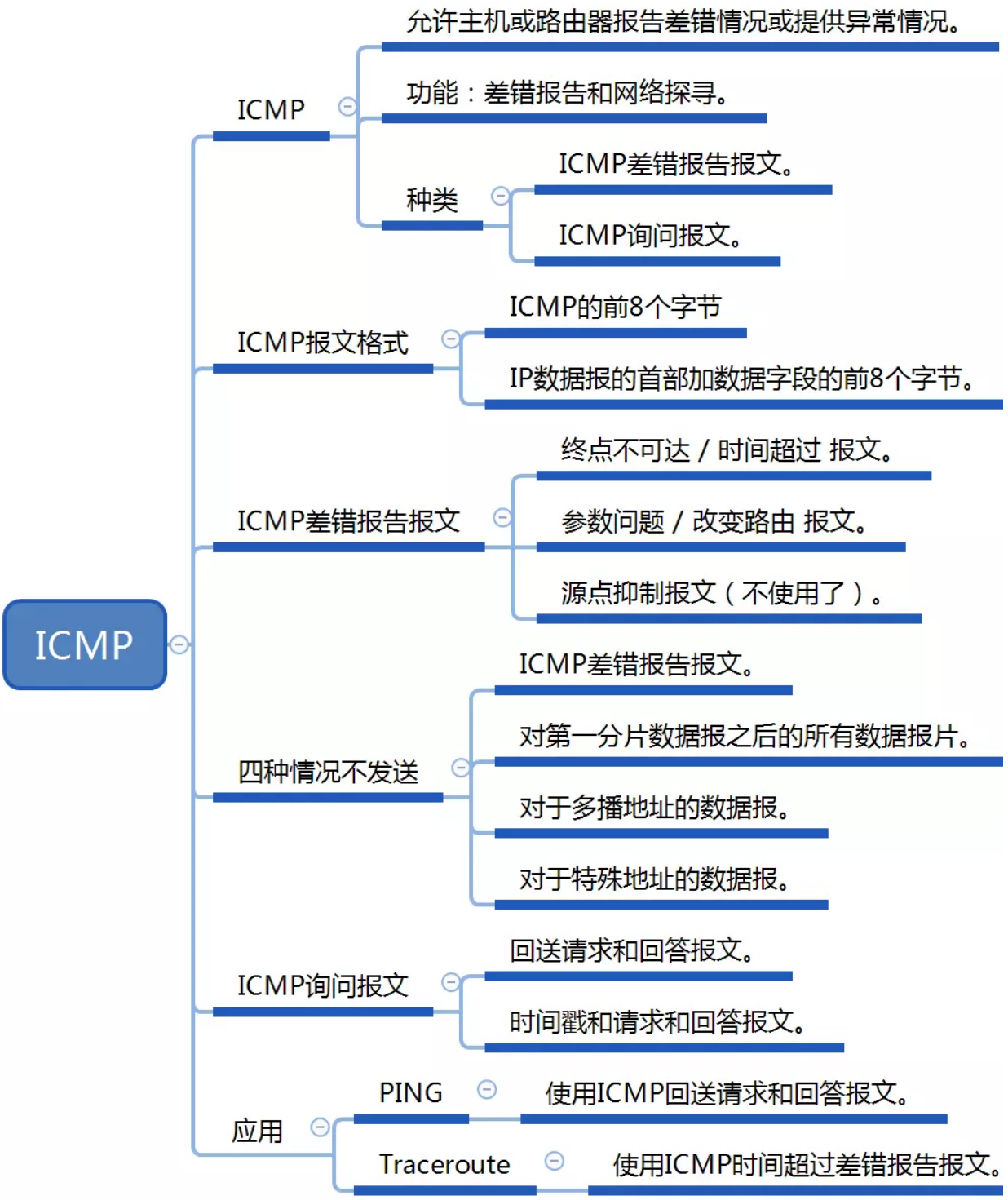
> (1) 第一组的数据报的生存时间TTL = 1，当这组数据报到达路径上的第一个路由器时，路由器收下后，接着把TTL值减1，由于TTL = 0，所以路由器丢弃该报文，并向源主机发送一个ICMP时间超过差错报告报文。
> (2) 源主机接着会发送第二组IP数据报，并把TTL 的值设为2，当数据报到达第二个路由器时被丢弃并向源主机返回一个ICMP时间超过差错报告报文。
> ...

> (3) 当最后一组数据刚刚到达目的主机时，TTL = 1，主机不转发数据报，也不把TTL的值减1，但是因IP数据报封装的是无法交付的运输层UDP用户数据报，因此目的主机要向源主机发送ICMP终点不可达差错报告报文。

这样源主机就达到了自己的目的，因为这些路由器和最后的目的主机发来的ICMP报文正好给出了主机到目的主机的路由信息——到达目的主机所要经过的路由器的IP地址，以及每个路由器的往返时间。

> 下图表示本机到百度网的发送的tracert命令所获得的结果。每组三个IP数据报，所以有3个往返时间，其中第一行的IP地址是主机的默认网关。

6.总结


ICMP
ICMP
允许主机或路由器报告差错情况或提供异常情况。
功能：差错报告和网络探寻。
种类
ICMP差错报告报文。
ICMP询问报文。
ICMP报文格式
ICMP的前8个字节
IP数据报的首部加数据字段的前8个字节。
ICMP差错报告报文
终点不可达 / 时间超过 报文。
参数问题 / 改变路由 报文。
源点抑制报文（不使用了）。
四种情况不发送
ICMP差错报告报文。
对第一分片数据报之后的所有数据报片。
对于多播地址的数据报。
对于特殊地址的数据报。
ICMP询问报文
回送请求和回答报文。
时间戳和请求和回答报文。
应用
PING
使用ICMP回送请求和回答报文。
Traceroute
使用ICMP时间超过差错报告报文。