网际控制报文协议ICMP

网际控制报文协议ICMP

Ip协议为了有效利用网络资源，提供了不可靠和无连接的数据报交付服务，它只提供把数据报从源点交付到终点，而不关心过程中是否有丢失或者损坏。

Ip协议缺少：差错控制和查询辅助机制

网际控制报文协议ICMP

实际网络都有哪些不可预知的错误发生?

例如:

1、路由器找不到最终终点

2、数据报生存时间为0而被丢弃

3、在有限时间内主机无法收到一个数据报的所有分片，而被迫丢弃已收到的分片

等等。。

网际控制报文协议ICMP

如果上述错误发生该怎么办?

因此ICMP协议就顺理成章得诞生了!

网际控制报文协议ICMP

ICMP协议：Internet Control Message Protocol

它对IP包无法传输时提供报告，这些差错报告帮助了发送方了解为什么无法传递，网络发生了什么问题，确定应用程序后续操作。

它还提供了一种查询机制，有利于网络环境分析和网络问题定位。

网际控制报文协议ICMP

ICMP 是互联网的标准协议。

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。

但 ICMP 不是高层协议，而是 IP 层的协议。

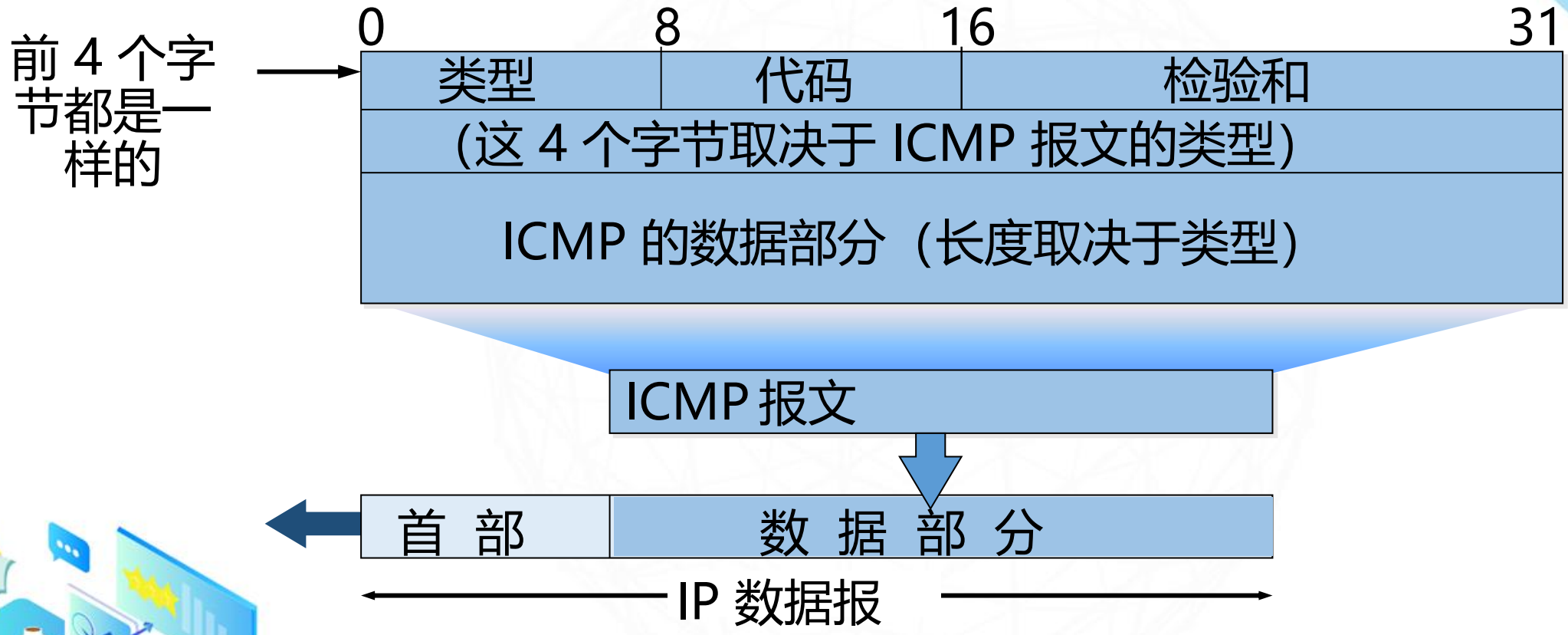
网际控制报文协议ICMP

ICMP 报文的种类有：

ICMP 差错报告报文
- 类型3：终点不可达
- 类型11：时间超过
- 类型12：参数问题
- 类型5：改变路由

ICMP 询问报文
- 类型8或0：回送请求或回答
- 类型13或14：时间戳请求或回答

ICMP 报文的格式


前 4 个字节都是一样的
0
8
16
31
类型
代码
检验和
(这 4 个字节取决于 ICMP 报文的类型)
ICMP 的数据部分（长度取决于类型）
ICMP 报文
首 部
数 据 部 分
IP 数据报

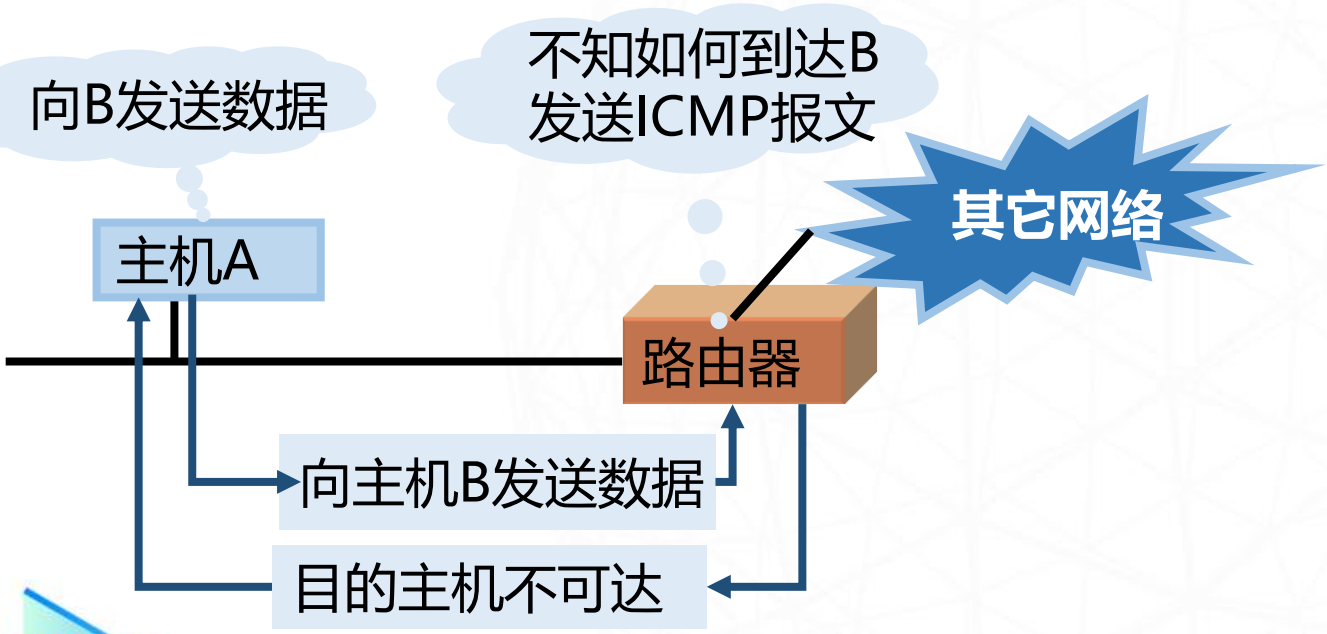
网际控制报文协议ICMP

代码(code): 提供报文类型的进一步信息；

检验和(checksum): 提供整个ICMP报文的校验和;

数据部分：包括出错数据报的报头及该数据报的前64bit数据；这些信息可以帮助信源机确定出错数据报.

ICMP差错报文 — 目的地不可达



当网络节点认为某数据报的目的地不可达时，就向该数据报的源主机发送一个目的地不可达的ICMP分组。

ICMP差错报文 — 时间超过

当网络结点发现某数据报的TTL域为零，需要丢弃此数据报时，需要向该数据报的源主机告知超时出错。

当目的主机在分段重组时，规定时间内由于分段丢失未完成重组，需要发送超时报文。

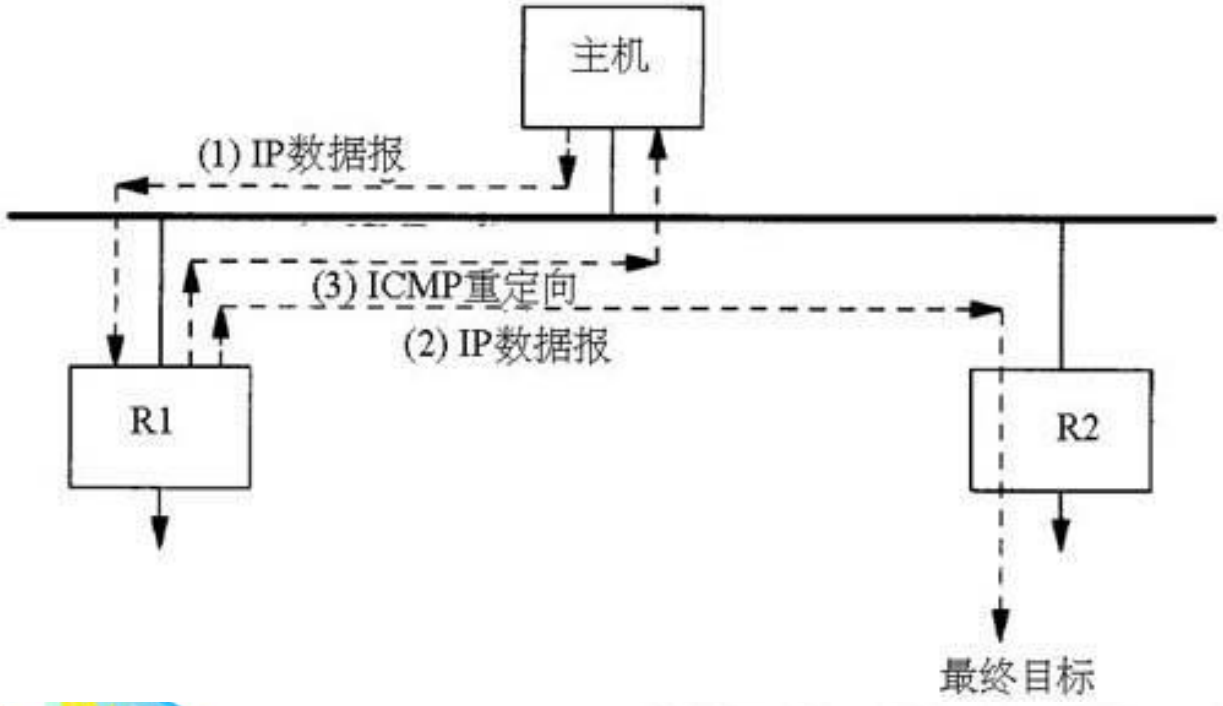
ICMP差错报文 — 参数问题

路由器或主机收到数据报首部中有的字段值不正确时，就丢弃该数据报，并向源站发送参数问题报文。

ICMP差错报文 — 改变路由

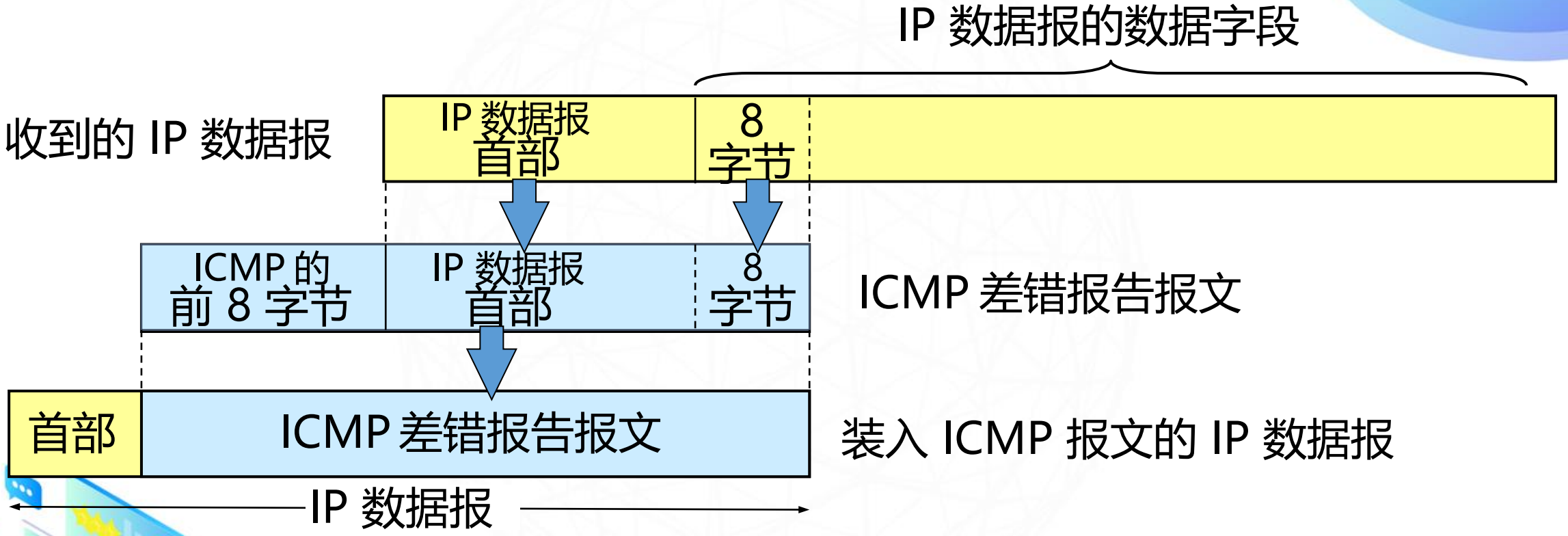
在Internet中，主机在启动时只知道最少的寻径信息，保证主机将数据报发送出去，但未必是最优路由。启动后，通过ICMP重定向报文，在数据传输过程中，主机可以不断从同一个网络的网络结点中得到新的路由信息。

ICMP差错报文 — 改变路由



路由器改变路由报文发送主机，让主机知道下一次将数据报发送给另外的路由器（可通过更好的路由）

ICMP 差错报告报文的数据字段的内容



不应发送 ICMP 差错报告报文的几种情况

对 ICMP 差错报告报文不再发送 ICMP 差错报告报文。

对第一个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。

对具有多播地址的数据报都不发送 ICMP 差错报告报文。

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。

ICMP询问报文

回送请求和回答：ICMP回送请求报文是由主机或路由器向一个特定的目的主机发出的询问。收到此报文的机器必须给源主机发送ICMP回送应答报文。这种询问报文用来测试目的站是否可达以及了解其有关状态。

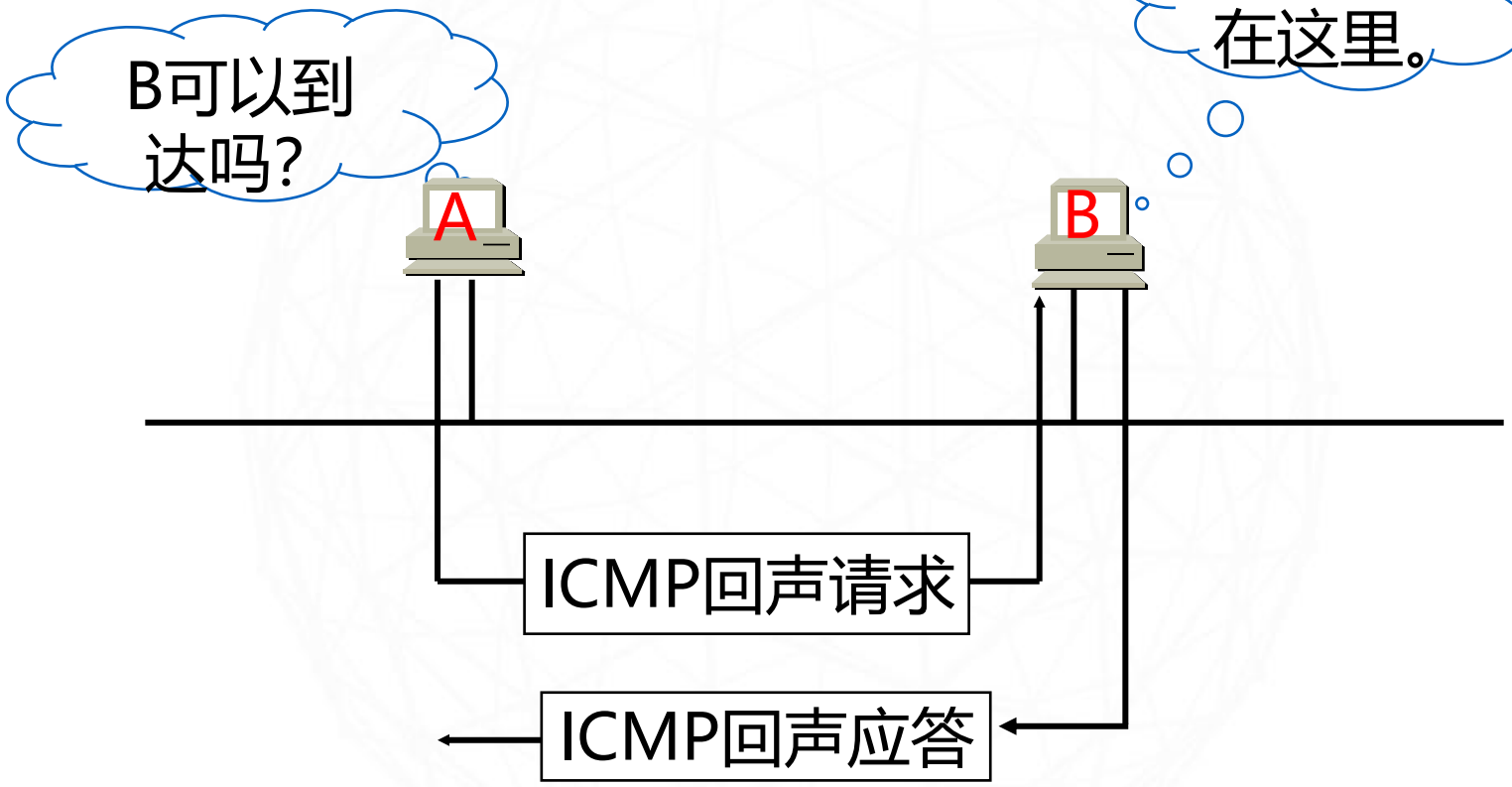
时间戳请求和回答：ICMP时间戳请求报文是请某台主机或路由器回答当前的日期和时间，可用于时钟同步和时间测量

ICMP的应用举例---PING

PING 用来测试两个主机之间的连通性。

PING 使用了 ICMP 回送请求与回送回答报文。

PING 是应用层直接使用网络层 ICMP 的例子，它没有通过运输层的 TCP 或UDP。



由PING命令产生的回声应答

```
C:\Users\Administrator>ping www.163.com

正在 Ping 163.xdwscache.ourglb0.com [112.253.19.196] 具有 32 字节的数据:
来自 112.253.19.196 的回复: 字节=32 时间=11ms TTL=57
来自 112.253.19.196 的回复: 字节=32 时间=11ms TTL=57
来自 112.253.19.196 的回复: 字节=32 时间=11ms TTL=57
来自 112.253.19.196 的回复: 字节=32 时间=10ms TTL=57

112.253.19.196 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 10ms, 最长 = 11ms, 平均 = 10ms
```

PING 举例

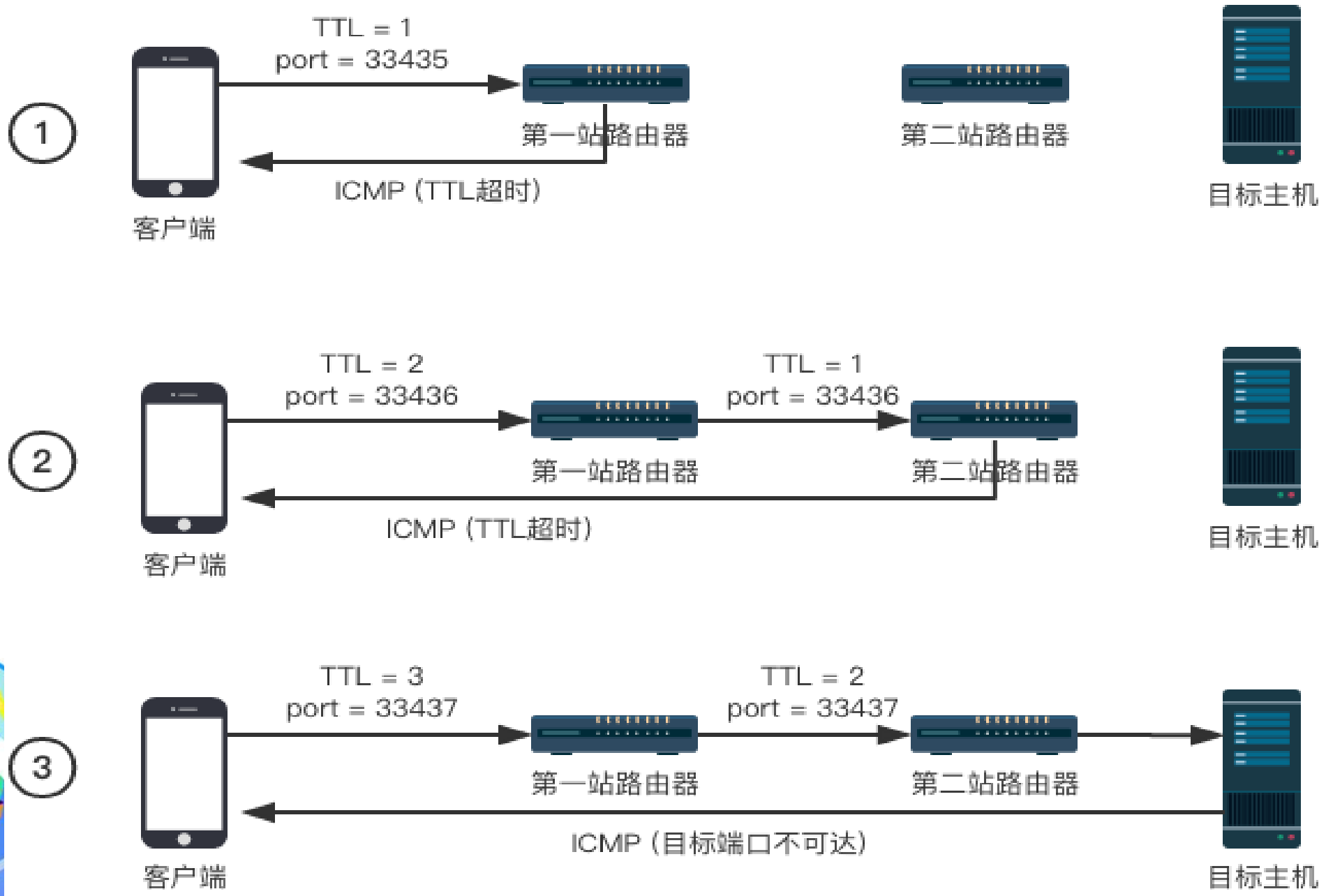
ICMP的应用举例- traceroute

在 Windows 操作系统中这个命令是 tracert。

用来跟踪一个分组从源点到终点的路径。

它利用 IP 数据报中的 TTL 字段和 ICMP 时间超过差错报告报文实现对从源点到终点的路径的跟踪。

Traceroute基于ICMP和UDP。



Traceroute原理示意图

```
C:\Users\Administrator>tracert www.163.com

通过最多 30 个跃点跟踪
到 163.xdwscache.ourglb0.com [150.138.170.223] 的路由:

  1    <1 毫秒    <1 毫秒    <1 毫秒 192.168.0.1
  2   256 ms    109 ms      2 ms  182.40.212.1
  3     3 ms      2 ms      4 ms  222.173.65.93
  4     2 ms      2 ms      2 ms  150.138.128.81
  5     9 ms      3 ms      3 ms  150.138.131.94
  6     6 ms      4 ms      4 ms  150.138.160.62
  7     2 ms      2 ms      3 ms  150.138.170.223

跟踪完成。
```

Traceroute 举例