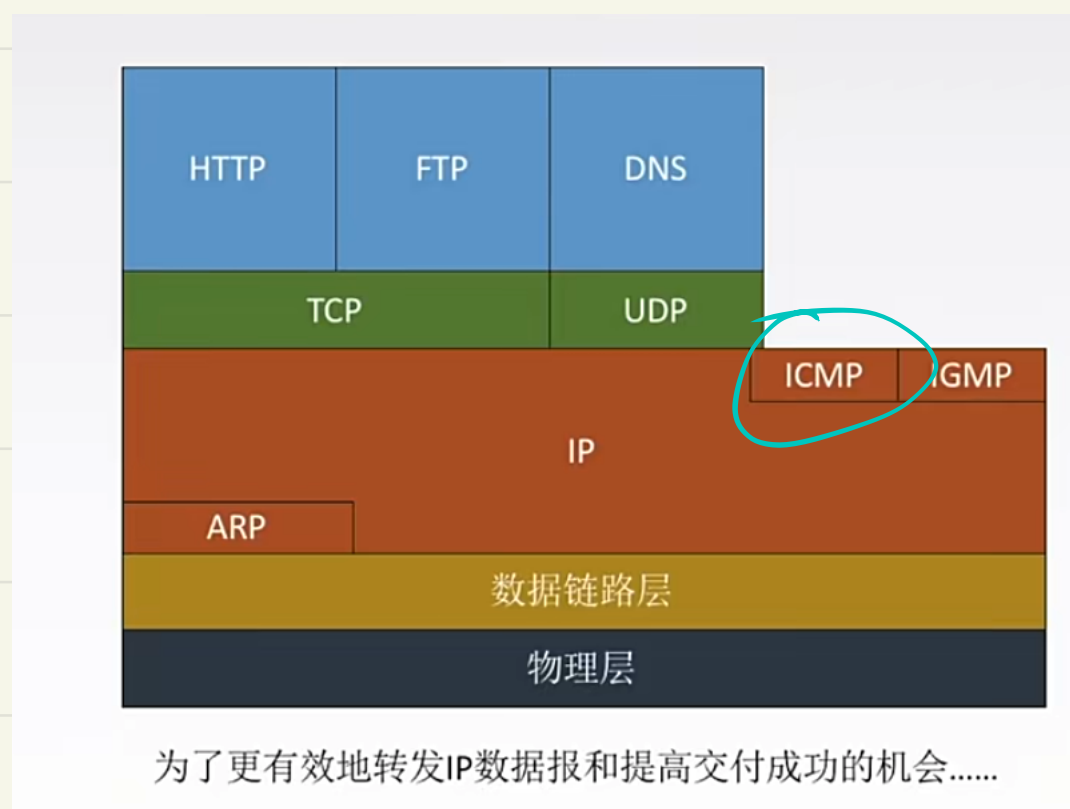
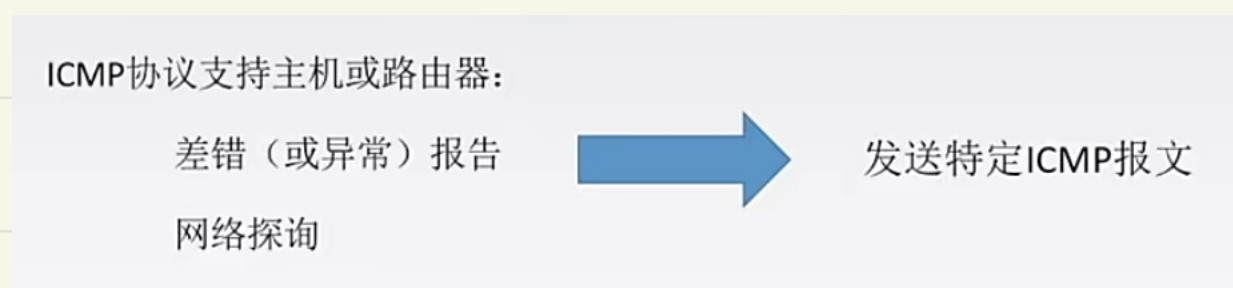


一. 回顾 TCP/IP 协议栈.



二. 网际控制报文协议 ICMP.



2.1 结构.



2.2. 类型

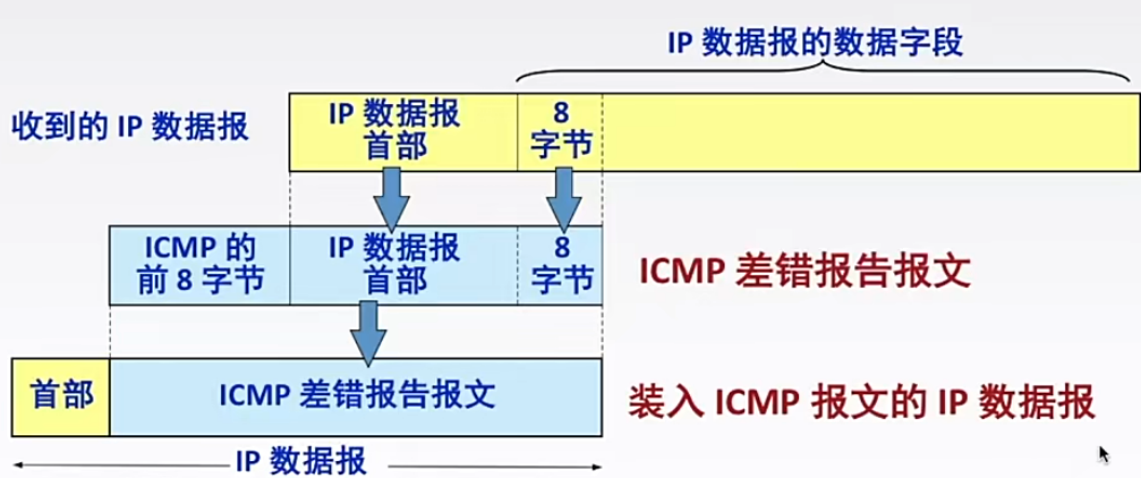
- ICMP 差错报文
- ICMP 询问报文

2.2.1 ICMP 差错报文 5种

源点抑制 (现不再使用)

- 1. 终点不可达: 当路由器或主机不能交付数据报时就向源点发送终点不可达报文。
无法交付
- 2. ~~源点抑制~~: 当路由器或主机由于拥塞而丢弃数据报时, 就向源点发送源点抑制报文, 使源点知道应当把数据报的发送速率放慢。
拥塞丢数据
- 3. 时间超过: 当路由器收到生存时间TTL=0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。当终点在预先规定的时间内不能收到一个数据报的全部数据报片时, 就把已收到的数据报片都丢弃, 并向源点发送时间超过报文。
TTL=0
- 4. 参数问题: 当路由器或目的主机收到的数据报的首部中有的字段的值不正确时, 就丢弃该数据报, 并向源点发送参数问题报文。
首部字段有问题
- 5. 改变路由 (重定向): 路由器把改变路由报文发送给主机, 让主机知道下次应将数据报发送给另外的路由器 (可通过更好的路由)。

ICMP 差错报告报文数据字段



不应发送 ICMP 差错报文的情况

- 1. 对 ICMP 差错报告报文不再发送 ICMP 差错报告报文。
- 2. 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。
- 3. 对具有组播地址的数据报都不发送 ICMP 差错报告报文。

部分地址，与广播不同，顾名思义吧。

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。

2.2.2 ICMP询问报文.

例如 Ping 命令.

- | | |
|---------------|---|
| 1.回送请求和回答报文 | 主机或路由器向特定目的主机发出的询问，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。测试目的站是否可达以及了解其相关状态。 |
| 2.时间戳请求和回答报文 | 请某个主机或路由器回答当前的日期和时间。用来进行时钟同步和测量时间。 |
| 3.掩码地址请求和回答报文 | } 不再使用 |
| 4.路由器询问和通告报文 | |

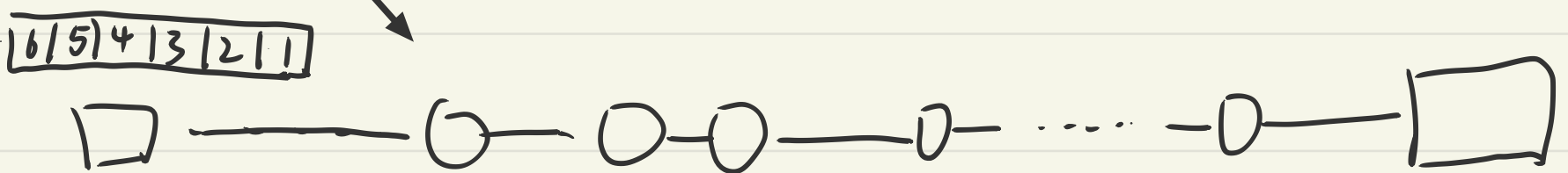
三. ICMP 的应用.

PING

测试两个主机之间的连通性，使用了ICMP回送请求和回答报文。

Traceroute

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。



主机

目的机.

主机发送一连串数据报，TTL 设置为 1, 2, 3, ...
分别到达第 1, 2, ... 个路由被丢弃，直到到达目的机
并由此测出路径