Beijing Forest Studio
北京理工大学信息系统及安全对抗实验中心

浅谈TCP/IP协议栈

王沛冉

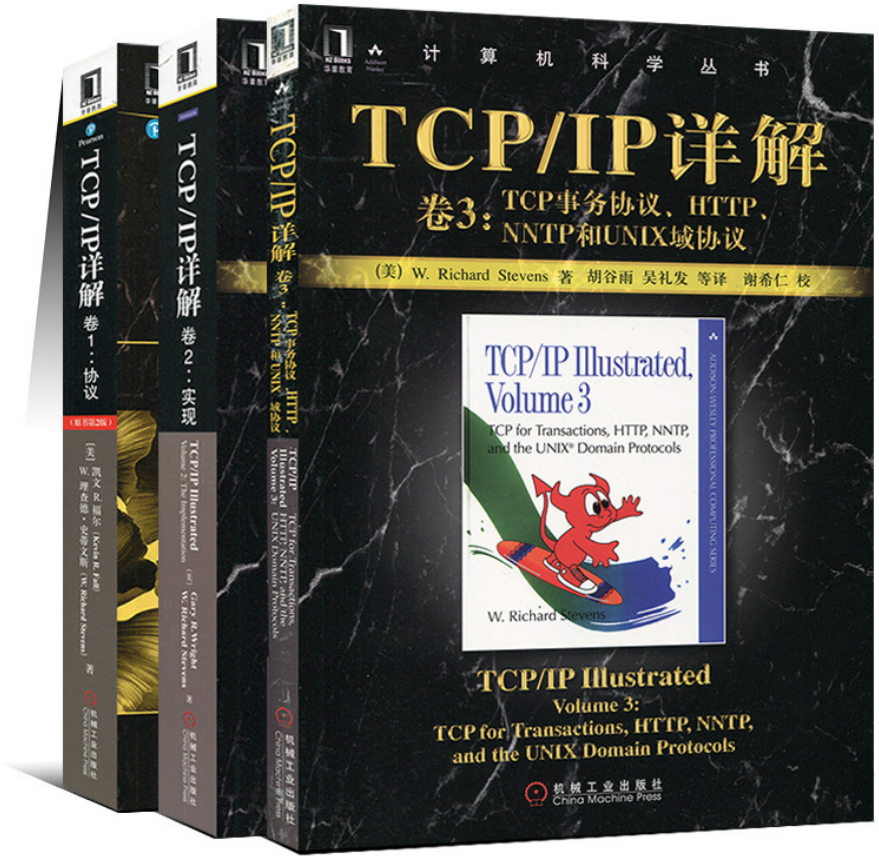
2020年01月05日

内容提要

- TCP/IP分层模型概述
- 数据链路层
- 网络层
- 传输层
- 实例

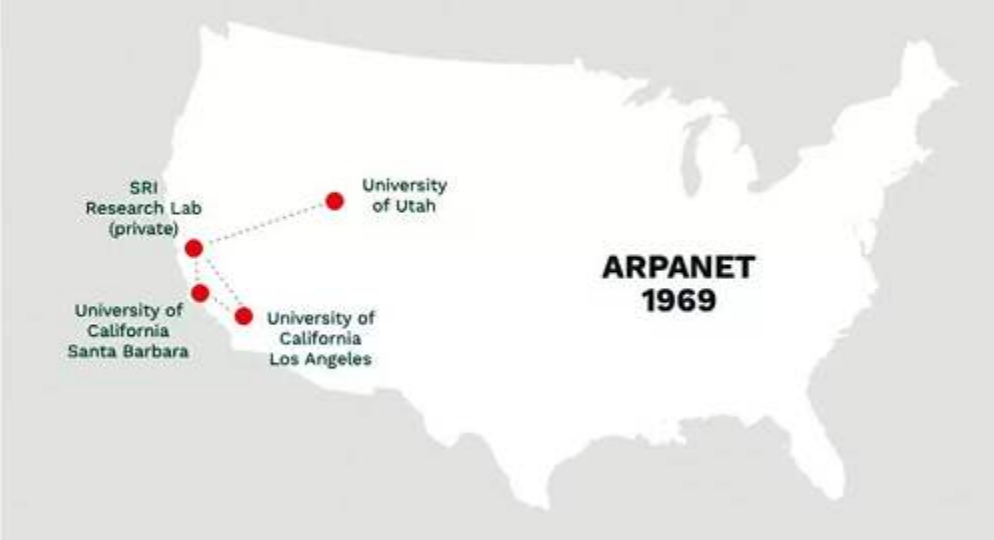
TCP/IP分层模型概述

- 为何是“浅谈”？



TCP/IP分层模型概述

- TCP/IP协议栈诞生于互联网的雏形——ARPANET中



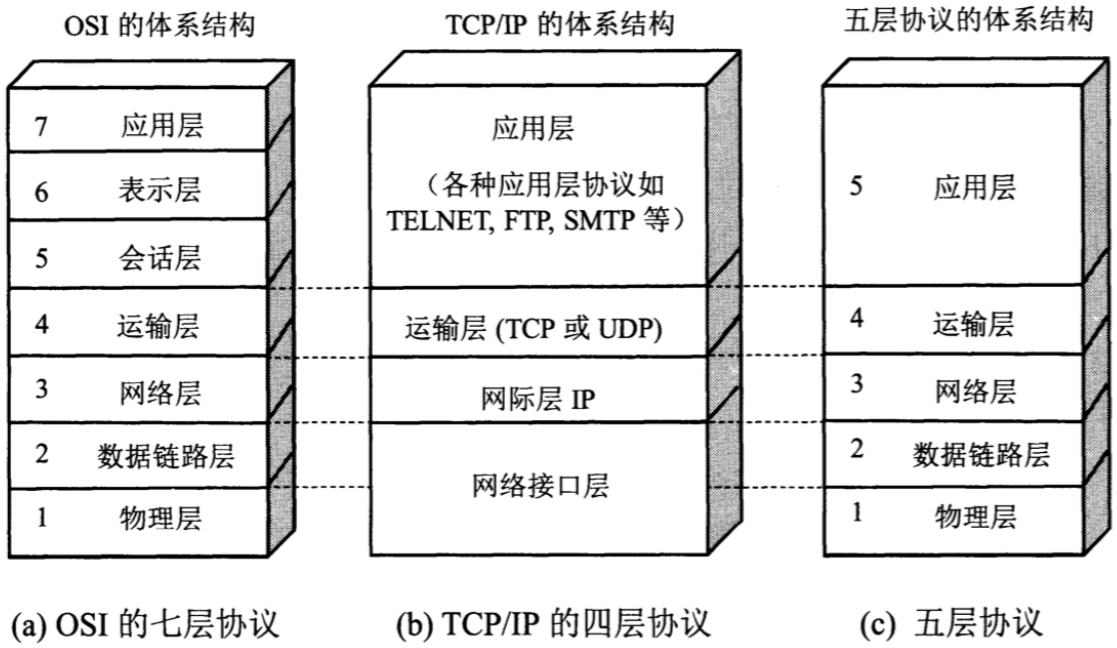
- 冷战期间为了连接离散的局域网络系统
- 之后先在美国的研究机构之间推广，到1985年扩展至欧洲等各国高校和研究机构

TCP/IP分层模型概述

- 国际标准化组织1981年推出了网络OSI 7层模型

– 物理层：定义了物理设备的标准，主要操作是进行数模、模数转换，以及传输模拟信号。对数据内容无感知。
– 数据链路层：定义了如何进行传输，控制器如何访问物理介质，提供了纠错机制
– 网络层：在位于不同地理位置之间的主机提供连接和路径选择
– 运输层：定义传输数据的协议和端口号
– 会话层：通过运输层（端口号：传输端口与接收端口）建立数据传输的通路。
– 表示层：确保两个系统的编码方式可以互相解码，表示层通过一种通用格式来实现多种数据格式之间的转换
– 应用层：为用户的应用程序提供网络服务

TCP/IP分层模型概述



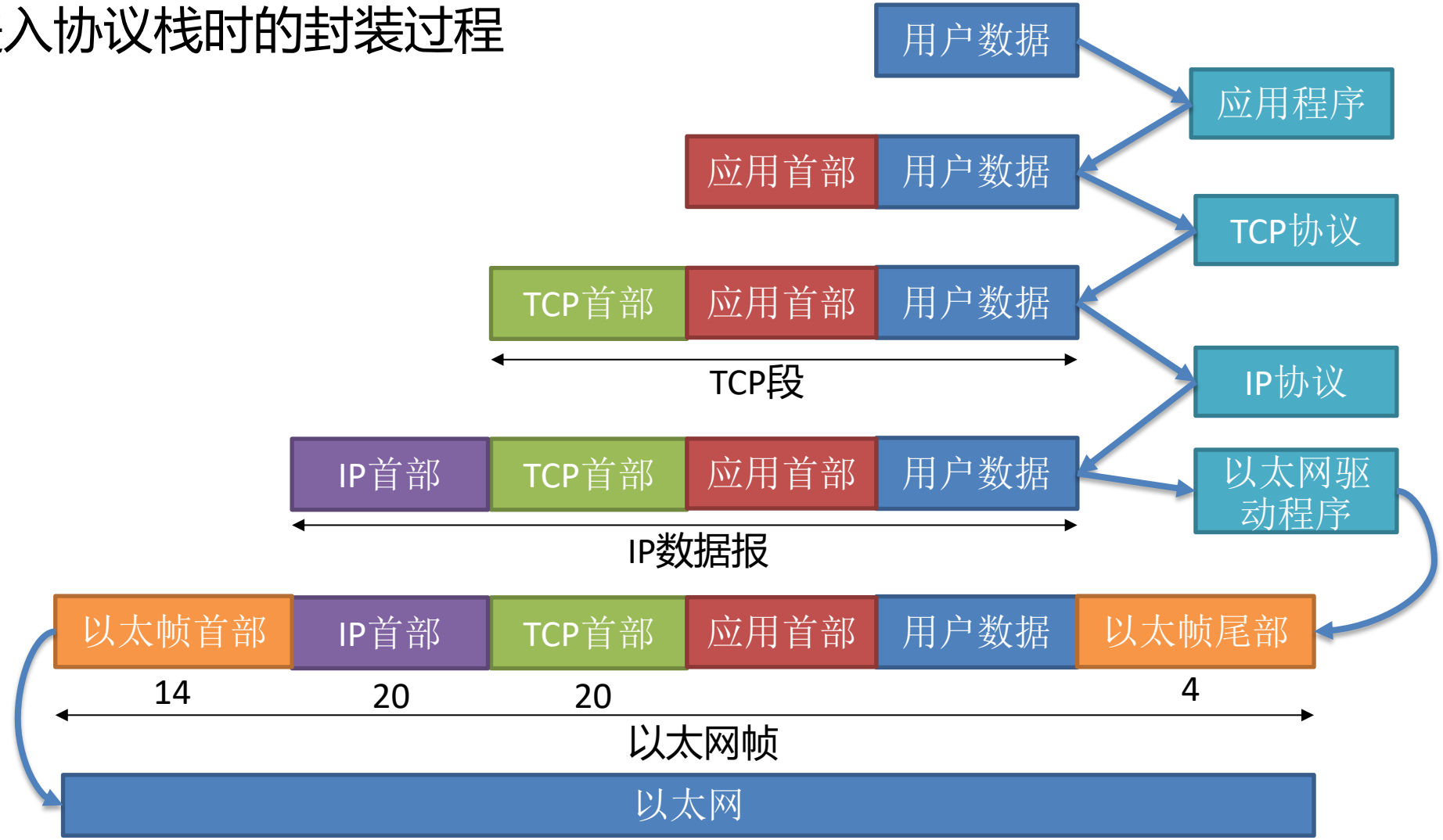
- OSI七层模型对层次划分的很细，具有较高的科学性，但是缺点是过于复杂了
- 结果就是起源于ARPANET项目中的TCP/IP四层模型成为了主流。

TCP/IP分层模型概述

- 由于TCP/IP协议栈中的协议数量众多，比较典型的如下：
  - 应用层：HTTP，DNS，SSH，FTP，DHCP
  - 传输层：TCP，UDP
  - 网络层：IP，ICMP，IGMP，IPsec， ARP， RARP
  - 链路层：WI-FI，Ethernet
- OSI模型和TCP/IP模型都是分层模型，为什么要分层？
  - 1.为了兼容更多的网络设备和操作系统
  - 2.分层可以使各层协议之间解耦合，适合后期协议版本更替
  - 3.分层可以让开发人员专注于其所开发的协议或程序所处的层次，只需在本层做好兼容即可。
  - 4.便于协议推广

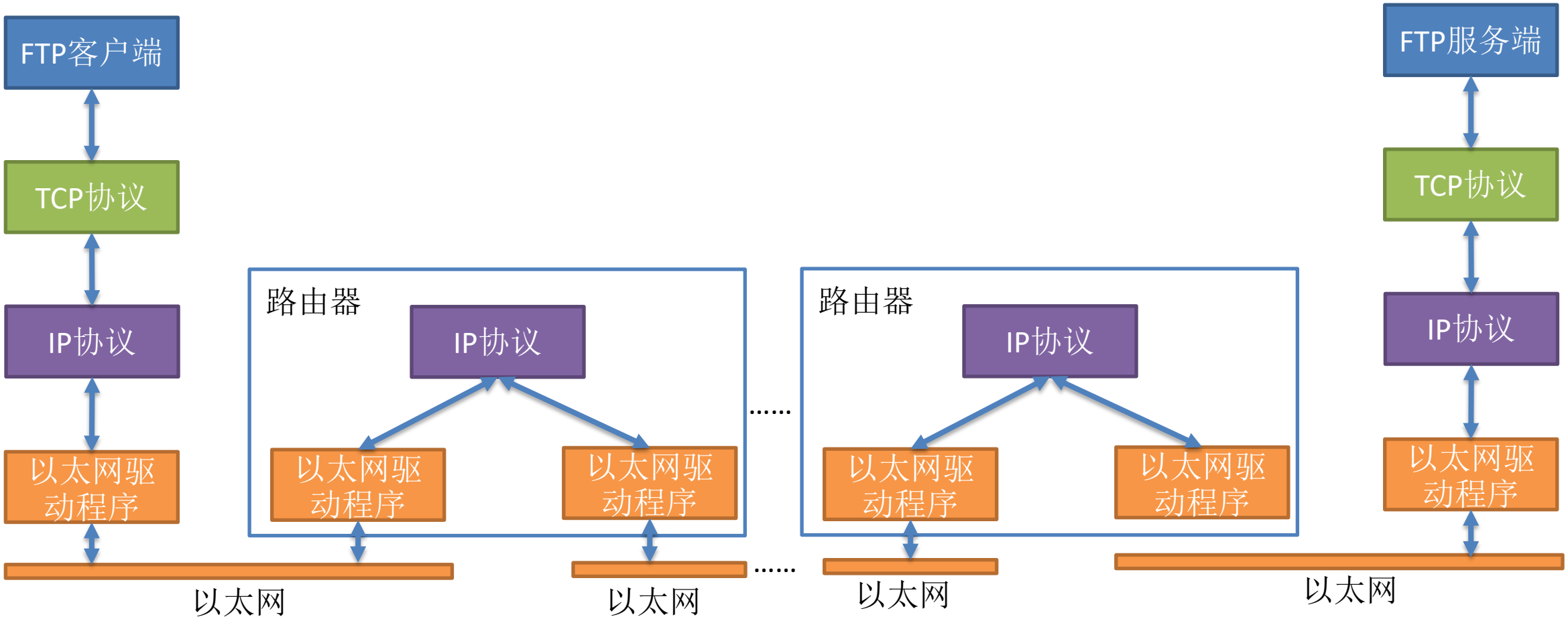
TCP/IP分层模型概述

- 用户数据进入协议栈时的封装过程



TCP/IP分层模型概述

- TCP/IP协议数据传输模型（FTP为例）



数据链路层

- 数据链路层又分为两个子层：
  - 逻辑链路控制（Logical Link Control）子层
  - 媒体接入控制（Media Access Control）子层

数据链路层

- 关于逻辑链路控制子层：由于目前绝大所多数TCP使用的网络均是DIX Ethernet V2标准，而不是IEEE 802.3 LAN，所以LLC层几乎被弃用。

- LLC层仍在使用的协议是STP协议，也叫生成树协议，通过协商的方法关闭某些交换机端口，从而保证该网络是一个无回路的树形拓扑结构。
- STP协议的意义：
  - 1.防止链路层广播风暴
  - 2.防止多帧复制
  - 3.防止MAC地址表不稳定

数据链路层

- 媒体接入控制（Media Access Control）子层
- 功能：

发送

  - 封装上层的IP数据包
  - 向以太网帧写入自己的物理地址为源地址
  - 通过ARP缓存表查询目标IP地址的物理地址
  - 将目标物理地址写入以太网帧
  - 等待**合适**的时机通过网卡发送

```
以太网适配器 以太网:

   连接特定的 DNS 后缀 . . . . . . . : lan
   描述. . . . . . . . . . . . . . . : Intel(R) Ethernet Connection (2) I219-V
   物理地址. . . . . . . . . . . . . : 70-85-C2-7D-92-69
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::a0db:3b36:4e45:f460%16(首选)
   IPv4 地址 . . . . . . . . . . . . : 192.168.123.12(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   获得租约的时间  . . . . . . . . . : 2020年1月4日 7:49:46
   租约过期的时间  . . . . . . . . . : 2020年1月5日 19:49:41
   默认网关. . . . . . . . . . . . . : 192.168.123.1
   DHCP 服务器 . . . . . . . . . . . : 192.168.123.1
   DHCPv6 IAID . . . . . . . . . . . : 108037570
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-25-84-0B-3A-70-85-C2-7D-92-69
   DNS 服务器  . . . . . . . . . . . : 192.168.123.1
   TCPIP 上的 NetBIOS . . . . . . . : 已启用
```

接收

  - 检查收到的以太网帧的目标地址是否与自己的物理地址相同
  - 如果相同，则解封移去以太网帧头和帧尾，移交给上一层处理
  - 如果不同，则丢弃这一帧

数据链路层

- MAC子层在合适的时间发送以太帧到物理层中（以有线网络为例）
  - 载波侦听多路访问/碰撞检测（CSMA/CD，在Ethernet及IEEE 802.3中使用）
  - 令牌环（Token Ring，在IEEE 802.5中使用）
  - 令牌环总线（Token Bus，在IEEE 802.4中使用）
  - 令牌传递（Token Passing，在FDDI中使用）

数据链路层

- 载波多路访问/碰撞检测（CSMA/CD）

- 要求设备在发送帧的同时要对信道进行侦听，以确定是否发生碰撞，若在发送数据过程中检测到碰撞，则进行如下碰撞处理操作：
  - 1.发送特殊阻塞信息并立即停止发送数据：特殊阻塞信息是连续几个字节的全1信号，此举意在强化碰撞，以使得其它设备能尽快检测到碰撞发生。
  - 2.在固定时间（一开始是1 contention period times）内等待随机的时间，再次发送。
  - 3.若依旧碰撞，则采用截断二进制指数避退算法进行发送。即十次之内停止前一次“固定时间”的两倍时间内随机再发送，十次后则停止前一次“固定时间”内随机再发送。尝试16次之后仍然失败则放弃发送。

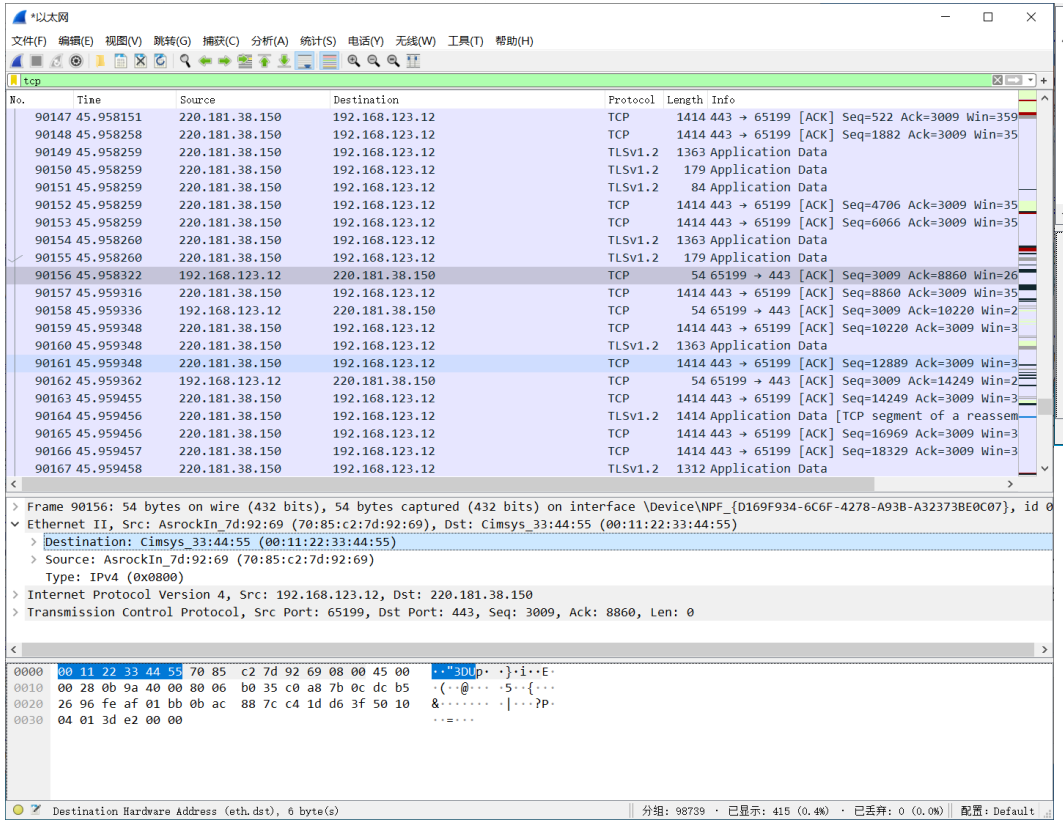
数据链路层

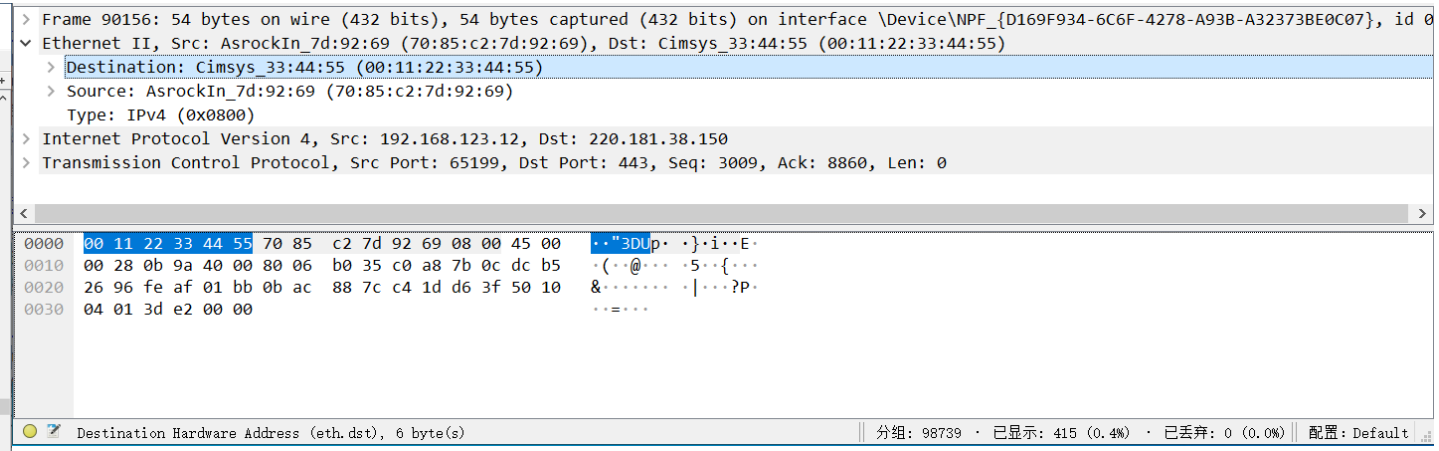
- Ethernet II协议的帧格式

D.MAC	S.MAC	Type	Data	FCS

- D.MAC：目标Mac地址
- S.MAC：源Mac地址
- Type：指Data中是什么协议的数据，用于决定解封之后的数据交给哪个上层协议继续处理。
  - 0x0800：IPv4
  - 0x0806：ARP
- Data：封装的上层协议数据
- FCS：校验位，4字节长，用于检验数据是否正确

数据链路层



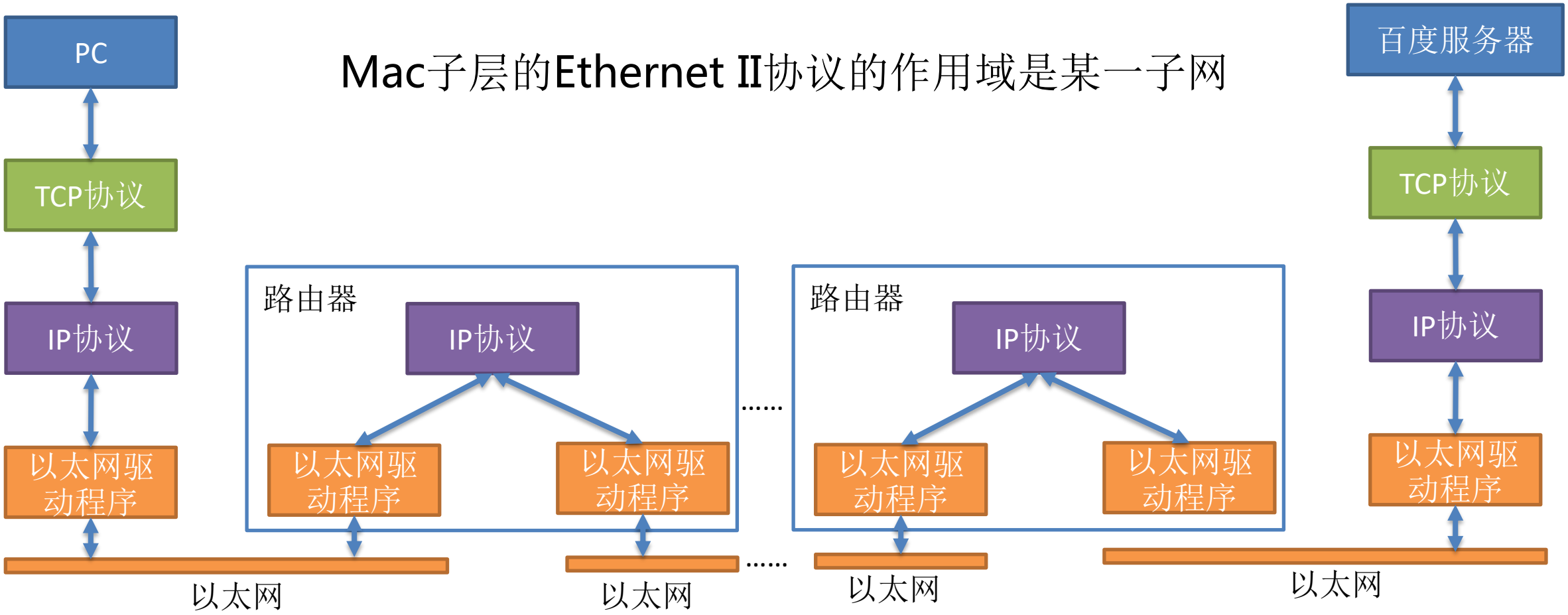


Wireshark抓不到FCS，是因为有些型号的网卡会自动除去FCS，再传递给系统

为什么访问百度的请求，目标D.MAC是“00:11:22:33:44:55”(我的路由器mac地址），而不是百度机房服务器的mac地址？

数据链路层

Mac子层的Ethernet II协议的作用域是某一子网

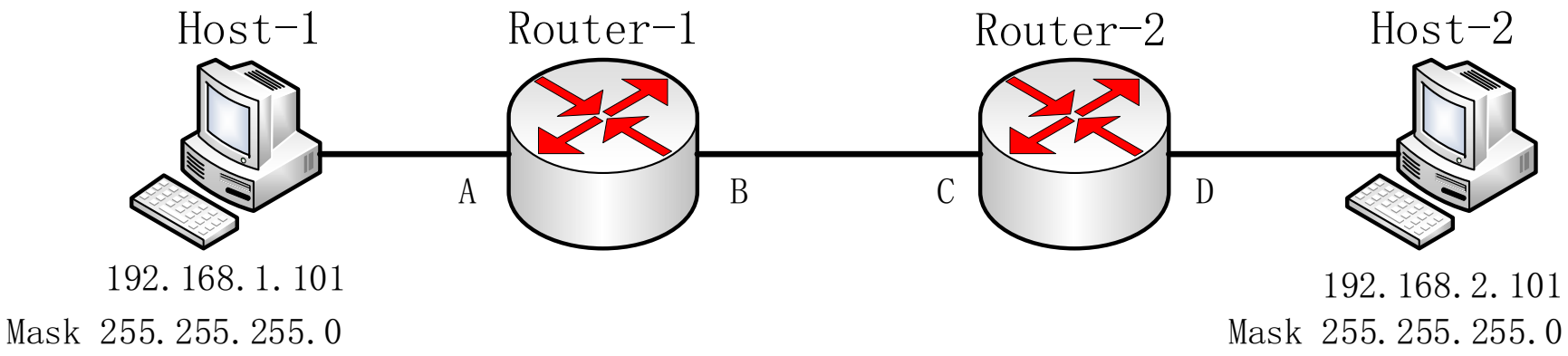


网络层

- **数据链路层是解决同一子网内节点之间的通信，而网络层主要解决不同子网之间的通信。**

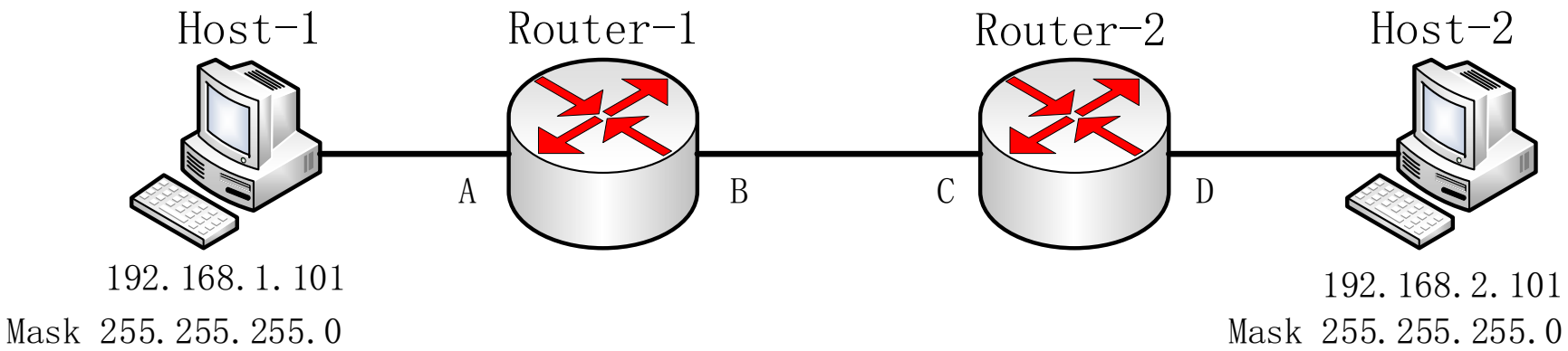
- 网络层主要任务：通过路由算法，为报文或分组通过通信子网选择最适当的路径。该层控制数据链路层与物理层之间的信息转发，建立、维持与终止网络的连接。

网络层



- 1.通过子网掩码发现不是同一子网，查询本机路由表发现需要网关Router-1转发
- 2.Host-1通过ARP缓存表或ARP请求获取网关的A口的MAC地址
- 3.Host-1将本机MAC作为源地址，Router-1的A口MAC作为目标地址，发送以太帧
- 4.Rotuer-1收到以太帧后，发现是发给自己的，因此解封，通过查询路由表，可知下一跳指向Router-2

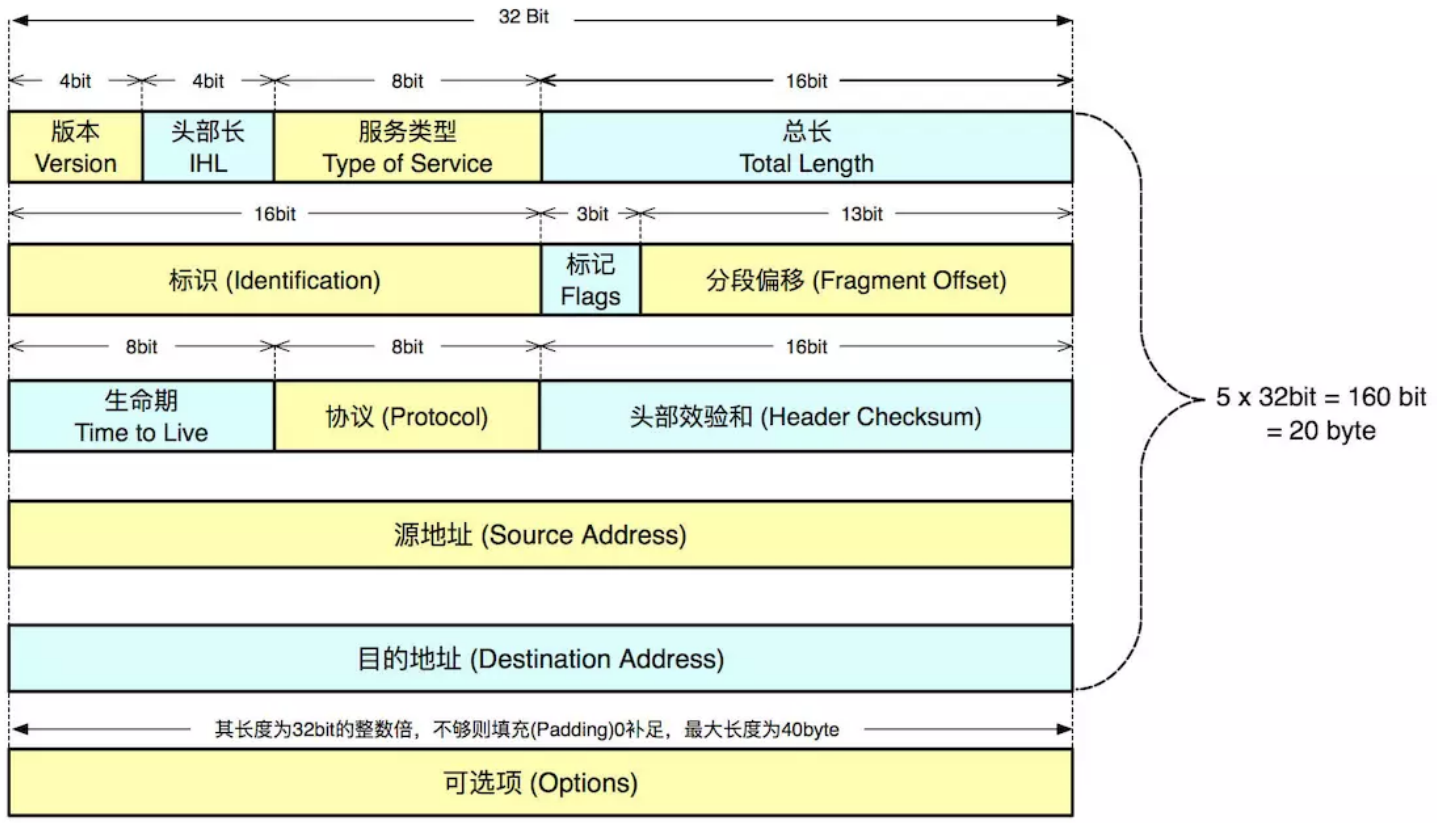
网络层



- 5.Router-1通过ARP缓存表或ARP请求到了Router-2的C口的MAC，因此原来以太帧的数据在Router-1的B口被重新包装，源MAC是Router-1的B口MAC，目标MAC是Router-2的C口MAC。
- 6.Router-2收到以太帧后，发现是发给自己的，因此解封，发现目标IP处于自己D口所在子网中，因此通过ARP请求到Host-2的mac地址后，在Router-2的D口再次重新包装以太帧，发往Host-2

网络层

- 路由表记录着从一个网络到另一个网络的路径，路由器是组成当今网络的核心网络设备，路由器依据路由表工作。



网络层-攻击

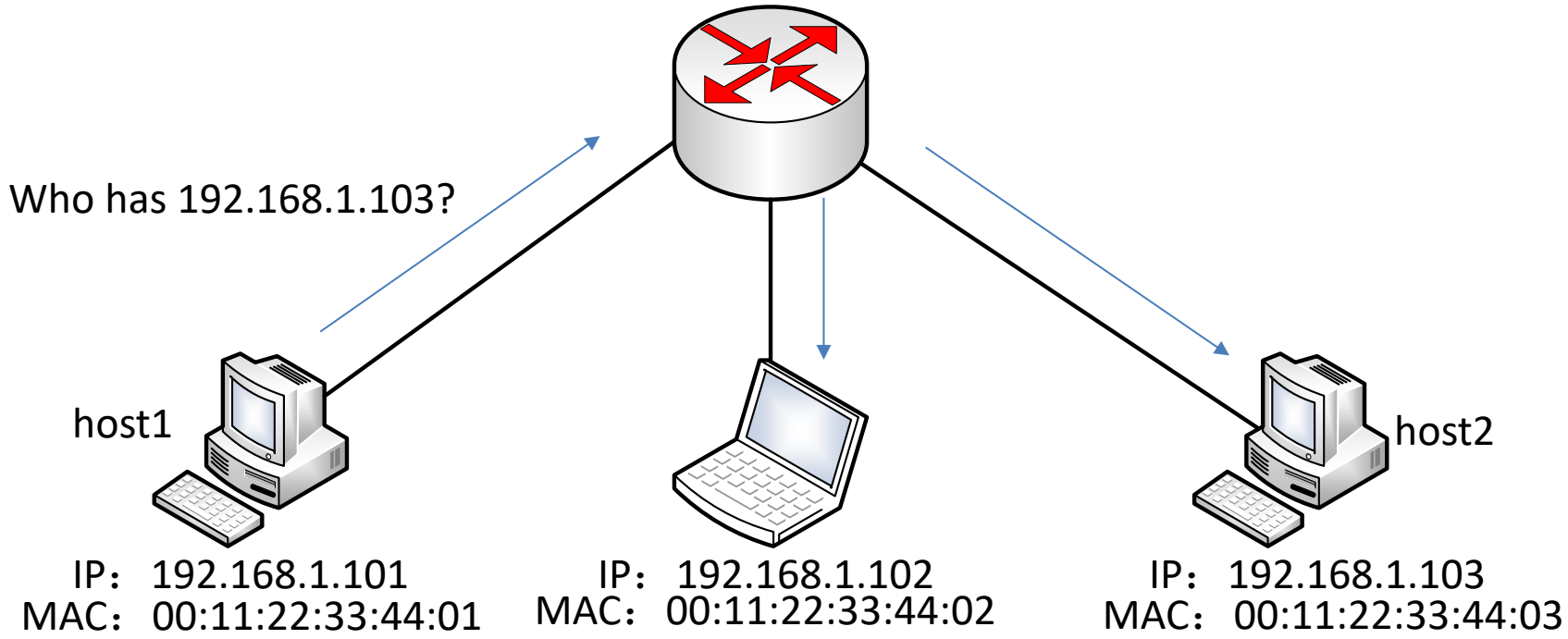
- 简要介绍ARP

Source	Destination	Protocol	Length	Info
Cimsys_33:44:55	AsrockIn_7d:92:69	ARP	60	Who has 192.168.123.12? Tell 192.168.123.1
AsrockIn_7d:92:69	Cimsys_33:44:55	ARP	42	192.168.123.12 is at 70:85:c2:7d:92:69

- ARP的特性：
  - 1.使用广播或单播的方式向子网中所有主机发送请求，以获取目标主机的MAC
  - 2.对于一次ARP请求，以先到的回应为准，后续到达的回应将被舍弃

网络层-攻击

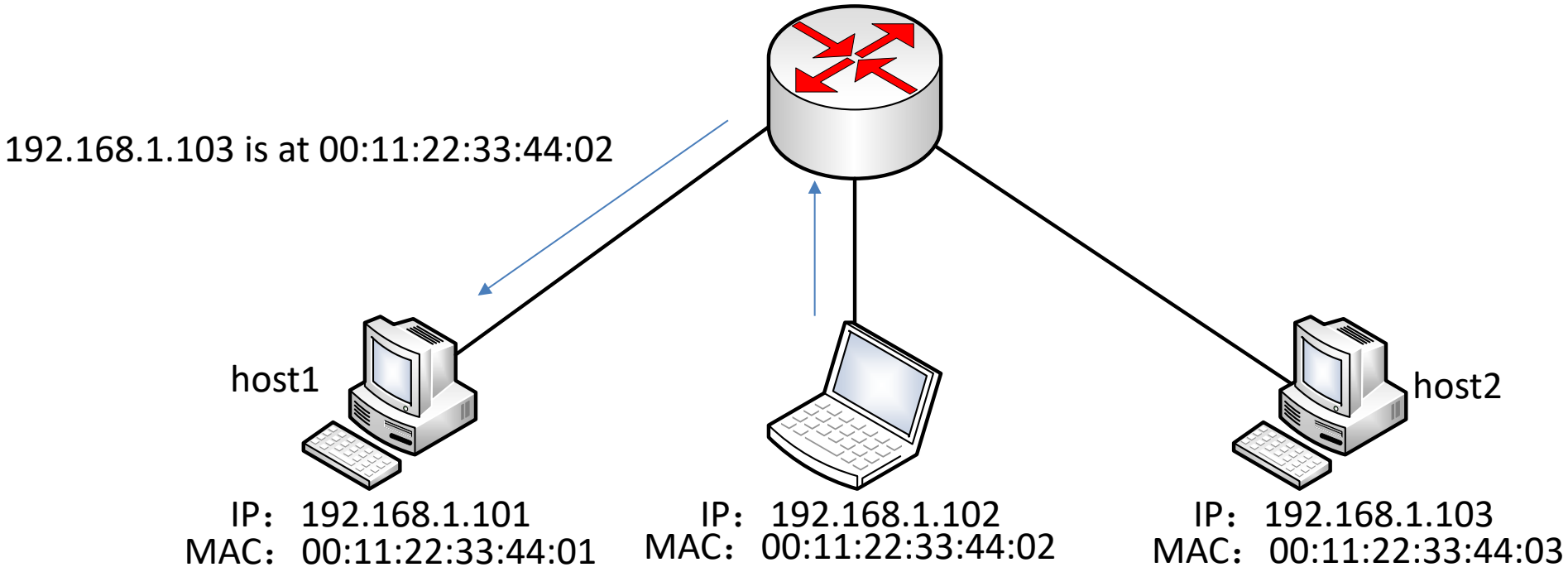
- ARP攻击原理概要



IP	MAC

网络层-攻击

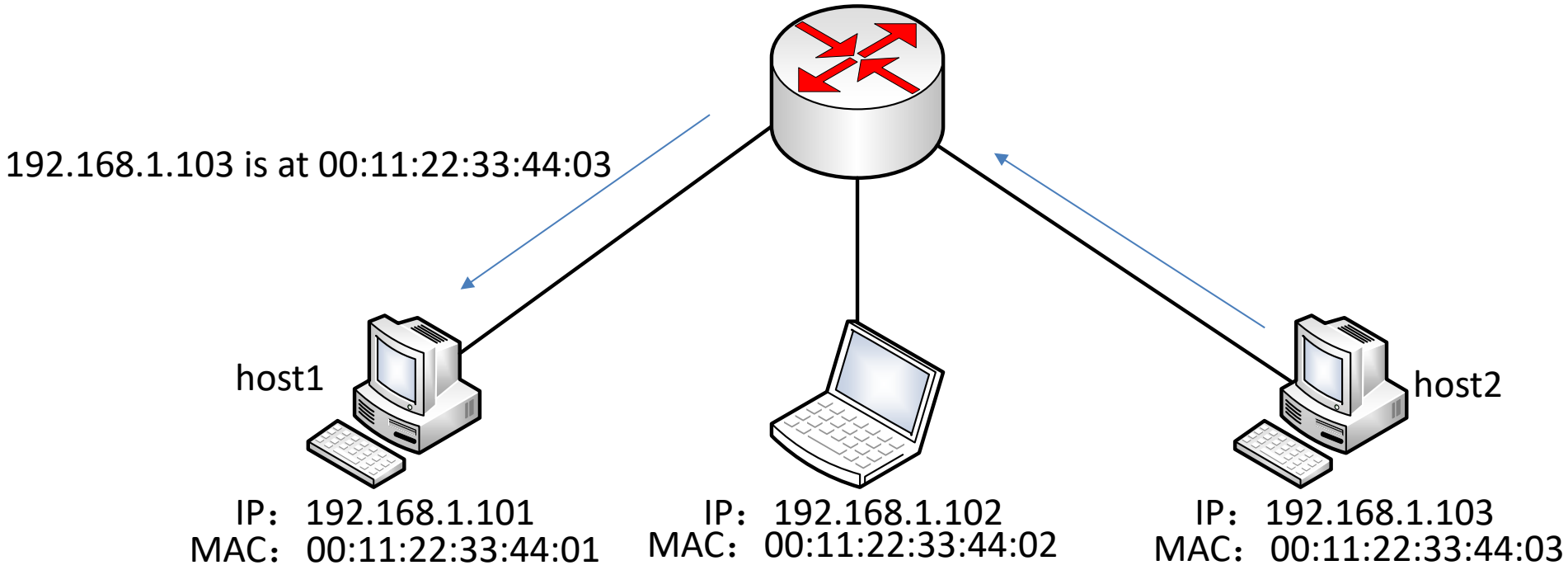
- ARP攻击原理概要



IP	MAC
192.168.1.103	00:11:22:33:44:02

网络层-攻击

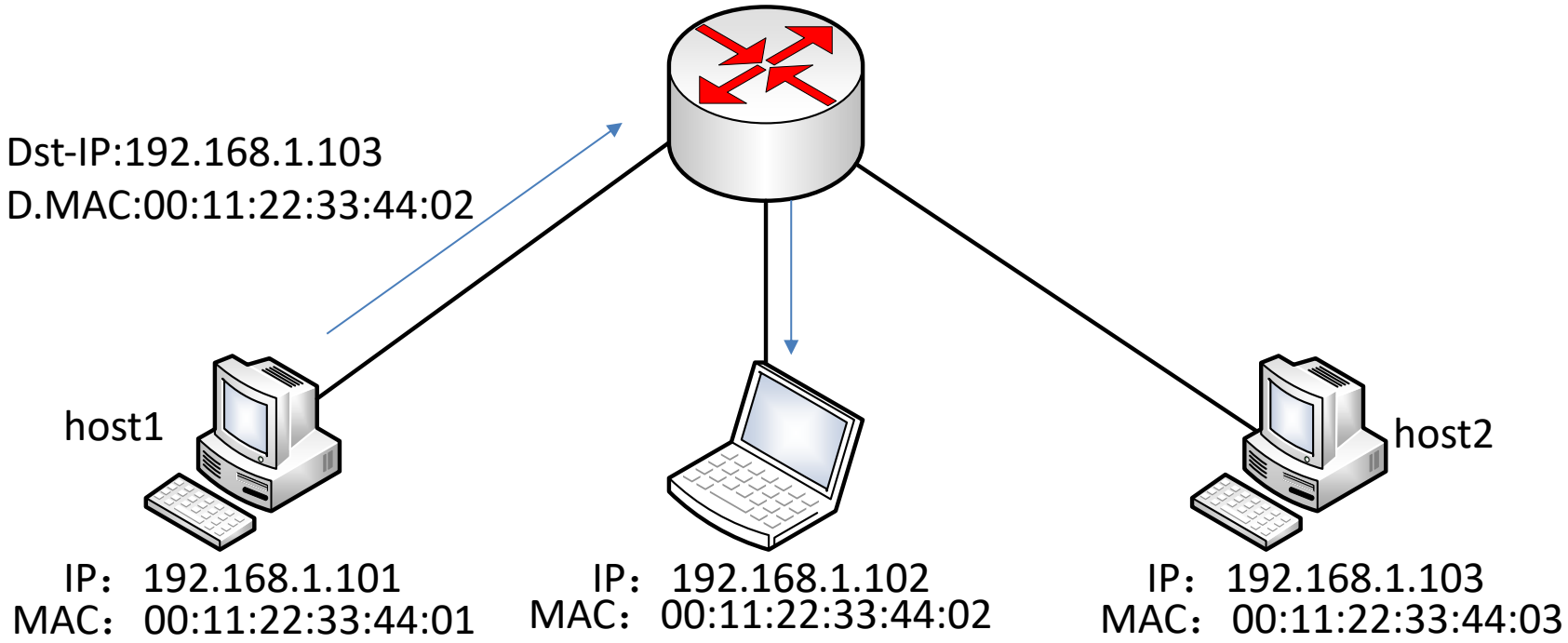
- ARP攻击原理概要



IP	MAC
192.168.1.103	00:11:22:33:44:02

网络层-攻击

- ARP攻击原理概要



IP	MAC
192.168.1.103	00:11:22:33:44:02

传输层

- **网络层是解决跨网段的两个主机之间传输数据的问题，而传输层解决的问题是两个主机进程之间端到端通信的问题。**
- 网络层只是根据网络地址将源结点发出的数据包传送到目的结点，而传输层则负责将数据可靠地传送到相应的端口。

- 最主要的两个传输层协议：TCP和UDP

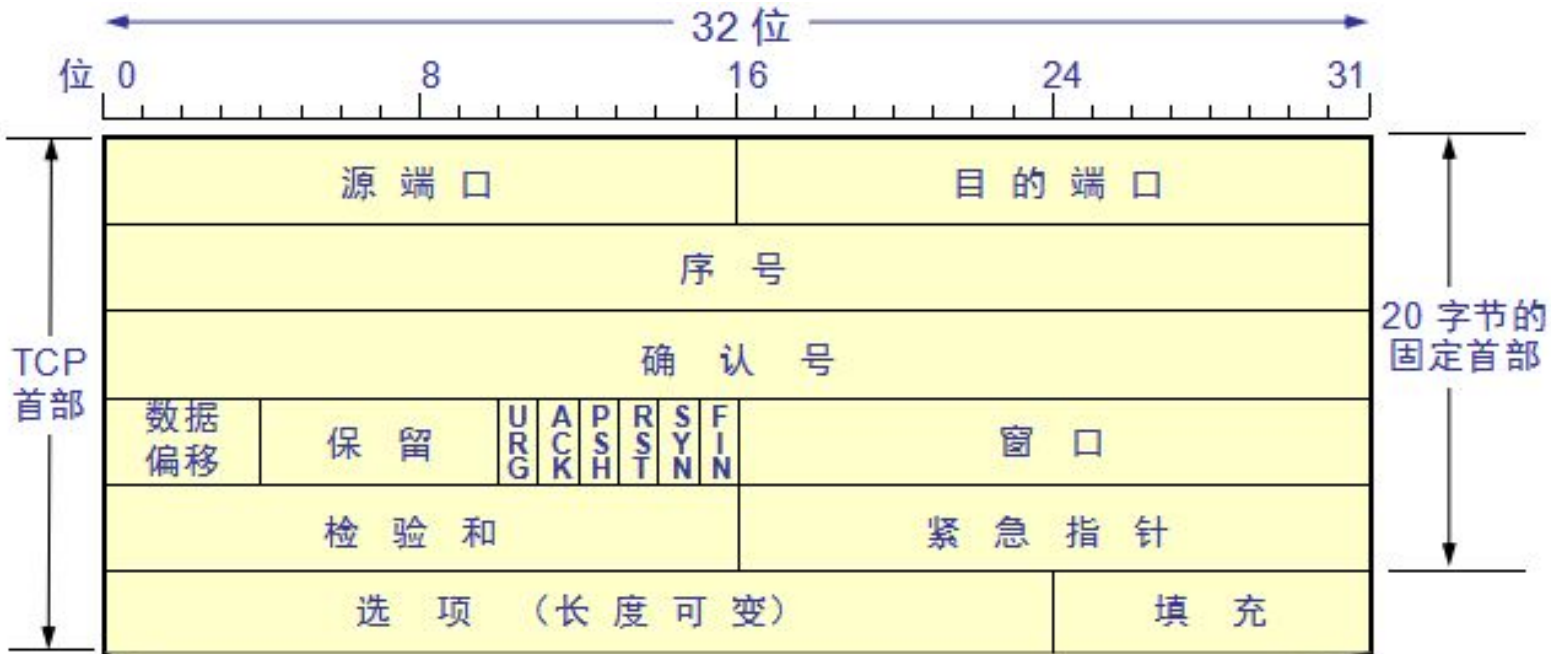
传输层

- TCP和UDP的主要区别

	TCP	UDP
是否连接	面向连接	面向非连接
传输可靠	可靠	不可靠
应用场景	传输少量重要数据	传输大量数据
速度	慢	快

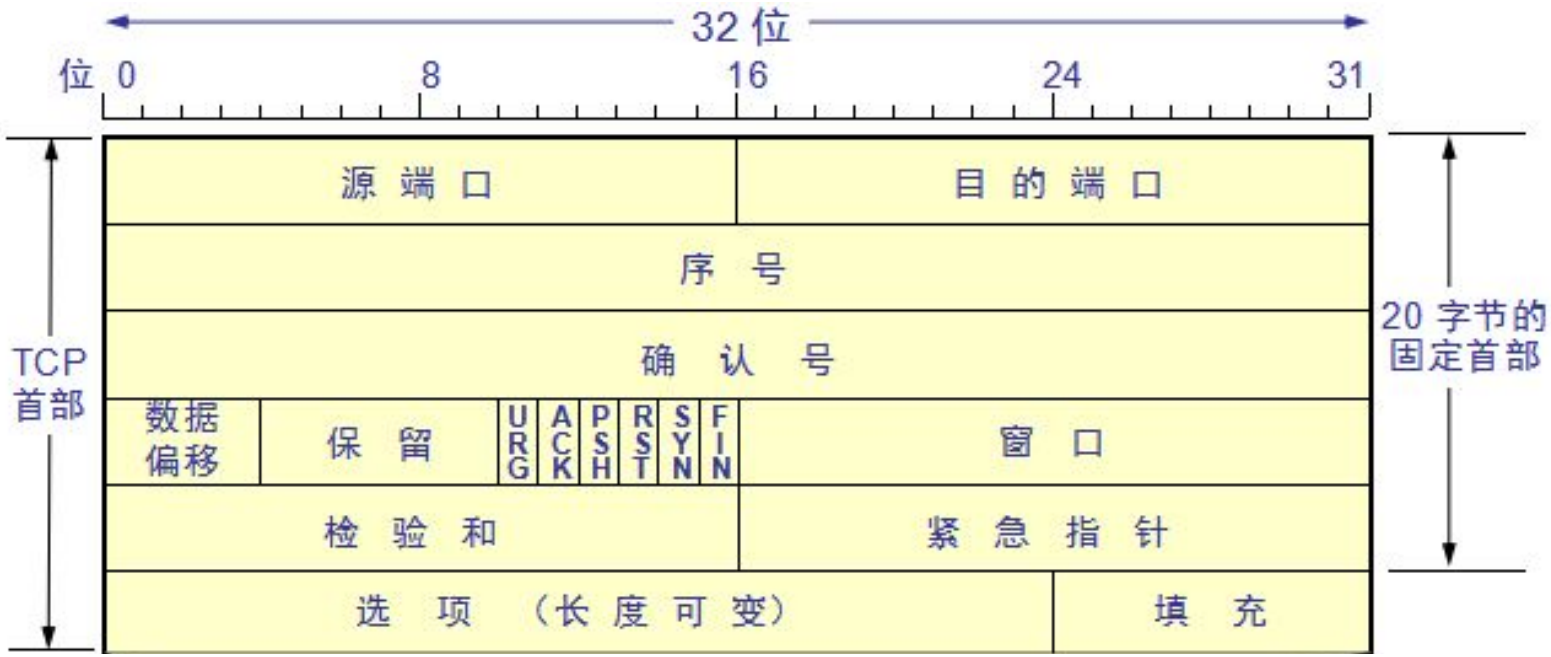
- TCP的应用场景：文件传输（FTP），Web服务（HTTP，HTTPS），邮件服务（POP3、SMTP）等
- UDP的应用场景：流视频（Web上的在线视频），语音通话（QQ，微信的视频通话等）

传输层-TCP



- URG:紧急指针是否有效
- ACK:表示确认号是否有效，携带ACK标志的报文段也称确认报文段
- PSH:提示接收端应用程序应该立即从TCP接受缓冲区中读走数据

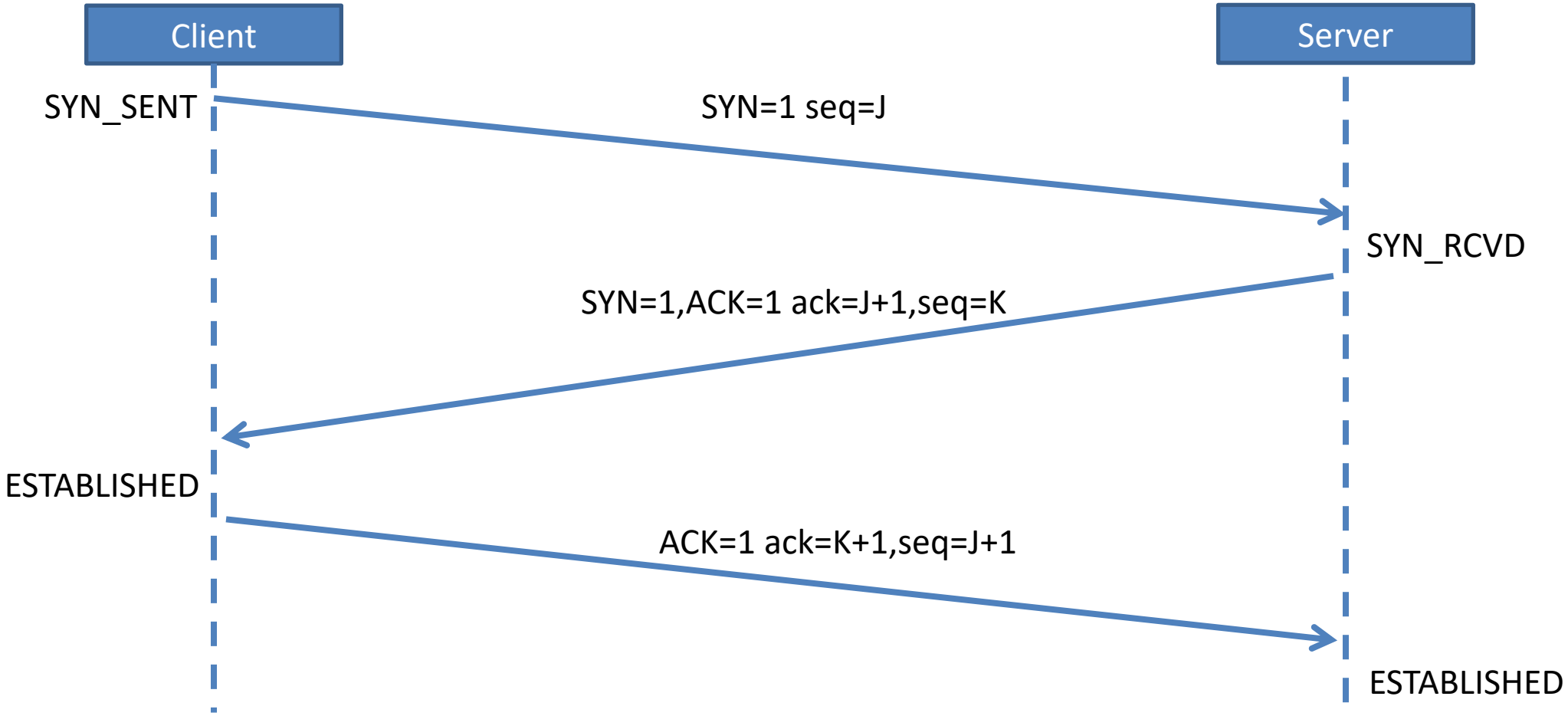
传输层-TCP



- RST:表示要求对方重建连接。带RST标志的TCP报文段也叫复位报文段。
- SYN:表示建立一个连接，携带SYN的tcp报文段为同步报文段
- FIN:表示告知对方本端要关闭连接了，之后进入关闭流程

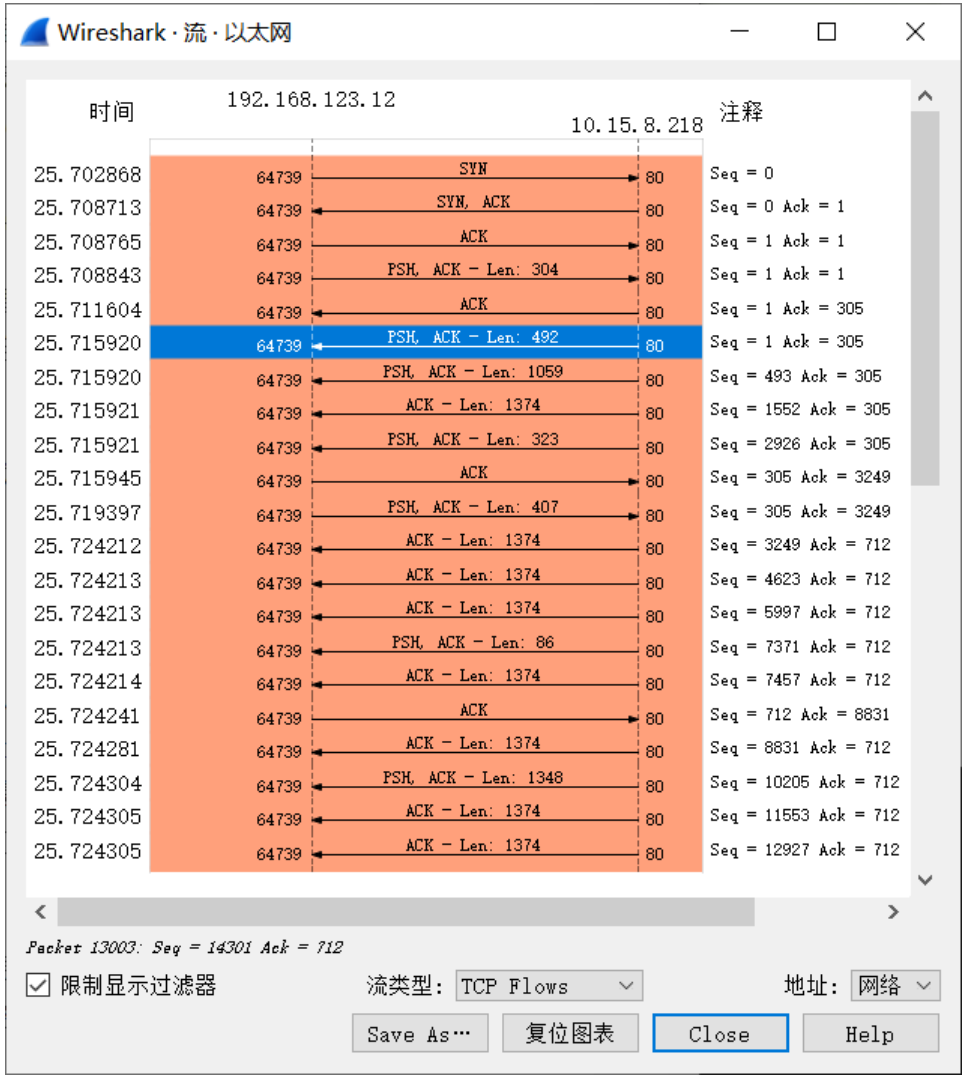
传输层-TCP

- 关于TCP的“面向连接”——三次握手



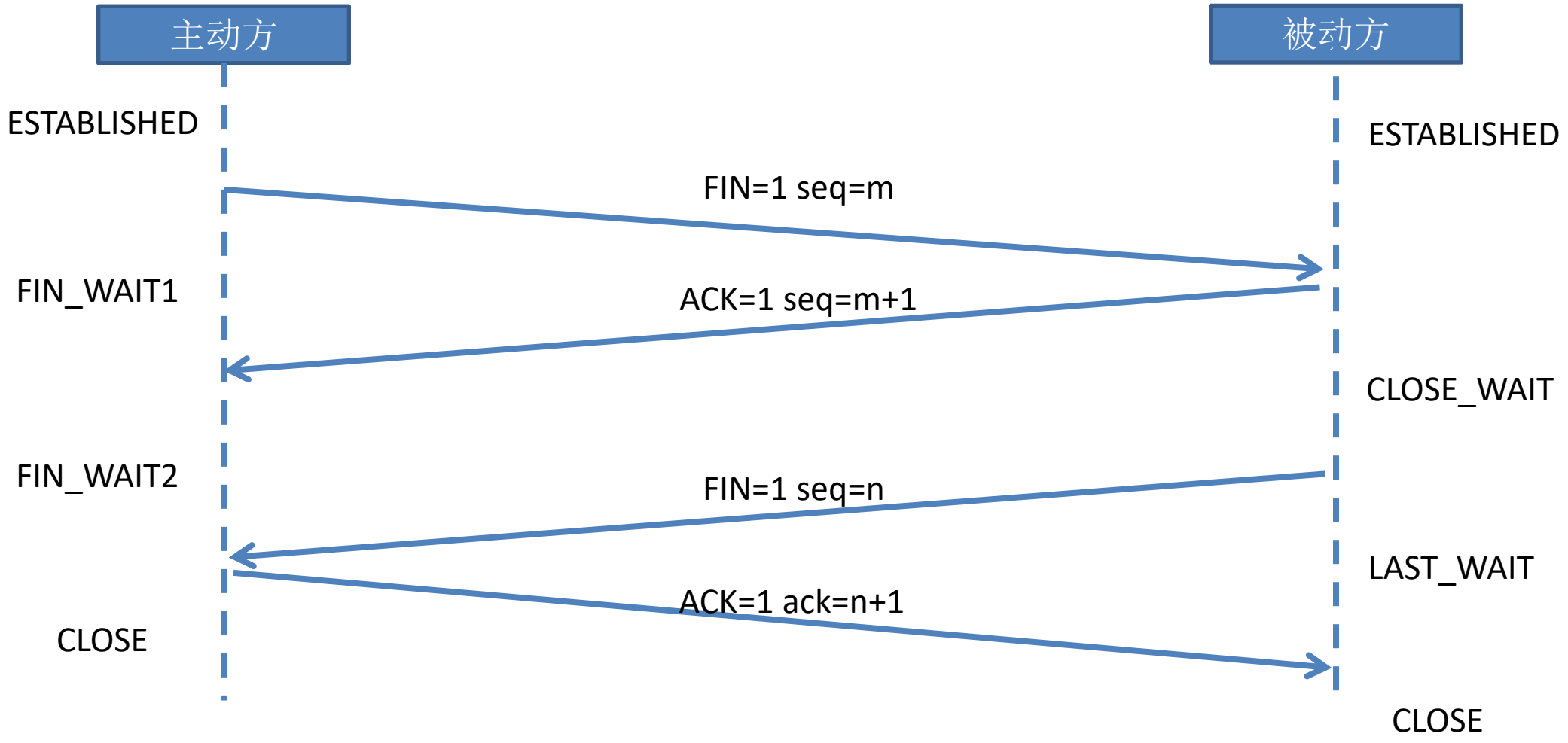
传输层-TCP

- 关于TCP的“可靠性”——序列码、确认码和校验和

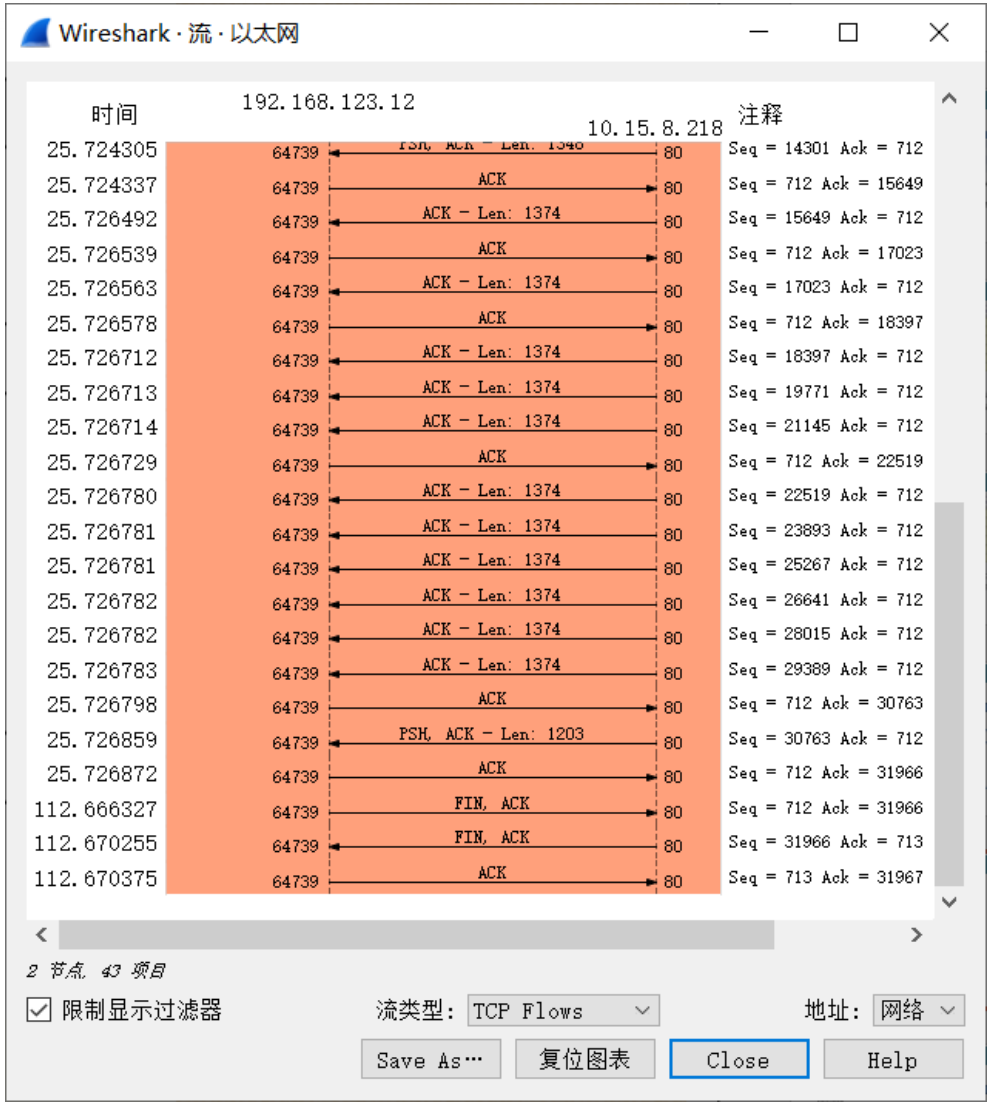


传输层-TCP

- 连接断开：方法一：FIN四次挥手



传输层-TCP

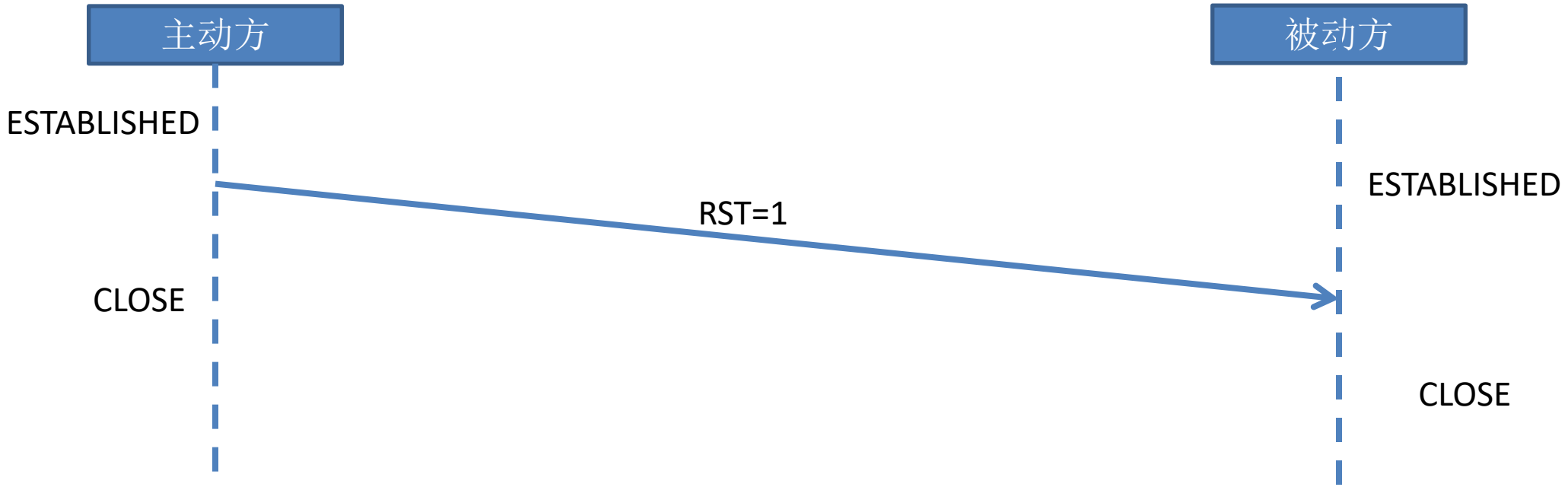


有时候第二次挥手和第三次握手会合并成一个，这样可以加快连接关闭速度

传输层-TCP

- 连接断开：方法二：RST一次断开连接

- 发送RST包关闭连接时，直接就丢弃缓存区的包发送RST包。而接收端收到RST包后，也不必发送ACK包来确认。



传输层-TCP-攻击

- SYN洪水攻击
  - 通过发送大量的SYN连接包到服务器，占满服务器的连接池，是DOS和DDOS攻击的途径之一
- RST攻击
  - 通过伪造源IP，恶意关闭其他主机与服务器之间的连接

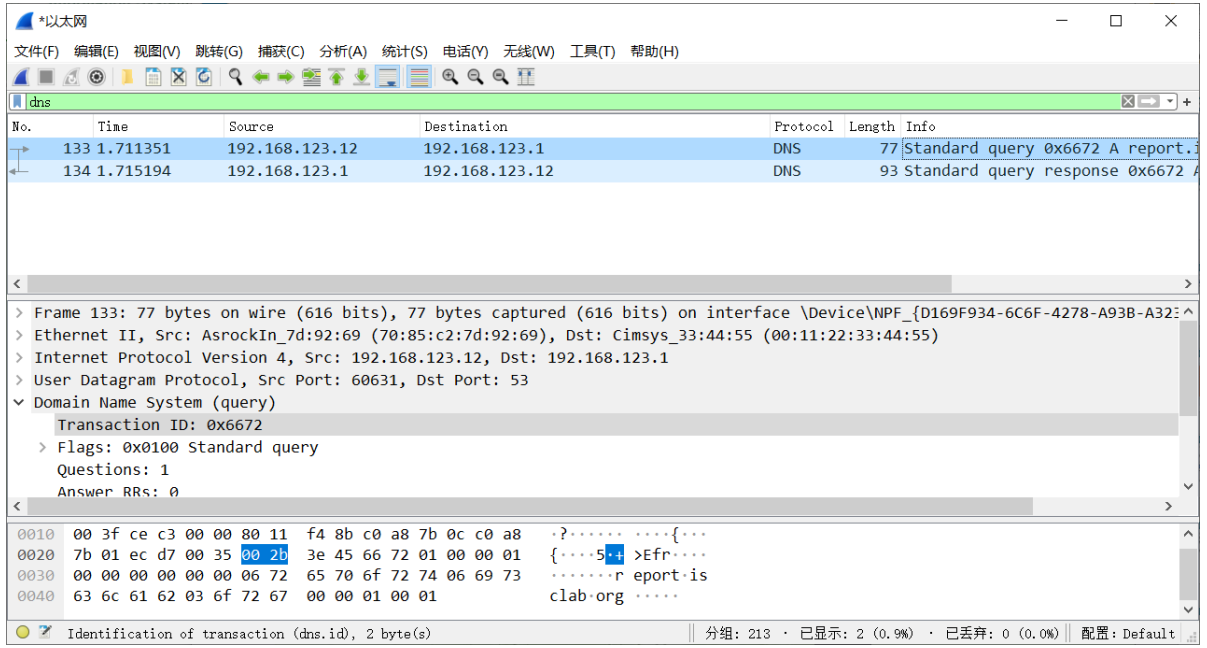
连接案例

http://report.isclab.org/
搜索...
BFS学术报告评分、工作总...
信息系统及安全对抗实验中心
Information System and Security & Countermeasures Experimental Center
厚德明理
慎独求是
BFS学术报告评分、工作总结报告提交系统
用户名:
用户密码:
登录
版权所有©2013 北京理工大学信息系统及安全对抗实验中心

连接案例

- Step1：DNS解析
  - 1.根据路由表找到去往DNS服务器的下一跳IP
  - 2.使用ARP协议找到下一跳的MAC地址
  - 3.将DNS协议内容封装（DNS->UDP->Ethernet II->比特流）
  - 4.通过网卡发送到物理链路上

  - 1.接收到DNS回应数据包
  - 2.通过协议栈逐层解封
    - Ethernet II->UDP->DNS
  - 3.保存目标站点的IP地址，准备连接



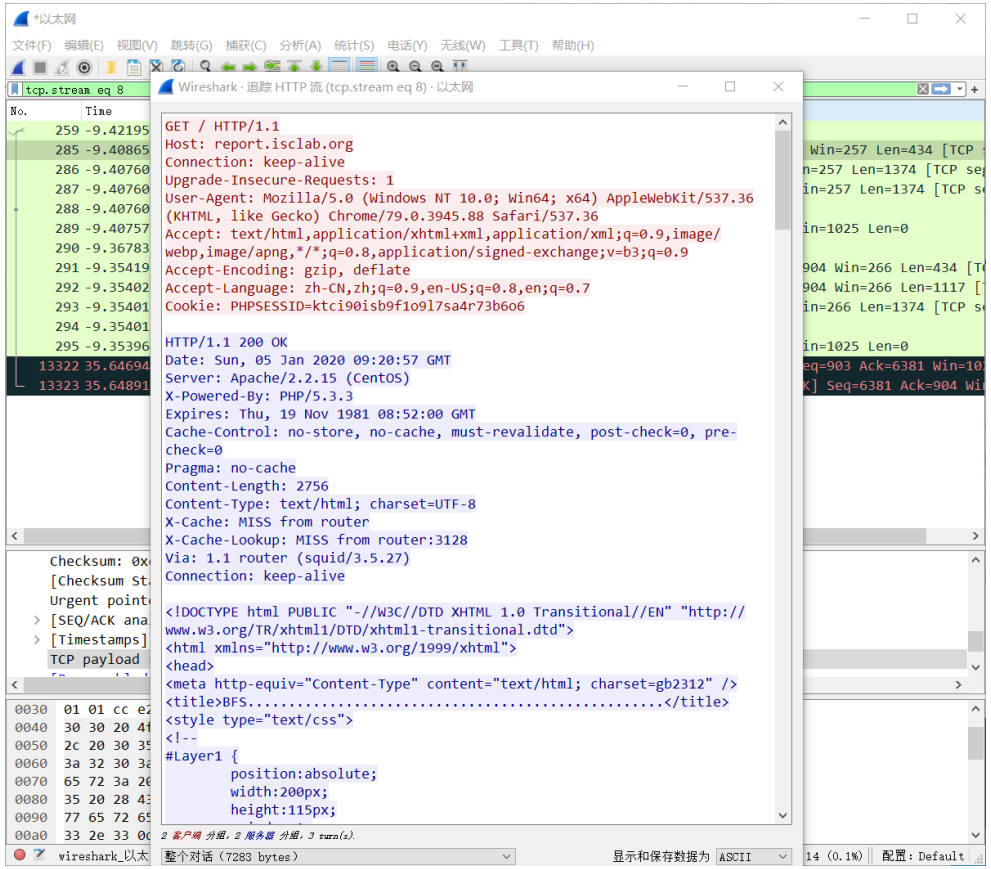
连接案例

- Step2：TCP连接建立（从此步开始ARP寻址略过）
  - 1.监听一个随机端口，将这个端口号作为TCP的源端口号，80端口号作为目标端口号，封装SYN请求的TCP段，传给下一层进行处理。
  - 2.根据上一步得到的IP、本机IP和上一层传递过来的数据封装成IP数据报，传递给下一层继续进行处理
  - 3.链路层发送（此步略）
  - 4.TCP三次握手之后TCP连接建立成功
  - 5. 之后将根据端口号信息，传递指定的浏览器进程

192.168.123.12	10.15.8.218	TCP	66	51573 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SA
10.15.8.218	192.168.123.12	TCP	66	80 → 51573 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=137
192.168.123.12	10.15.8.218	TCP	54	51573 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0

连接案例

- Step3：HTTP请求
- 1.HTTP使用GET请求以此请求页面上的所有资源
- 2.随着资源的加载，浏览器完成页面渲染



关于网络编程

- 现代操作系统中，用户只能指定应用层数据，其他层分别由系统内核（传输层和网络层）以及驱动程序（链路层）完成，系统在用户态留好了接口，被称为socket，使用socket可以轻松地指定传输层协议和网络层协议，并由操作系统自动完成，开发者只需专注于提供和处理应用层数据即可。
- （分层设计的优势）

道德经

上善若水。水善利万物而不争，处众人之所恶，故几於道。居善地，心善渊与善仁，言善信，正善治，事善能，动善时。夫唯不争，故无尤。

谢谢！