电子科技大学
University of Electronic Science and Technology of China

网络安全技术

赵洋 副教授

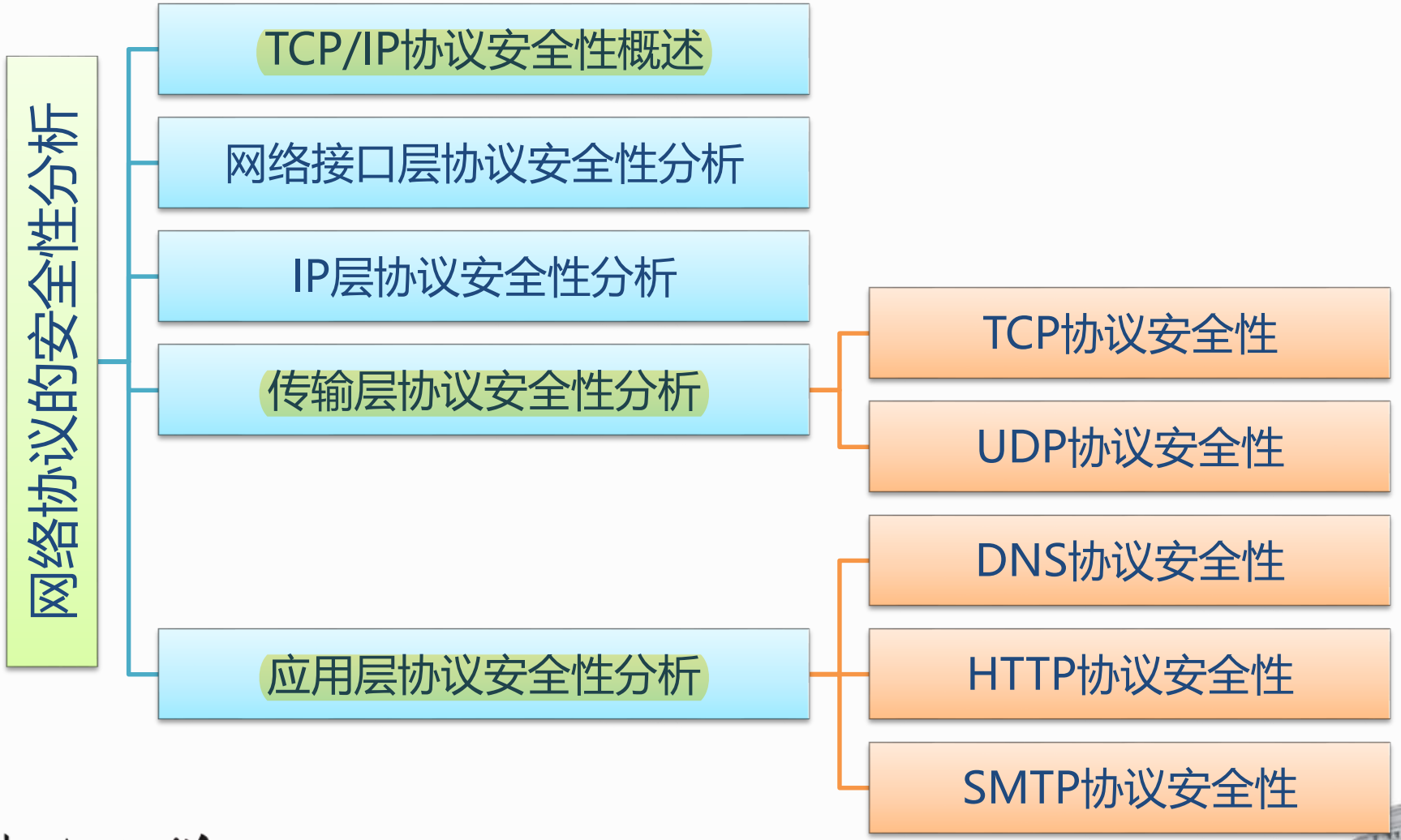
电子科技大学 信息与软件工程学院

2019年9月10日星期二

第二讲 网络协议的安全性分析

了解网络协议的安全状况、理解网络协议安全威胁产生的原因，掌握常见的网络协议安全威胁的基本工作原理和过程。

内容安排


网络协议的安全性分析
TCP/IP协议安全性概述
网络接口层协议安全性分析
IP层协议安全性分析
传输层协议安全性分析
TCP协议安全性
UDP协议安全性
应用层协议安全性分析
DNS协议安全性
HTTP协议安全性
SMTP协议安全性

1、TCP/IP协议安全概述 —— 协议基础

TCP协议简介

- TCP/IP网络系统最初是20世纪60年代，冷战时期由美国国防部主导开发的阿帕网（Aparnet），目的是为美国军方作为冷战时期对标准数据通信系统的支撑。

1、TCP/IP协议安全概述 —— 协议基础

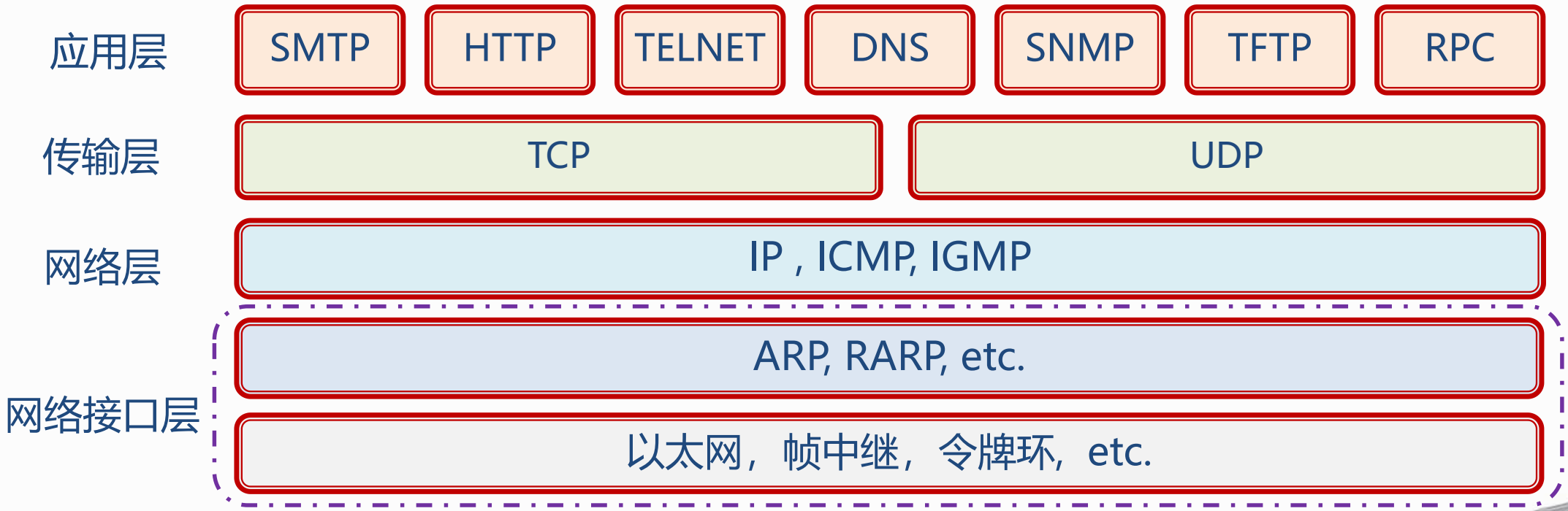
TCP/IP协议栈

应用层	• 直接为网络应用提供服务，使得应用程序能通过网络收发数据
传输层	• 为应用层实体提供端到端的通信功能，提供有连接的服务和无连接的服务
网际互联层	• 提供可靠、无连接的数据报传递服务。网际层负责对数据包进行路由选择
网络接口层	• 负责在实际网络中传输、发送、接收端到端数据包

◆OSI模型是在协议开发前设计的, 具有通用性。TCP/IP是先有协议集然后建立模型, 不适用于非TCP/IP网络。
◆实际市场应用不同（OSI模型只是理论上的模型，并没有成熟的产品，而TCP/IP已经成为“实际上的国际标准”）

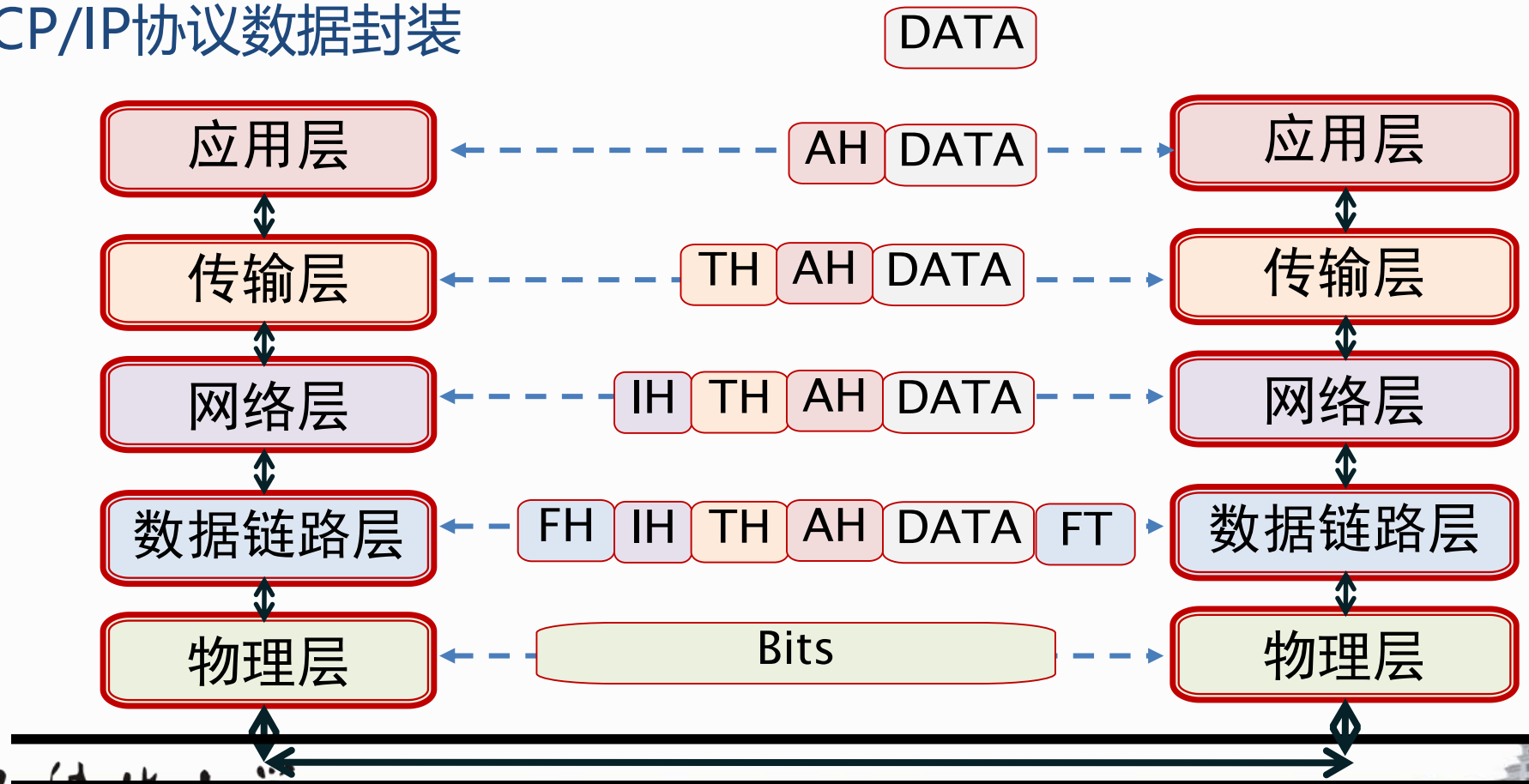
1、TCP/IP协议安全概述 —— 协议基础

TCP/IP协议族



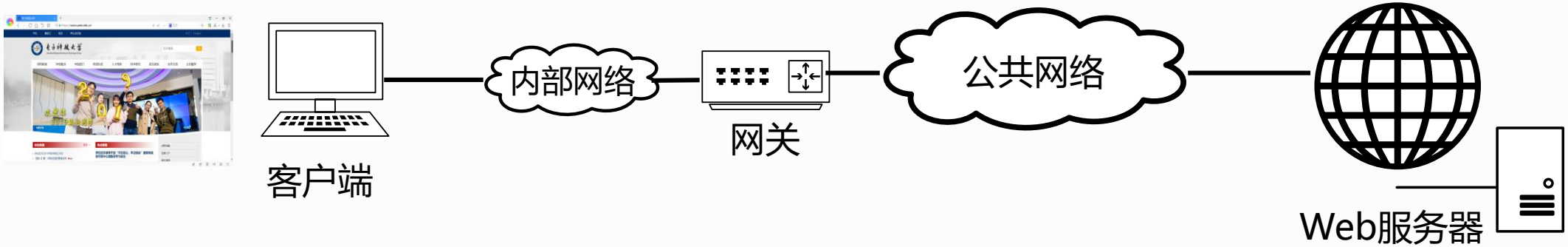
1、TCP/IP协议安全性概述 —— 协议基础

- TCP/IP协议数据封装



1、TCP/IP协议安全性概述 —— 协议基础

Web访问过程

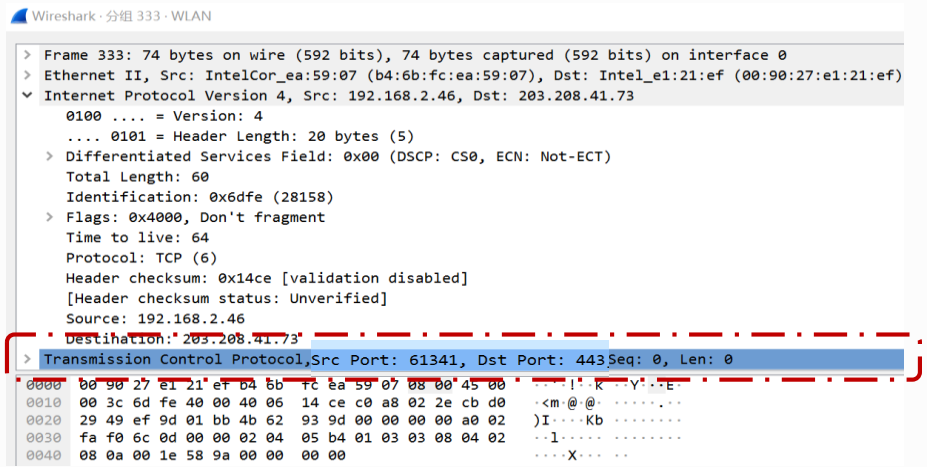


正确的MAC帧头 | 正确的IP包头 | 正确的TCP报头 | GET https://www.uestc.edu.cn

1、TCP/IP协议安全性概述 —— 协议基础

◘ 正确的TCP报头

➢ 要访问https://www.uestc.edu.cn首先要和www.uestc.edu.cn服务器建立连接， 建立连接所使用的端口号由应用层协议指定。



TCP包头部分包括源端口、目的端口、TCP标志、TCP选项等内容。

正确的MAC帧头 | 正确的IP包头 | 正确的TCP报头 | GET https://www.uestc.edu.cn

1、TCP/IP协议安全性概述 —— 协议基础

正确的IP包头

- 目的IP地址通过本地缓存的host文件或通过DNS解析确定。

Wireshark · 分组 333 · WLAN

```
Frame 333: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: IntelCor_ea:59:07 (b4:6b:fc:ea:59:07), Dst: Intel e1:21:ef (00:90:27:e1:21:ef)
Internet Protocol Version 4, Src: 192.168.2.46, Dst: 203.208.41.73
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x6dfe (28158)
  > Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x14ce [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.2.46
    Destination: 203.208.41.73
```

```
0000  00 90 27 e1 21 ef b4 6b  fc ea 59 07 08 00 45 00   ··'·!··k ··Y···E·
0010  00 3c 6d fe 40 00 40 06  14 ce c0 a8 02 2e cb d0   ·<m·@·@· ·····,··
0020  29 49 ef 9d 01 bb 4b 62  93 9d 00 00 00 00 a0 02   )I····Kb ········
0030  fa f0 6c 0d 00 00 02 04  05 b4 01 03 03 08 04 02   ··l····· ········
0040  08 0a 00 1e 58 9a 00 00  00 00                     ····X··· ··
```

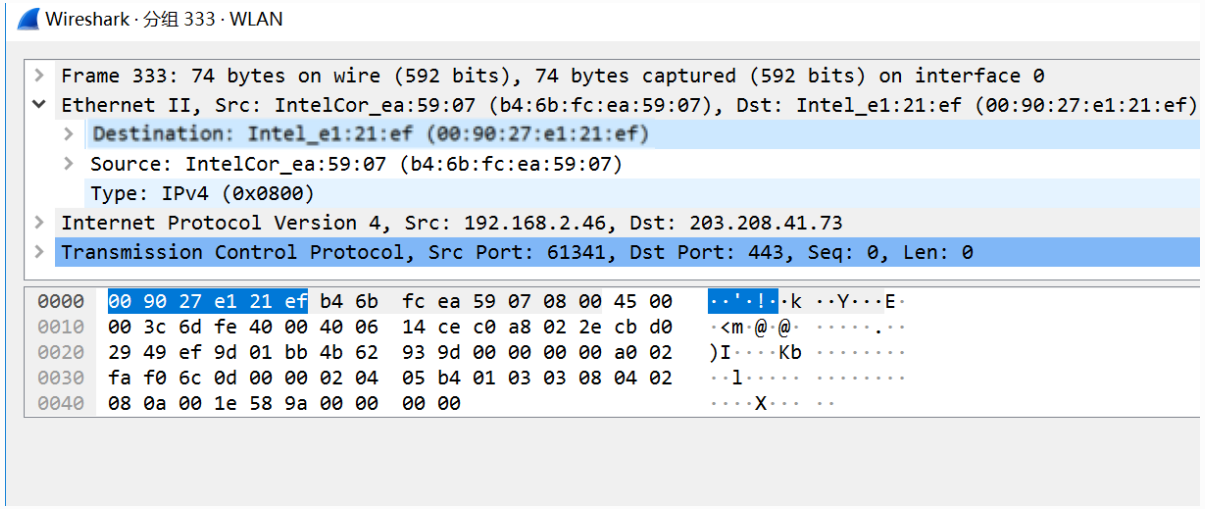
IP包头部分包括源IP地址、目的IP地址、IP标志等内容。

正确的MAC帧头 | 正确的IP包头 | 正确的TCP报头 | GET https://www.uestc.edu.cn

1、TCP/IP协议安全性概述 —— 协议基础

◘ 正确的MAC帧头

- 由路由表信息和ARP缓存信息，可以确定帧头的目的MAC地址。



MAC帧头部分包括前导码、帧开始符、目的MAC地址等内容。

正确的MAC帧头 | 正确的IP包头 | 正确的TCP报头 | GET https://www.uestc.edu.cn

1、TCP/IP协议安全性概述 —— 协议基础

◘ 主机路由表与ARP缓存

```
C:\Users\zhaoy>route print
===========================================================================
接口列表
 16...8c 16 45 ab 23 dd ......Intel(R) Ethernet Connection (4) I219-V
 11...00 ff 7c bd b5 68 ......Sangfor SSL VPN CS Support System VNIC
 10...02 00 4c 4f 4f 50 ......Npcap Loopback Adapter
 18...b6 6b fc ea 59 07 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  7...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
  8...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  5...b4 6b fc ea 59 07 ......Intel(R) Dual Band Wireless-AC 8265
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0    192.168.2.1    192.168.2.46     50
        127.0.0.0        255.0.0.0         在链路上         127.0.0.1    331
        127.0.0.1  255.255.255.255         在链路上         127.0.0.1    331
  127.255.255.255  255.255.255.255         在链路上         127.0.0.1    331
```

- route print显示当前主机的路由表信息
- DestIP & Netmask == Network Destination，选择相应的Interface和Gateway发送数据

```
C:\Users\zhaoy>arp -a

接口: 192.168.2.46 --- 0x5
  Internet 地址         物理地址              类型
  192.168.2.1           00-90-27-e1-21-ef     动态
  192.168.2.2           00-90-27-e1-21-ef     动态
  192.168.2.3           00-90-27-e1-21-ef     动态
  192.168.2.11          08-9b-4b-9d-22-d3     动态
  192.168.2.15          f0-9f-fc-88-6e-79     动态
  192.168.2.30          04-d4-c4-ae-76-84     动态
  192.168.2.32          04-d4-c4-01-35-b1     动态
  192.168.2.36          04-d4-c4-ae-7d-b7     动态
```

- Arp命令显示了本机的arp缓存
- Arp缓存记录了IP地址与MAC地址的映射

1、TCP/IP协议安全性概述 ——安全问题的来源

- 互联网设计之初的使用目的是用于科学研究，其基本假设就是节点的诚实性；由于计算机网络的广泛使用，这种假设在今天已经无法成立，因此可能导致各种各样的攻击。
- 安全性问题分类
  - 设计缺陷导致的安全性问题
    - 协议设计的缺陷，这类安全性问题会一直存在，直至该协议更新
  - 实现缺陷导致的安全性问题
    - 协议实现的缺陷，这类安全性问题会随着软件的更新而消除

1、TCP/IP协议安全性概述 ——安全威胁

- 信息泄露
  - TCP/IP协议在设计时没有考虑保密性服务，所有消息均通过明文方式传输，导致消息在传输过程中存在信息泄露的安全威胁。
- 消息伪造
  - TCP/IP协议在设计时没有考虑身份鉴别和完整性服务，导致消息容易被伪造。
- 拒绝服务
  - TCP/IP协议在设计时没有考虑可用性服务，导致拒绝服务攻击。

1、TCP/IP协议安全性概述 —— 安全威胁

安全威胁分布

应用层

- DNS欺骗，XSS，邮件炸弹……

传输层

- SYN Flood攻击，会话挟持，……

网络层

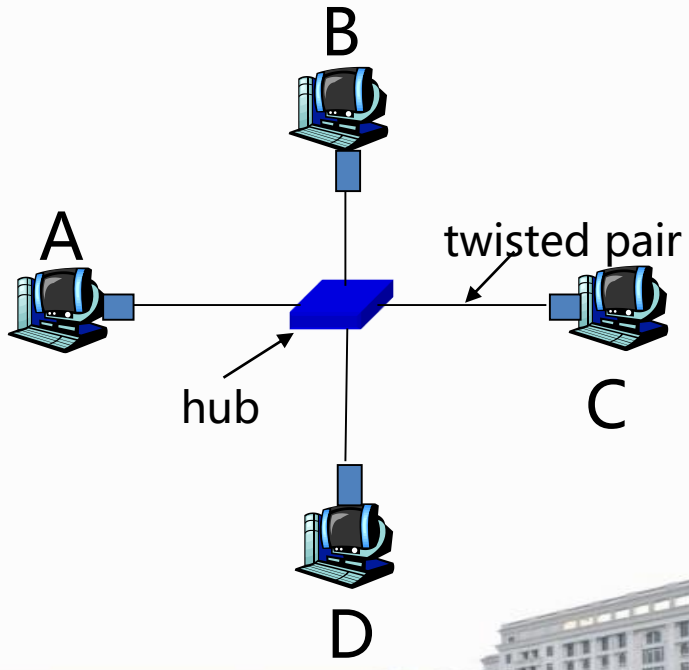
- ICMP重定向攻击，IP分片攻击，……

网络接口层

- 嗅探，ARP欺骗，交换机毒化，……

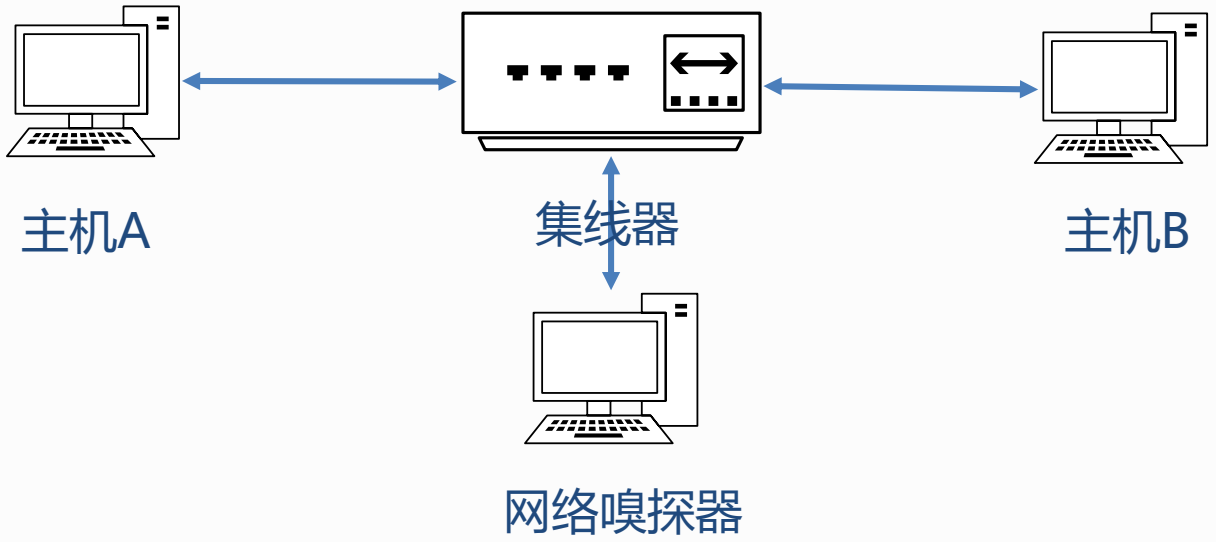
2、网络接口层协议安全分析—— 网络嗅探

- 共享环境下的网络嗅探
  - 以太网采用星型拓扑结构，使用集线器（hub）或者交换机（switch）连接网络节点。
  - 集线器本质上是物理层的中继器：
    - 处理的基本单位是位
    - 信号放大，延长网络距离
    - 收到的位发送给所有其它连接节点
    - 多个端口使用相同的传输速率，没有帧缓存
    - 没有CSMA/CD：由计算机的网卡检测冲突



2、网络接口层协议安全分析—— 网络嗅探

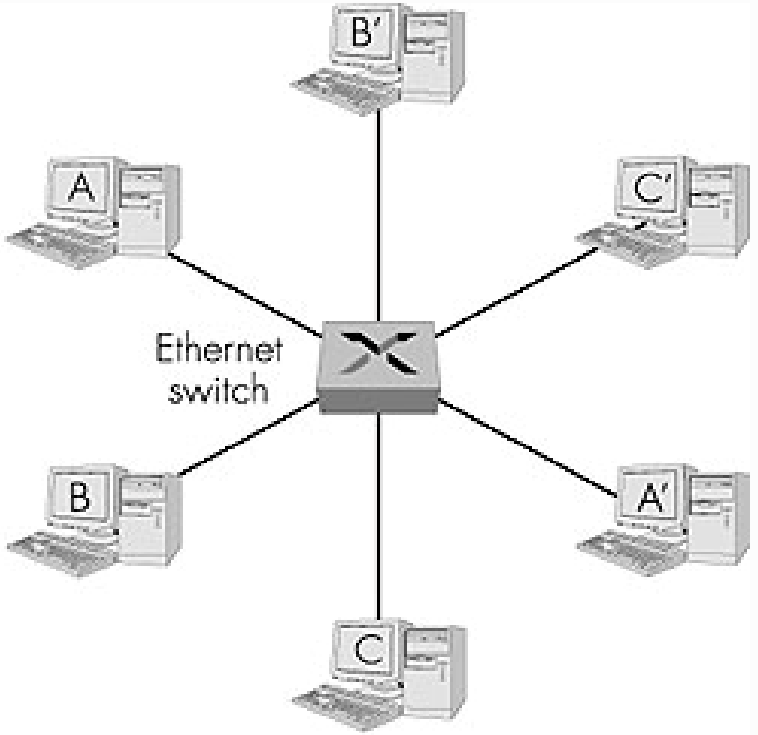
- 共享环境下的网络嗅探



工作原理：网络嗅探器是通过对网卡的编程来实现的。对网卡的编程是使用原始套接字方式来进行，Windows环境下通过创建原始套接字s=socket(AF_INET,SOCK_RAW,IPPROTO_RAW);设置为对IP头亲自操作setsockopt(s,IPPROTO_IP,IP_HDRINCL,(char*)&bFlag,sizeof(bFlag));设置SOCK_RAW为SIO_RCVALL，以便接收所有的IP包 ioctlsocket(s, SIO_RCVALL, &dwValue)，可以将网卡设置为混杂模式，来获取网络接口上侦听到的所有的数据包。

2、网络接口层协议安全分析—— 网络嗅探

- 交换环境下的网络嗅探
  - 交换机采用接口转发方式实现主机间的通信。
    - 交换机工作在链路层
    - 基于帧转发, 实现MAC地址过滤
    - 物理上和逻辑上都是星型结构
    - 交换：A-to-A′ 和 B-to-B′ 同时工作，不冲突

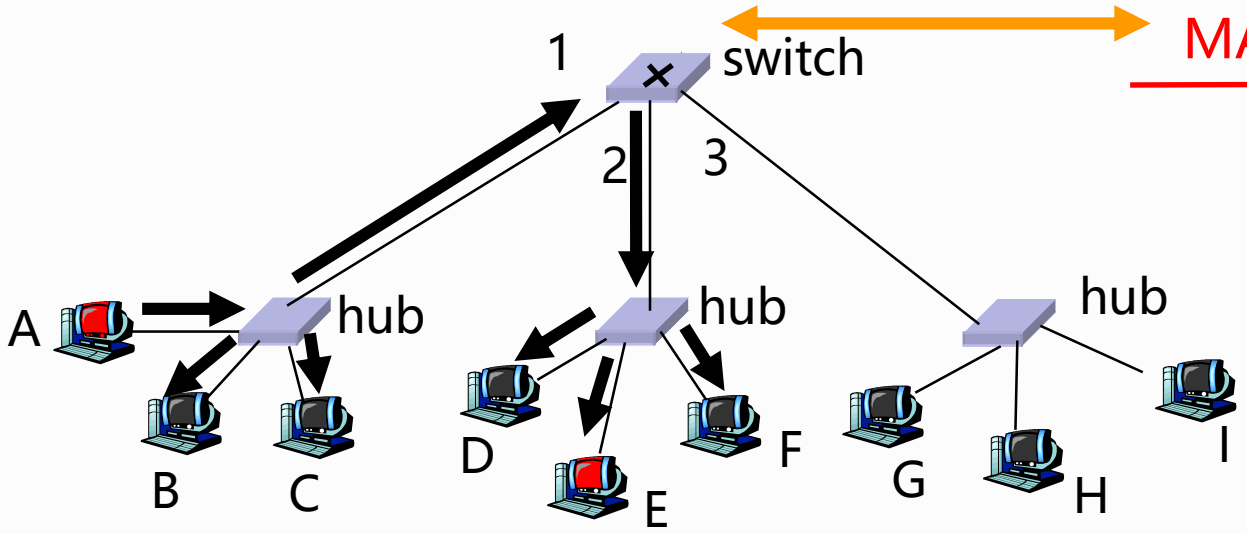


2、网络接口层协议安全分析—— 网络嗅探

- 交换环境下的网络嗅探（需要通过交换机毒化或ARP欺骗）
  - 交换机内部保存一个源地址表又称为交换表
    - 交换表的表项: (MAC地址, 接口, 时间)
    - 交换表中过期的表项将被删除 (TTL 可以是60分钟)
    - 交换机学习哪一个主机可以通过哪一个接口到达交换机当接收一数据帧时,交换机“学习”发送者的位置:即数据进入交换机的LAN网段与接口之间的对应关系，在交换表中记录发送者/位置对应关系
  - 上述机制称之为交换机的“自学习”

2、网络接口层协议安全分析—— 网络嗅探

- 交换机工作过程（交换表有记录）

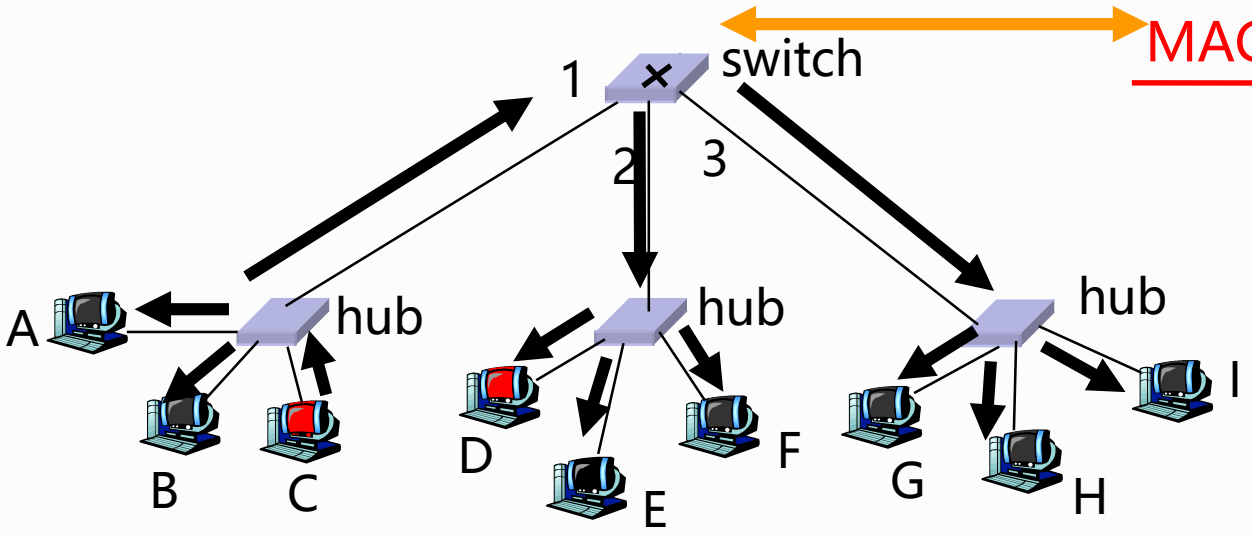


MAC地址	接口
A	1
B	1
E	2
G	3

- 假定假设A发送数据帧到E
  - 交换机接收来自A的数据帧
    - 注意在交换表中A在交换机的接口1上，E在交换机的接口2上
    - 交换机将转发数据帧到接口
  - 数据帧被E接收

2、网络接口层协议安全分析—— 网络嗅探

- 交换机工作过程（交换表无记录）

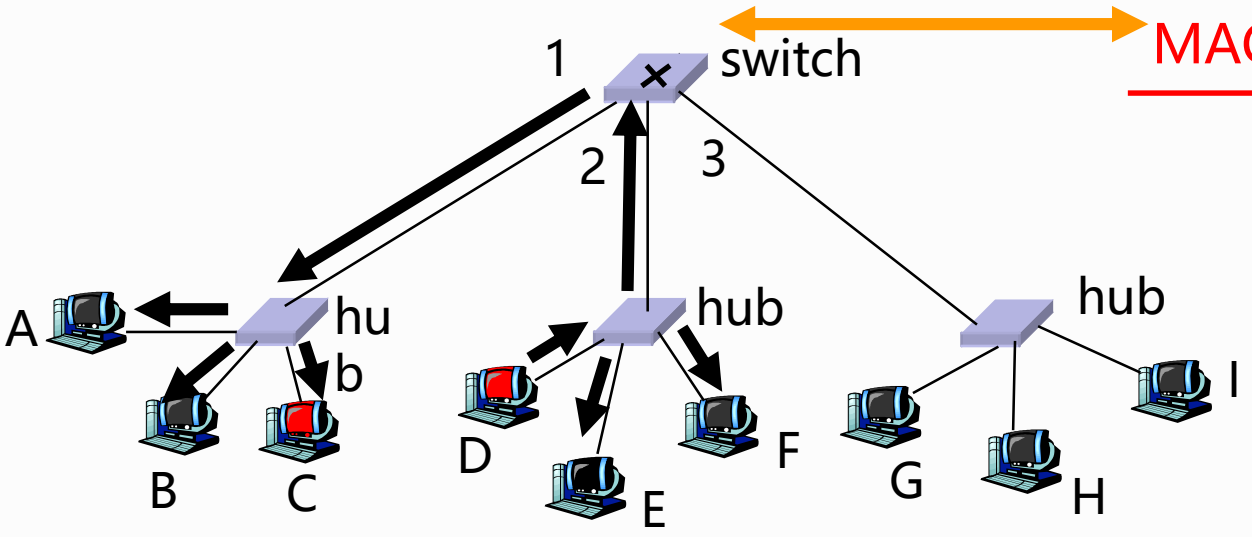


MAC地址	接口
A	1
B	1
E	2
G	3
C	1

- 假设C发送数据帧到D
  - 交换机接收来自C的数据帧
    - 记录C所对应的接口号1
    - 因为D不在交换表中,交换机将转发数据帧到接口2和3
  - 数据帧被D接收

2、网络接口层协议安全分析—— 网络嗅探

- 交换机工作过程（交换表无记录）

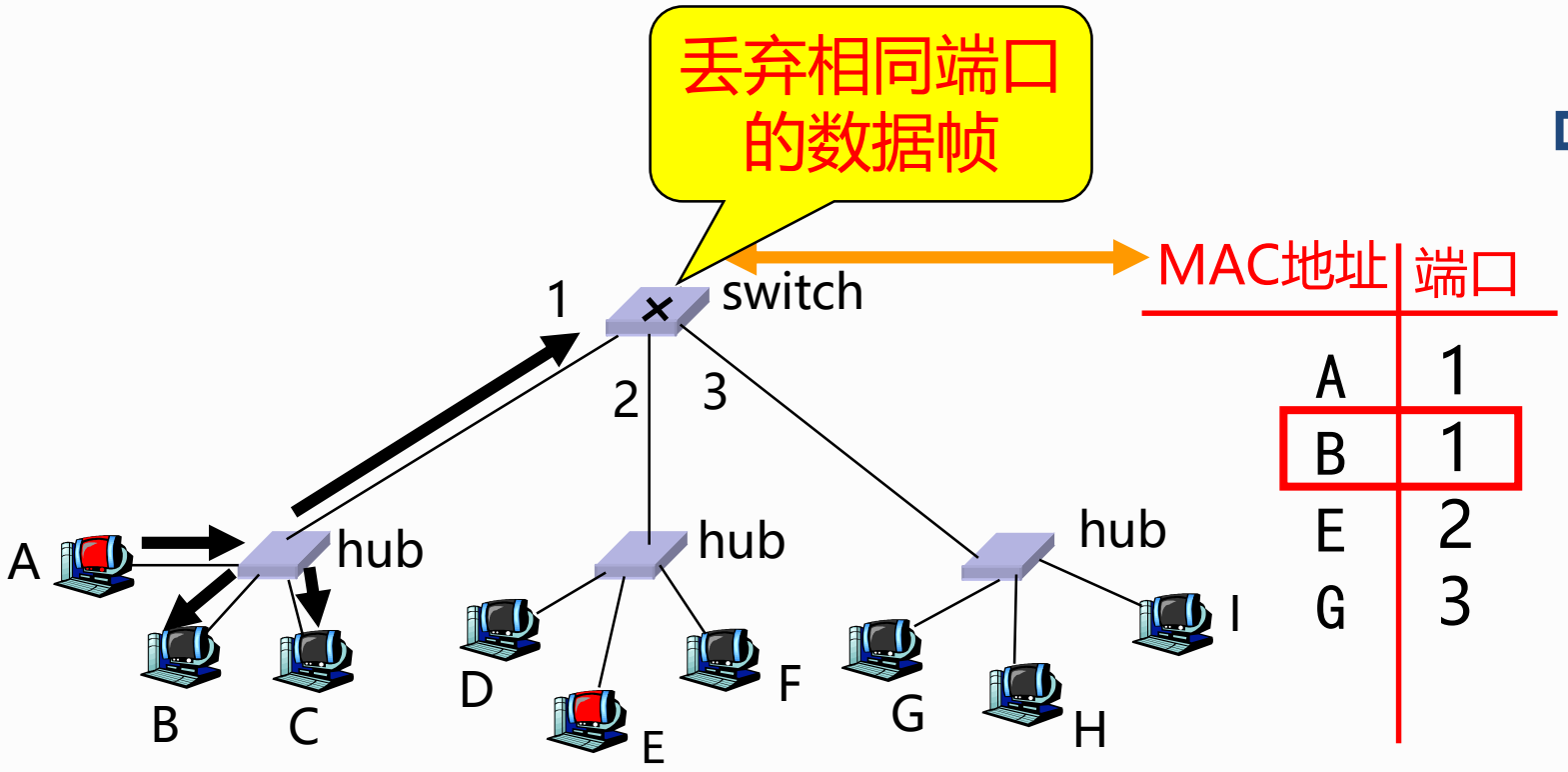


MAC地址	接口
A	1
B	1
E	2
G	3
C	1
D	2

- 假设D回复数据帧给C
  - 交换机接收来自D的数据帧
    - 记录D所对应的接口号为2
    - 因为C在交换表中，并且接口为1，则交换机只向接口1转发数据帧
  - 数据帧被C接收

2、网络接口层协议安全分析—— 网络嗅探

交换机工作过程（接口相同情况）

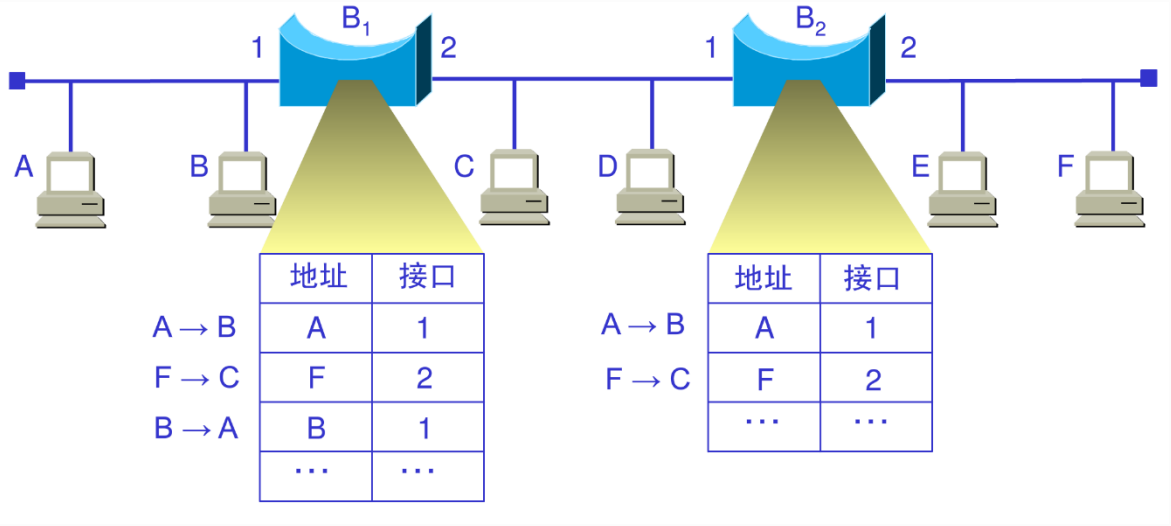


MAC地址	端口
A	1
B	1
E	2
G	3

- 假设A发送数据帧到B
  - 交换机接收来自A的数据帧
    - 注意在交换表中A在交换机的接口1上,B也在交换机的接口1上
  - 数据帧将被交换机丢弃

2、网络接口层协议安全分析—— 网络嗅探

交换机毒化攻击（嗅探）



- 交换表的空间是有限的，新的“MAC地址——接口”映射对的到达会替换旧的表项。
- 如果攻击者发送大量的具有不同伪造源MAC地址的帧，由于交换机的自学习功能，这些新的“MAC地址—接口”映射对会填充整个交换机表，而这些表项都是无效的，结果交换机完全退化为广播模式，攻击者达到窃听数据的目的。

2、网络接口层协议安全分析—— ARP欺骗

ARP协议的功能

- 在互联网上是使用IP地址来定位主机，而但在交换机上是通过MAC—接口映射来实现主机间数据帧的发送，因此需要使用协议完成IP地址和MAC地址的转换。
  - ARP协议：IP地址→MAC地址
  - RARP协议：MAC地址→IP地址

ARP协议位于网络层与数据链路层之间

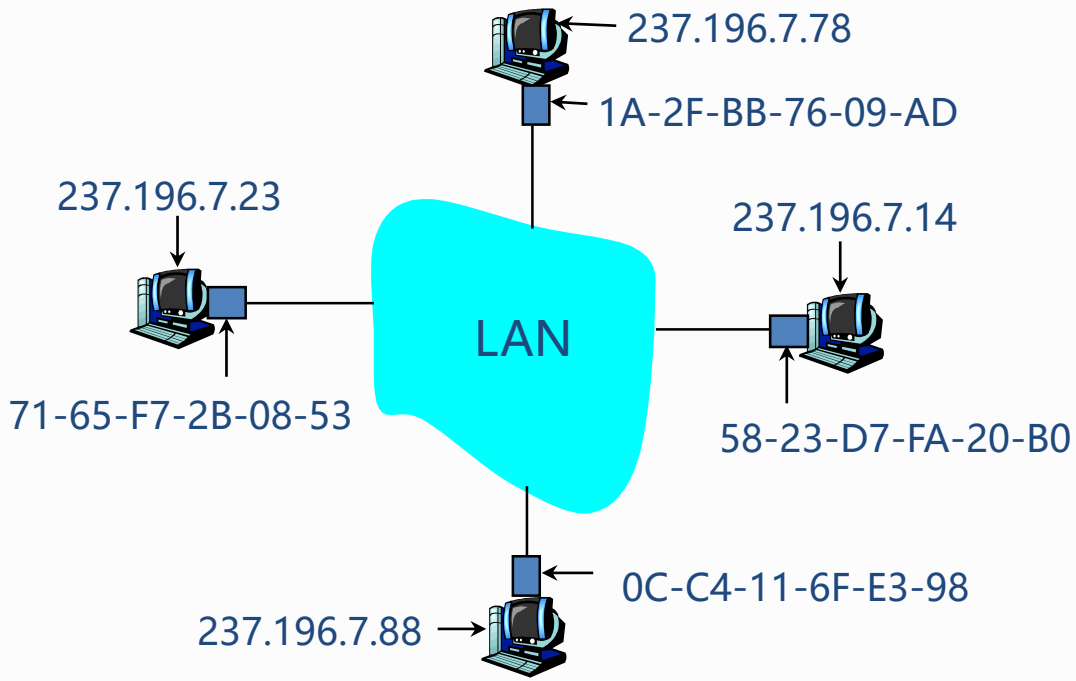
2、网络接口层协议安全分析—— ARP欺骗

- ARP头部结构

1： Ethernet (10 Mb)
3： Amateur Radio AX.25
4： Token Ring
6： IEEE 802 networks
11： Local talk

2、网络接口层协议安全分析—— ARP欺骗

ARP协议工作原理



- 每个在局域网上的IP节点（Host, Router)都有ARP表
- ARP表:局域网上（部分）节点的IP/MAC地址映射

<IP address; MAC address; TTL>

- TTL (Time To Live): 映射地址的失效时间 (典型为20分钟)

2、网络接口层协议安全分析—— ARP欺骗

- ARP协议工作原理：ARP是即插即用的，无需网络管理员干预，节点就能创建ARP表。
  - A想发送分组给 B，A知道 B的IP地址，假设B的MAC地址不在A的ARP表中

步骤一：A广播包含B的IP地址的ARP查询包

- 目的MAC地址= FF-FF-FF-FF-FF-FF

步骤二：B收到 ARP包，回给A一个带有B的MAC地址的包

- 包单播unicast发送给A的MAC地址

步骤三：A缓存IP-to-MAC地址对在 ARP表中，直到信息过期

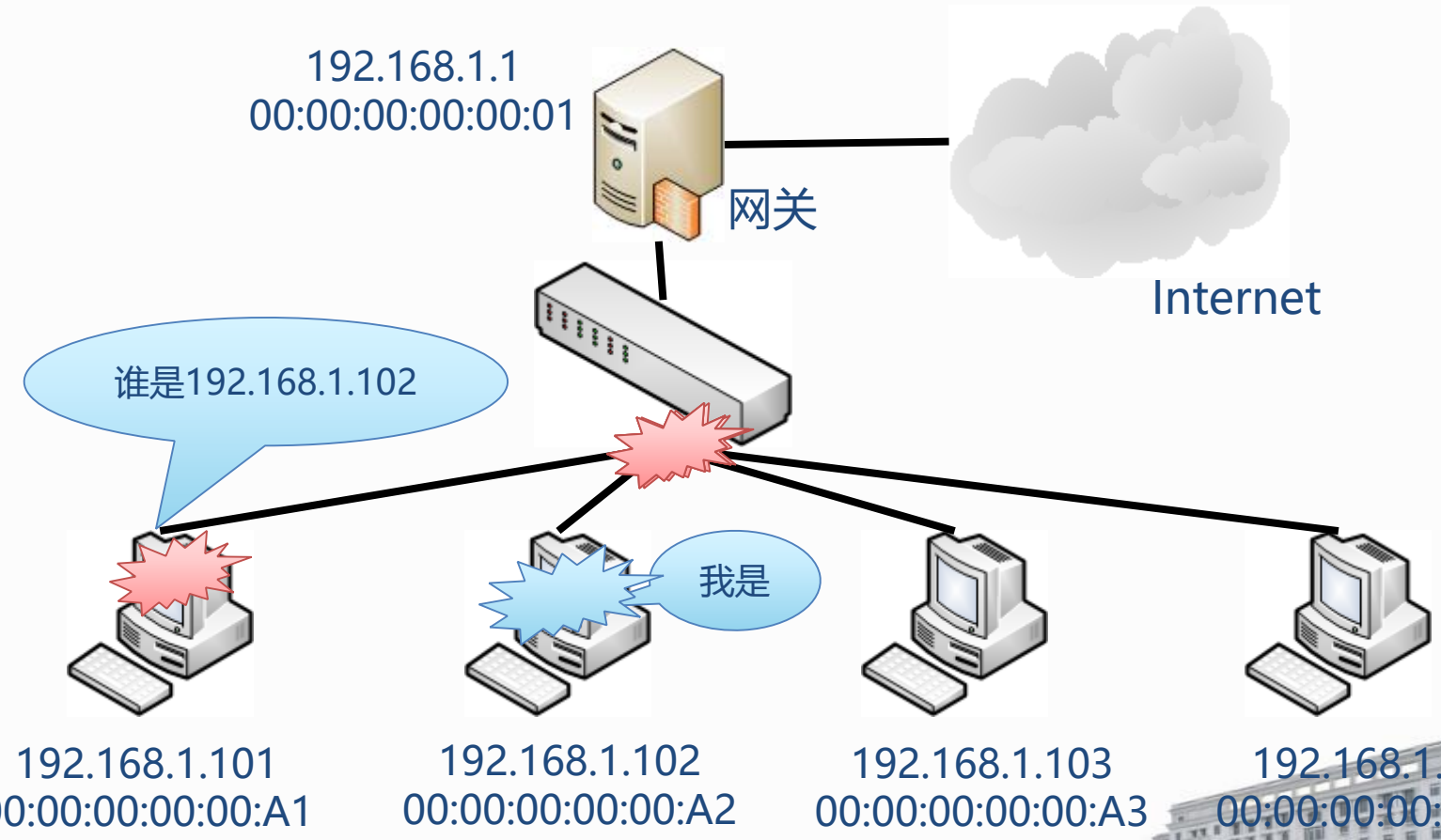
- 如果ARP表的信息在一定时间内没有刷新，则信息将过期。

2、网络接口层协议安全分析—— ARP欺骗

ARP协议工作过程

192.168.1.101主机的本地ARP缓存

192.168.1.1	00:00:00:00:00:01
192.168.1.101	00:00:00:00:00:A1
192.168.1.102	00:00:00:00:00:A2
192.168.1.103	00:00:00:00:00:A3
192.168.1.104	00:00:00:00:00:A4



2、网络接口层协议安全分析—— ARP欺骗

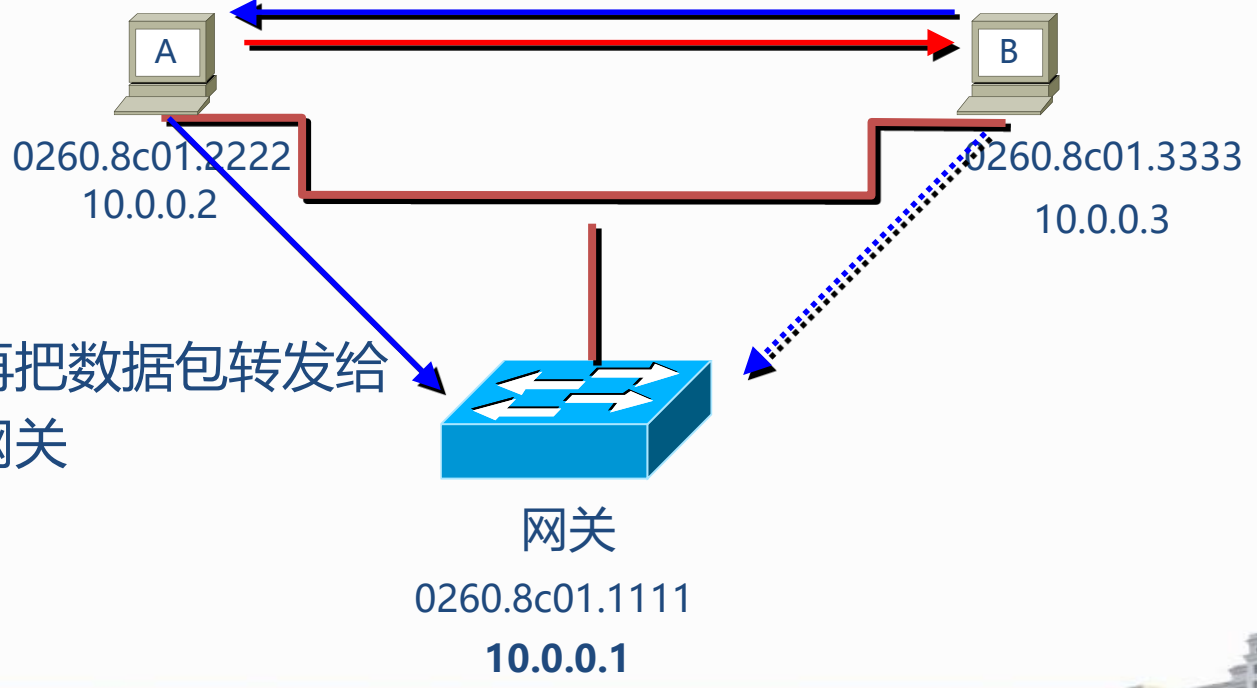
- ARP协议的特殊设计（改进效率）
  - 响应ARP请求的主机将请求者的IP - MAC映射缓存。
  - 主动的ARP应答会被视为有效信息接受
- ARP协议的缺陷
  - ARP协议设计之初没有考虑认证问题，所以任何计算机都可以发送虚假的ARP数据包。
  - ARP协议的无状态性。响应数据包和请求数据包之间没有什么关系，如果主机收到一个ARP响应却无法知道是否真的发送过对应的ARP请求。
  - ARP缓存需要定时更新，给攻击者以可乘之机。

2、网络接口层协议安全分析—— ARP欺骗

◘ ARP欺骗攻击过程

攻击者在局域网段发送虚假的IP/MAC对应信息，篡改网关MAC地址，使自己成为假网关

假网关（攻击者）分析接收到的数据包，把有价值的数据包记录下来（比如QQ以及邮箱登录数据包）

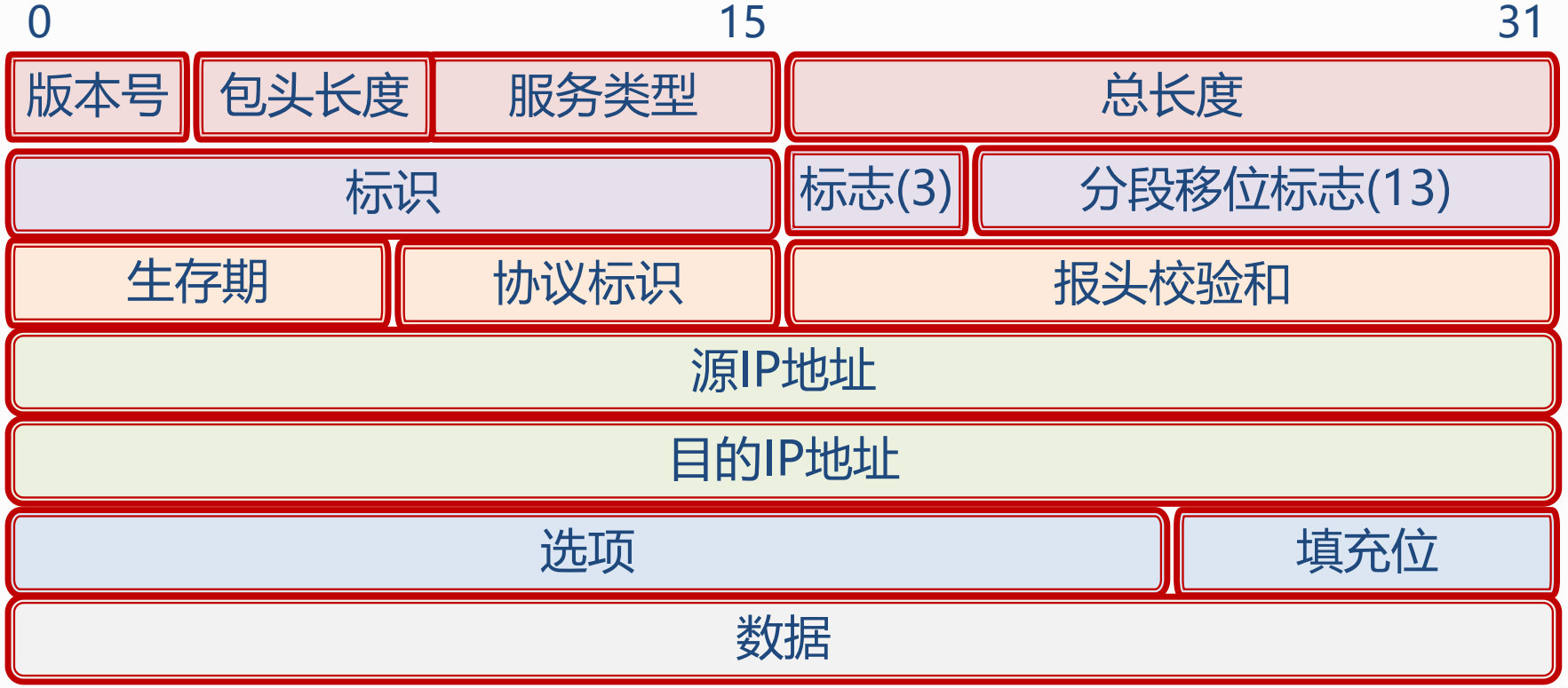


2、网络接口层协议安全分析—— ARP欺骗

- ARP欺骗攻击的特点
  - 危害
    - 嗅探
    - 中间人攻击
    - 拒绝服务攻击
  - 局限性
    - ARP欺骗只能被用于局域网（攻击者必须已经获得局域网中某台机器的访问权）。

3、网络层协议安全分析 —— IP假冒攻击

- IP包头结构



3、网络层协议安全分析 —— IP假冒攻击

- 攻击原理
  - IP协议本身没有验证源IP地址真实性的机制
- 攻击类型
  - 拒绝服务
    - 避免被追踪而受到惩罚，构造针对同一目的 IP 地址的 IP 分组，而源 IP 地址为随机的IP地址
  - 基于 IP 地址认证的网络服务欺骗
    - 假冒可信的IP 地址而非法访问计算机资源，X-window、rlogin、rsh等

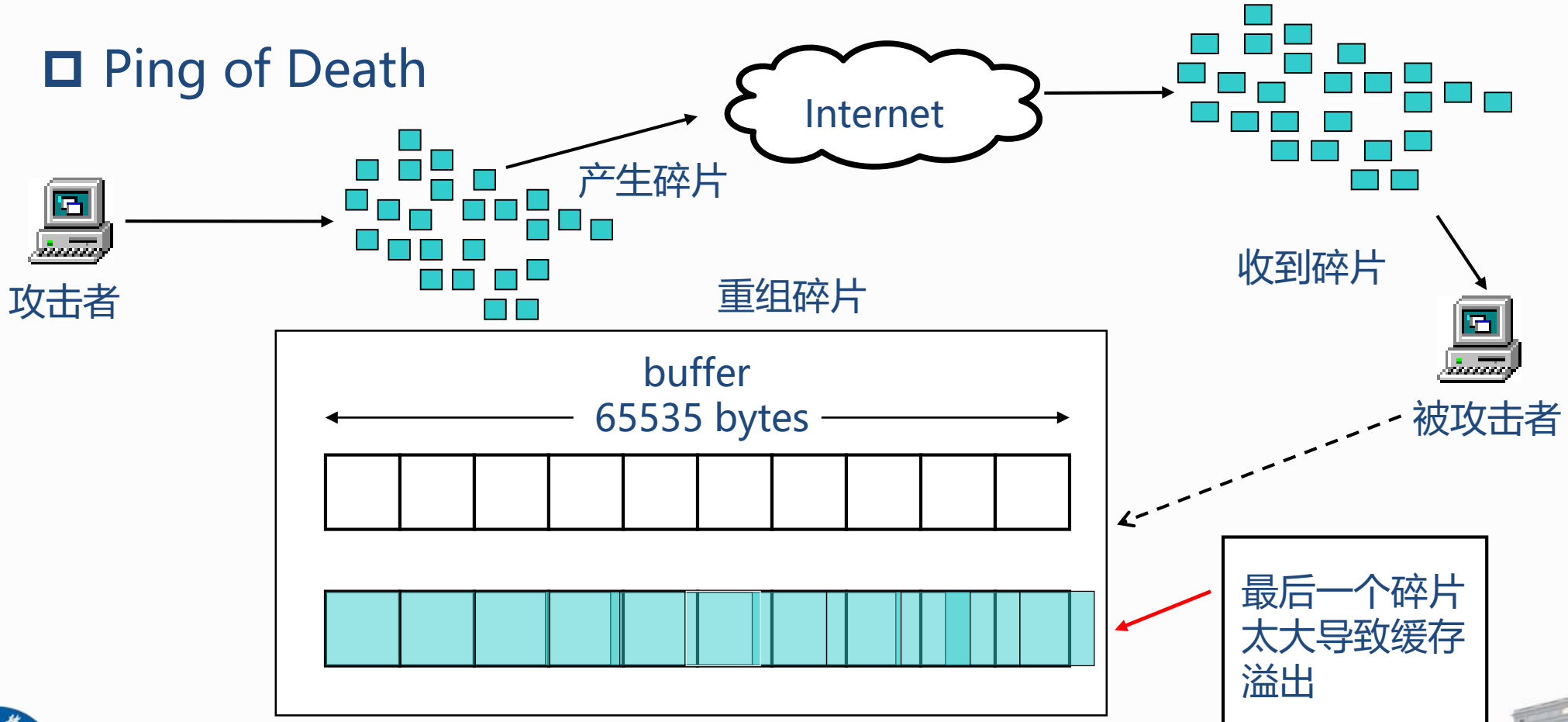
3、网络层协议安全分析 —— IP碎片攻击

攻击原理

- 链路层具有最大传输单元MTU这个特性，它限制了数据帧的最大长度，不同的网络类型都有一个上限值，以太网的MTU是1500。如果IP层有数据包要传，而且数据包的长度超过了MTU，那么IP层就要对数据包进行分片(fragmentation)操作，使每一片的长度都小于或等于MTU。
- IP首部有两个字节表示整个IP数据包的长度，所以IP数据包最长只能为0xFFFF，就是65535字节。如果有意发送总长度超过65535 的IP碎片，或构造畸形的IP碎片，部分老的操作系统在进行碎片重组处理时会导致崩溃或拒绝服务。

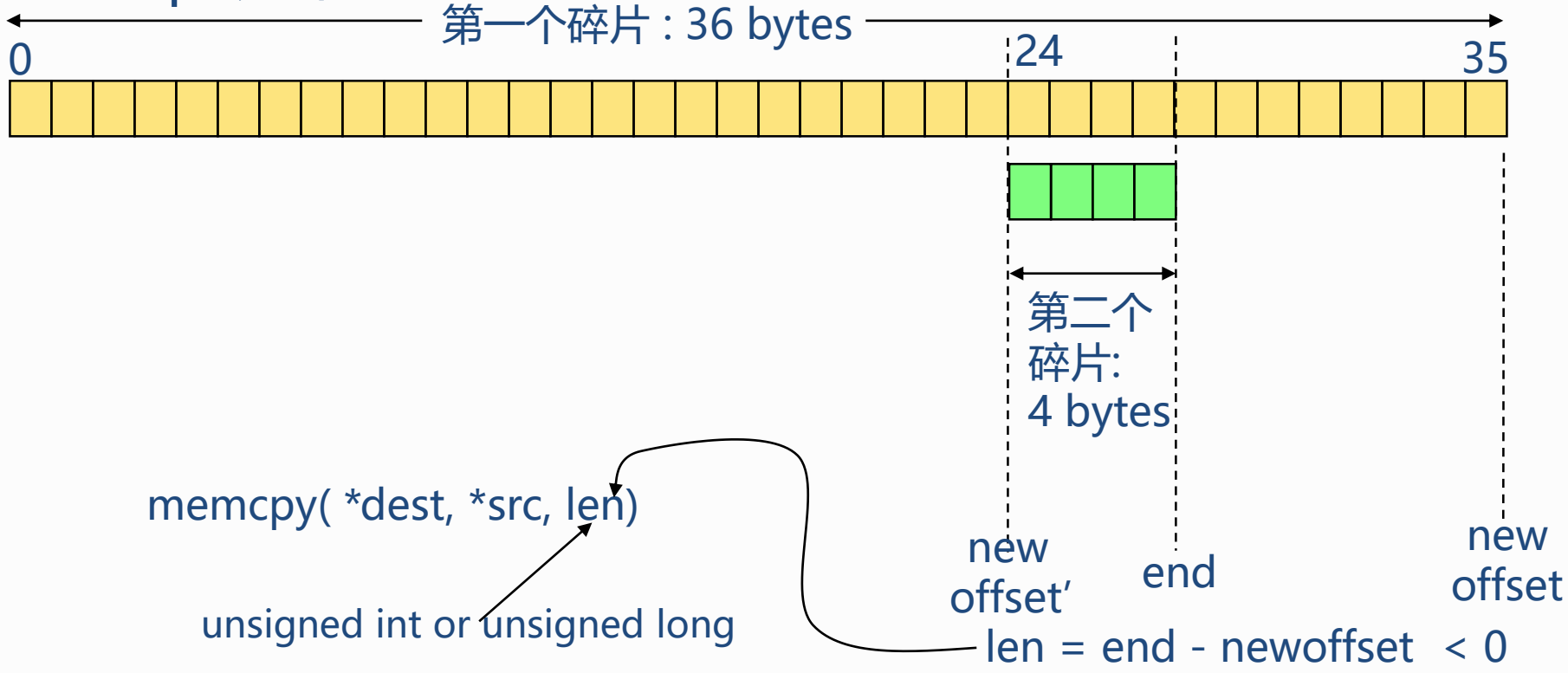
3、网络层协议安全分析 —— IP碎片攻击

- Ping of Death



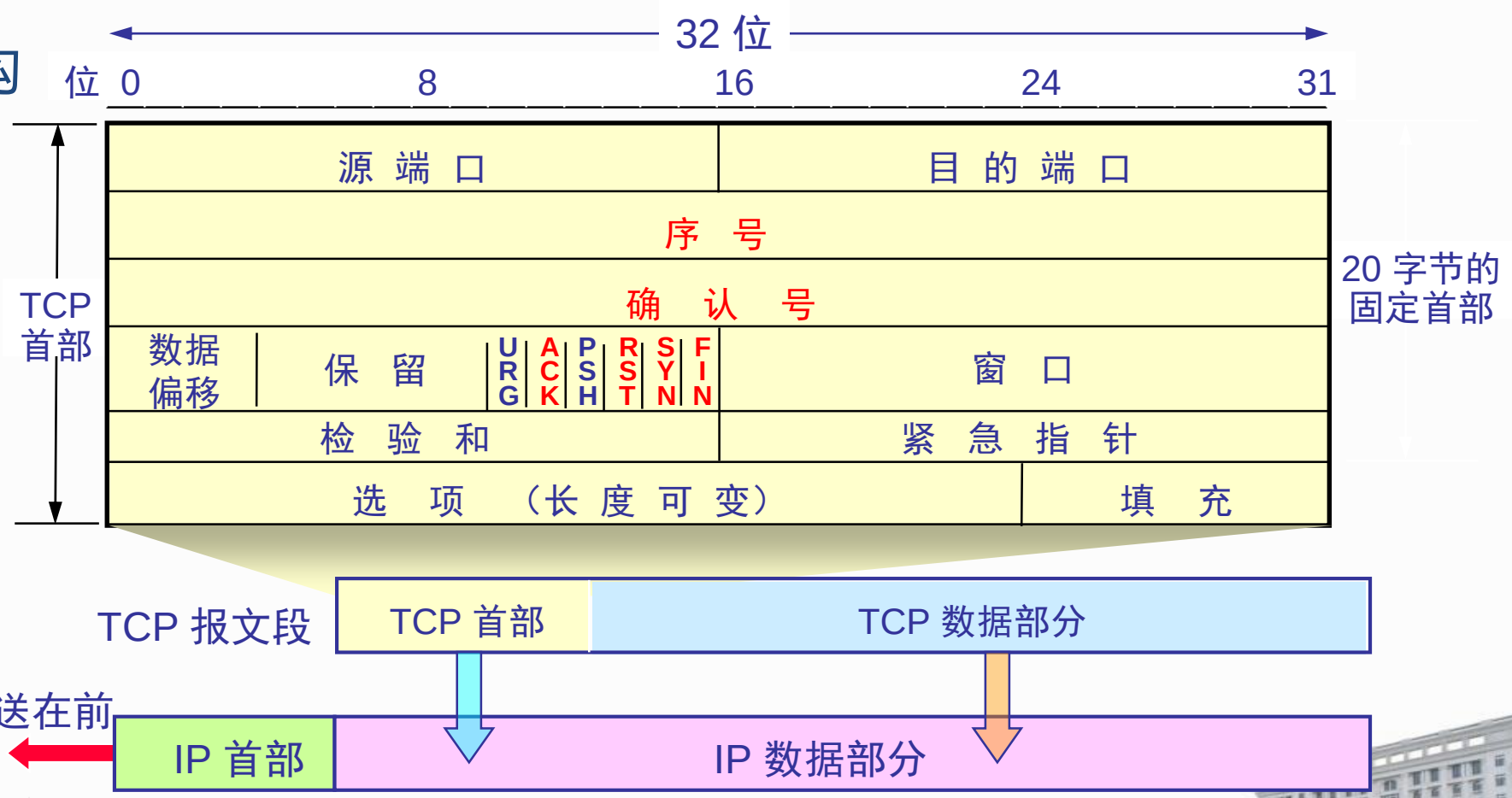
3、网络层协议安全分析 —— IP碎片攻击

- Teardrop 攻击



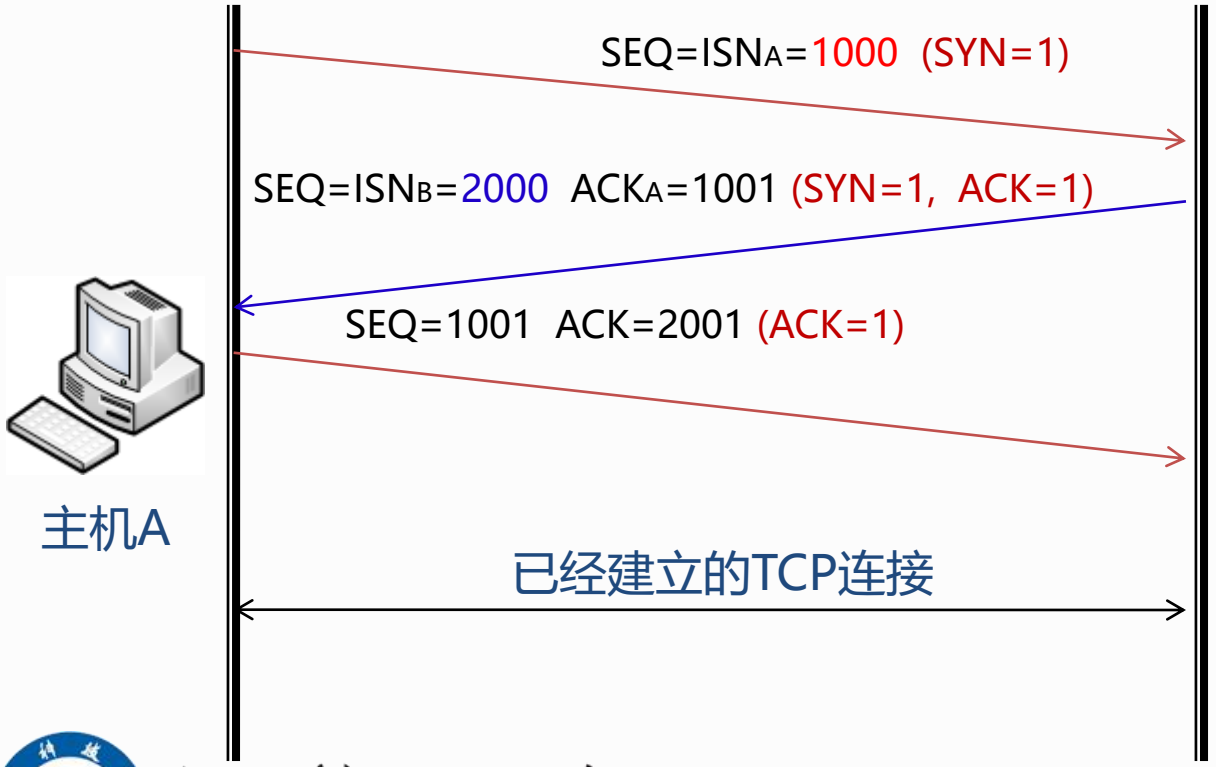
4、传输层协议安全分析 —— TCP协议安全威胁

TCP报头结构



4、传输层协议安全分析 —— TCP协议安全威胁

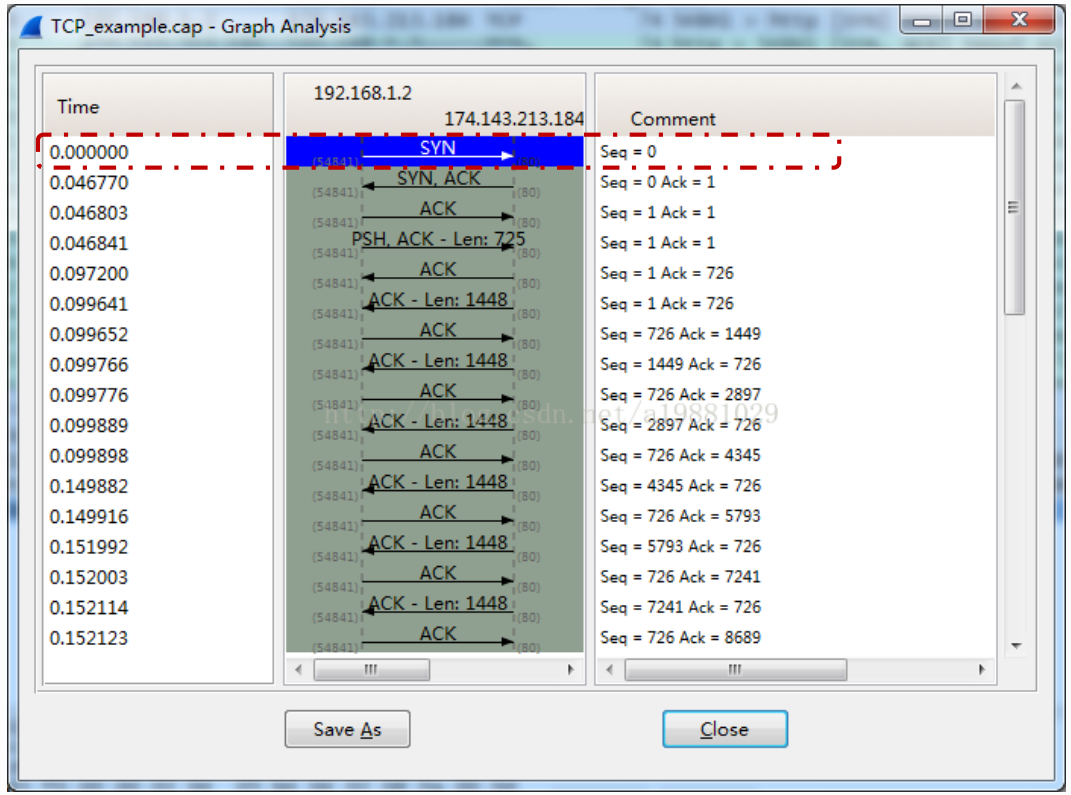
TCP建立连接过程



Protocol	Length	Info
TCP	74	60368 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK…
TCP	76	443 → 60368 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1200 W…
TCP	54	60368 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0

4、传输层协议安全分析 —— TCP协议安全威胁

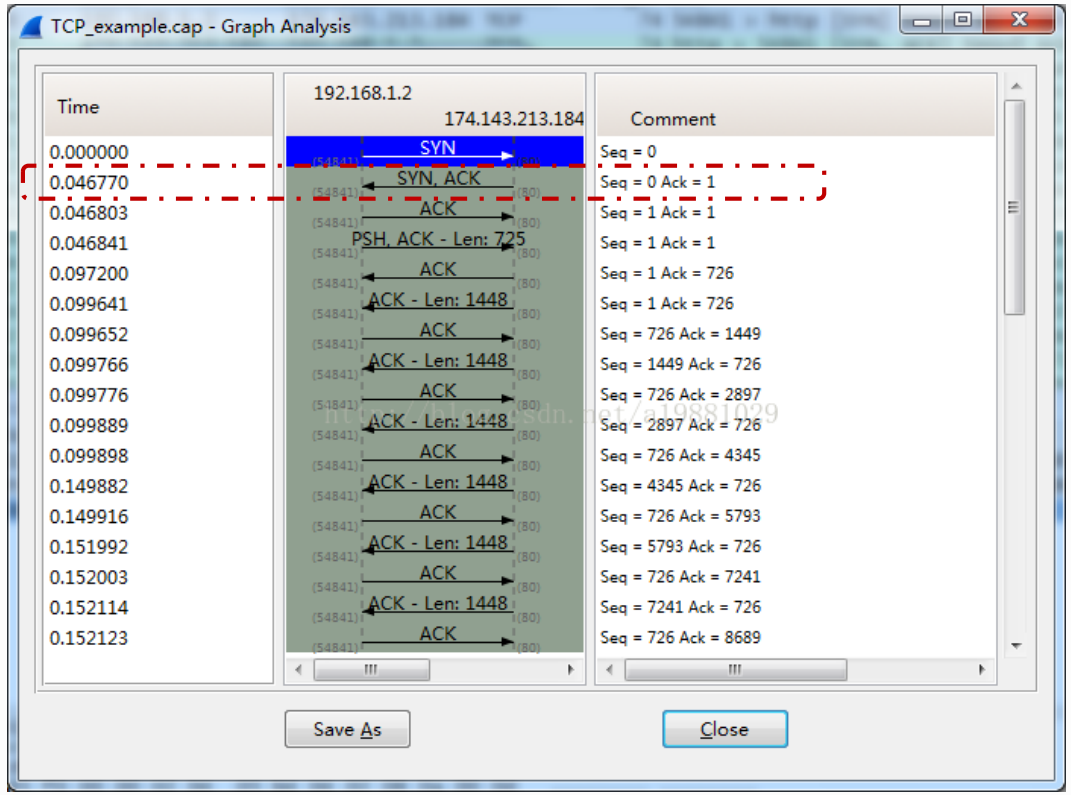
□ 序列号和确认号



包1：TCP会话的每一端的序列号都从0开始，同样的，确认号也从0开始，因为此时通话还未开始，没有通话的另一端需要确认。

4、传输层协议安全分析 —— TCP协议安全威胁

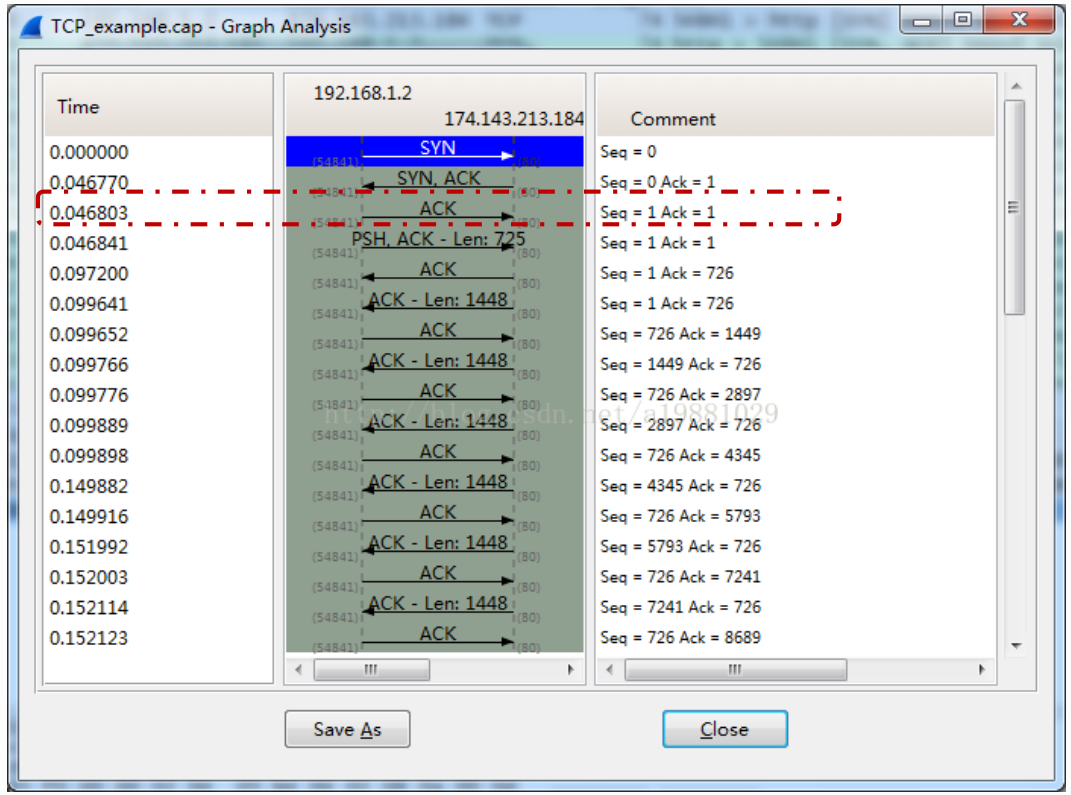
序列号和确认号



- **包2**：服务端响应客户端的请求，响应中附带序列号0（由于这是服务端在该次TCP会话中发送的第一个包，所以序列号为0）和相对确认号1（表明服务端收到了客户端发送的包1中的SYN）。
- 需要注意的是，尽管客户端没有发送任何有效数据，确认号还是被加1，这是因为接收的包中包含SYN或FIN标志位（并不会对有效数据的计数产生影响，因为含有SYN或FIN标志位的包并不携带有效数据）

4、传输层协议安全分析 —— TCP协议安全威胁

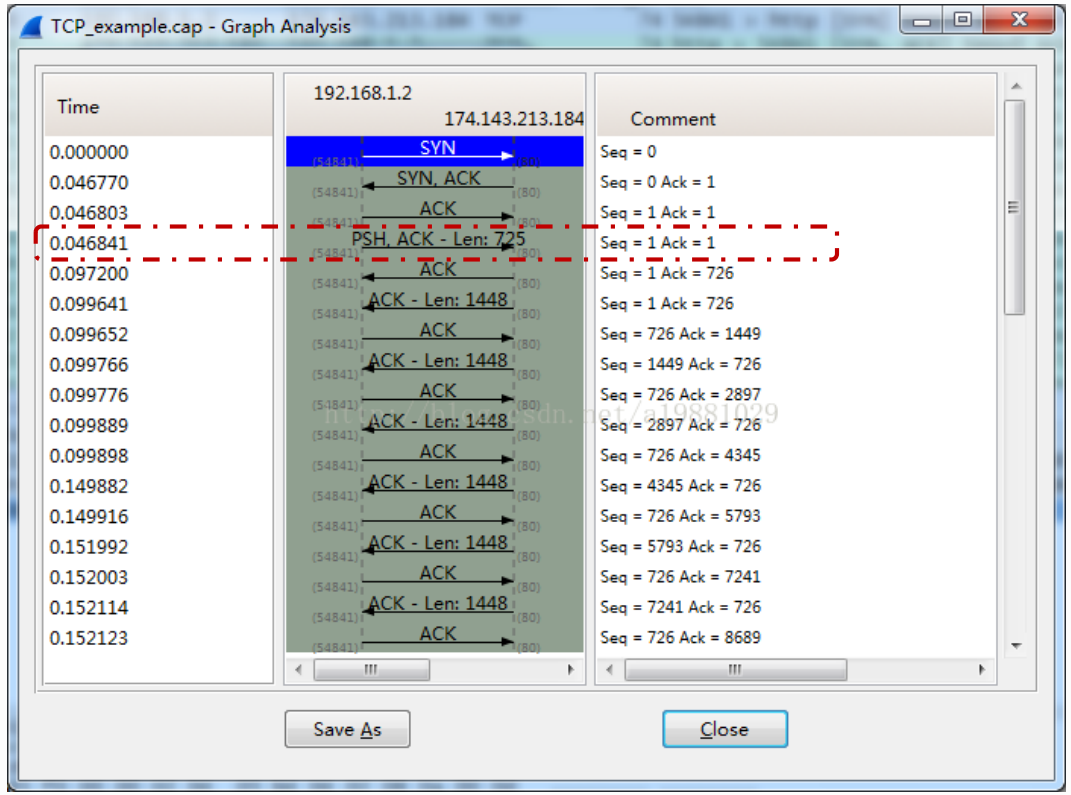
□ 序列号和确认号



- **包3**：和包2中一样，客户端使用确认号1响应服务端的序列号0，同时响应中也包含了客户端自己的序列号（由于服务端发送的包中确认收到了客户端发送的SYN，故客户端的序列号由0变为1），此时，通信的两端的序列号都为1，通信两端的序列号增1发生在所有TCP会话的建立过程中。

4、传输层协议安全分析 —— TCP协议安全威胁

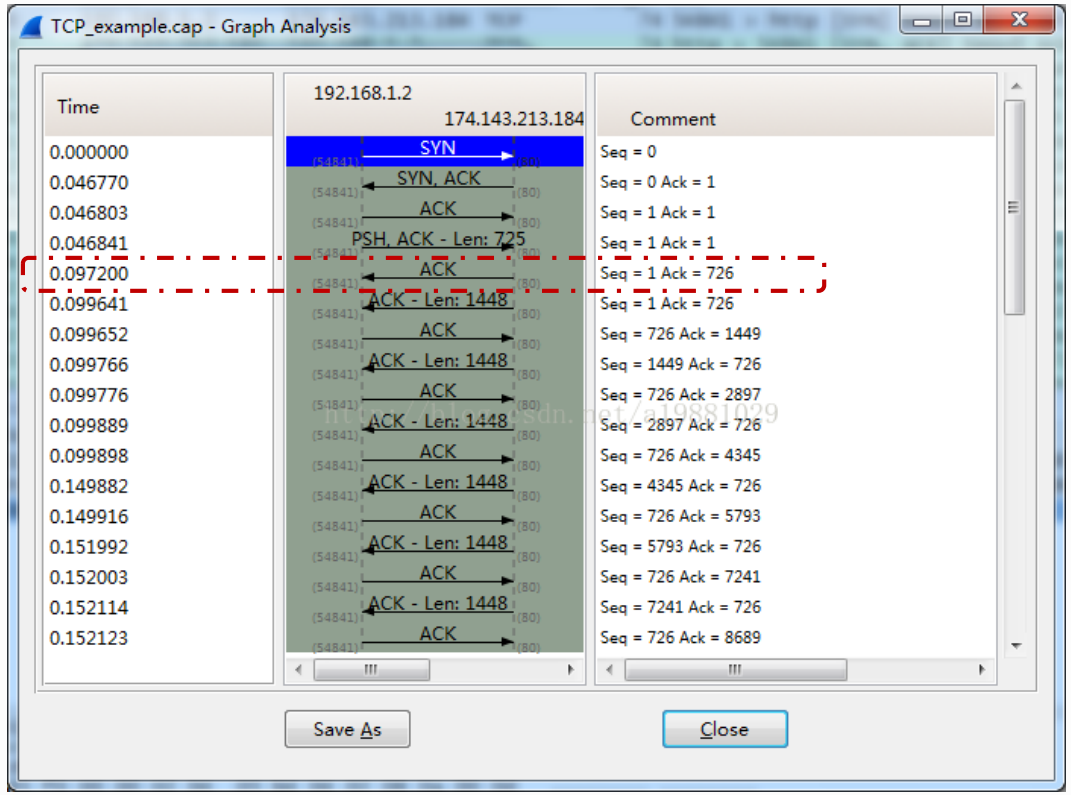
□ 序列号和确认号



- **包4**：这是流中第一个携带有效数据的包（确切的说，是客户端发送的HTTP请求），序列号依然为1，因为到上个包为止，还没有发送任何数据，确认号也保持1不变，因为客户端没有从服务端接收到任何数据。（包内携带发送给服务器的数据为725个字节）

4、传输层协议安全分析 —— TCP协议安全威胁

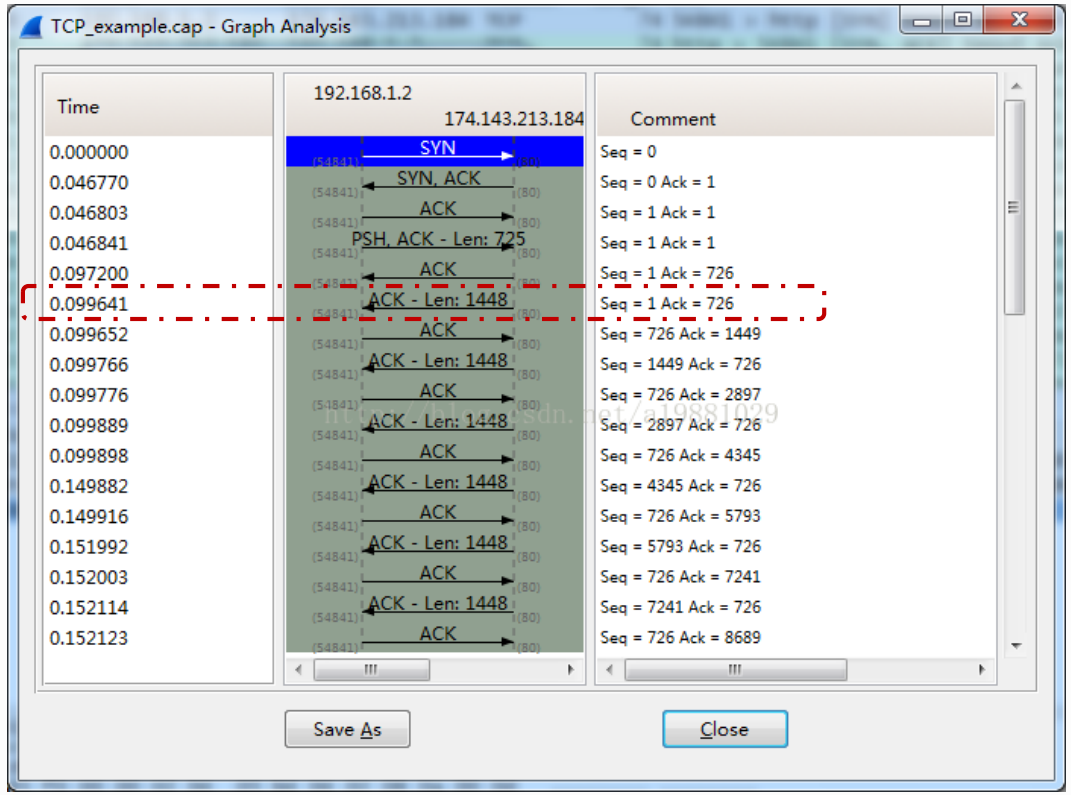
□ 序列号和确认号



包5：当上层处理HTTP请求时，服务端发送该包来确认客户端在包4中发来的数据，需要注意的是，确认号的值增加了725（725是包4中有效数据长度），变为726，简单来说，服务端以此来告知客户端端，目前为止，我总共收到了726字节的数据，服务端的序列号保持为1不变。

4、传输层协议安全分析 —— TCP协议安全威胁

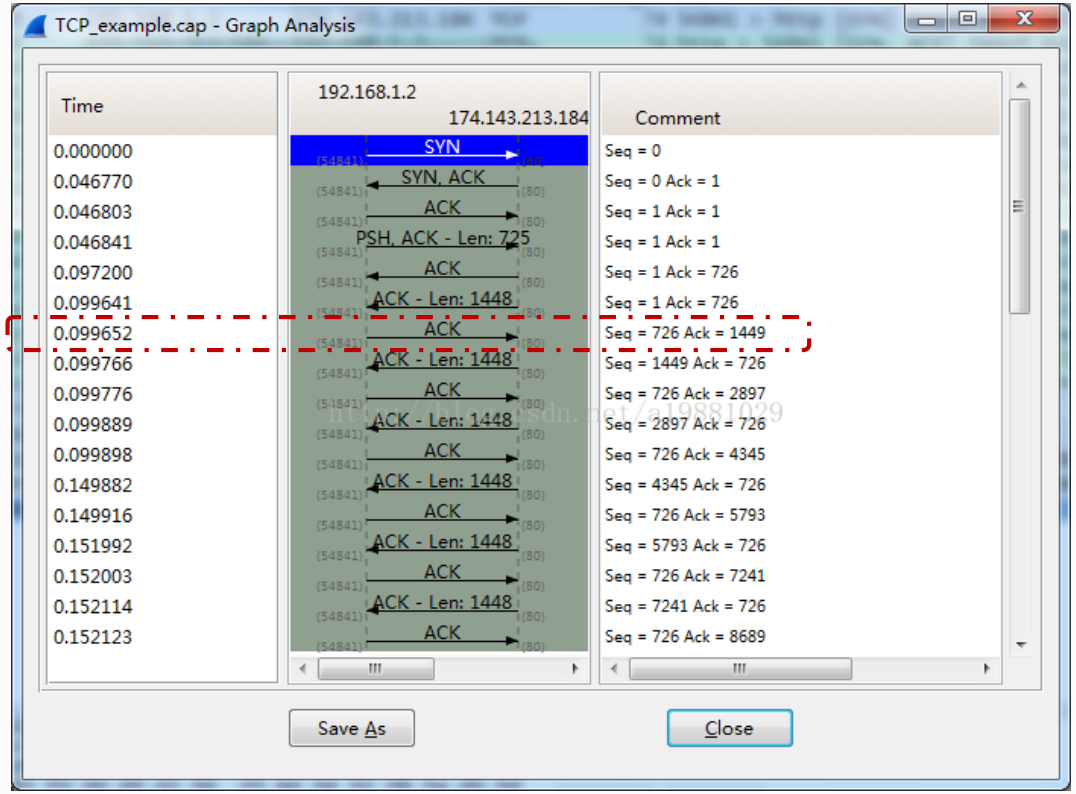
□ 序列号和确认号



- 包6：这个包标志着服务端返回HTTP响应的开始，序列号依然为1，因为服务端在该包之前返回的包中都不带有有效数据，该包带有1448字节的有效数据。

4、传输层协议安全分析 —— TCP协议安全威胁

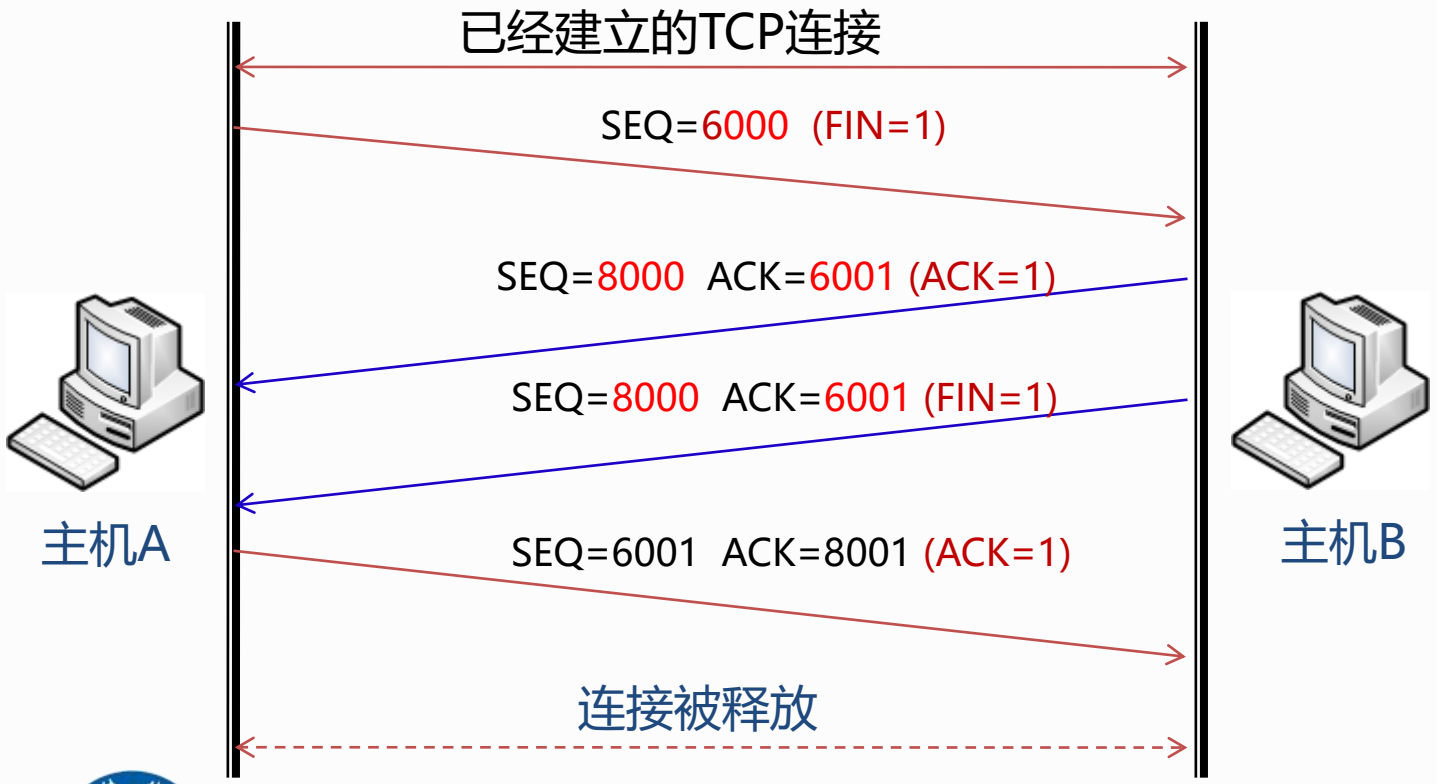
□ 序列号和确认号



包七：由于上个数据包的发送成功，TCP客户端的序列号增长至726，从服务端接收了1448字节的数据，客户端的确认号由1增长至1449。

4、传输层协议安全分析 —— TCP协议安全威胁

TCP释放连接过程




```
60 443 → 60368 [FIN, ACK] Seq=4594 Ack=1498 Win=28288 Len=0
54 60368 → 443 [ACK] Seq=1498 Ack=4595 Win=261120 Len=0
54 60368 → 443 [FIN, ACK] Seq=1498 Ack=4595 Win=261120 Len=0
54 [TCP Retransmission] 60368 → 443 [FIN, ACK] Seq=1498 Ack=459…
54 [TCP Retransmission] 60368 → 443 [FIN, ACK] Seq=1498 Ack=459…
54 [TCP Retransmission] 60368 → 443 [FIN, ACK] Seq=1498 Ack=459…
54 [TCP Retransmission] 60368 → 443 [FIN, ACK] Seq=1498 Ack=459…
54 [TCP Retransmission] 60368 → 443 [FIN, ACK] Seq=1498 Ack=459…
54 60368 → 443 [RST, ACK] Seq=1499 Ack=4595 Win=0 Len=0
```

思考：这是连接百度后，客户端无请求，服务器断开连接的过程，请说明服务器是如何处理的？

4、传输层协议安全分析 —— TCP协议安全威胁

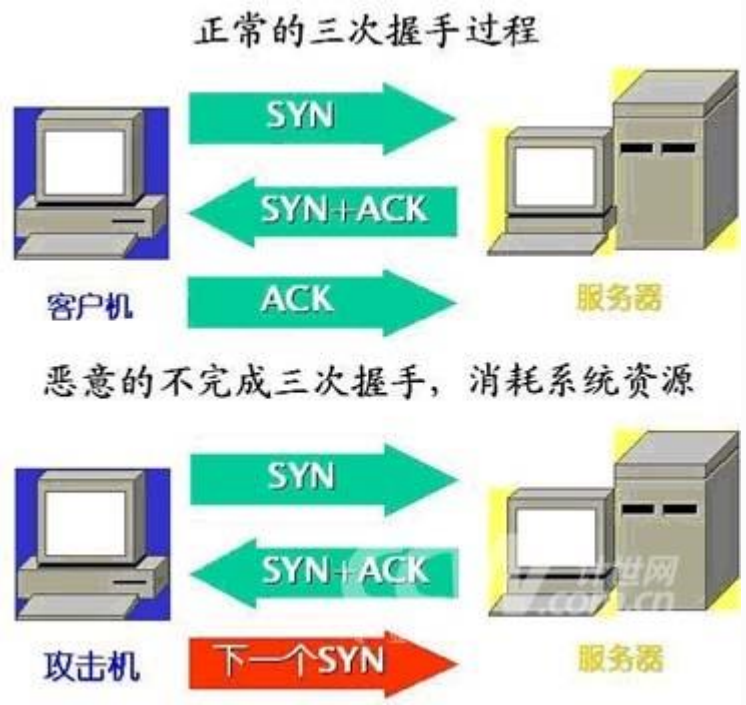
- TCP协议的特点
  - 全双工连接(full-duplex connection)
    - 该连接的两端有两条彼此独立、方向相反的传输通道
  - 面向连接(connection-oriented)
    - 通信双方在开始传输数据前，必须通过“三次握手”的方式在二者之间建立一条逻辑上的链路（虚电路），用于传输数据
  - 可靠性(reliable)
    - 自动分片；保证传送给应用层的数据顺序是正确的； 自动过滤重复的封包； 确认-重传确保数据包可靠到达
  - 面向字节流(byte-stream)
    - 将应用程序和网络传输相分割，为流传输服务提供了一个一致的接口

4、传输层协议安全分析 —— TCP协议安全威胁

- 拒绝服务（Denial of Service）
  - DoS攻击是指利用网络协议漏洞或其他系统以及应用软件的漏洞耗尽被攻击目标资源，使得被攻击的计算机或网络无法正常提供服务，直至系统停止响应甚至崩溃的攻击方式。即攻击者通过某种手段，导致目标机器或网络停止向合法用户提供正常的服务或资源访问
  - 利用TCP面向连接的特点
    - 三次握手过程需要存储连接状态，因此会产生系统开销

4、传输层协议安全分析 —— TCP协议安全威胁

SYN Flooding



攻击者向服务器发送众多的带有虚假地址的请求，服务器发送回复信息后等待回传信息。

由于地址是伪造的，所以服务器一直等不到回传的消息，分配给这次请求的资源就不会被立即释放。

当服务器等待一定的时间后，连接会因超时而被切断，攻击者会再度传送新的一批请求，在这种反复发送伪地址请求的情况下，服务器资源最终会被耗尽。

4、传输层协议安全分析 —— TCP协议安全威胁

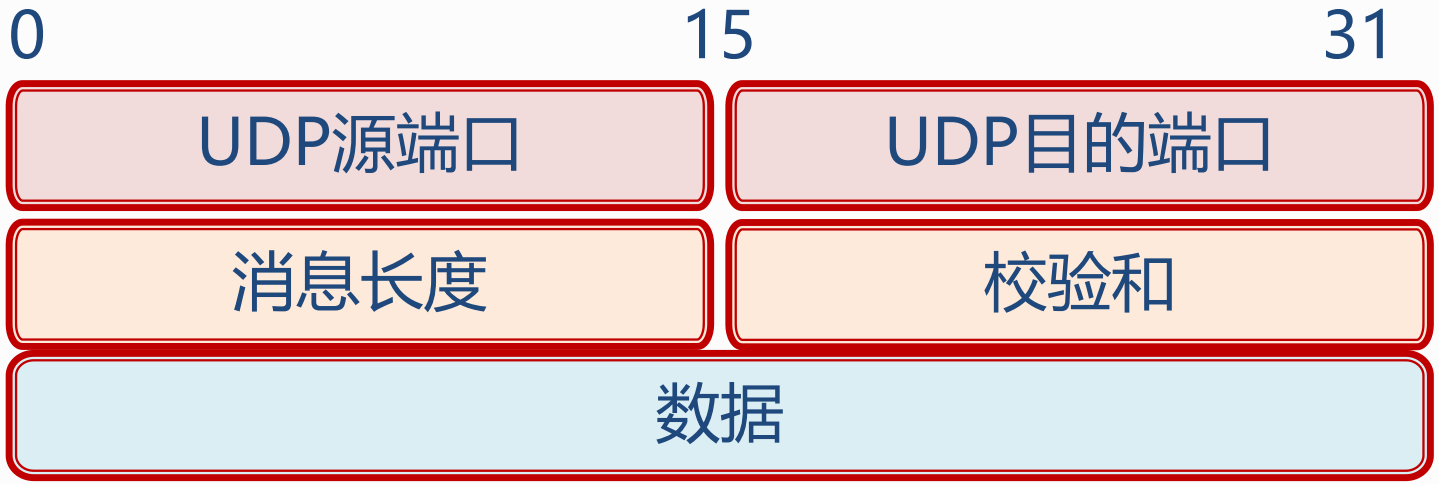
- SYN Flooding
  - 特点
    - 针对TCP/IP协议的薄弱环节进行攻击；
    - 发动攻击时，只要很少的数据流量就可以产生显著的效果；
    - 攻击来源无法定位；
    - 在服务端无法区分TCP连接请求是否合法。
  - 防御措施
    - 在防火墙上过滤来自同一主机的后续连接；
    - 采用SYN Cookie（无法防范全连接拒绝服务）

4、传输层协议安全分析 —— TCP协议安全威胁

- 其他针对TCP协议的攻击
  - ACK Flooding
    - 主机接收到带有ACK状态的数据包，需要检测数据包所包含的连接四元组是否存在，如存在需要检查数据包状态数据是否合法。
  - 序列号猜测攻击（会话劫持）
    - 攻击者通过猜测序列号，在TCP会话中插入自己构造的数据包。
  - Land攻击
    - 构造一个SYN包，其源地址和目标地址都被设置成某一个服务器地址；导致接收服务器向它自己的地址发送SYN-ACK消息，结果这个地址又发回ACK消息并创建一个空连接；每一个这样的连接都将保留直到超时。

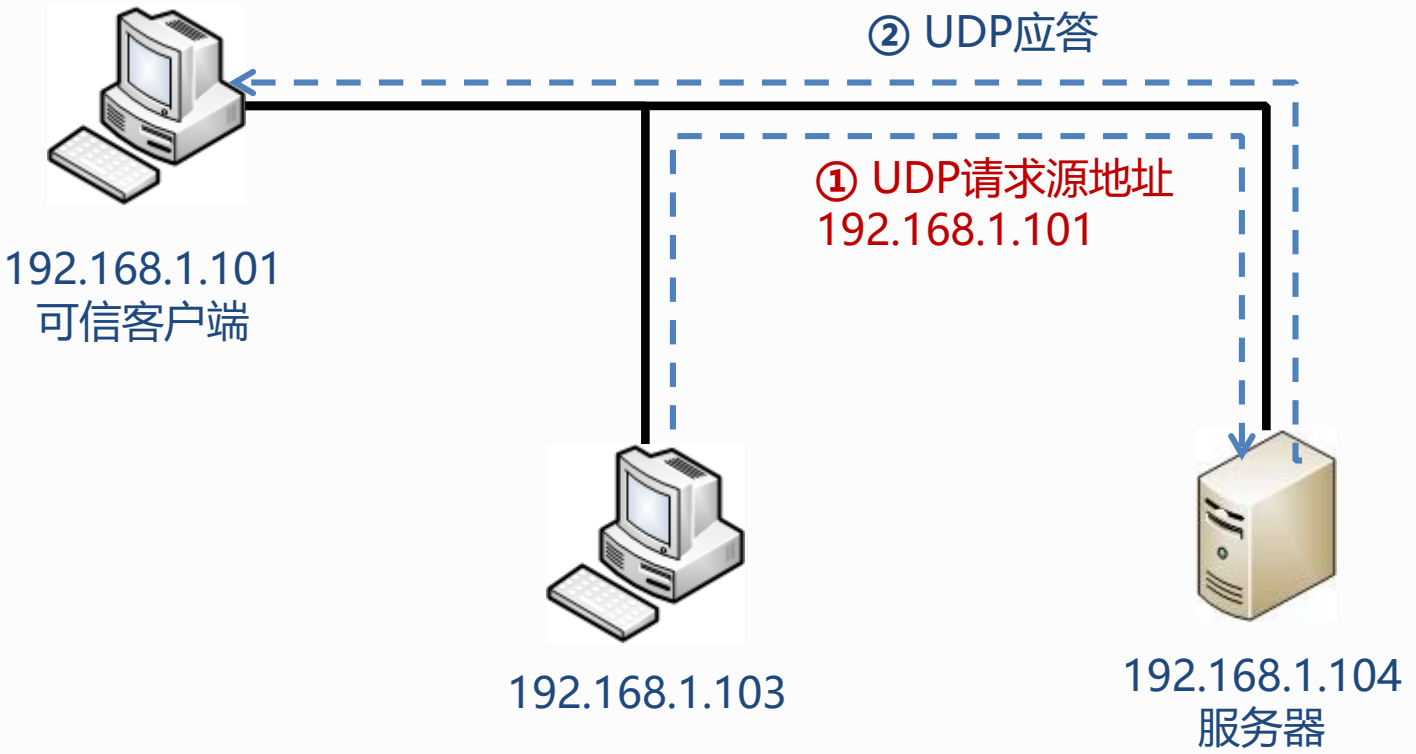
4、传输层协议安全分析 —— UDP协议安全威胁

- UDP协议报头



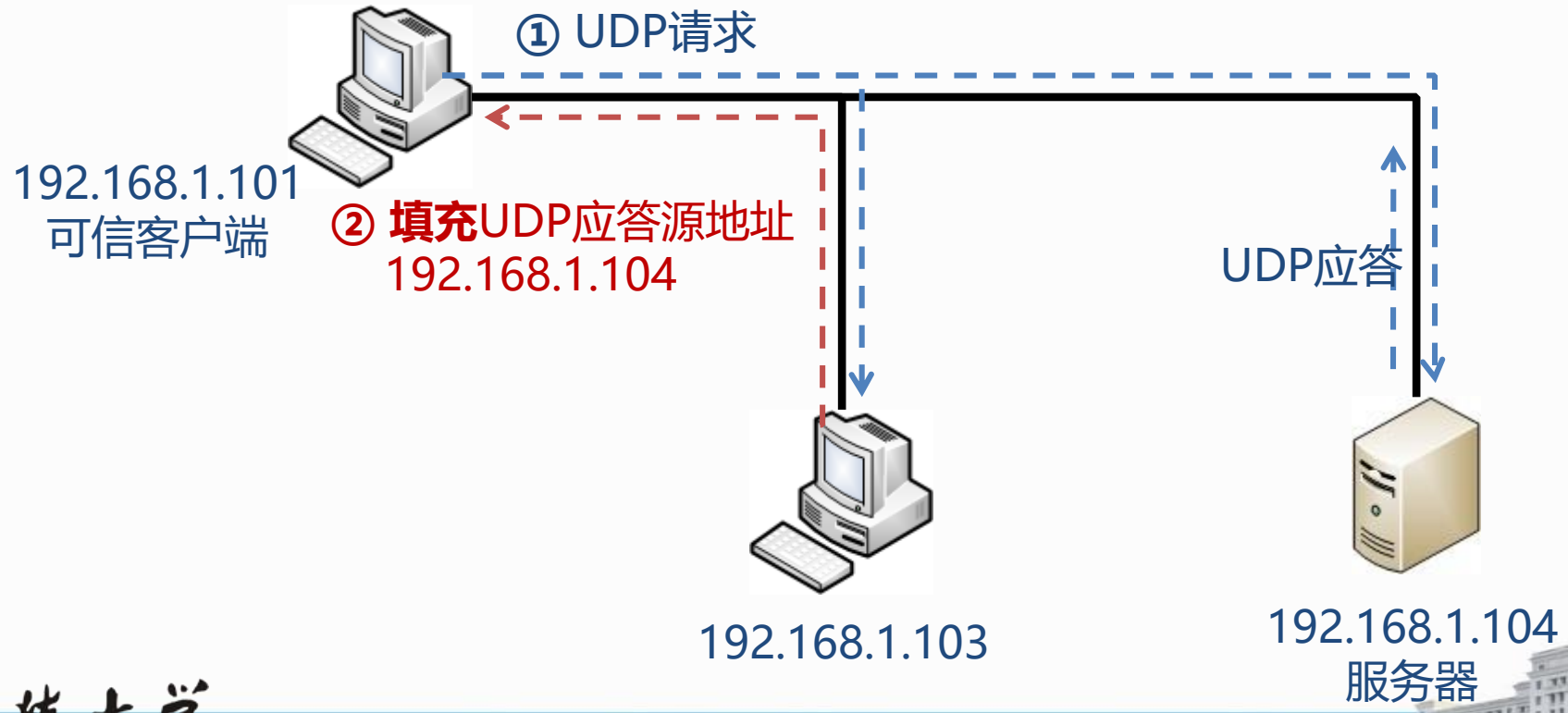
4、传输层协议安全分析 —— UDP协议安全威胁

UDP假冒



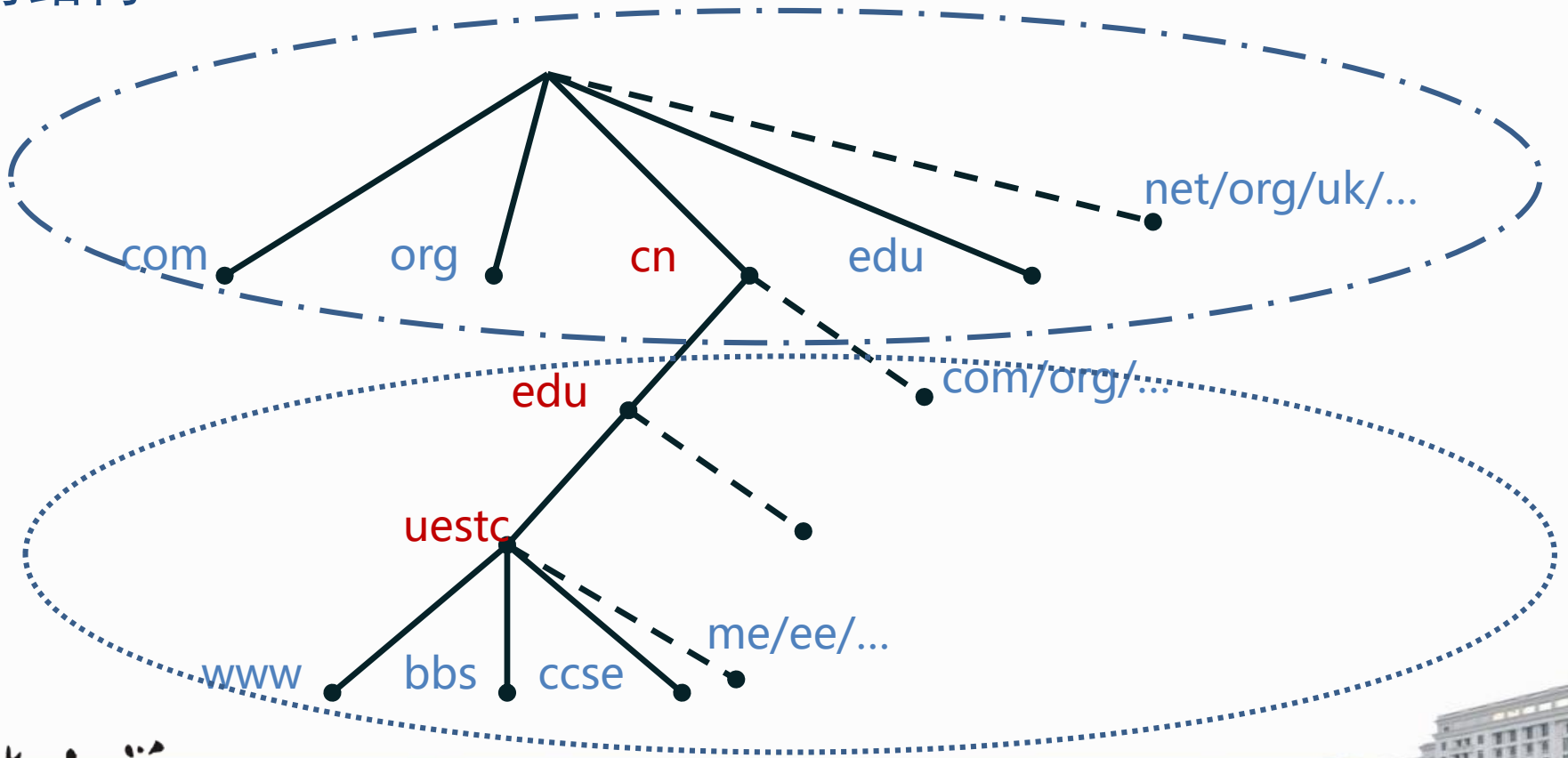
4、传输层协议安全分析 —— UDP协议安全威胁

UDP劫持



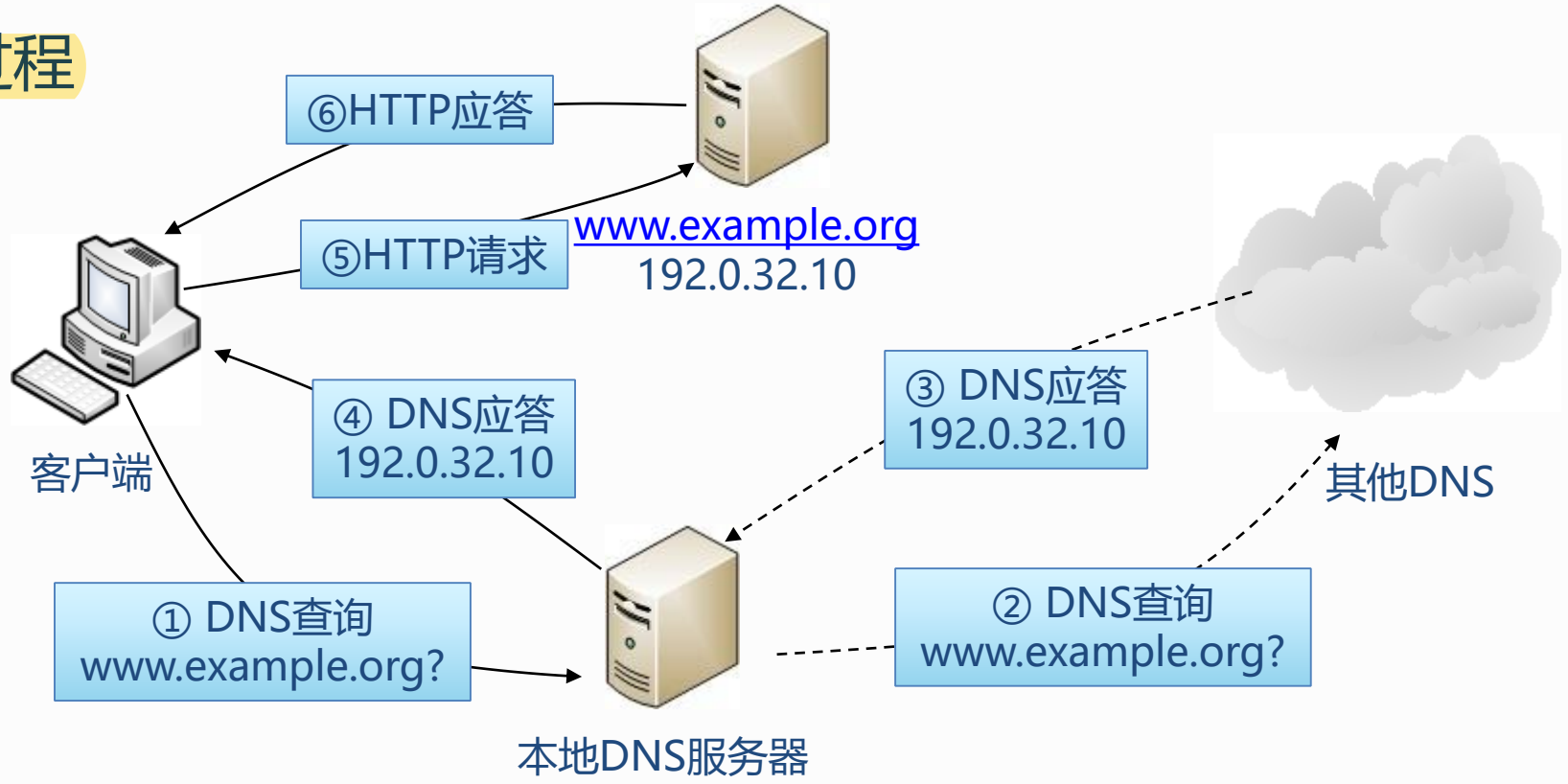
4、应用层协议安全分析 —— DNS协议安全威胁

- 域名服务结构



4、应用层协议安全分析 —— DNS协议安全威胁

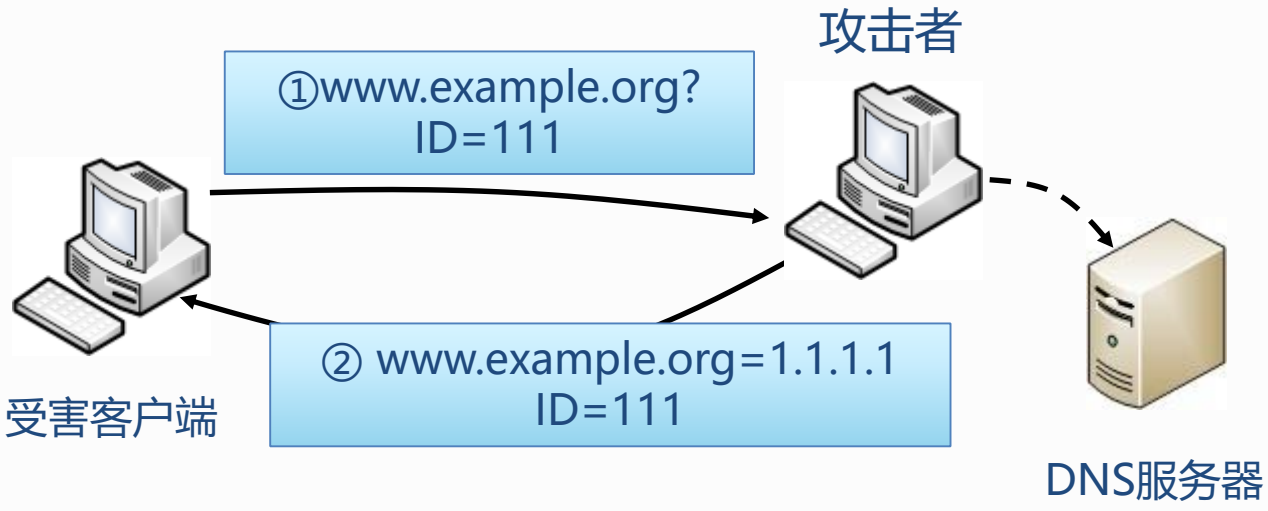
- 域名解析过程



DNS查询和应答是基于UDP的应用，验证不同的查询/应答是依靠报文中的标识段（ID）

4、应用层协议安全分析 —— DNS协议安全威胁

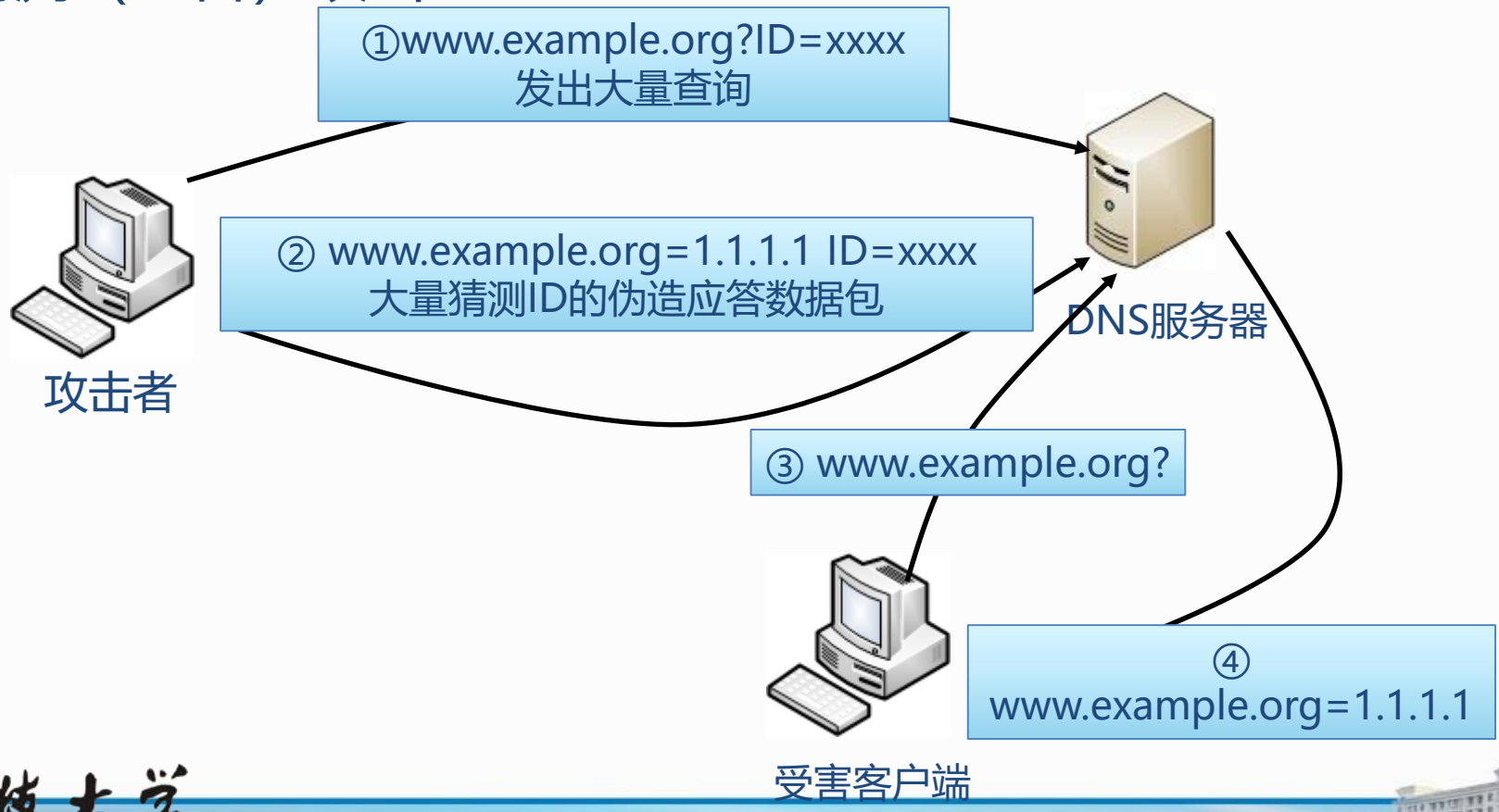
DNS欺骗



- 客户端以特定的标识ID向DNS服务器发送域名查询数据包
- DNS服务器查询之后以同样的ID返回给客户端响应数据包
- 攻击者拦截该响应数据包，并修改其内容，返回给客户端
- 难点在于如何获得标识号ID：可以结合ARP欺骗或ICMP重定向等手段，采用嗅探的方法得到

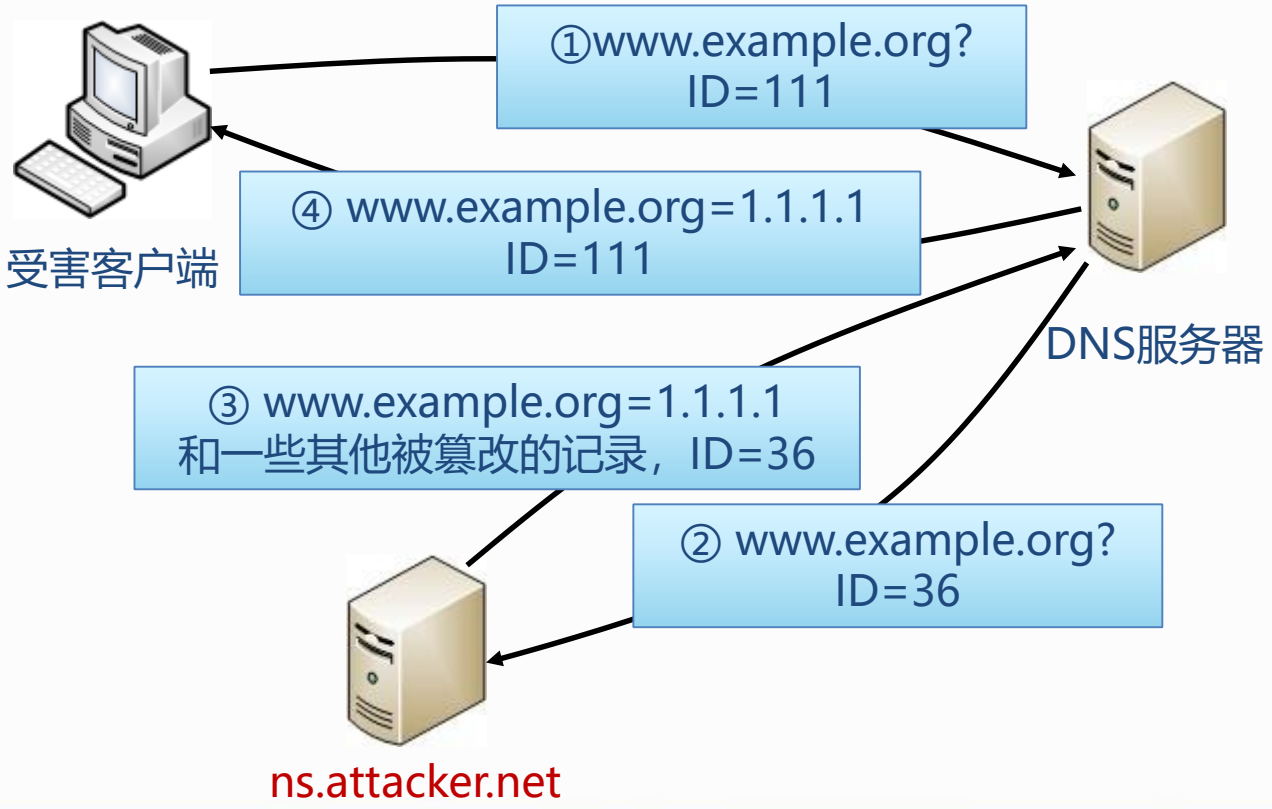
4、应用层协议安全分析 —— DNS协议安全威胁

- DNS猜测（生日）攻击



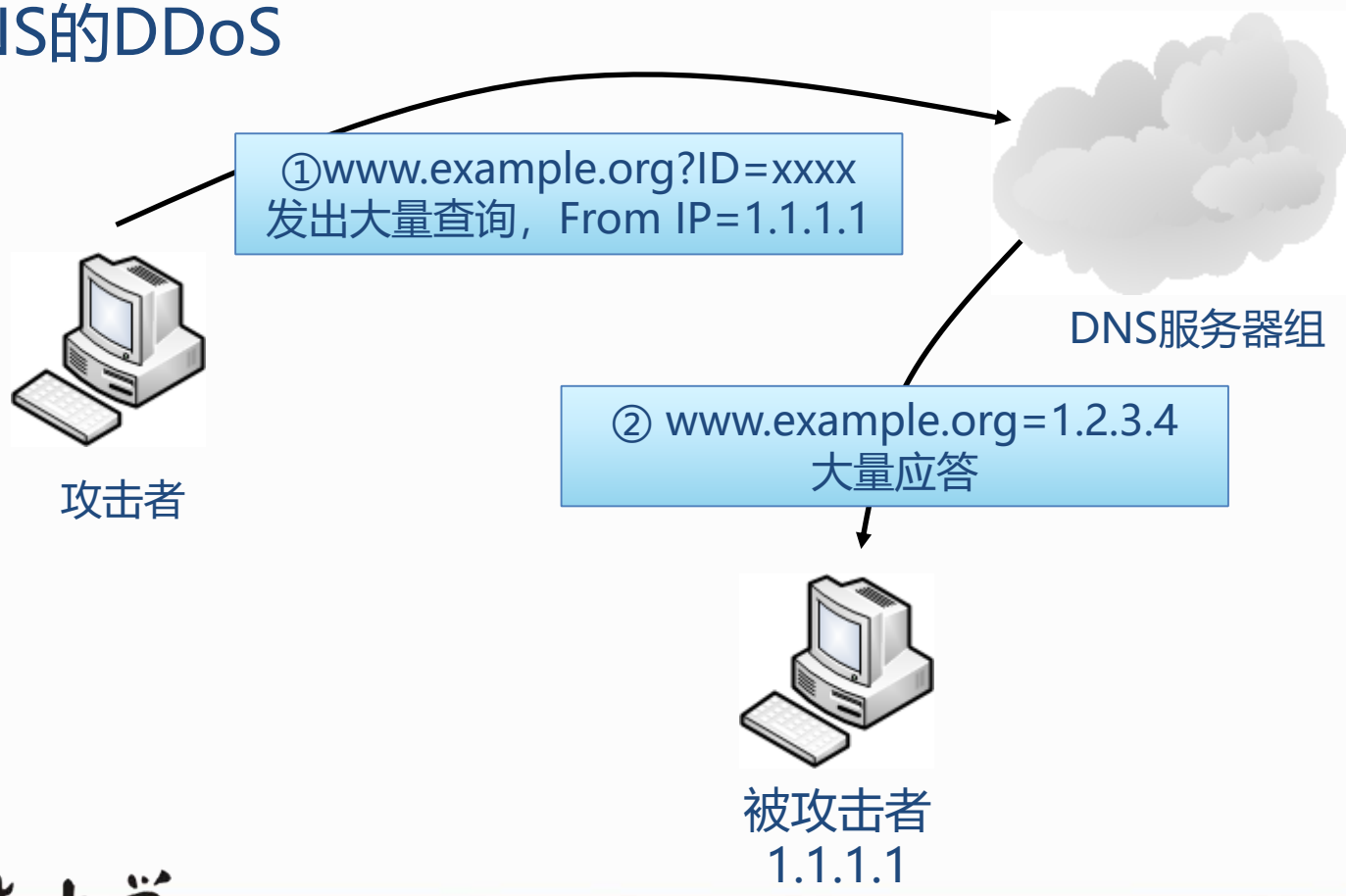
4、应用层协议安全分析 —— DNS协议安全威胁

- DNS缓存毒化



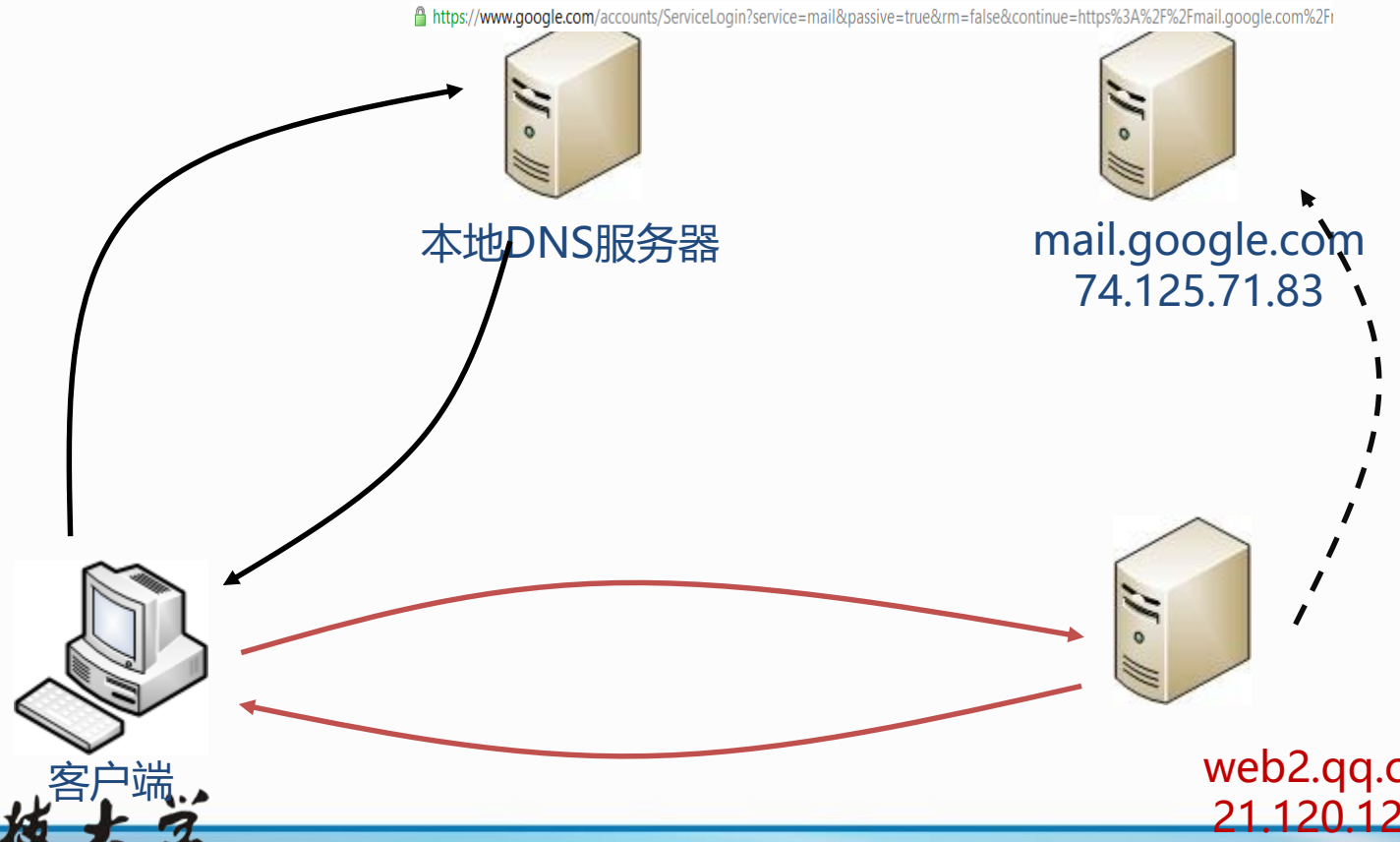
4、应用层协议安全分析 —— DNS协议安全威胁

- 基于DNS的DDoS



4、应用层协议安全分析 —— HTTP协议安全威胁

- HTTP钓鱼攻击



4、应用层协议安全分析 —— HTTP协议安全威胁

跨站攻击

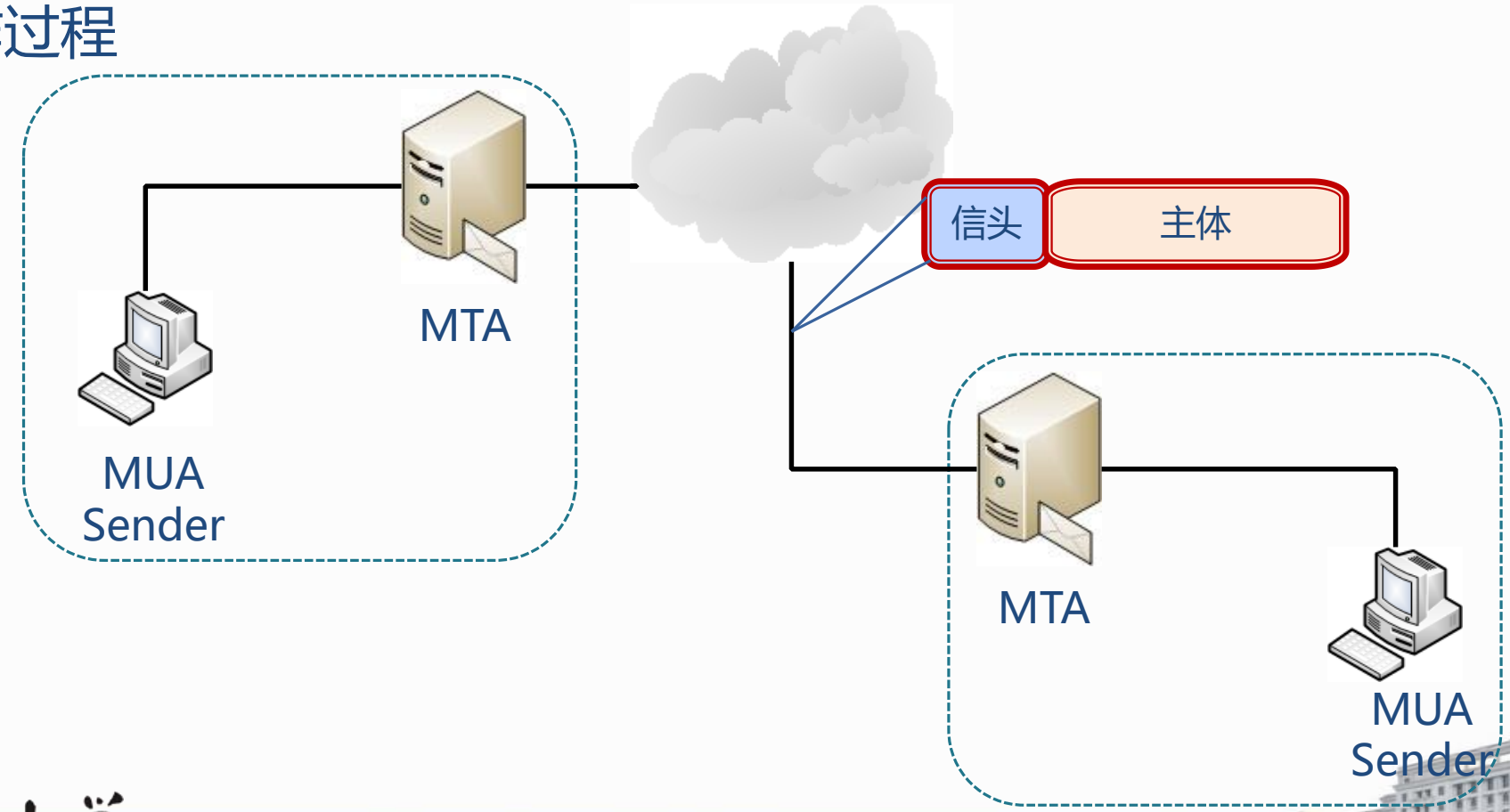
- 浏览器对网页的展现是通过解析HTML代码实现的，如果传入的参数含有代码浏览器会解析它而不是原封不动的展示。
- 示例
  - <?PHP
    echo "欢迎您，".$_GET['name'];
    ?>
  - 这段PHP代码的意思是在页面输出字符串“欢迎您，”和URL中name参数的值，比如用浏览器访问这个文件：http://localhost/test23.php?name=user，页面上就会出现“欢迎您，user”字样。

4、应用层协议安全分析 —— HTTP协议安全威胁

- 跨站攻击类型
  - 持久性跨站（persistent XSS or stored XSS）
    - 攻击数据存放于服务器。当用户访问正常网页时，服务端会将恶意的指令夹杂在正常网页中传回给用户
  - 非持久性跨站（non-persistent XSS or reflected XSS）
    - 当服务端未能正确地过滤客户端发出的数据，并根据用户提交的恶意数据生成页面时，就有可能生成非持久性跨站攻击。
  - DOM 跨站（DOM-based XSS）
    - 如果客户端脚本（例如JavaScript）动态生成 HTML的时候，没有严格检查和过滤参数，则可以导致 DOM 跨站攻击。

4、应用层协议安全分析 —— 电子邮件协议安全威胁

- 协议工作过程



4、应用层协议安全分析 —— 电子邮件协议安全威胁

- 电子邮件协议
  - SMTP：主要负责底层的邮件系统如何将邮件从一台机器传至另外一台机器
  - POP：目前的版本为 POP3，POP3 是把邮件从电子邮箱中传输到本地计算机的协议
  - IMAP：目前的版本为 IMAP4，是POP3的一种替代协议，提供了邮件检索和邮件处理的新功能
  - S/MIME:支持邮件加密的传输协议
- 电子邮件协议的安全
  - 传输安全、发送者身份确认、接收者已收到确认、邮箱炸弹攻击

- 测试点2-1
  - 在查询相关技术资料或进行实际验证的基础上回答以下问题：
    - 如果主机A跳过与主机B建立TCP连接的前两个步骤，直接发送三次握手中最后一个带ACK标志的包，主机B会如何处理?
    - 如果应用程序在释放连接的过程中（参见教材图2-6-3），由于应用程序异常终止来不及通知TCP协议释放连接，试问在实际情况中应该如何处理这种异常。
  - IP协议安全威胁产生的根本原因是什么？请举例分析。
  - TCP协议安全威胁产生的根本原因是什么？请举例分析。
  - UDP协议安全威胁产生的根本原因是什么？请举例分析。
  - 域名解析协议中主要存在哪些安全威胁？简要说明威胁过程和原理。

- 课后练习
  - 在虚拟机上安装部署Kali Linux，并验证ARP攻击原理和过程。
  - 安装过程参考：https://blog.csdn.net/KNIGH_YUN/article/details/79949512
  - 注意：在实验时以本机上的其他虚拟机作为攻击目标机，从事网络安全技术学习的前提是谨守职业规范和遵纪守法。

结束语

感 谢 聆 听!

zhaoyang@uestc.edu.cn

特别说明：PPT中所有来自于网络的图片和素材仅用于教学，并保证在未经原作者同意的情况下，不用于任何商业目的。