局域网安全实验

金舒原
jinshuyuan@mail.sysu.edu.cn
计算机学院

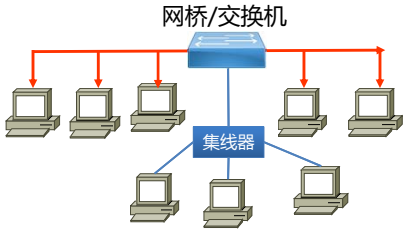
提纲

1. 局域网概述
   - 广播域与冲突域
   - 局域网中的标识与认证
   - 以太网帧格式
   - 交换机的自学习
   - 标识的映射
   - ARP协议
2. 局域网常见攻击及攻击原理
   - 交换机中的嗅探
   - ARP攻击
3. 实验说明
   - 实验目的和实验环境
   - 实验1: ARP缓存投毒攻击
   - 实验2: ARP中间人劫持攻击

局域网相关背景知识

- Layer1:
  - ✓集线器、网线
- Layer 2
  - ✓网桥, 交换机

- 广播域：FF-FF-FF 可以到达的范围
- 冲突域：同时通信会产生冲突的范围



上面的网络中：
- 有几个冲突域（Collision Domain）？
- 有几个广播域（Broadcast Domain）？

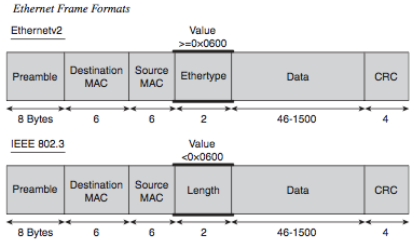
局域网中的标识与认证

- 标识（Identifiacation）：
  在一个局域网中，一台计算机的标识（Identification）是什么?
- 认证（Authentication）：
  如何证明这个标识是真实的，而不是假冒的？即，如何认证标识的合法性?

Ethernet PDU 帧格式

Ethernet Frame： Ethernet II，802.3 , SNAP

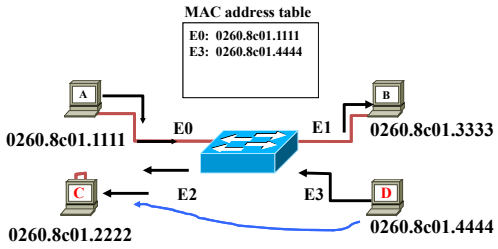
http://standards.ieee.org/getieee802/802.3.html



MAC Address：Burned-In-Address
Broadcast Address：FF-FF-FF

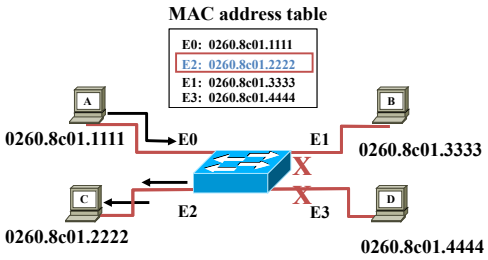
提问：网卡地址可以修改吗?

交换机是如何知道其所连接的机器的位置的？



- 主机 D 要发送数据帧给主机 C
- 交换机通过自学习，缓存主机 D 的MAC地址与 port E3 相连
- 当不知道主机C在哪里时，交换机将在所有端口（除了端口E3 ）进行广播

交换机是如何过滤/转发数据帧的？

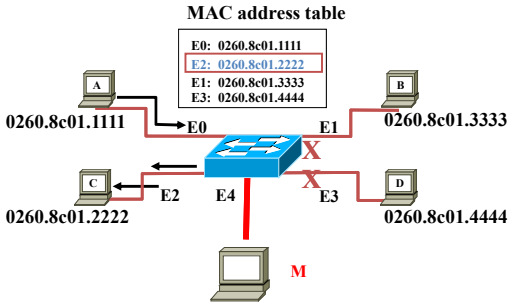


- 主机 A 发送数据给主机 C
- 目标C已知，帧不会被洪泛

当帧达到交换机时:

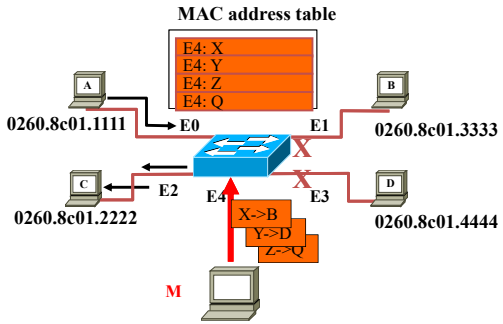
1. 记录到达的接口x以及发送主机的MAC地址
2. 使用目的MAC地址对交换表进行索引
3. if 为目的地址找到对应表项
   then {
   if 目的地址对应的接口为x
   then 丢弃该帧
   else 将该帧转发到表项指定的接口
   }
   else 洪泛 /* 即将该帧转发到除x外的所有接口*/

交换机中的嗅探（Sniffering）



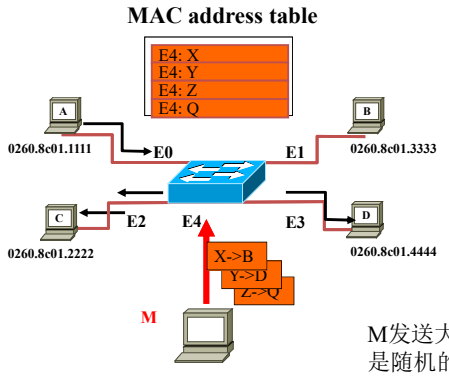
M可以嗅探A和C之间的流量吗?

MAC洪泛攻击（MAC Flooding attack）



9

MAC洪泛攻击（MAC Flooding attack）

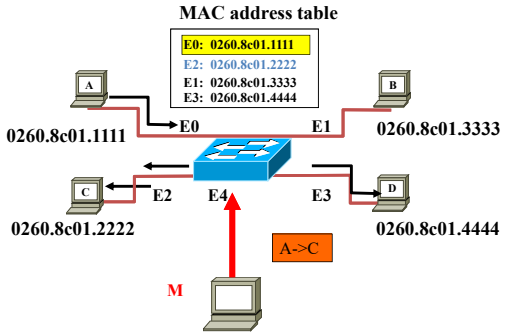


M发送大量Frame，源MAC是随机的

M现在可以嗅探A和C之间的流量吗?

10

MAC欺骗攻击（MAC spoofing attack）



M发送Frame，假冒A的MAC地址（A-C）；
交换机把C回复给A的Frame转发给谁呢?

11

如何防止，缓解?
交换机中的嗅探（MAC洪泛、 MAC欺骗）

请讨论

12

网络中的标识和认证

- 在网络的不同层上都有哪些标识ID?
  - ✓UserID: userid or email address
  - ✓HostID: domain name
  - ✓IP Address
  - ✓MAC address
- 认证
  - ✓标识 和 验证

如何判断所收到的数据源地址（MAC或IP）是真的?

13

标识的映射

- Domain name ←→ IP : DNS
  - ✓What is your DNS server? (really?)
  - ✓Is the reply from your DNS server true?
- IP ←→ MAC
  - ✓ARP/RARP
- DHCP
  - ✓IP address, Gateway, DNS, …

14

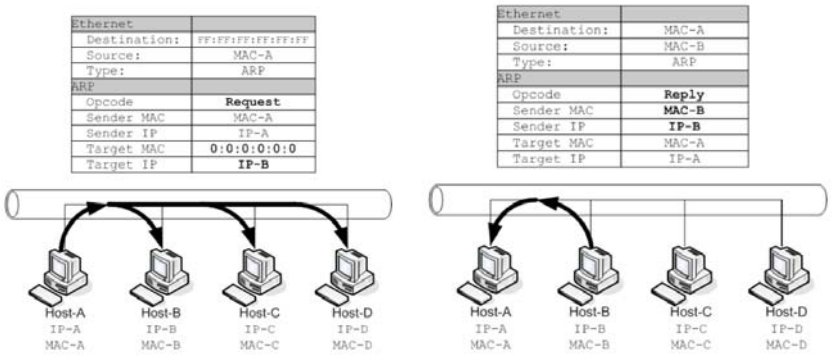
ARP / RARP

- RFC 826，11/1982, Informational, not standard
  - ✓The purpose of this RFC is to present a method of Converting Protocol Addresses (e.g., IP addresses) to Local Network Addresses (e.g., Ethernet addresses). This is a issue of general concern in the ARPA Internet community at this time. The method proposed here is presented for your consideration and comment. This is not the specification of a Internet Standard.

  Reference: https://tools.ietf.org/pdf/rfc826.pdf

15

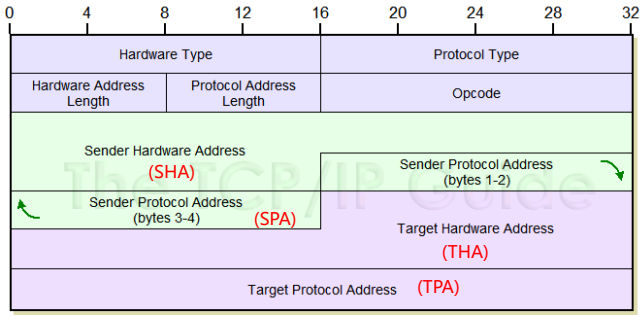
ARP Request and Reply



16

ARP协议PDU

- 两种报文格式：Request / Reply



http://www.tcpipguide.com/free/t_TCPIPAddressResolutionProtocolARP.htm

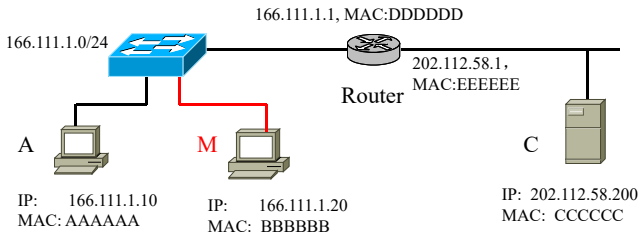
17

ARP Cache

- To limit the ARP traffic
- ARP Cache Entries
  - ✓Static ：arp -s
  - ✓Dynamic
- ARP reply, unsolicited (未经请求的、主动提供的)
  - ✓Sent actively after booting, to refresh caches of neighbors
  - ✓Unicast

18

ARP欺骗（ARP Spoofing）

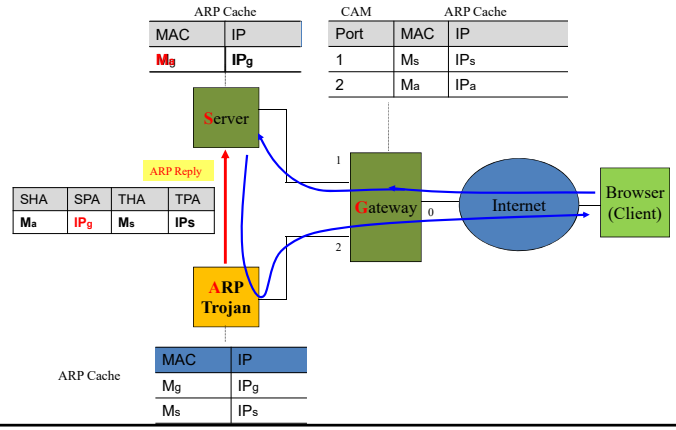


主机A向C发送的应用数据包（如http），用什么地址封装?

srcMAC	dstMAC	srcIP	dstIP	DATA
?	?	?	?	DATA

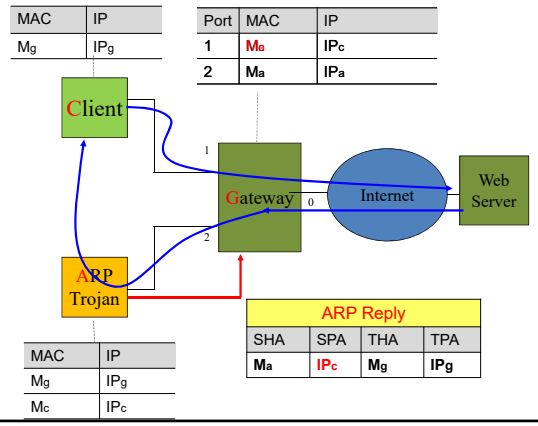
19

使用ARP欺骗假冒网关



20

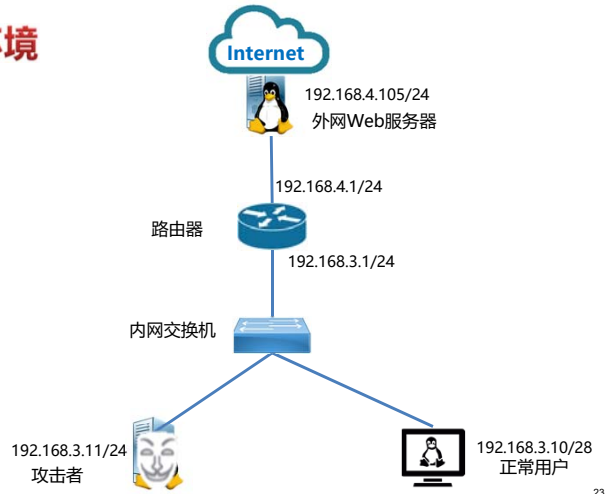
使用ARP欺骗假冒主机



如何防止，缓解 ARP欺骗（假冒网关、假冒主机）？

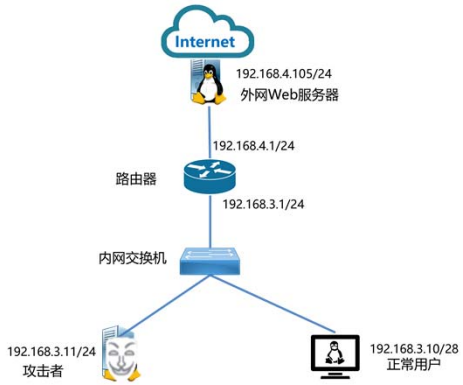
请讨论

局域网安全实验环境



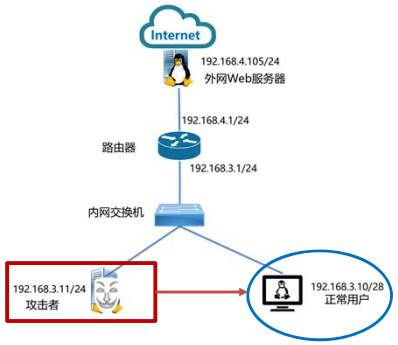
实验目的

- 掌握ARP协议的工作原理及作用
- 掌握ARP投毒攻击的基本原理
- 深入理解局域网中交换机和路由器的作用和工作原理
- 深入理解局域网中的标识
- 思考并掌握防范ARP攻击的技术



实验内容

- 实验1 ARP缓存投毒攻击
  - 观察正常用户的arp缓存
  - 获取正常用户主机MAC地址
  - 在攻击者主机上编写攻击脚本，分别用两种方式实现对正常用户网关地址的假冒攻击
  - 思考如何防御

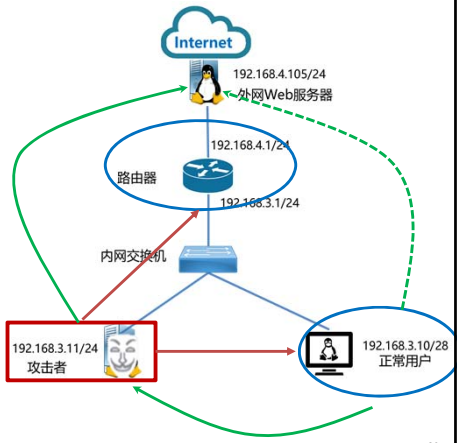


ARP缓存中的IP与MAC地址的对应关系			
	IP地址	MAC地址	谁假冒了谁
攻击前			
ARP Request缓存投毒后			
ARP Reply缓存投毒后			

25

实验内容

- 实验2 基于ARP缓存投毒的中间人攻击
  - 基于实验1的攻击方法，对正常用户和网关进行arp缓存投毒攻击
  - 同时污染正常用户主机与网关的缓存，使得：
    - 在用户主机缓存中，网关IP对应的是攻击者MAC;
    - 在网关缓存中，正常用户主机IP对应的是攻击者的MAC。
  - 观察中间人攻击效果
  - 窃取正常用户访问外网Web服务器的用户名和口令



26