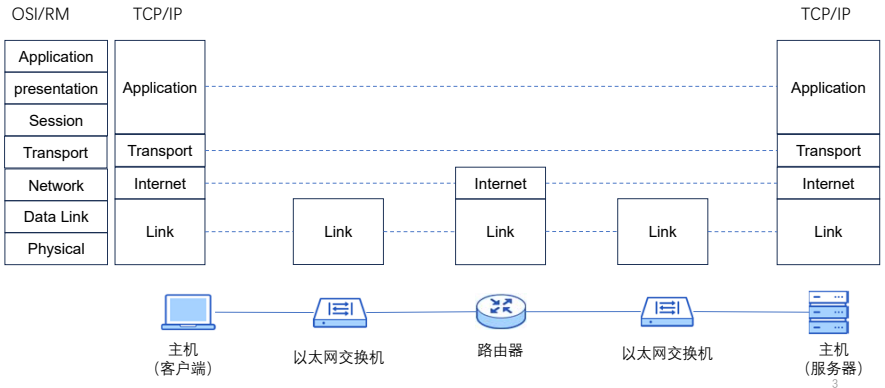
第一章 计算机网络基础及常用工具

金舒原
计算机学院
jinshuyuan@mail.sysu.edu.cn

提纲

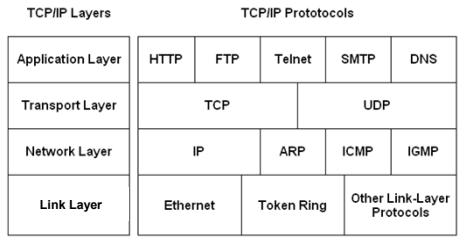
1. TCP/IP协议基础及网络环境
   - TCP/IP协议栈
   - 常用网络设备和网络服务
   - 子网划分与子网掩码
   - 多个层次的标识与映射
   - 实例分析Web 访问流程
2. 常用网络工具
   - TCPDUMP
   - Wireshark
   - Scapy
3. 实验说明
   - 实验目的和实验环境
   - 实验1: 用tcpdump 分析ICMP
   - 实验2: 用Wireshark 分析Web访问
   - 实验3: 用Scapy构造ICMP 请求

OSI/RM的七层模型 和 TCP/IP的四层模型



TCP/IP 协议族

- OSI/RM只是概念，没有实现
  - OSI/RM只是个美丽的梦，而TCP/IP生活在梦一样的现实里
- 但是OSI七层模型的概念被主流网络教材采纳，故课程也使用这些概念，如
  - 链路层是第二层
  - 网络层对应 internet layer
  - 应用层协议是“第七层”协议



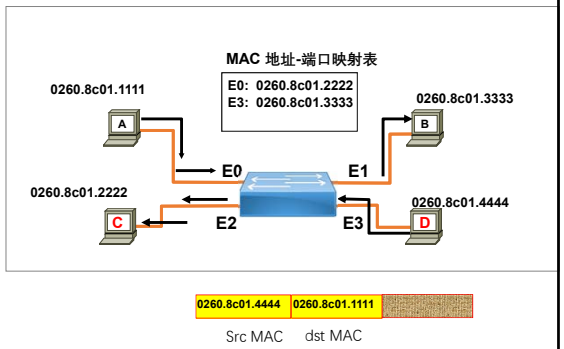
链路层设备：以太网交换机

常见的以太网交换机外形

本课程中的图标

以太网交换机

- 以太网交换机工作原理：
  - 根据数据帧的目标MAC地址，查找MAC地址和端口映射表，转发数据帧
- MAC地址映射表的学习过程
  - 初始为空
  - 收到一个Frame时，源端口源MAC加入映射表
  - 向所有端口转发（广播）
  - 回复的包源端口、源MAC加入映射表
- 广播地址： FF:FF:FF



提问：D发送了一个数据帧，交换机的MAC地址表中没有，该如何处理

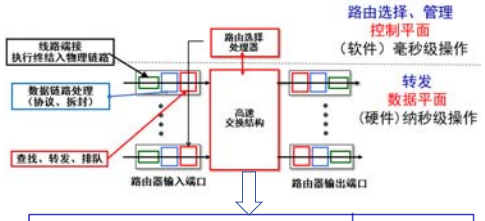
网络层设备：路由器

常见的路由器外形

本课程中的图标

路由器的转发功能

- 路由器的转发原理：
  - 根据目的IP地址、查找路由器内部的路由表，把数据包转发到路由器相应的输出端口
- 路由表的构建
  - 对每台路由器进行适当配置
  - 每路由器控制：由每台路由器通过配置的路由协议建立
  - 逻辑集中式控制：软件定义网络
- 对于广播地址：
  - FF:FF:FF，实际应用中的路由器通常会丢弃广播包。

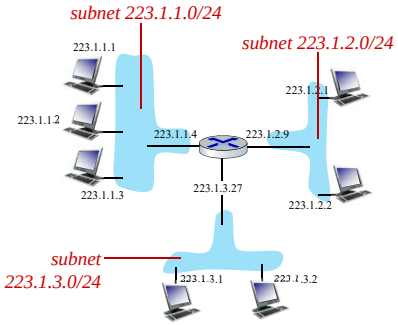


目的地址范围	链路接口
11001000 00010111 00010*** ********	0
11001000 00010111 00011000 ********	1
11001000 00010111 00011*** ********	2
otherwise	3

提问：11001000 00010111 00011000 10101010
路由器会转发到哪个出口?

子网

- 什么是子网?
  - 无需通过中间路由器即可物理连接到对方的设备接口
- 定义子网的方法:
  - 将每个接口与其主机或路由器分离，创建隔离网络的“孤岛”
  - 每个隔离的网络称为子网
- IP地址具有以下结构:
  - 子网部分: 同一子网中的设备具有共同的高位
  - 主机部分: 剩余低位

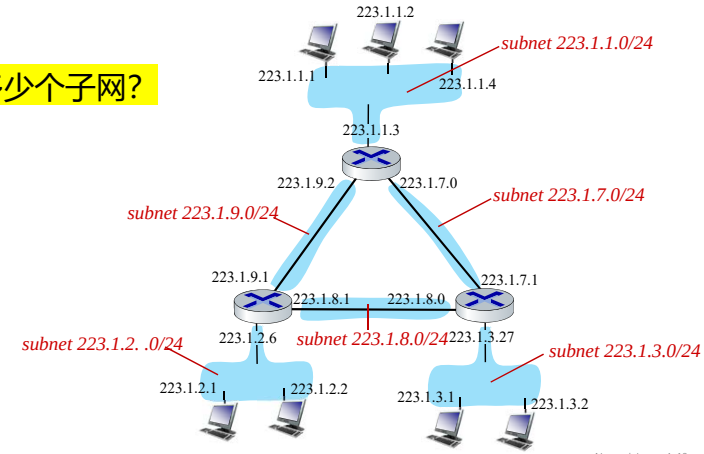


子网掩码: /24
(最左侧的24 比特: IP地址的子网部分)

子网

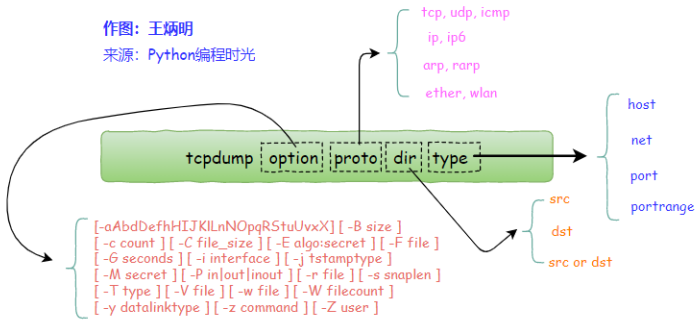
提问：有多少个子网?

答：6个



tcpdump

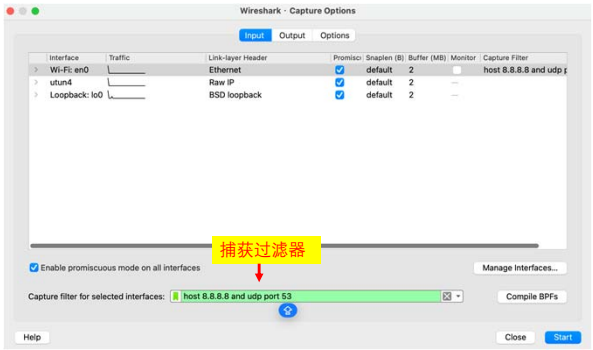
tcpdump -i eth0
tcpdump src 192.168.0.10 and dst port 22
tcpdump port 80
tcpdump arp
... ...



Wireshark

Wireshark 的捕获过滤器

- 选择或排除将要捕获的的流量
- Capture
  -Options
  --Input:
- 使用BPF（Berkeley Packet Filter）语法

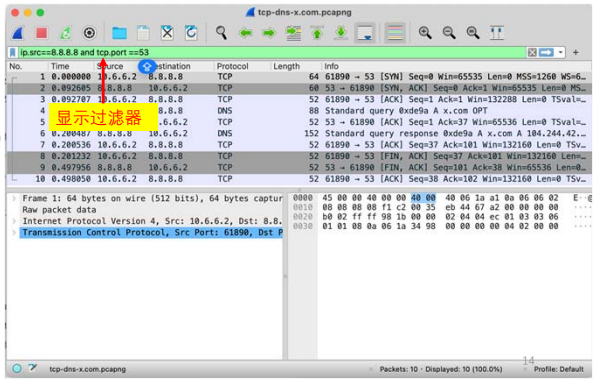


Wireshark 的显示过滤器

- 只显示符合规则的数据包
- 数据包里表上输入
- 使用与捕获过滤器（BPF）不同的语法：

  ip.src==8.8.8.8

  BPF：src 8.8.8.8



Wireshark 参考文献

[WS]Wireshark 官方网站： https://www.wireshark.org

[WS-BOOK] [美]克里斯.桑德斯(Chris Sanders)著 诸葛建伟 陆宇翔 曾皓辰译 Wireshark 数据包分析实战（第3版）人民邮电出版社

[WS-DISPLAY] Wireshark Display Filters , https://wiki.wireshark.org/DisplayFilters

[TCPDUMP] TCPDUMP 官方网站：https://tcpdump.org

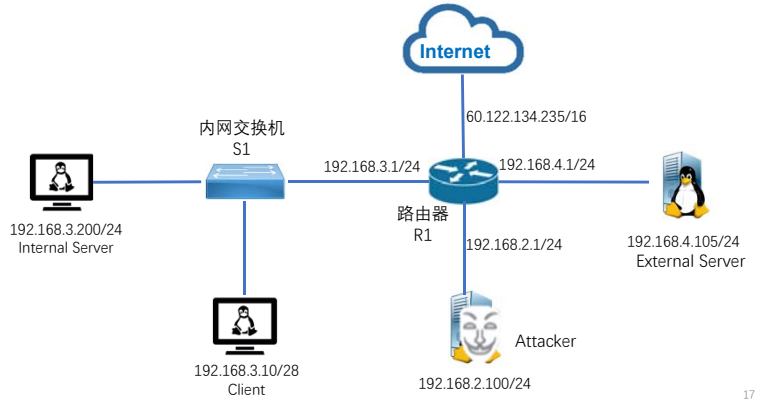
[TCPDUMP-MAN] tcpdump 命令手册：https://www.tcpdump.org/manpages/tcpdump.1.html

scapy

- 用 Python 语言编写的功能强大的交互式数据包构造、解析程序和库，支持多种协议。
- 简单、灵活的数据包构造功能，可以自动匹配网络请求并发送响应等等。
- 本课程主要用scapy构造数据包，实现扫描、地址假冒等攻击测试。

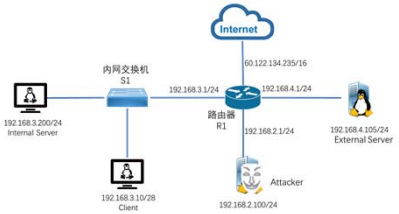
https://scapy.net/

网络基础实验环境



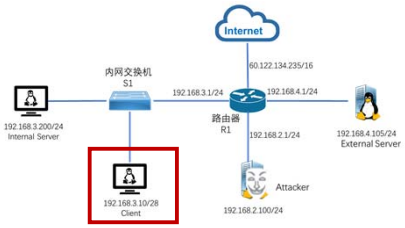
实验目的

- 通过分析网络流量理解交换机、路由器等工作原理，理解子网划分和子网掩码，进一步理解网络原理，为学习以后的章节准备基础知识
- 熟练使用tcpdump、 wireshark等流量分析工具进行网络流量分析
- 掌握Scapy的用法，能够使用scapy构造常见的协议数据包
- 为后面章节的实验准备基本的操作技能



实验内容

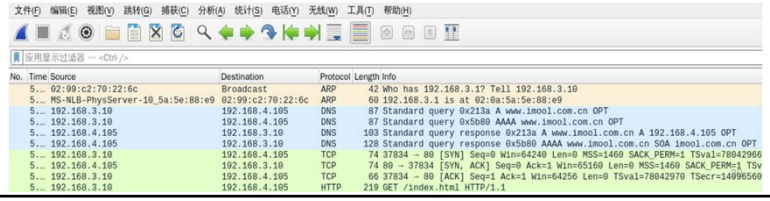
- 实验1 使用tcpdump分析ICMP流量
  - 登录Client
  - 用tcpdump 监听端口eth0
  - 在Client机器上观察并记录子网内、跨子网和掩码配置错误下的ARP请求、ARP响应，ICMP ECHO请求及响应



操作	ARP请求		ARP响应		ICMP ECHO请求		ICMP ECHO 响应	
	源MAC	目标MAC	源MAC	目标MAC	源IP	目标IP	源IP	目标
子网内								
跨子网								
掩码错								

实验内容

- 实验2 使用wireshark分析Web访问过程流量
  - 在Client上先运行wireshark，选择监听以太网网卡eth0的所有流量
  - 根据wireshark中捕获到的流量，解释从访问www.imool.com.cn到关闭浏览器整个过程中Client主机都发生了哪些网络活动
- 特别关注
  - 域名解析过程涉及哪些IP包，请求和响应分别是什么?
  - ARP解析过程中，网关的MAC地址是什么?
  - Client和www.imool.com.cn的连接建立过程、连接拆除过程
  - 使用Wireshark的协议流追踪功能，提取Web访问的Cookie信息



实验内容

- 实验3 使用Scapy构造ICMP Echo Request数据包
  - Attacker机器中提供有Scapy工具，可通过Scapy交互式界面或在python脚本中导入Scapy库的方式进行操作
  - 利用Scapy，从Attacker机器伪造一个ICMP Echo Request（通常称为 ping）并为其添加负载，发送出去。
  - 在Client上捕获从External Server发送来的ICMP Echo reply包