

实验基础 (2)

金舒原
jinshuyuan@mail.sysu.edu.cn
计算机学院

1

本章内容

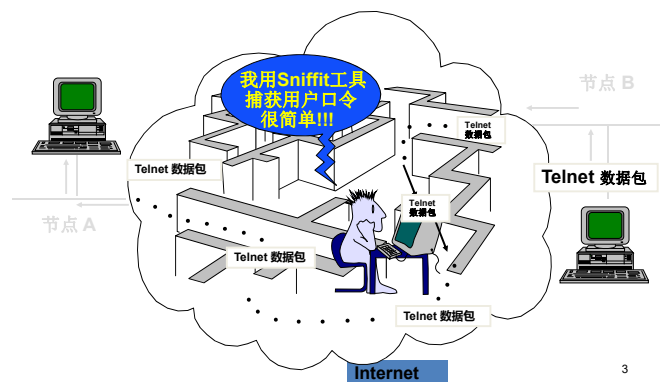
- 协议分析软件
- 网络仿真软件
- 绘制拓扑图
- 路由器、交换机原理
- 实验报告的书写要求

学会使用协议分析软件Wireshark

学会使用网络仿真软件Packet Tracer

2

网络协议分析软件



3

网络协议分析软件Wireshark

- Wireshark 是常用网络包分析工具。网络包分析工具的主要作用是尝试捕获网络包，并显示包的尽可能详细的情况
- Wireshark对于网络上的异常流量行为，不会产生警示或是任何提示。通过仔细分析Wireshark截取的数据包能够帮助使用者对于网络行为有更清楚的了解
- Wireshark没有数据包生成器，因而只能查看数据包而不能修改，它只会反映出被抓取的数据包资讯，并对其内容进行分析
- 该软件可到<https://www.wireshark.org/download.html> 载最新版本。

4

Wireshark软件 (p20-29)

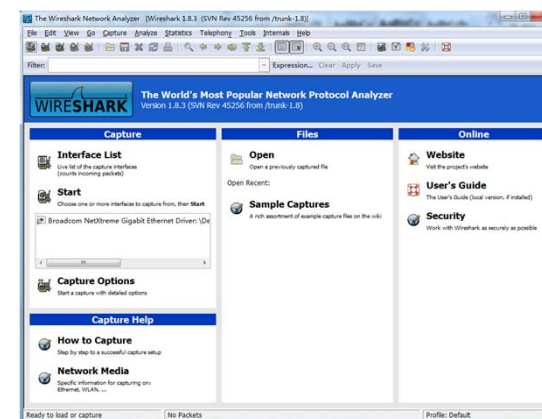
是一款功能强大而操作相对简便的抓包软件。在进行网络实验时，往往采用抓包分析的方法来验证一些实验，故应熟练掌握此工具软件



Gerald Coombs
1997年开始撰写 ethereal
1998/7 V0.2.0

5

Wireshark主界面



6

Wireshark主窗口组成

- 菜单：提供了对Wireshark进行配置的若干功能项目
- 主工具栏：提供快速访问菜单中经常用到的项目功能
- 过滤工具栏：提供处理当前显示过滤的方法
- “数据帧列表”面板：显示打开文件的每个帧的摘要。单击面板中的每个条目，帧的其他情况将会显示在另外两个面板中
- “数据帧详情”面板：显示在“数据帧列表”面板中所选帧的数据解析结果
- “数据帧字节”面板：显示在“数据帧列表”面板中所选帧的原始数据，以及在“数据帧详情”面板高亮显示的字段
- 状态栏：显示当前程序状态以及捕获数据的更多详情


7

Wireshark主菜单

File	Edit	View	Go	Capture	Analyze	Statistics	Telephony	Tools	Internals	Help
打开或保存捕获的信息	查找或标记封包，进行全局设置	查看Wireshark视图	跳转到捕获的数据	设置捕捉过滤器并开始捕捉	设置分析选项	查看Wireshark的统计信息	显示与电话业务相关的若干统计窗口，包括媒体分析、流程图、协议层次统计等	工具的启动项，比如创建防火墙访问控制规则等	比如罗列Wireshark支持的协议等，包含Wireshark内部信息的若干启动项	查看本地或者在线帮助

8

Wireshark主工具栏



缩小字体

增大字体

开启关闭实时捕捉时自动滚动包列表

切换是否以彩色方式显示包列表

跳转到最后一个包

跳转到第一包

弹出一个设置跳转到指定的包的对话框

跳转到历史记录中的上一个

返回历史记录中的上一个

打开一个对话框，查找包

打印捕捉文件的全部或部分

重新载入当前文件

关闭当前文件。若未保存将会提示是否保存

保存当前文件为任意其他的文件

启动打开文件对话框，用于载入文件

停止当前捕捉，并立即重新开始

停止当前的捕捉

使用最后一次的捕捉设置立即开始捕捉

打开捕捉选项对话框

打开接口列表对话框

9

Wireshark "Filter" 工具栏

Filter:

Expression...

Clear

Apply

Save

保存过滤串

应用当前输入框的表达式为过滤器进行过滤

清除输入框

打开用以从协议字段列表中编辑过滤器的对话框

过滤输入框

如果输入的格式不正确，或者未输入完成，则背景显示为红色；直到输入合法的表达式，背景会变为绿色。可以点击下拉列表选择先前键入的过滤字符。即使重新启动程序，列表也会一直保留。输入完后点击右边的Apply按钮或者回车，使过滤生效

打开构建过滤器对话框

10

“数据帧列表” 面板

- 列表中的每行显示捕获文件的一个数据帧。如果选择其中一行，该数据帧的更多情况会显示在“数据帧详情”面板和“数据帧字节”面板中，右击数据帧，可以显示对数据帧进行相关操作的上下文菜单
- No.: 数据帧的编号，编号不会发生改变，即使进行了过滤也同样如此
- Source: 数据帧的源地址
- Destination: 数据帧的目标地址
- Protocol: 数据帧的协议类型的简写
- Length: 数据帧的长度
- Info: 数据帧内容的附加信息

11

“数据帧详情” 面板

- “数据帧详情”面板显示当前数据帧（在“数据帧列表”面板被选中的数据帧）的详情列表
- 该面板显示“数据帧列表”面板选中数据帧的协议及协议字段，以树状方式组织。右击这些字段会获得相关的上下文菜单
- 其中，某些协议字段会以特殊方式显示，例如：
 - Generated fields/衍生字段：Wireshark会将自己生成附加协议字段加上括号。衍生字段是通过该数据帧相关的其他数据帧结合生成的。例如：Wireshark 在对TCP流应答序列进行分析时，将会在TCP协议中添加[SEQ/ACK analysis]字段。
 - Links/链接：如果Wireshark检测到当前数据帧与其他数据帧的关系，将会产生一个到其他数据帧的链接。链接字段显示为蓝色字体，并加有下划线。双击它会跳转到对应的数据帧。

12

“数据帧字节” 面板

- “数据帧字节” 面板以十六进制转储方式显示当前选择数据帧的数据
- 通常在十六进制转储形式中，左侧显示数据帧数据偏移量，中间栏以十六进制表示，右侧显示为对应的ASCII字符。用来显示数据包在物理层上传输时的最终形式

13

状态栏

- 状态栏用于显示信息，通常状态栏的左侧会显示相关上下文信息，右侧会显示当前包数目
- 初始状态栏：该状态栏显示的是没有文件载入时的状态，如：刚启动Wireshark时

Ready to load or capture No Packets

- 载入文件后的状态栏：左侧显示当前捕捉文件信息，包括名称、大小、捕捉持续时间等。右侧显示当前包在文件中的数量，会显示如下值
 - P 捕捉包的数目
 - D 被显示的包的数目
 - M 被标记的包的数目

File: test.cap 14 KB 00:00:02 P: 120 D: 120 M: 0

- 已选择协议字段的的状态栏

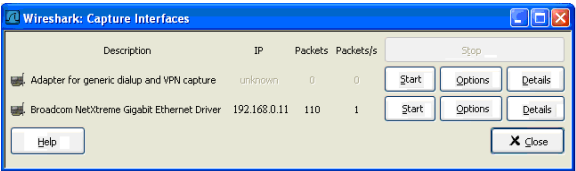
Ethernet II (Encapsulated), 2 bytes P: 120 D: 120 M: 0

- 如果已经在"Packet Detail/包详情"面板选择了一个协议字段，将会显示上图

14

Wireshark使用方法

- ①使用下图按钮，打开捕捉接口对话框，浏览可用的本地网络接口，选择需要进行捕捉的接口启动捕捉



Packets: 从此接口捕捉到的包的数目。如果一直没有接收到包，则会显示为灰色
Packets/s: 最近一秒捕捉到包的数目。如果最近一秒没有捕捉到包，将会是灰色显示
Stop: 停止当前运行的捕捉
Capture: 从选择的接口立即开始捕捉，使用最后一次捕捉的设置。
Options: 打开该接口的捕捉选项对话框
Details: 打开对话框显示接口的详细信息

15

Wireshark使用方法

- ②使用捕捉选项按钮，启动捕捉选项配置对话框；有时需要配置高级选项，例如需要捕获一个文件，或者限制捕获的时间或大小，可以单击主菜单Capture的 options
- ③如果前次捕捉时的设置和现在的要求一样，可以点击图中开始捕捉按钮或者是菜单项立即开始本次捕捉
- ④启动捕捉后，即开始捕捉接口信息。当不再需要捕捉时，可使用捕捉信息对话框上的"stop"按钮停止

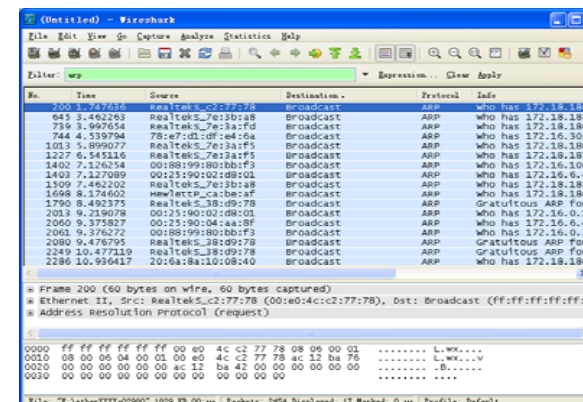
16

Wireshark的过滤规则

- Wireshark的一个重要功能，就是Filter。由于其所捕捉的数据较复杂，要迅速、准确的获取我们需要的信息，就要使用过滤工具
- 可以有两次过滤：第一次是捕捉过滤，用来筛选需要的捕捉结果；第二次是显示过滤，只将需要查看的结果显示
- Filter位于主工具栏上，可按规则输入过滤条件
- 常用的过滤规则包括（见书P32-33）

17

数据包捕获实例



分为七列，分别表示：编号（编号不会发生改变）、时间戳、源IP、目的IP、最高层协议、分组长度、附加信息。

18

网络协议分析软件

- Wireshark窗口的数据包列表的每一行都对应着网络上的单独一个数据包。默认情况下，每行会显示数据包的时间、源地址和目标地址，所使用的协议及关于数据包的一些信息。通过单击此列表中的某一行，可以获悉更详细的信息
- 中间的树状信息包含着上部列表中选择的某数据包的详细信息。“+”图标揭示了包含在数据包内的每一层信息的不同的细节内容。这部分的信息分布与查看的协议有关，一般包含有物理层、数据链路层、网络层、传输层等层信息
- 底部的窗格以十六进制及ASCII形式显示出数据包的内容，其内容对应于中部窗格的某一行

19

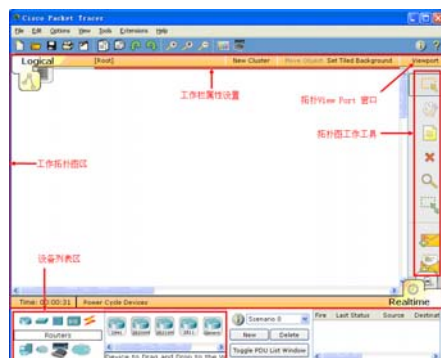
网络模拟软件Packet Tracer(p29-45)

- Packet Tracer 是Cisco 公司针对其CCNA 认证开发的一个用来设计、配置和故障排除网络的模拟软件
- Packet Tracer是一个辅助学习工具。利用该软件可以学习网络连接方法、理解网络设备对数据包的处理、学习IOS的配置、以及锻炼故障排查能力
- 使用者可在软件的图形用户界面上直接使用拖放方法创建网络拓扑，并通过一个图形接口配置该拓扑中的设备。该软件还提供数据包在网络中进行的详细处理过程，以便观察网络实时运行情况

20

网络模拟软件Packet Tracer

• Packet Tracer 5.3界面



21

网络模拟软件Packet Tracer

设备列表区

- 设备列表主要是为了创建网络拓扑使用列表，分为两部分，一部分是设备类别选择，另一部分是某个类别设备的详细型号选择。如下图所示



22

网络模拟软件Packet Tracer

Realtime mode(实时模式)和 Simulation mode (模拟模式)

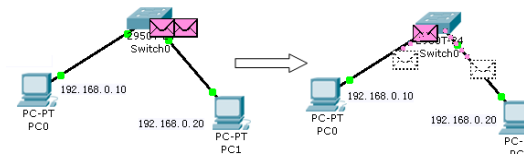
- Packet Tracer使用实时、模拟两个操作模式呈现网络的行为
- 在主界面的最右下角有两个切换模式，分别是Realtime mode (实时模式) 和Simulation mode (模拟模式)
- 实时模式中网络行为和真实设备一样，对所有网络行为将即时响应
- 模拟模式中用户可以看和控制时间间隔、数据传输的内部流程、数据跨越网络的演化

23

网络模拟软件Packet Tracer

数据包的Flash动画。

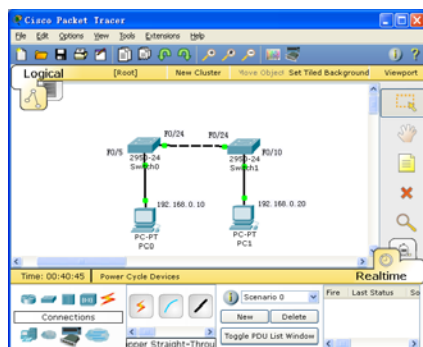
- 在Simulation mode模式下，只需点击位于工作拓扑图区下边界的“Auto Capture/play”(自动捕获/播放)，再在最右边的工具栏中，选择信封带十号的，在主机A上点一下，再到主机B上点一下，数据流效果就出来了，直观、生动的Flash动画即显示了网络数据包的来龙去脉，这是该软件的一大闪光点。下图中信封正在流动



24

网络模拟软件Packet Tracer

- Packet Tracer使用实例：“单交换机划分Vlan”的实验。



25

绘制网络拓扑图(p40)

- 网络拓扑结构是指网络电缆与物理设备连接的布局特征，抽象地讨论网络系统中各个端点相互连接的方法、形式与几何形状，可表示出网络服务器、工作站、网络设备的网络配置和相互之间的连接。网络拓扑包括物理拓扑和逻辑拓扑
- 物理拓扑是指物理结构上各种设备和传输介质的布局
- 逻辑拓扑定义了发送数据的主机访问传输介质的方式
- 网络拓扑图是指用传输媒体互连各种设备的物理布局

26

绘制网络拓扑图

- 交换机类图标



- 路由器类图标、服务器、PC机、防火墙



- 线路图标



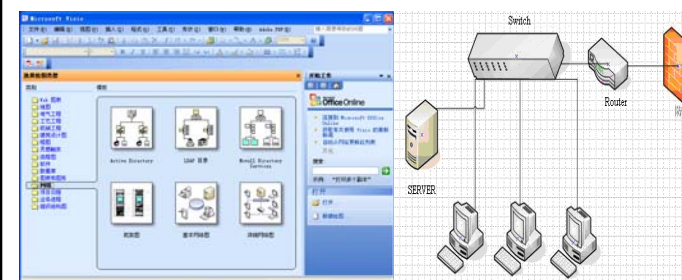
- Internet区域



27

拓扑图绘制工具(p41)

- Office的 Visio绘图软件



28

路由器、交换机原理 (p157-163、223-230)

29

路由器技术基础

- 路由器实际上就是一种用于网络互连的专用计算机，和常见的PC一样，路由器有CPU、内存和BOOT ROM。但路由器没有键盘、硬盘和显示器。路由器多了NVRAM、FLASH及各种各样的接口。IOS是Cisco路由器、交换机等网络设备操作系统，是一种嵌入式系统
- 路由器工作在OSI参考模型的网络层（第三层），它的主要功能是存储转发数据分组，并进行路由。

30

路由器技术基础

路由的基本概念

- 路由是指通过相互连接的网络把信息从源节点传输到目标节点的活动。路由技术要解决的关键问题是如何确保选择某条最佳路径将信息送到目标节点。
- 如下图所示，路由技术实现了PC1和PC2之间的数据流动。



31

路由器技术基础

- 连接线缆有60针的同步串口线和异步串行线缆。



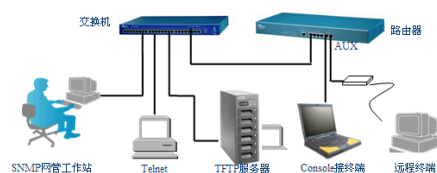
同步串口线（左） 异步串行线缆（中） V.35线缆（右）

32

路由器技术基础

路由器配置

- 路由器不象交换机插上线路就能使用，而是需要根据所连接的网络及用户的需求进行一定的设置才能使用，一般来说，可以用5种方式来设置路由器。



33

• 交换机技术基础



34

交换机技术基础

- 没有路由功能的交换机工作在OSI的数据链路层，是一种基于MAC地址识别，能够完成数据帧封装、转发功能的网络设备
- 交换机可以在传统的LAN中消除竞争和冲突，数据帧通过一个无碰撞的交换矩阵到达目的端口
- 以太网交换机类似于一台专用的计算机，它由中央处理器（CPU）、随机存储器（RAM）和接口组成工作在OSI模型中的第二层，所以又称“二层交换机”，适用于连接工作站、服务器、路由器和交换机

35

交换机技术基础

交换机的工作原理

- 在网络通信中，交换机中的数据不是发往所有的端口，而是发往目的端口。交换机检查收到的所有数据帧，根据交换机中的地址表决定帧发往哪个目的端口
- 交换机在初始化后通过自学习形成一个MAC地址表，根据MAC地址表实现对数据帧的过滤和转发，减少错误数据帧的发生概率
- 交换机执行两个基本操作：一是交换数据帧，将从某一端口收到的数据帧转发到该帧的目的端口；二是维护交换操作，构造和维护动态MAC地址表

36

交换机技术基础

交换机的端口配置线缆

- 交换机的端口配置线缆有4种，分别适用于不同的接口组合，如下图所示



37

交换机技术基础

交换机基本配置

- 交换机的基本配置命令包括
 - 给交换机命名
 - 限制到交换机的访问、设置访问交换机的口令和划分特权级别
 - 定义交换机的IP地址、子网掩码及默认网关
 - 设置系统的日期和时间
 - 显示交换机的系统信息
 - 验证连通性、保存配置等

38

实验报告的书写要求

- 对实验过程进行监控
- 注意实验前后的对比、分析
- 实验截图
 - 当前活动窗口（同时按下Alt+PrScrn键）
 - 整个屏幕（按下PrScrn键）
 - 窗口中的任意部分（使用Windows附件中的截图工具）
 - 截图加工（使用Windows附件中的图画工具）
- 撰写实验报告

39

实验截图图例

- 实验过程的截图



40

实验截图图例



41

请完成以下实验任务

- 学会使用协议分析软件Wireshark
- 学会使用网络仿真软件Packet Tracer
- 尝试使用路由器及交换机的常见配置命令
(参加实验书中相关部分)

42