

计算机网络实验



谢逸
中山大学·计算机学院
2024. Fall



计网实验课要求

- 分组协作完成每次实验, 每组4人, 自由组合;
- 按要求完成实验报告, 上传到网盘(将在企业微信中发布链接);
- 每次实验进行考勤登记;
- 不设期中考试, 期末采用现场完成指定实验进行考核;
- 期末总评 = 平时成绩(60%) + 期末考试(40%) 初定
- 建议提前了解实验内容、原理、操作;
- 实验中遇到问题可以通过网络寻找解决方法;
- 可以在实验开放的其他时间继续完成实验

2

课程安排

时间	内容
第1周:	实验0-实验基础(1)
第2周:	实验0-实验基础(2)
第3周:	实验1-FTP协议分析
第4周:	实验2-编程实验
第5周:	实验3-VLAN
第6周:	实验4-生成树
第7周:	实验5-链路聚合
第8周:	实验6-端口镜像
第9周:	实验7-静态路由

时间	内容
第10周:	实验8-RIP
第11周:	实验9-OSPF
第12周:	实验10-ACL
第13周:	实验11-NAT
第14周:	实验12-VPN
第15周:	实验13-Ad-Hoc
第16周:	实验14-网络规划
第17周:	
第18周:	期末考试

本学期内容

章节次序	主要教学内容	所需学时
第1章 实验基础	IP协议, 协议分析软件, 网络设备的配置命令, 实验网络环境的设置, 网络基本配置实验	6
第2章 应用层协议	FTP协议, FTP协议分析实验	2
第3章 网络编程	网络编程, 网络编程实验	2
第4章 网络路由	路由协议, 路由器配置实验, 静态路由实验, RIP实验, OSPF实验	10
第5章 访问控制技术	访问控制技术, 访问控制技术实验	4
第6章 交换机技术	VLAN, VLAN实验	4
第7章 链路层协议	链路聚合技术, 链路聚合实验, 生成树协议, 生成树协议实验	6
期末考查	完成指定实验	2

4

教学环节安排

- 为保证实验教学顺利进行，在本课程开始时先开展“实验基础”的教学，以令学生获得后续实验所需的基础知识、掌握实验工具的使用方法等。
- 开放网络实验室，以保障在课内不能完成实验的学生、可以利用课外时间到实验室继续完成实验。
- 在每个新实验由学生动手做之前，均会由教师先行讲解本次实验所涉及的设备的使用方法、所涉及的技术原理和实验步骤，明确实验要求，以便学生对实验所涉及的网络技术原理的理解和掌握、对实验的目标与步骤等有更清晰的认知。

5

教学方法

- 本课程以实验为主，全部教学活动均在实验室进行。开课时任课教师需向学生讲清课程的性质、任务、要求、课程安排、进度、考核内容等。
- 本课程以综合和设计性实验为主，辅以部分验证性实验。实验前学生需进行预习，了解实验所涉及的相关知识。
- 每个新实验开始做之前，教师先行讲解本次实验所涉及的设备的使用方法、所涉及的技术原理和实验步骤，明确实验要求，再由学生动手完成实验。
- 实验以小组为单位，每组4人，强调小组成员合作的学习方式，培养团队精神。

6

教材与参考书

- 《计算机网络实验教程（第2版）》，王盛邦编著，清华大学出版社，2017年
- 参考书
 - 《网络工程设计与应用》，王相林编著，清华大学出版社，2011

7

成绩评定

- 考核方式：考查
- 成绩录入方式：百分制
- 成绩评定：期末开卷考查**60%**，平时作业（每个实验逐个考核）**35%**，考勤（每次实验课）**5%**。
- 平时作业和期末考查评分方法：学生按要求完成实验并提交实验报告，实验报告由实验题目、实验目的、实验设备、实验原理、方法与步骤、实验验证、分析和讨论等部分构成，其中实验原理、实验过程、实验分析和讨论是评分重点。

8

注意事项

- 禁止带食物进入实验室，防止水杯倾倒损坏设备。
- 禁止在实验室从事与实验课无关事务，违规者记录并扣分。
- 实验结束必须关闭所有设备电源、交回线缆、整理桌椅。
- 实验硬件问题：找助教、任课老师、陈老师。
- 实验常见问题：接口松动、电源关闭、线缆损坏
- 实验室可用的时间表：除了上课以外，其他时间都可以用，包括周六、周日。每天至晚上**10:00PM**清楼。

9

实验基础(1)

10

本章内容

- IPv4地址
- 常用命令行命令
- 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

11

IPv4地址表示

- 在IPv4系统中，IP地址是一个32位的二进制地址
- 如：11001010 01110010 11001110 11001010
- 为便于记忆，将其划为4组，每组8位，由小数点分开，用四个字节来表示。
- 如：11001010.01110010.11001110.11001010
- 用点分开的每个字节的数值范围是0-255，称为“点分十进制表示法”
- 如：202.114.206.202

12

IPv4地址结构

- IPv4的IP地址包括两个部分：NETID和HOSTID,
- NETID标识一个网络。
- HOSTID标识在该网络上的一个主机。
- IP地址格式：NetID + HostID
- 网络标识 (NetID)：表示主机所在网络；
- 主机标识 (HostID)：表示主机在网段中的唯一标识。



13

IPv4地址分类

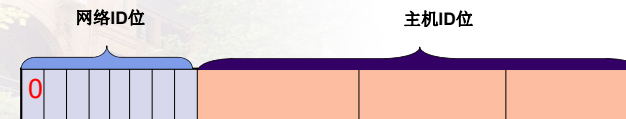
- 私有IP地址范围：
 - A: 10.0.0.0~10.255.255.255 即10.0.0.0/8
 - B: 172.16.0.0~172.31.255.255即172.16.0.0/12
 - C: 192.168.0.0~192.168.255.255 即192.168.0.0/16
- 这些地址是会被Internet分配的，它们在Internet上也不会被路由，虽然它们不能直接和Internet网连接，但通过技术手段仍旧可以和 Internet通讯（NAT技术）

网络地址：主机号全0表示为某网络号网络本身
广播地址：全

IPv4地址分类

- **IPV4地址分类：**
- **A类：1-126**（127是回环和诊断测试保留用）
- **B类：128 - 191**
- **C类：192 - 223**
- **D类：224 - 239**（保留，主要用于IP组播）
- **E类：240 - 254**（保留，研究测试用）

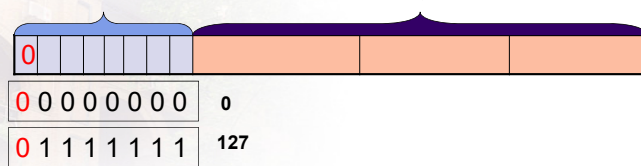
IPv4 A类地址



- A 类网络 ID 被分配给拥有大量主机的网络
- A 类网络 ID 的前缀长度只有 8 位
- 剩余的 24 位可用来标识16,777,214 个主机 ID
- 较短的前缀长度使可接受 A 类网络 ID 的网络数量限制为 126 个

16

IPv4 A类地址

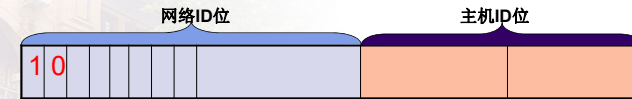


- A 类网络 ID 的最高位为 0，A 类网络 ID 的数量从 256 个减少到 128 个
- 首八位设置成 00000000 的地址是不能被分配的，因为它们构成了被保留的网络 ID
- 首八位设置成 01111111（十进制的 127）地址是不能被分配的，因为是为环回地址保留的
- 后面两个约定将 A 类网络 ID 的数量从 128 个减少到 126 个

A类地址范围 (1. 0. 0. 0到126. 255. 255. 255)

17

IPv4 B类地址



- B 类网络 ID 被分配给中型和大型网络
- 其中 14 位表示 B 类网络 ID，16 位表示主机 ID
- B 类地址可以分配给 16,384 个网络，每个网络可以有 65,534 个主机

B类地址 (128. 1. 0. 0—191. 254. 255. 255)

18

IPv4 C类地址

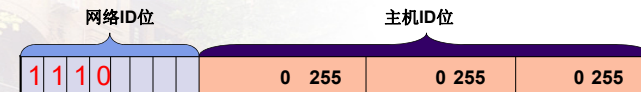


- C 类地址被分配给小型网络
- C 类地址的三个最高位为 110，前 24 位中剩余21位指定特定的网络，后 8 位指定特定的主机
- 可以将 C 类地址分配给 2,097,152 个网络，每个网络可以有 254 个主机。

C类地址 (192. 0. 1. 0—223. 255. 255. 255)

19

IPv4 D类地址



- D 类地址是为 IPv4 多播地址保留
- D 类地址的四个最高位为 1110
- D 类地址的地址范围是224.0.0.0--239.255.255.255

D类地址 (224. 0. 0. 0—239. 255. 255. 255)

20

IPv4私有IP地址

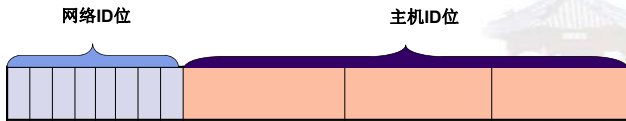
- 全局IP地址：用于因特网—公共主机
- 专用IP地址：仅用于组织的专用网内部—本地主机

10.0.0.0~10.255.255.255 1个A类地址
172.16.0.0~172.31.255.255 16个连续的B类地址
192.168.0.0~192.168.255.255 256个连续的C类地址
这些私有地址常被用于局域网内部地址

21

IPv4地址特殊表示

- 网络地址（“0”地址）
主机号全为0的IP地址表示某网络号的网络本身
- 广播地址（“1”地址）
主机号各位全为1的IP地址表示本网广播或称为本地广播
- 回环地址
A类地址第一段十进制数值为127是保留地址，用于环路反馈等测试。
如127.0.0.1代表本机地址
- 全“0”地址
整个IP地址全为0代表一个未知的网络如：0.0.0.0。在路由器的配置中，用于默认路由的配置



22

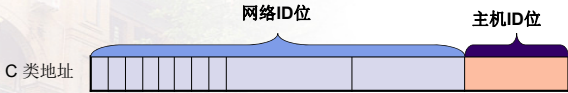
网络掩码

- 作用：标识一个IP地址的网络号范围
- 结构：掩码长度32bit，由一串1和紧随的一串0组成。1对应于IP地址中的网络号（子网号），0对应于IP地址中的主机号

A类地址掩码	11111111	0	0	0
B类地址掩码	11111111(255)	11111111(255)	0	0
C类地址掩码	11111111(255)	11111111(255)	11111111(255)	0

23

有类网络地址面临的问题



每个C类网络拥有主机数目： $2^8-2=254$

- (1) 当网络中主机数目少于254台时，将浪费254-N个IP地址空间（N为网络内主机数量）
- (2) 当网络中主机数目多于254台时，则IP地址不够使用
- (3) C类空间不够时，则只能分配B类网络IP给主机使用，类似于第1种情况的计算，有可能浪费空间更大:浪费 $2^{16}-N$

24

子网掩码与子网划分

- 子网掩码：是一个与IP地址相对应的32位的数，掩码中的各个位与IP地址的各个位相对应
- 如果IP地址的一个位对应的子网掩码位为1，那么该IP地址的位属于地址的网络部分。如果IP地址中的一个位对应的子网掩码比特为0，那么该IP地址位属于主机部分

地址：
202.114.206.202

11001010	01110010	11001110	11001010
----------	----------	----------	----------

掩码：255.255.255.0

11111111	11111111	11111111	00000000
----------	----------	----------	----------

- 子网掩码取代了传统的地址类别来决定一个比特是否属于地址的网络或主机部分。这样也就能够实现对一个网络进行子网划分

25

子网掩码与子网划分

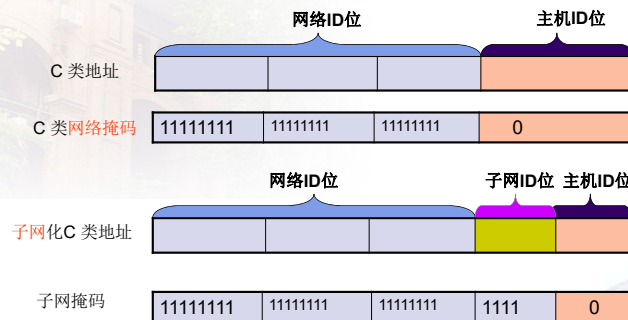
- 划分子网：可以提高IP地址的利用率，减少在每个子网上的网络广播信息量，使互连网络更加易于管理
- 存在问题：子网划分使一些地址不能使用（主机号全0和全1的地址不能用），造成了地址浪费
- 子网与主机个数计算

子网个数的计算方法：子网个数 = $2^{\text{子网位数}} - 2$

每个子网主机个数的计算：主机个数 = $2^{\text{主机个数}} - 2$

26

子网划分



通过缩短主机空间位数，减小了容纳主机数量，达到减小地址空间浪费的目的，使网络的划分更灵活

27

IP地址的表示方式

- 192.168.1.0
不表示一个具体IP地址，而是表示一网段的网络地址
- 192.168.1.255
表示一个广播地址
- 192.168.1.1/24
用CIDR表示的IP，斜杠后的数字表示掩码的高24位为1，其余为0

28

计算IP的网段号

使用给定的掩码与IP地址进行逻辑与操作，计算的结果就IP地址的网络号

地址: 202.114.206.202 → 11001010 01110010 11001110 11001010
逻辑与
掩码: 255.255.255.0 → 11111111 11111111 11111111 00000000
结果
网络号: 202.114.206.0 ← 11001010 01110010 11001110 00000000

29

判断主机是否在同一网段

IP地址: 172.16.30.100 → 10101100 00010000 00011110 01100100
逻辑与
子网掩码: 255.255.192.0 → 11111111 11111111 11000000 00000000
结果
网络号: 172.16.0.0 ← 10101100 00010000 00000000 00000000

IP地址: 172.16.20.100 → 10101100 00010000 00010100 01100100
逻辑与
子网掩码: 255.255.192.0 → 11111111 11111111 11000000 00000000
结果
网络号: 172.16.0.0 ← 10101100 00010000 00000000 00000000

30

判断主机是否在同一网段

IP地址: 172.16.30.100 → 10101100 00010000 00011110 01100100
逻辑与
子网掩码: 255.255.192.0 → 11111111 11111111 11000000 00000000
结果
网络号: 172.16.0.0 ← 10101100 00010000 00000000 00000000

IP地址: 172.16.80.100 → 10101100 00010000 01010000 01100100
逻辑与
子网掩码: 255.255.192.0 → 11111111 11111111 11000000 00000000
结果
网络号: 172.16.0.0 ← 10101100 00010000 01000000 00000000

31

网络IP划分实例

- 实例
网吧新建4个机房，每个机房有25台机器，给定一个网络地址空间：192.168.10.0，现需要将其划分为4个子网。要求尽可能做到IP地址的最小浪费，而且要满足现有IP地址需求

32

网络IP划分实例

- 分析：192.168.10.0是一个C类的IP地址，标准掩码为255.255.255.0，如下图所示



33

网络IP划分实例

- 要划分为4个子网必然要向最后的8位主机号借位，需考虑借那几位的问题
- 实际要求中有4个机房，每个房间有25台机器，也就是需要4个子网，每个子网下面最少25台主机
- 依据子网内最大主机数来确定借几位。依公式 $2^n - 2 \geq \text{最大主机数}$ ，求最小n值
- $2^n - 2 \geq 25$ ，满足该不等式的n为5，相对应的子网需要借3位。如下图所示

34

网络IP划分实例



35

网络IP划分实例

- 确定了子网部分，前面的网络部分不变，最后的8位如下图所示



36

网络IP划分实例

得到6个可用的子网地址：全部转换为点分十进制表示

- 11000000 10101000 00001010 00100000 = 192.168.10.32
- 11000000 10101000 00001010 01000000 = 192.168.10.64
- 11000000 10101000 00001010 01100000 = 192.168.10.96
- 11000000 10101000 00001010 10000000 = 192.168.10.128
- 11000000 10101000 00001010 10100000 = 192.168.10.160
- 11000000 10101000 00001010 11000000 = 192.168.10.192

子网掩码：

- 11111111 11111111 11111111 11100000 = 255.255.255.224

这就得出了所有子网的网络地址

37

网络IP划分实例

- 注意在一个网络中主机地址全为0的IP是网络地址，全为1的IP是网络广播地址，不可占用。所以得到的子网地址和子网主机地址如下：

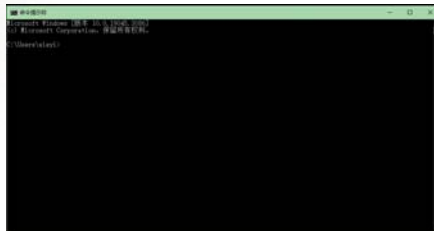
- 子网1
192.168.10.32 掩码: 255.255.255.224 主机IP: 192.168.10.33~62
- 子网2
192.168.10.64 掩码: 255.255.255.224 主机IP: 192.168.10.65~94
- 子网3
192.168.10.96 掩码: 255.255.255.224 主机IP: 192.168.10.97~126
- 子网4
192.168.10.128 掩码: 255.255.255.224 主机IP: 192.168.10.129~158
- 子网5
192.168.10.160 掩码: 255.255.255.224 主机IP: 192.168.10.161~190
- 子网6
192.168.10.192 掩码: 255.255.255.224 主机IP: 192.168.10.193~222

- 只要取出前面的4个子网就可以满足要求

38

常用DOS命令 (P1-13)

- ping命令
- tracert命令
- ipconfig命令
- netstat命令
- arp命令
- route命令



39

Ping命令

- 在Windows环境下，ping命令语法如下：

```
ping [-t] [-a] [-n count] [-l size]
      [-f] [-i TTL] [-v TOS]
      [-r count] [-s count] [[-j
      host-list] | [-k host-list]]
      [-w timeout] target_name
```

- 最常用形式：“ping IP地址”或“ping 域名”
- 注意参数t、l、s用法

实例

- C:\> ping www.sohu.com
- C:\> ping 118.228.148.143
- C:\> ping www.sysu.edu.cn -t
- C:\> ping -r 6 -l 200 172.18.187.254
- C:\> ping -s 4 -l 200 172.18.187.254

养成良好的实验习惯：尝试上述命令，记下显示的结果，并进一步分析结果

40

tracert命令

- tracert（跟踪路由）是路由跟踪实用程序，用于获得IP数据报访问目标时从本地计算机到目的主机的路径信息。
- 在Windows环境下，Tracert命令语法如下：
`tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name`
- 最常用形式：“tracert IP地址”或“tracert 域名”

实例

- `C:\>tracert www.sina.com`
- `C:\>tracert 172.16.0.88 -d`

参数d指定不将地址解析为计算机名。这样可加速显示tracert的结果

41

ipconfig命令

- ipconfig命令可以显示所有当前的TCP/IP网络配置值（如IP地址、网关、子网掩码）、刷新动态主机配置协议（DHCP）和域名系统（DNS）设置。
- 在Windows环境下，语法格式为：
`ipconfig [/? | /all | /renew [adapter] | /release [adapter] | /flushdns | /displaydns | /registerdns | /showclassid adapter | /setclassid adapter [classid]]`
- 最常用形式：“ipconfig”或“ipconfig/all”

实例

- `ipconfig`：显示所有适配器的基本TCP/IP配置
- `ipconfig /all`：显示所有适配器的完整TCP/IP配置

42

netstat命令

- netstat命令可以显示当前活动的TCP连接、计算机侦听的端口、以太网统计信息、IP路由表、IPv4统计信息（对于IP、ICMP、TCP和UDP协议）以及IPv6统计信息
- 在Windows环境下，netstat的语法格式为：
`netstat [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]`
- 最常用参数：`-an`、`-e -s`

实例

- `netstat -an`：显示所有活动的TCP连接以及计算机侦听的TCP和UDP端口
- `netstat -e -s`：显示以太网统计信息，如发送和接收的字节数、数据包数

arp命令

- ARP把基于TCP/IP的软件使用的IP地址解析成LAN硬件使用的媒体访问控制地址。
- 其语法格式为：
`arp [-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]] [-d InetAddr [IfaceAddr]] [-s InetAddr EtherAddr [IfaceAddr]]`
- 最常用参数：`-a`、`-d`

44

arp命令

实例

- `arp -a`
显示所有接口的ARP 缓存表。
- `arp -a -N 192.168.1.100`
显示IP 地址为 192.168.1.100 的接口ARP 缓存表。
- `arp -s 10.0.0.80 00-AA-00-4F-2A-9C`
将 IP 地址 10.0.0.80与物理地址 00-AA-00-4F-2A-9C绑定(静态ARP缓存项)。
- 注意：在IPv6协议下，已经取消了arp协议，代之以NDP（邻居发现）协议。

45

Route命令

- 使用 Route 命令行工具查看并编辑计算机的 IP 路由表。Route 命令和语法如下所示：
- `route [-f] [-p] [command [destination] [MASK netmask] [gateway] [METRIC metric] [IF interface]`

- 最常用参数：print

实例

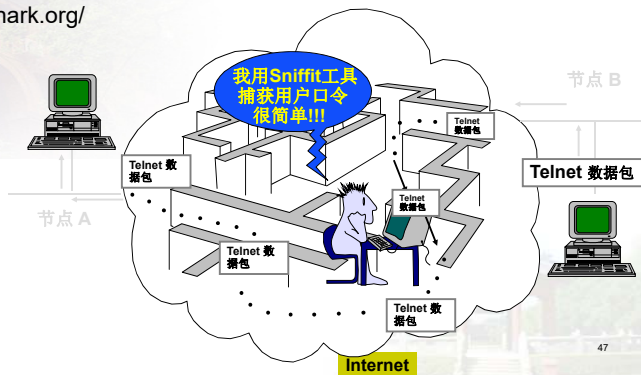
- `route print` : 显示 IP 路由表的完整内容。
- `route print 10.*` : 显示 IP 路由表中以 10. 开始的路由。

46

网络协议分析软件

- Wireshark软件 (p20-26)

<https://www.wireshark.org/>



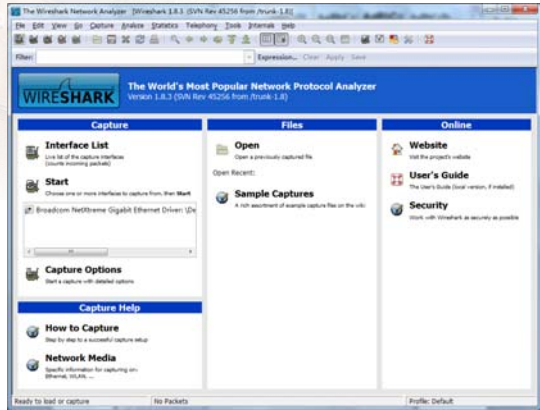
47

网络协议分析软件

- 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Wireshark 的官方网站<http://www.wireshark.org/download.html>下载最新版本。

48

Wireshark主界面



49

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

50

Wireshark主菜单

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

- 查看本地或者在线帮助
- 比如罗列Wireshark支持的协议等，包含Wireshark内部信息的若干启动项，工具的启动项，比如创建防火墙访问控制规则等
- 查看Wireshark的统计信息
- 设置分析选项
- 设置捕捉过滤器并开始捕捉
- 跳转到捕获的数据
- 查看Wireshark视图
- 查找或标记封包，进行全局设置
- 打开或保存捕获的信息

51

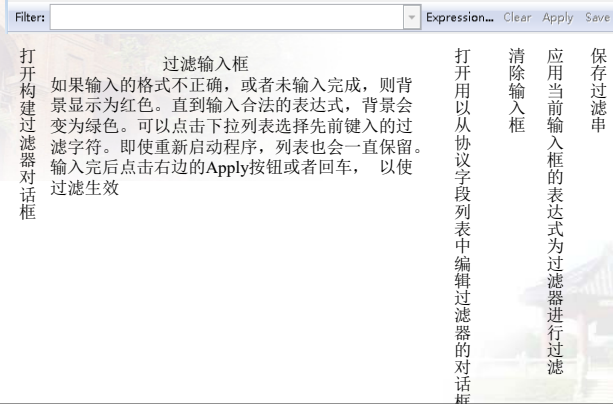
Wireshark主工具栏



- 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
- 跳转到第一个包
- 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包
- 返回历史记录中的上一个包
- 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

52

Wireshark "Filter"工具栏



“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

“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。

“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

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
- 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
- 已选择协议字段的状态栏
- 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

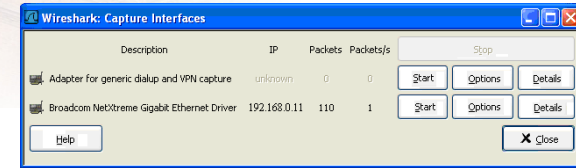
File: test.cap 14 KB 00:00:02 P: 120 D: 120 M: 0

Decode (as uploaded, 2 bytes) P: 120 D: 120 M: 0

57

Wireshark使用方法

- 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

58

网络协议分析软件

- 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
- 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
- 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

59

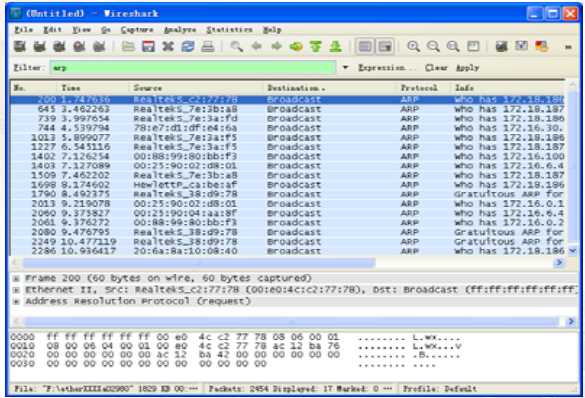
网络协议分析软件

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）

60

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。

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、传输层等各层信息
- 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

网络协议分析软件

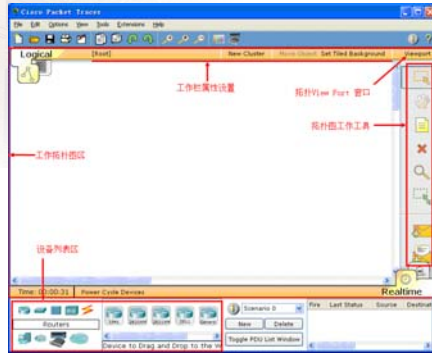
- Wireshark是一款功能强大而操作相对简便的抓包软件。在进行网络实验时，往往采用抓包分析的方法来验证一些实验，故应熟练掌握此工具软件

网络模拟软件PacketTracer(p29-39)

- 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行进的处理过程，以便观察网络实时运行情况

网络模拟软件Packet Tracer

• Packet Tracer 5.3界面



65

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



66

网络模拟软件Packet Tracer

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

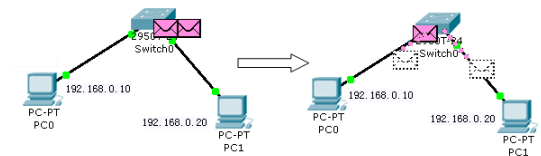
- Packet Tracer使用实时、仿真两个操作模式呈现网络的行为
- 在主界面的最右下角有两个切换模式，分别是Realtime mode(实时模式)和Simulation mode (模拟模式)
- 实时模式中网络行为和真实设备一样，对所有网络行为将即时响应
- 仿真模式中用户可以看到和控制时间间隔、数据传输的内部流程、数据跨越网络的演化

67

网络模拟软件Packet Tracer

数据包的Flash动画。

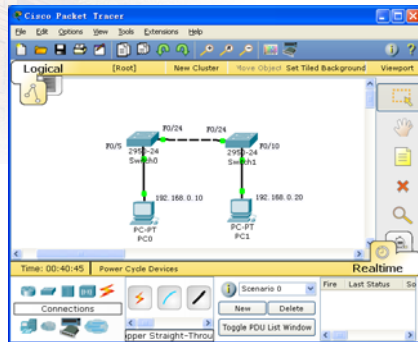
- 在Simulation mode模式下，只需点击位于工作拓扑图区下边界的“Auto Capture/play”（自动捕获/播放），再在最右边的工具栏中，选择信封带十号的，在主机A上点一下，再到主机B上点一下，数据流效果就出来了，直观、生动的Flash动画即显示了网络数据包的来龙去脉，这是该软件的一大闪光点。下图中信封正在流动



68

网络模拟软件Packet Tracer

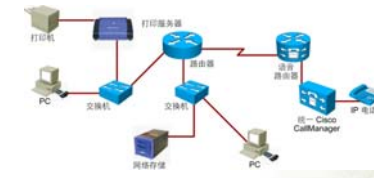
- Packet Tracer使用实例：“单交换机划分Vlan”的实验。



69

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



70

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



71

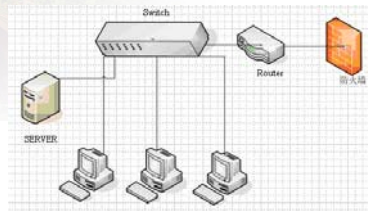
拓扑图绘制工具(p41)

- Office的 Visio绘图软件



72

拓扑图绘制工具



绘制实例

73

路由器、交换机原理(p157-162、223-230)

74

路由器技术基础

连通两个不同子网的器件

- 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是路由器、交换机等网络设备操作系统，这是一种嵌入式系统
- 路由器工作在OSI参考模型的网络层（第三层），它的主要功能是为收到的报文寻找正确的路径并把它们转发出去



路由技术实现了PC1和PC2之间的数据流动。这条数据通路的生成依赖于路由表和路由生成算法

75

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。这条数据通路的生成依赖于路由表和路由生成算法。



76

路由器技术基础

连接线缆

- 连接线缆有60针的同步串口线和异步串行线缆。



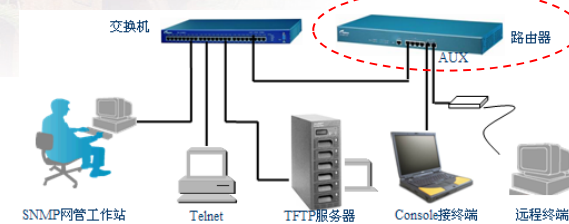
同步串口线（左）异步串行线缆（中）V.35线缆（右）

77

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路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。



78

交换机技术基础



Console 接口

光纤接口

RJ-45 接口

79

交换机技术基础

连接相同子网的主机访问互联网

以太网交换机

- 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、路由器和其他交换机
- 以太网交换机的主要作用是快速高效、准确无误地转发数据帧



Console 接口

光纤接口

RJ-45 接口

80

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

81

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



82

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

83

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）
- 根据实验报告模板撰写实验报告

84

实验截图图例

● 实验过程的截图

```
19-RSR10-1#config terminal
Enter configuration commands, one per line.
19-RSR10-1(config)#access-list 1 deny 192.168.1.2
19-RSR10-1(config)#show access-list 1

ip access-list standard 1
10 deny 192.168.4.0 0.0.0.255
19-RSR10-1(config)#
19-RSR10-1 CON0 is now available

Press RETURN to get started

19-RSR10-1#configure
Enter configuration commands, one per line.
19-RSR10-1(config)#interface fastEthernet 0/1
19-RSR10-1(config-if)#ip access-group 1 out
19-RSR10-1(config-if)#show ip interface fastEthernet 0/1
FastEthernet 0/1
IP interface state is: UP
IP interface type is: BROADCAST
IP interface MTU is: 1500
IP address is:
```

阻止列表

设置方向

把对 F0/1 应用 access-list 1,
设为 out, 表示禁止从 F0/1 往外发送数据包

85

实验截图图例

```
IP: Source address = [192.168.1.2]
IP: Destination address = [192.168.1.1]
IP: No options
IP:

TCP: ----- TCP header -----
TCP: Source port = 2521
TCP: Destination port = 22
TCP: Sequence number = 2531156735
TCP: Next expected Seq number = 2531157247
TCP: Acknowledgment number = 2339544911
TCP: Data offset = 20 bytes
TCP: Reserved Bits: Reserved for Future Use (Not shown in the Hex Dump)
TCP: Flags = 18
TCP: .0. = (No urgent pointer)
TCP: .1. = Acknowledgment
TCP: .1. = Push
TCP: .0. = (No reset)
TCP: .0. = (No SYN)
TCP: .0. = (No FIN)
TCP: Window = 17500
TCP: Checksum = F4BE (correct)
TCP: Urgent pointer = 0
TCP: No TCP options
TCP: [512 Bytes of data]
```

SSH 的客户机 IP

SSH 的服务器 IP

SSH 的端口号

SSH 传递的数据

86

本次任务

- 熟悉常用命令
- 熟悉wireshark
 - 访问一个视频网站;
 - Wireshark选定相应网卡;
 - 启动抓包;
 - 熟悉窗口分组信息含义 (查阅网络)
- 熟悉packetTracer
- 完成实验小组分组

实验基础(2)

88

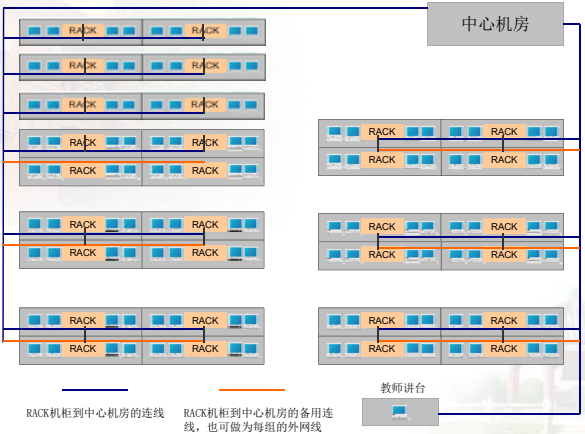
本章内容

- 计算机网络实验室
 - 实验室布局方式和布线图
 - 实验台布局方式和布线图
- 实验室拓扑图
- 实验平台连接示意图
- 实验室IP规划
- RCMS

网络工程实验室

- 实验室共27组基础实验平台，每组包括4台基础实验设备
 - 三层交换机RG-S5750两台
 - 路由器RG-RSR20两台
- 每组实验平台最多可供4人使用，同时控制组与组之间的设备访问
- 每组实验平台使用一个8口的交换机连接到核心，8口交换机主要连接4台PC、1台RCMS (RACK Control & Management Serve)、核心S5750
- 每台PC使用3块网卡
 - 一块网卡用于连接实验台网络设备
 - 一块网卡用于搭建实验网络
 - 一块无线网卡用于无线实验网络

实验室布局方式和布线图

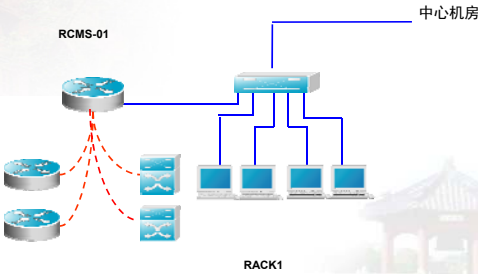


实验台布局方式和布线图

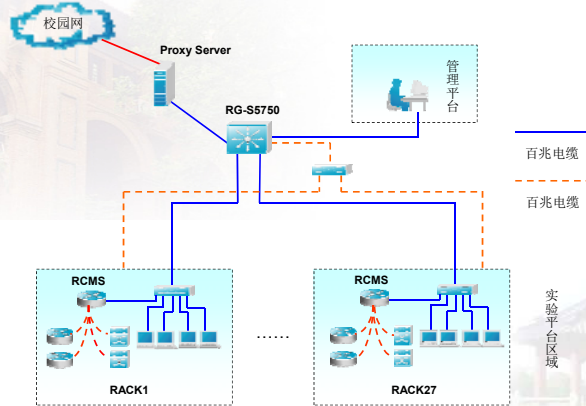
实验台RACK说明



- 共27组RACK：分别为RCMS-01、RCMS-02、.....、RCMS-27
- 实验台布线如下图

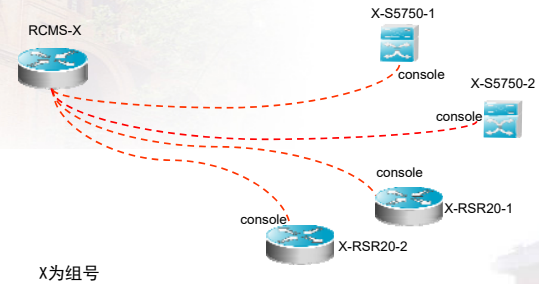


实验室拓扑图



93

RCMS逻辑连接图

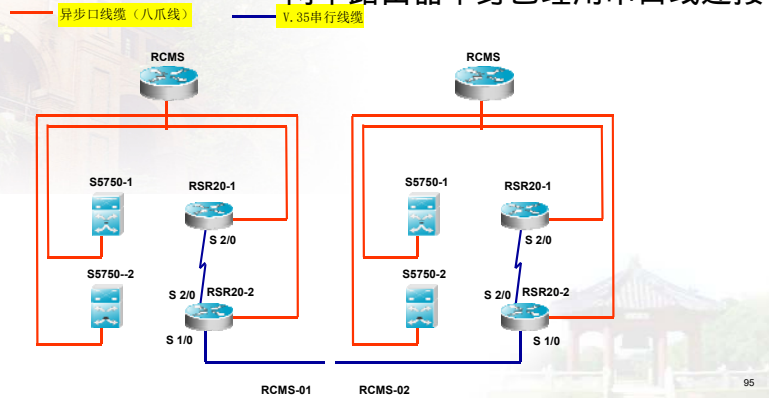


94

第三段为组号，第四段从RCM从5开始（前面有2交换，2路由）

实验平台连接示意图

两个路由器本身已经用串口线连接



95

实验室IP规划

● 27组RACK的IP地址在同一个IP地址段，IP地址如下表

设备	接口	IP地址	核心S5750	学生IP	学生网关
RCMS-01	Fa 1/0	172.16.1.5/16	172.16.0.2/16	172.16.1.1-4/16	172.16.0.1
RCMS-02	Fa 1/0	172.16.2.5/16		172.16.2.1-4/16	172.16.0.1
RCMS-03	Fa 1/0	172.16.3.5/16		172.16.3.1-4/16	172.16.0.1
.....
RCMS-27	Fa 1/0	172.16.27.5/16		172.16.27.1-4/16	172.16.0.1

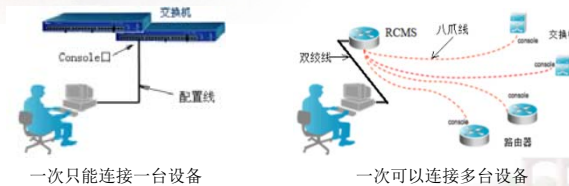
● 为防止本组学生实验时访问其他组设备而相互影响，在核心上进行了组与组设备间的隔离处理

● 核心S5750连接到代理服务器，其IP地址为172.16.0.1/16,通过代理服务器连接到校园网

机架控制和管理服务器--RCMS

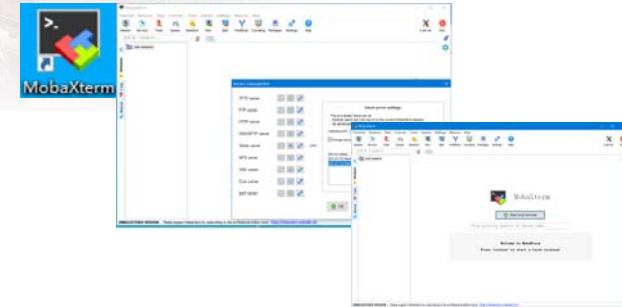
- RG-RCMS: RACK Control & Management Server, 实验室机架控制和管理服务器
- RG-RCMS可以同时管理和控制8-16台的网络设备, 不需要进行控制线的拔插
- 统一管理和控制实验台上的多台网络设备
- 提供“一键清”功能, 一键清除实验台上网络设备的配置, 方便多次实验

红色线已经连好, 需要检查是否插紧

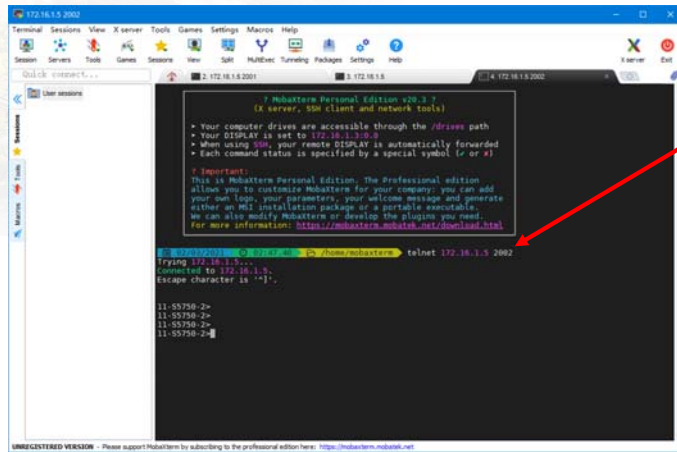


RCMS配置使用方法

- MobaXterm 又名 MobaXVT, 是一款增强型终端, 可以开启多个终端视窗



RCMS配置使用方法



以第1组为例:
第1组的RCMS的
IP地址为:
172.16.1.5, 访问
端口2002

交换机配置

- 须先安装telnet工具
- 登录设备, 进入特权配置模式
`> enable 14`
Password:b402
- 进入全局配置模式
`# configure terminal`

实验设备配置模式

- 普通用户模式: `>`
有限操作, 仅能进行基本测试、显示系统信息
- 特权模式: `#`
提供更多的命令和权限, 例如调试命令, 以及更详细的测试
- 全局配置模式: `(config)#` 接口配置模式
配置全局系统和相应的详细配置, 将影响整个交换机的全局参数
- 不同的模式对应不同的命令集, 只有进入了相关的模式后才可以执行相应的配置命令(注意注意)

实验设备基本配置

- 子模式
 - 线路配置模式
主机名 `(config-line)#`
配置交换机的线路参数
 - 接口配置模式
主机名 `(config-if)#`
配置交换机的接口参数
-

102

实验设备基本配置

设备命名

- 设备名称 `(config)#hostname value` 换名字
 - 注: value为要命名设备的名称
- 例: 要把交换机名称设为01-S5750-1
- 执行前
 - Switch `(config)#hostname 01-S5750-1`
- 执行后
 - 01-S5750-1 `(config)#`

命令行其他功能

(1) 获得帮助

Switch#`?` 全部命令查看
Switch#`show ?` 命令参数查看

查看在某模式下有哪些命令时, 可以输入“?”, 可以查看到此模式下所有命令; 当不清楚命令后面参数时, 可在命令后输入“?” (中间有空格)

(2) 命令简写, 为了方便起见, 交换机支持命令简写, 如

Switch# `configure terminal` 全写
Switch# `config` 简写

简写原则: 能识别出唯一命令, 如configure terminal 不可简写成c, 因为以c开头的命令并不只是configure terminal

(3) 使用历史命令, 用键盘上的向上向下方向键可以调出曾经输入的历史命令, 并可以通过上下键上下选择

Switch# (向上键)
Switch# (向下键)

104

接口编号规则

- 配置设备时，经常要涉及到设备接口，因而需要熟悉接口编号规则
- 交换机：插槽号/端口在插槽上的编号
- 例如：端口所在的插槽编号为0，端口在插槽上的编号为3，则端口对应的接口编号为 0/3
- 进入gigabitethernet 0/1接口的示例：注意对应命令的插口（0号插槽的第1个网口）
Switch(config)# interface gigabitethernet 0/1
- fastethernet（百兆） gigabitethernet（千兆）
- 路由器：接口插槽号/端口号
- 槽号表示该接口在路由器的哪个槽上（主板上接口的槽号为0），端口号表示该接口在某个槽上的顺序号
- 进入2/0接口的示例：
Router (config)# interface serial 2/0

启用/禁止接口

- 接口的两种管理状态：up和down
- 当端口被关闭时，端口的管理状态为down，否则为up。下面的例子描述如何关闭接口gigabitethernet 0/2：

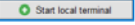
Switch(config)#interface gigabitethernet 0/2

Switch(config-if)#shutdown （if意味着正在配置接口）


- no形式重新启动一个接口。例如

Switch(config-if)#no shutdown

实验步骤

- 启动MobaXterm，点击主菜单severs，点击Telnet server，OK，
- 输入telnet 172.16.xx.5 端口 xx是机柜号(组号)，端口是2001~2004
- 机柜号：1~27
- 设备端口号

在该模式下只能做一些简单的操作。配置时需进入特权模式：

 enable 14 ! 进入特权模式，14表示特权级别
b402 ! 输入密码（密码没有回显） 登录密码:b402
正常情况下，便进入特权模式

实验测试与验证

- 根据实验拓扑，准备设备、网线等
- 连接设备，配置实验网IP地址、子网掩码、网关等
- 实验前测试：记录现场情况
- 按要求进行各项配置管理，记录重要的场景
- 配置完成后，要进行实验验证
- 验证时分析是否达到预期要求
- 撰写实验报告

实验截图

- 桌面截图：PrintScreen键
- 焦点窗口截图：Alt-PrintScreen键
- 工具截图：Win7附件“截图工具”
- 截图编辑：Win7附件“画图”

109

一键清功能

- 实验结束后，应将实验时对设备的配置清除，以免影响下一批的学生配置设备。清除时可使用“一键清”的功能
- 所谓“一键清”，是指使用一条指令，即可把所有链接在RCMS上的网络设备的配置恢复到当初缺省配置，提供一个干净的环境给下一组学生作实验。实际上，就是通过一个简单的指令，便把所有的实验台上的网络设备的配置清除掉
- 在RCMS上进行一键清操作步骤：注意在RCMS上执行一键清除，不是在其他地方
 - 在DOS命令提示符窗口里，输入：
telnet 172.16.xx.5
telnet到一台RCMS上，x为组号地址

110

一键清功能

非常重要!!!

- 提示密码输入，这里输入b402密码
- >模式下，输入命令：
- enable 14
进入到特权模式("#")
- 提示密码输入，这里输入b402密码
- 在#模式下，输入命令：
exec clear.txt
执行一键清
- clear.txt脚本执行完成后，各设备会自动软重启，重启后，设备就恢复到原配置

111

清除串口堵塞

- 登录RCMS
 - telnet 172.16.xx.5
 - en 14
- 发命令
 - clear line tty 设备号码
- 设备号码指1-4之间，1-2表示交换机，3-4表示路由器

