

实验一 网络设备认识和线缆制作及测试

实验 1.1 网络设备的认识

【实验目的】

通过对网络设备和连接线缆的观察，建立对计算机网络的一个基本的感性认识。

【实验任务】

- 1、实际观察交换机、路由器等设备外观，识别这些设备的网络连接接口。
- 2、识别用于连接设备的线缆。
- 3、观察一个实际的网络，认识其中的网络设备及其连接线缆和连接方式。

建议实验学时：1 学时。

【实验背景】

网络设备主要包括路由器、交换机等，Cisco 公司作为网络设备的主要提供商，提供各种系列的产品，尽管这些产品的处理能力和所支持的网络连接接口数目有相当大的差异，但它们都由相似的硬件构件所组成。系统的主要构成单元包括：中央处理器、闪存、只读存储器、随机存取存储器、非易失随机存取存储器、输入 / 输出接口和特定介质转换器等。了解路由器和交换机的内外部特性，对理解它们的功能和工作原理是有帮助的。

【实验设备】

Catalyst2912 交换机、集线器、Cisco2620 路由器、PC 机、CAT5UTP（直通线、交叉线、反转线）若干、DTE/DCE 电缆。

【实验步骤】

步骤 1 认识路由器（Cisco 2620）、交换机（Catalyst 2912）、集线器的指示灯、端口及其连线。

步骤 1.1 认识路由器的接口和指示灯。

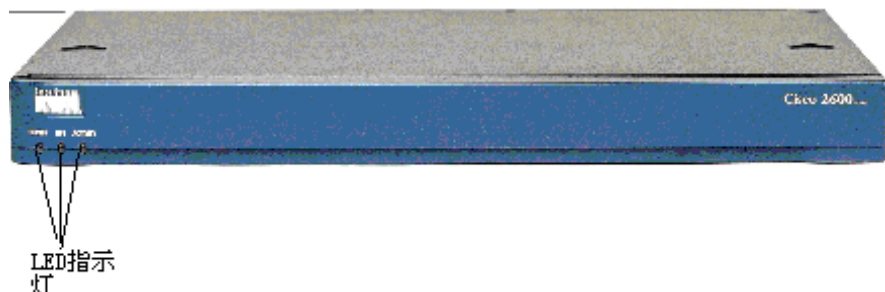


图 1.1 Cisco 2620 路由器前面板

如图 1.1 所示：依次为电源指示灯、远程电源供应指示灯、活动指示灯。

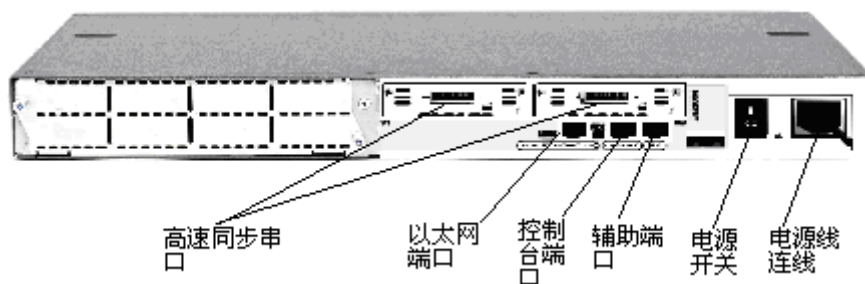


图 1.2 Cisco 2620 路由器后面板

路由器接口主要用来将路由器连接到网络，它分为局域网接口和广域网接口两种。由于路由器型号的不同，接口个数和类型也不一样。常见的接口主要有以下几种：

- (1) 高速同步串口：可连接 DDN、帧中继(Frame Relay)、X.25、PSTN(模拟电话线路)。
- (2) 同步 / 异步串口：可用软件将端口设置为同步工作方式。
- (3) AUI 接口：即粗缆口。一般需要外接转换器(AUI-RJ45)连接 10Base-T 以太网。
- (4) ISDN 接口：可以连接 ISDN 网络(2B+D)，可作为局域网接入 Internet 之用。
- (5) AUX 接口：该端口为异步端口，主要用于远程配置，也可用于拨号备份，可与 MODEM 连接。支持硬件流控制(Hardware Flow Control)。

(6) Console 接口：该端口为异步端口，主要连接终端或运行终端仿真程序的计算机，在本地配置路由器。不支持硬件流控制。

(7) Ethernet 接口：用来连接以太网。有的路由器还有 Fast Ethernet(快速以太网)端口。

在路由器配置时要引用一个端口，可直接引用其接口号。引用的形式用于指定一个特定的端口：type slot# / port# 其中，Interface type 表示接口类型；slot#表示插槽号；port#表示某一插槽中的端口号。例：FastEthernet 0/0。

步骤 1.2 认识交换机的端口和指示灯



图 1.3 Catalyst 2900 系列交换机

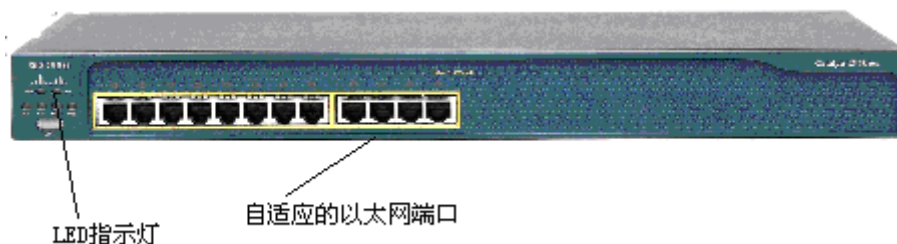


图 1.4 Catalyst2912 交换机前面板

从上到下，从左往右依次是系统指示灯、远程电源供应指示灯、交换机状态指示灯、交换机利用率指示灯、模式按钮指示灯、接口双工指示灯、接口速度指示灯。自适应的 Ethernet 接口，可用来连接有 10/100bps 或者是 10/100/1000bps 以太网接口的设备。



图 1.5 Catalyst2912 交换机后面板

Console 接口：该接口为异步口，主要连接终端或运行终端仿真程序的计算机，在本地配置路由器。支持硬件流控制。

步骤 1.3 认识集线器的端口



图 1.6 集线器

一般的集线器至少有一个 Uplink 接口，其余接口均为带 x 标识的或不带 x 标识的接口，当集线器的端口与其它设备的端口相连时，如果两个端口上都标有 x 或者都没标 x 则使用交叉线，否则使用直通线连接。

级联是另一种集线器端口扩展方式，它是指使用集线器普通的或特定的端口来进行集线器间的连接的。所谓普通端口就是通过集线器的某一个常用端口进行连接，而所谓特殊端口就是集线器为级联专门设计的一种“级联端口”，一般都标有“UPLink”字样。因为有两种级联

方式，所以事实上所有的集线器都能够进行级联。下面来分别看看这两种级联方式。(1) 利用直通的双绞线将 Uplink 端口连接至其他集线器上除"Uplink 端口"外的任意端口。(2) 通过集线器的普通端口进行级联不过要注意的是这时所用的连接双绞线要用交叉线了。

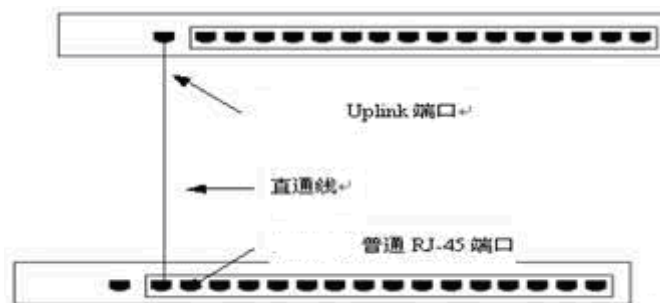


图 1.7 集线器级联方式 (1)

交叉连接的方法就是一端的第 1-3 与 2-6 脚下对调，连接如下图所示。

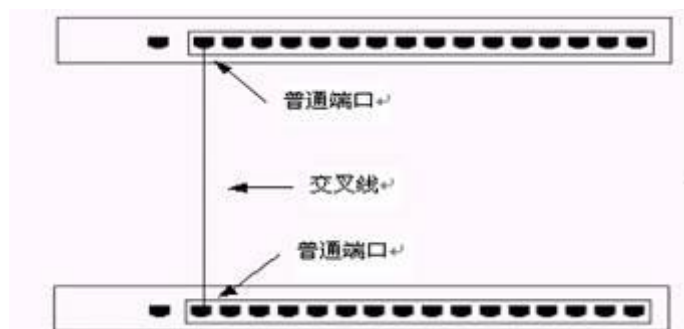


图 1.8 集线器级联方式 (2)

步骤 2 认识各种线缆

步骤 2.1 认识直通线、交叉线



图 1.9 做好接头的双绞线

直通双绞线的线序遵循 EIA-568B 标准，按（左起：白橙——橙——白绿——蓝——白蓝——绿——白棕——棕）进行排列，如果是交叉线就是按照 EIA/TIA568A 规格（左起：白绿——绿——白橙——蓝——白蓝——橙——白棕——棕）进行排列并整理好，通常我们

制作直通线或交叉线都会粘上标签。

直通线用于下列连接：交换机到路由器、交换机到 PC 或服务器、集线器到 PC 或服务器。交叉线用于下列连接：交换机到交换机、交换机到集线器、集线器到集线器、路由器到路由器、PC 到 PC、路由器到 PC。

步骤 2.2 认识反转线



图 1.10 做好接头的反转线



图 1.11 (a) RJ-45 到 DB-9 适配器图
接计算机串口一侧



图 1.11 (b) RJ-45 到 DB-9 适配器
接反转线一侧



图 1.11 (c) 连接了适配器的反转线

反转线缆也称控制线，线缆两端的线序相反。反转线一端通过 RJ-45 到 DB-9 适配器连接计算机(通常称作终端)的串行口。通常情况下，在交换机（或路由器）的包装箱中都会随机赠送这么一条 Console 线和相应的 DB-9 或 DB-25 适配器。

步骤 2.3 DTE/DCE 连接线缆



图 1.12 DCE/DTE cable

所谓的 DTE 是用户设备的终端点，DCE 是用于将来自 DTE 的用户数据从 DTE 转换为提供广域网服务的设备所能接收的形式。在我们实验中，一般情况下是用来连接两台路由器。其中一台为 DTE，另一台为提供时钟的 DCE。通常，DCE 设备提供到网络的物理连接、转发流量并提供用于同步 DCE 和 DTE 设备间数据传输的定时信号。

步骤 3 观察一个实际的设备连接，将下图和实验室实际网络对照，认识设备、接口、线缆和它们的互联。

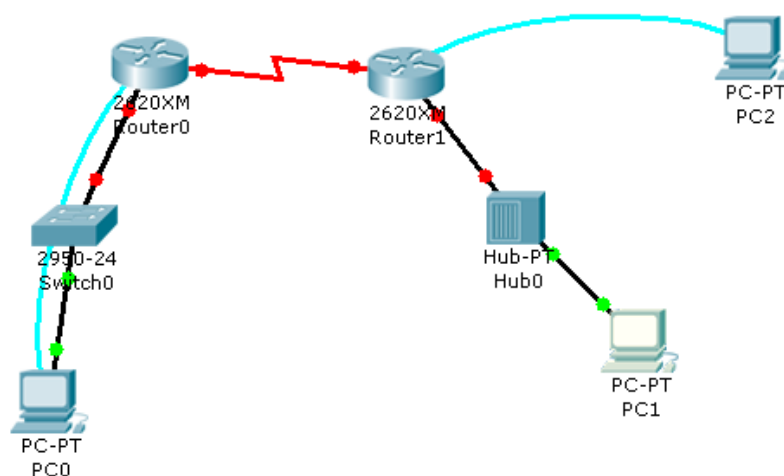


图 1.11 网络拓扑图

如上图拓扑所示，在 packet tracer 4.0 中黑线都是直通线连接设备的以太网口，蓝线为反转线连接终端(或仿真终端)的串行口 (COM 口) 和路由器的 Console 口，红线为 DCE/DTE 线缆连接在两个路由器串行口上的，在实际环境中要观察各种线缆的标签或参考上图所提供的图片来识别线缆。

【注意事项】

1、不同类型的路由器和交换机的接口类型、数量、所处的位置并不相同，有的是模块化的，有的是固定配置的。不过，倒不用担心无法找到端口，在该端口的上方或侧方都会有标识。

2、在连接设备好以前，必须将其电源开关关闭。在开开关以前，必须再检查一遍各个端口的连接线缆是否正确。

实验 1.2 网线的制作和测试

【实验目的】

掌握直通线和交叉线的制作和测试方法，了解标准 568A 与 568B 网线的线序。

【实验任务】

1、制作直通线并测试。

2、制作交叉线并测试。

建议实验学时：1 学时。

【实验背景】

本实验将帮助初学者认识连接线缆和连接部件帮助了解网络设备间的通信方式和技术，并用非屏蔽双绞线制作直通线和交叉线及对其进行测试。

【实验设备】

非屏蔽双绞线，卡线钳， RJ-45 连接件（常称水晶头），电缆测试仪

【实验步骤】

步骤 1 剥线

剥线就是利用压线钳剥线刃口将双绞线的外皮除去 5cm 左右。剥线在网线的制作过程中算是一个难点，在剥双绞线外皮时，手握压线钳要适当，剥线刀刃口间隙过小，就会损伤内部线芯，甚至会把线芯剪断；剥线刀刃口间隙过大，就不能割断双绞线的外皮。

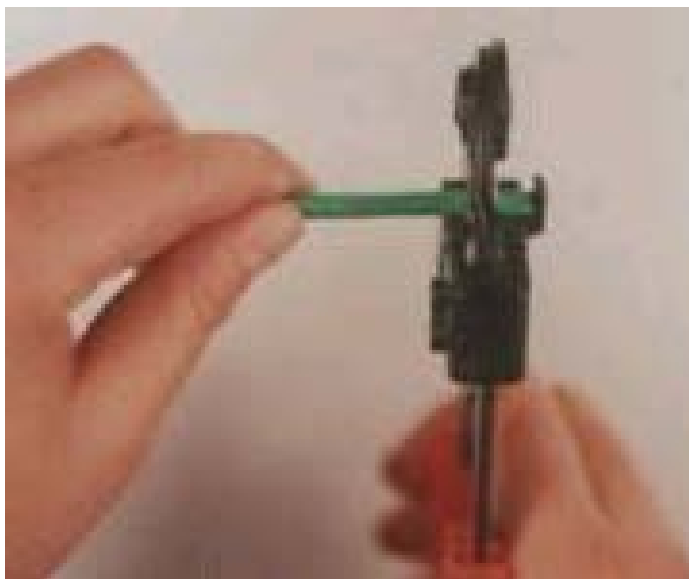


图 1.12 剥线

步骤 2 理线

理线就是把剥好的双绞线里的 4 股 8 根线芯，如果是制作直通线就是两端按照 EIA/TIA568B 规格（左起：白橙——橙——白绿——蓝——白蓝——绿——白棕——棕）进行排列并整理好，如果是制作交叉线就是一端按照 EIA/TIA568A 规格（左起：白绿——绿——白橙——蓝——白蓝——橙——白棕——棕），另一端按照 EIA/TIA568B 规格（左起：白橙——橙——白绿——蓝——白蓝——绿——白棕——棕）进行排列并整理好。

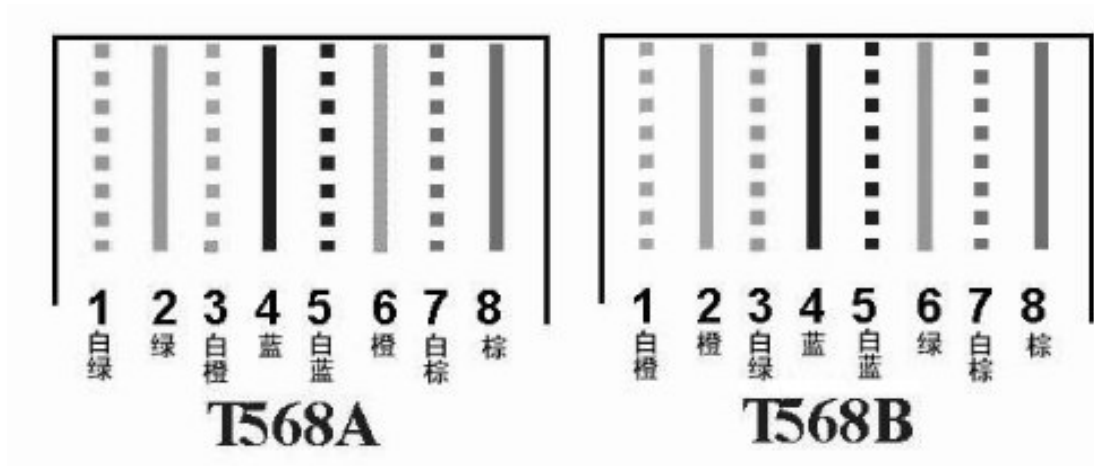


图 1.13 T568A 和 T568B

步骤 3 插线

在插线前用压线钳的切线刃口在剥线的 1.2cm 处将线切齐。一只手捏住水晶头（水晶头有弹片的一侧向下，进线口朝向身里时导体簧片从左到右的顺序为 1—8），另一只手捏平双绞线，稍稍用力将排好的线平行插入水晶头内的线槽中，8 条导线顶端应插入线槽顶端。

步骤 4 压线

确认所有导线都到位后，将水晶头放入压线钳夹槽中，用力捏几下压线钳，压紧线头即可。



图 1.14 压线

步骤 5 检测

这里用的是电缆测试仪,测试仪分为信号发射器和信号接收器两部分,各有 8 盏信号灯。测试时将双绞线两端分别插入信号发射器和信号接收器,打开电源。如果制作的直通线成功的话,则发射器和接收器上同一条线对应的指示灯会亮起来,依次从 1 号到 8 号。如果制作的交叉线成功的话,则是 1 号和 3 号对应着亮,2 号和 6 号对应着亮,其余的一一对应。

如果网线制作有问题,灯亮的顺序就不可预测。比如:若发射器的第一个灯亮时,接收器第七个灯亮,则表示线做错了(不论是直通线还是交叉线,都不可能有 1 对 7 的情况);若发射器的第一个灯亮时,接收器却没有任何灯亮起,那么这只引脚与另一端的任何一只引脚都没有连通,可能是导线中间断了,或是两端至少有一个金属片未接触该条芯线。一定要经过测试,否则断路会导致无法通信,短路有可能损坏网卡或集线器。

【注意事项】

1、步骤 1 中注意剥线刀口非常锋利,握卡线钳力度不能过大,否则会剪断芯线,只要看到电缆外皮略有变形就应停止加力,慢慢旋转双绞线;剥线的长度为 3cm—5cm 不宜太长或太短。

2、步骤 3 中注意将并拢的双绞线插入 RJ-45 接头时,制作直通线在两端都要把白橙线要对着 RJ-45 的第一只引脚。制作交叉线在一端要把白绿线对着 RJ-45 的第一只引脚,在另一端要把白橙线要对着 RJ-45 的第一只引脚。

3、步骤 4 中注意如果测试网线不通,应先把水晶头再用卡线钳狠夹一次,把水晶头的金属片压下去。新手制作的网线不通大多数是由由此造成的。

【实验思考】

- 1、怎样构建本地配置路由器、交换机的环境?
- 2、如果两个接头的线序发生同样的错误,网线还能用吗?
- 3、给出反转线的制作和测试方法。
- 4、已制作好的直通线在两端剥去的外皮太多对线的质量有什么不利影响?

实验二 路由器配置方式及基本操作

【实验目的】

通过对路由器设备的几种配置手段、配置模式和基本配置命令的认识，获得路由器的基本使用能力。

【实验任务】

- 1、认识路由器的配置方式
- 2、按照给出的参考拓扑图构建逻辑拓扑图。
- 3、按照给出的配置参数表配置各个设备。
- 4、练习路由器的一些基本命令。

建议实验学时：2 学时。

【实验背景】

路由器是计算机网络的桥梁，是连接网络的主要设备。通过它不仅可以连通不同的网络，选择数据传送的路径，还能阻隔非法访问等。对 CISCO 路由器进行配置的一个方法是通过控制台将 PC 机的串口直接通过反转线与路由器控制台端口（Console 端口）相连，在 PC 计算机上运行终端仿真软件，与路由器进行通信，完成路由器的配置。另一个方法是通过虚拟终端远程登录（Telnet）路由器，这种方式要求路由器已有一些基本配置，即至少有一个端口（如 Ethernet 口）有效连接网络并可用 IP 协议通信，这样就可通过运行 Telnet 程序的计算机作为路由器的虚拟终端远程登录路由器，完成路由器的配置。在使用路由器操作系统时（Cisco IOS），首先需要熟悉路由器的不同的配置模式和每种模式下的基本命令。这是各种路由器功能配置的基础。

【实验拓扑与参数配置】

实验的参考拓扑图和参考配置参数如图所示。

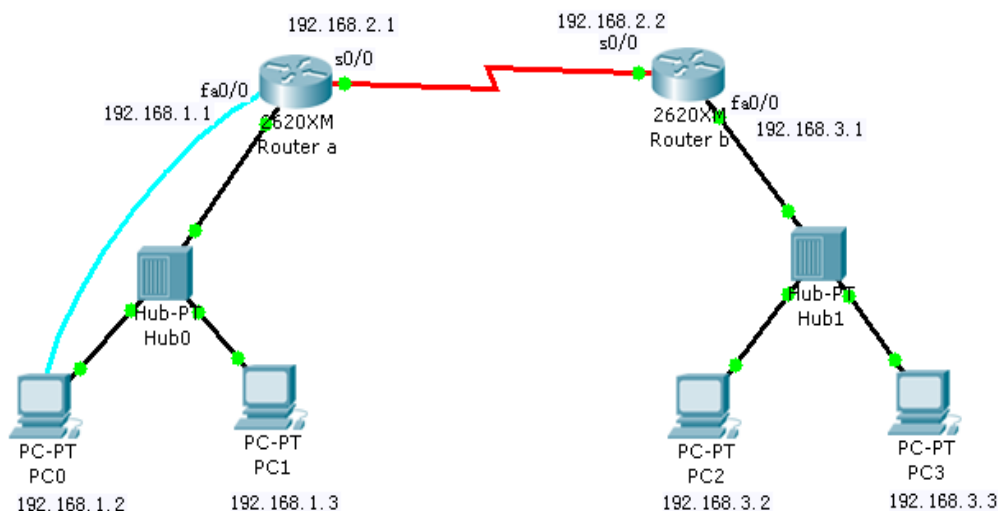


图 2.1 参考拓扑图

表 2.1 配置参数表

路由器的信息(子网掩码均为 255.255.255.0)				
路由器名	类型	IP 地址	RIP 路由网络	时钟频率
Router a	2620XM	Fa0/0: 192.168.1.1 S0/0: 192.168.2.1	192.168.1.0 192.168.2.0	56000
Router b	2620XM	Fa0/0: 192.168.3.1 S0/0: 192.168.2.2	192.168.2.0 192.168.3.0	
PC 信息 (子网掩码均为 255.255.255.0)				
主机名		IP 地址	缺省网关	所属网段
PC0		192.168.1.2	192.168.1.1	192.168.1.0
PC1		192.168.1.3	192.168.1.1	192.168.1.0
PC2		192.168.3.2	192.168.3.1	192.168.3.0
PC3		192.168.3.3	192.168.3.1	192.168.3.0
Hub 信息				
名称		类型	所属网段	
Hub 0		Hub-PT	192.168.1.0	
Hub 1		Hub-PT	192.168.3.0	

【实验设备】

PC 机 4 台；Cisco 路由器 2620XM 2 台；反转线 1 根；串行线缆一对；HUB 2 台，直通线 6 根。（本实验在 packet tracer 4.0 环境下完成）。

【实验步骤】

步骤 1 认识路由器的配置方式

步骤 1.1 构建本地配置环境（通过 Console 口配置）

用带有超级终端程序的 PC 机连接到路由器作为控制台，通过路由器的 Console 口配置路由器。

下面我们以思科的一款路由器 2620 来讲述这一配置过程。步骤如下：

步骤 1.1.1 建立本地配置环境。将反转线缆一端通过 DB-9 适配器连接到 PC 机的串口（或称 COM 口）。反转线缆的另一端与路由器的 Console 口连接。

步骤 1.1.2 检查 PC 机是否安装有“超级终端”(Hyper Terminal)组件。如果在“附件”(Accessories)中没有发现该组件，可通过“添加/删除程序”(Add/Remove Program)的方式添加该 Windows 组件。“超级终端”安装好后我们就可以与路由器进行通信了(当然要连接好，并打开路由器电源了)。在使用超级终端建立与路由器通信之前，必须先对超级终端进行必要的设置。

步骤 1.1.3 单击“开始”按钮，在“程序”菜单的“附件”选项中单击“超级终端”，弹出如图 2.2 所示界面。



图 2.2 超级终端界面

步骤 1.1.4 图 2.2 界面中弹出的如图 2.3 所示连接描述对话框。这个对话框是用来对立一个新的超级终端连接项。



图 2.3 连接描述对话框

步骤 1.1.5 在“名称”文本框中键入需新建的超级终端连接项名称，这主要是为了便于识别，没有什么特殊要求，我们这里键入“Cisco”，如果您想为这个连接项选择一个自己喜欢的图标的话，您也可以在下图的图标栏中选择一个，然后单击“确定”按钮，弹出如图 2.4 所示的“连接到”对话框。

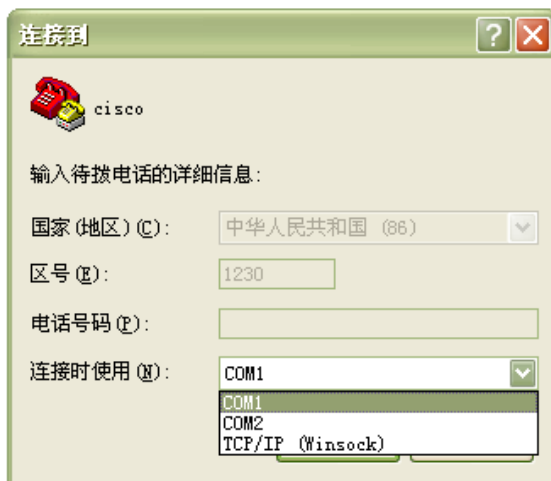


图 2.4 “连接到”对话框

步骤 1.1.6 在“连接时使用”下拉列表框中选择与路由器相连的计算机的串口。单击“确定”按钮，弹出如图 2.5 所示的 COM1 属性对话框。

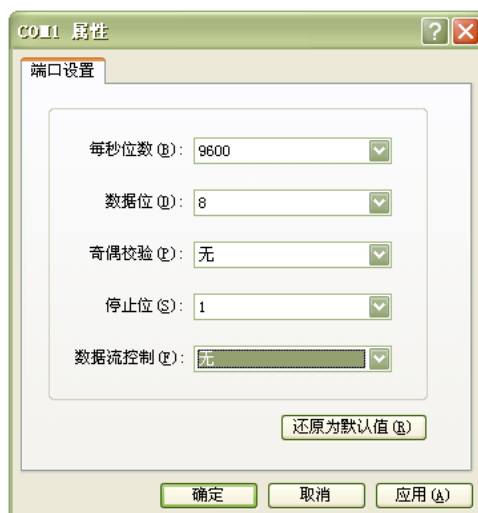


图 2.5 COM1 属性对话框

步骤 1.1.7 在 COM1 属性中设置终端通信参数为：波特率为 9600b/s、8 位数据位、1 位停止位、无校验和无流量控制。单击“确定”按钮进入下一步。

步骤 1.1.8 如果已经将线缆按照要求连接好，并且路由器机已经启动，此时按 Enter 键，将进入路由器的用户视图并出现标识符：Router>；否则启动路由器，超级终端会自动显示路由器的整个启动过程。

步骤 1.2 进入仿真环境下路由器的命令行配置方式（在模拟软件 PacketTracer4.0 中实现）

步骤 1.2.1 双击 PacketTracer4.0 进入仿真环境。

步骤 1.2.1.1 点击左下角的设备框中的路由器图标，在右边的框内会有多种路由器可供选择，选择 2620XM 路由器，然后再将 2620XM 的图标拖放到工作区。

步骤 1.2.1.2 点击设备框中的终端设备图标，选择 PC-PT，再将它的图标拖放到工作区

即可。如图 2.6 所示。

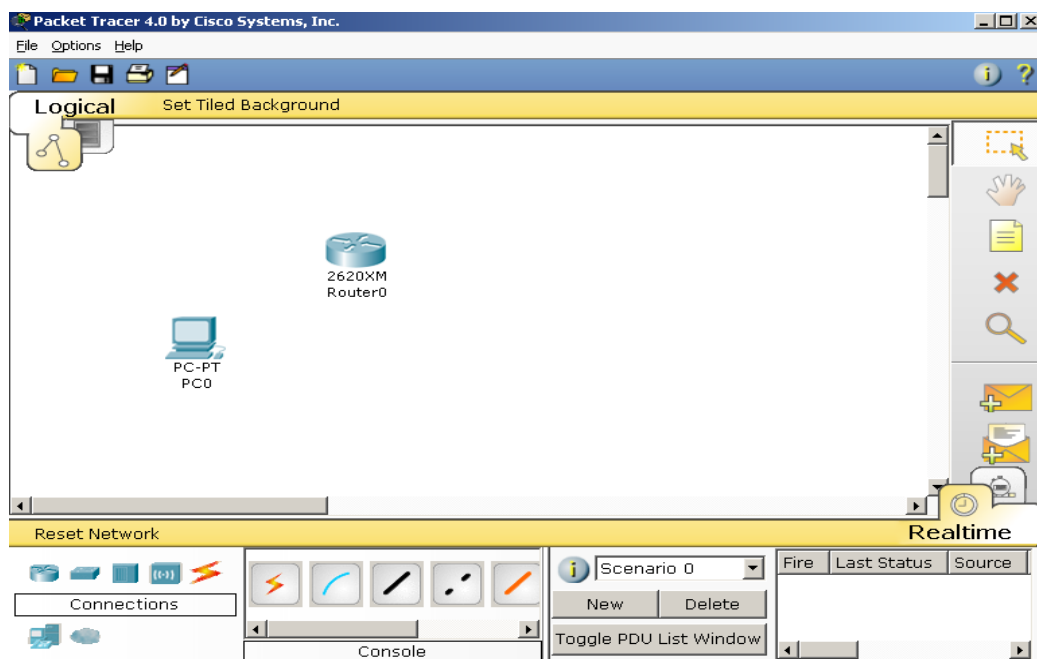


图 2.6 工作界面视图

步骤 1.2.2.用 Console 线将 PC 机与路由器连起来。

步骤 1.2.2.1 点击设备框中线缆图标，选择蓝色的 Console 线，然后单击 P C 机，会弹出端口选择条，选择 RS232 端口（如图 2.7 左图所示）。

步骤 1.2.2.2 单击路由器，在弹出的端口选择条中选择 console 端口（如图 2.7 右图所示）。

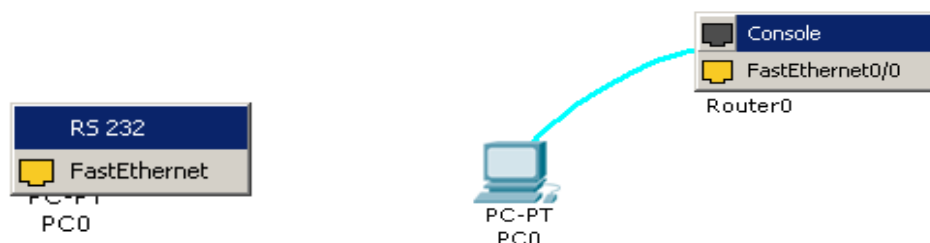


图 2.7 端口选择图示

步骤 1.2.3 .单击 PC 机，弹出 PC 机的配置图（如图 2.8 所示）。选择 Desktop 标签，然后再选择该标签下的 Terminal 图标，弹出如图 2.9 所示的对话框，其中参数的配置跟前面图 2.5 一样。点击 OK，将进入路由器的用户视图并出现标识符：Router>。

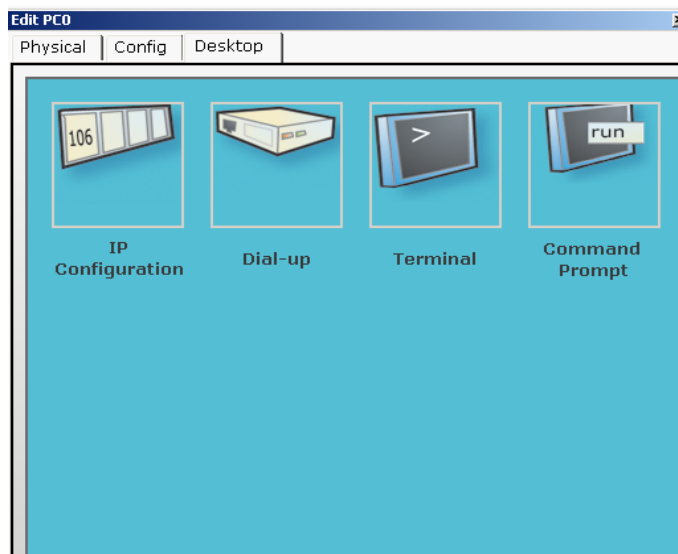


图 2.8 PC 机的配置图

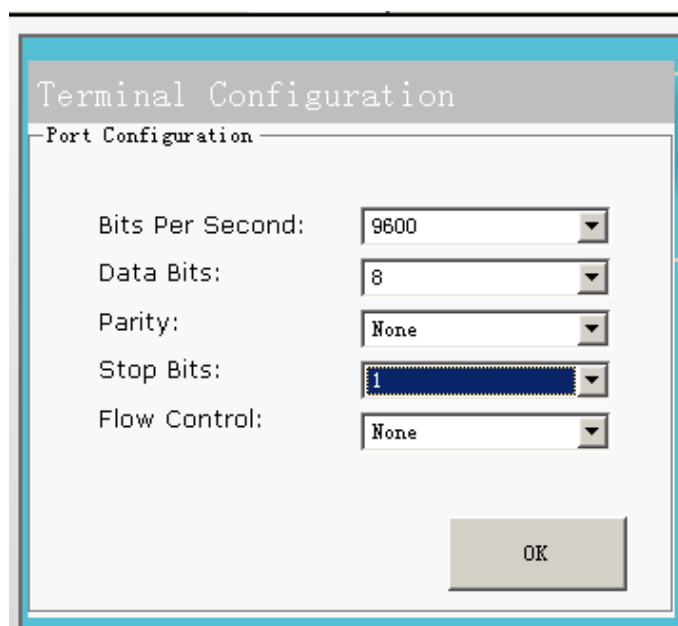


图 2.9 参数配置图

说明：路由器还有其他配置手段，可通过 Telnet，Web，远程拨号等手段进行配置。在这里不再详述。

步骤 2 基本命令使用

步骤 2.1 参考附录中 PacketTracer4.0 的使用方法，按照图 2.1 参考拓扑图构建逻辑拓扑图。并按照表 2.1 参数配置表配置各个设备。

步骤 2.2 识别路由器模式、命令和功能。

路由器有几种命令模式：

（在仿真环境中，单击一下路由器，在弹出的配置界面中选择 CLI 标签就可以直接进入路由器的命令行界面；或者从超级终端进入 CLI。前面已有介绍。）

(1) 普通用户模式：开机直接进入普通用户模式，模式指示符为“>”，在该模式下我们只能查询路由器的一些基础信息，如版本号等。

例： Router>

(2) 特权用户模式：在普通用户模式下输入 **enable** 命令即可进入特权用户模式，模式指示符为“#”，在该模式下我们可以查看路由器的配置信息和调试信息等等。

例： Router>enable

Router#

(3) 全局配置模式：在特权用户模式下输入 **configure terminal** 命令即可进入全局配置模式，在该模式下主要完成全局参数的配置。

例： Router# configure terminal

Router(config)#

(4) 接口配置模式：在全局配置模式下输入 **interface interface-list** 即可进入接口配置模式，在该模式下主要完成接口参数的配置。

例： Router(config-if)#

表 2.2 路由器的各种配置模式总结

模式	访问方式	提示符	退出方法	描述
用户 EXEC (User EXEC)	在路由器上启动一个会话	Router>	输入 Logout 或 quit	使用该模式完成基本的测试和系统显示功能
特权 EXEC (Privileged EXEC)	在用户 EXEC 模式下，输入 enable 命令	Router#	输入 disable 或 exit	使用该模式来检验所输入的命令。一些配置命令也可以使用。可以用口令来保护对此模式的访问
全局配置 (Global configuration)	在特权 EXEC 模式下，输入 configure 命令	Router(config)#	要退回到特权 EXEC 模式输入 exit、end 或按下 ctr-z	使用该模式配置用于整个路由器的参数
接口配置 (Interface configuration)	在全局配置模式下，输入 interface 命令以及特定端口号	Router(config-if)#	要退回到全局配置模式，输入 exit。要退回特权 EXEC 模式，按下 ctr-z 或输入 end	采用此模式为以太网接口配置参数
连接配置 (Line configuration)	在全局配置模式下，使用 line vty 或 line console 命令，并指定连接编号	Router(config-line)#	要退回到全局配置模式，输入 exit。要退回特权 EXEC 模式，按下 ctr-z 或输入 end	使用该模式配置针对终端连接或 console 连接的参数

步骤 2.3 熟悉基本的路由器命令。

步骤 2.3.1 修改路由器的名字(Hostname)。

例: Router(config)# hostname Ra // (改名为 Ra)

步骤 2.3.2 将路由器能够显示历史命令的空间扩大到 100;

例: Router #terminal history size 100

键入 show history 查看你已经执行过的命令; 也可以用 ↑ ↓ 键来选择历史命令。

步骤 2.3.3 配置路由器的口令 (用 enable password 命令设定的口令可以限制对特权模式的访问, 这个口令是可以在配置文件中看到的。要在特权模式下输入加密的口令, 需要使用 enable secret 命令。如果配置了 enable secret 口令, 它就会代替 enable 口令)。

Ra#configure terminal

Ra (config)# **enable password** cisco // (仿真环境中不能使用)

Ra#configure terminal

Ra (config)# **enable secret** cisco // (仿真环境中可以使用)

设置口令后, 对特权模式访问时需要输入密码。如下所示:

Ra >enable

Password:

步骤 2.3.4 配置以太网接口

Ra (config)# **interface** FastEthernet0/0 //注意接口的引用方式 interfacetype slot#/port#

Ra (config-if)# **ip address** 192.168.1.1 255.255.255.0 //为该接口配置 IP 地址

Ra (config-if)# no shutdown // (缺省时, 接口都是关闭的。输入此命令开启接口)

步骤 2.3.5 配置串行接口

Ra(config)# **interface** Serial0/0

Ra(config-if)# **bandwidth** 56 // (串行线两端都需要设定带宽)

Ra(config-if)# **clock rate** 56000 // (串行线中 DCE 端需设定时钟, DTE 端则不需要)

Ra(config-if)# **ip address** 192.168.2.1 255.255.255.0

Ra(config-if) #no shutdown // (缺省时, 接口都是关闭的。输入此命令开启接口)

步骤 2.3.6 配置路由协议

Ra(config)# router rip //启用 RIP 路由协议

Ra(config-router)#**network** 192.168.1.0 //加入路由通报网络

Ra(config-router)#**network** 192.168.2.0

步骤 2.3.7 键入 show running-config 查看当前运行的配置文件;

键入 show startup-config 查看 NVRAM 里面的配置信息;

键入 show flash 查看 flash 里面的 IOS 文件信息;

以下基本命令可以试验:

表 2.3 显示命令

命令	任务
? (特权或者用户模式)	显示常用的命令的列表
Router# show version	查看版本及引导信息
Router# show flash	查看 I O S 文件信息
Router# show running-config	查看运行配置信息
Router# show startup-config	查看开机配置信息
Router# show history	查看曾经键入过的命令的历史记录

Router# show interface type slot#/port#	显示端口信息
Router# copy running-config startup-config	将 RAM 中的当前配置保存到 NVRAM 中
Router# copy startup-config running-config	加载来自 NVRAM 的配置信息
Router# show ip router	显示路由信息

表 2.4: 基本设置命令

命令	任务
Router(config)# username username password password	设置访问用户及密码
Router# enable secret password	设置特权密码
Router(config)# hostname name	设置路由器名

【注意事项】

- 1、在实验中使用路由器的命令时，应该注意这些命令所在的模式。
- 2、一些命令在实际环境中能够使用，但是仿真软件不能使用。
- 3、show running-config 命令中出现 more 时，用空格来显示下一页。

【参考配置】

```

Ra# show running-config
version 12.2
hostname Ra
enable secret 5 $1$f6.A$stAe2JNr7F3UF0eBFfsp00
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0
 ip address 192.168.2.1 255.255.255.0
 clock rate 56000
interface Serial0/1
 no ip address
 shutdown
interface Serial0/2
 no ip address
 shutdown
interface Serial0/3
 no ip address
 shutdown
router rip
 network 192.168.1.0
 network 192.168.2.0

```

```
ip classless  
line con 0  
end
```

【实验思考】

- 1、CiscoIOS 及其配置信息各存放在怎样的存储器中？
- 2、路由器的几种配置手段分别在什么场合使用比较合适？
- 3、你认为本实验中的那几种命令的使用频率会最大？
- 4、路由器为什么不需要固定的操作器和键盘？

实验三 简单结构局域网组建与配置

【实验目的】

了解一个局域网的基本组成，掌握一个局域网设备互通所需的基本配置，掌握报文的基本传输过程。

【实验任务】

- 1、根据所认识的设备设计一个简单的局域网并在仿真环境中画出其逻辑拓扑。
 - 2、配置拓扑中的各设备连通所需的参数。
 - 3、在模拟模式下进行包传输路径跟踪测试。
- 建议实验学时：2 学时。

【实验背景】

简单的局域网主要由交换机、HUB、PC 等设备组建。他们的连接和配置比较简单，本实验构建的简单局域网对应在一个办公室或几个办公室的 PC 的组网。

【实验拓扑与参数配置】

实验的参考拓扑图和参考配置参数如图所示。

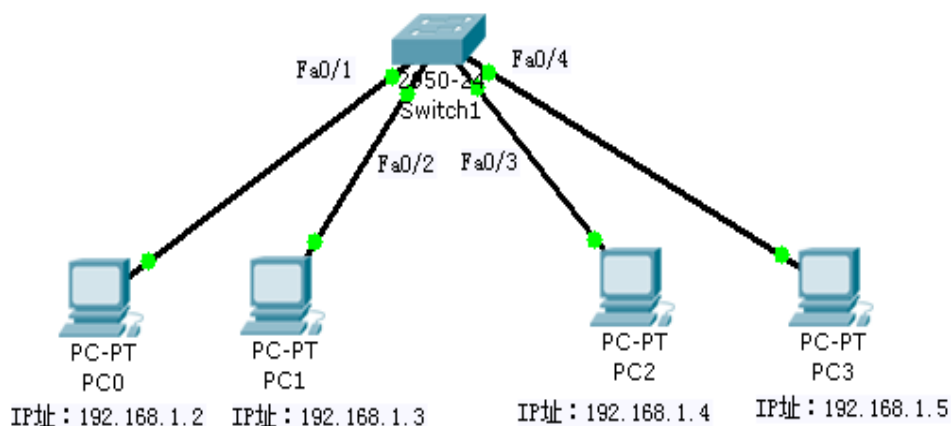


图 3.1 参考拓扑图

表 3.1 配置参数表

PC 信息 (子网掩码均为 255.255.255.0)			
主机名	IP 地址	缺省网关	所属网段
PC0	192.168.1.2	192.168.1.1	192.168.1.0
PC1	192.168.1.3	192.168.1.1	192.168.1.0
PC2	192.168.1.4	192.168.1.1	192.168.1.0
PC3	192.168.1.5	192.168.1.1	192.168.1.0

【实验设备】

根据你所设计的局域网需要选择实验设备。在示例的拓扑中，使用了 2950 交换机 1 台，

PC 机 2 台。（本实验在 packet tracer 4.0 环境下完成）。

【实验步骤】

步骤 1 设计一个局域网，并按照所设计的拓扑图进行连接。注意接口的选择以及连线所使用的线缆类型。（参考附录中 PackeTracer4.0 的使用方法，按照图 3.1 参考拓扑图构建逻辑拓扑图。）

步骤 2 按照表 3.1 参数配置表完成局域网中各主机，接口等的配置。

步骤 2.1 主机的配置。主机的 IP 址和网关根据配置参数表分配好的地址进行设计即可。

步骤 2.1.1 主机 PC1 的配置。

主机 IP 址和网关的配置在模拟环境下有两种方式。

（1）单击拓扑图中的 PC1 图标。在弹出的配置界面中，选择 Config 标签，点击左侧 GLOBAL 下的 Settings（如图 3.2 所示）便可以配置网关。点击左侧 INTERFACE 下的 FastEthernet（如图 3.3 所示）便可以配置 IP 址和掩码。

（2）单击拓扑图中的 PC1 图标。在弹出的配置界面中，选择 Desktop 标签，在选择 IP Configuration，便可配置主机 IP 址和网关。（如图 3.4 所示）

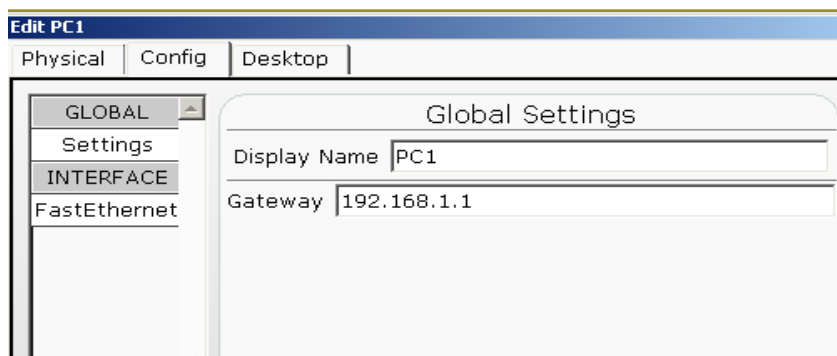


图 3.2 PC 配置界面

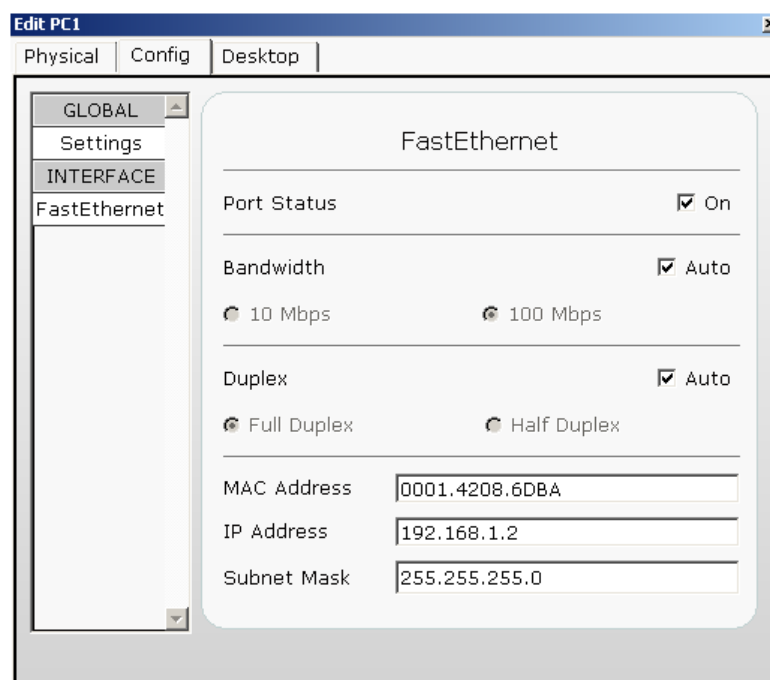


图 3.3 Config 标签界面

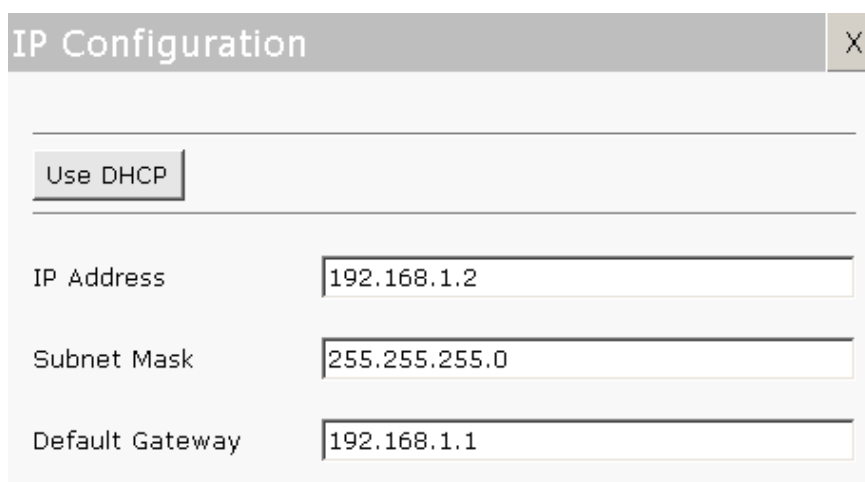


图 3.4 Desktop 标签界面

步骤 2.1.2 按例给出其它主机的配置。

步骤 2.1.3 实际 Windows 环境的 IP 配置。

在实际 Windows 环境中的“开始”中选择“设置”中的“控制面板”。在“控制面板”窗口中选择“网络连接”。鼠标右键选择“本地连接”（或者相应的网卡名称），选择“属性”。在“属性”窗口中选择“TCP/IP 协议”，就可配置相应的参数。（如图 3.5 所示）这里注意一点：若是静态 IP 址，则选择“使用下面的 IP 地址”选项，若需 DHCP 动态分配，则选择“自动获得 IP 地址”。

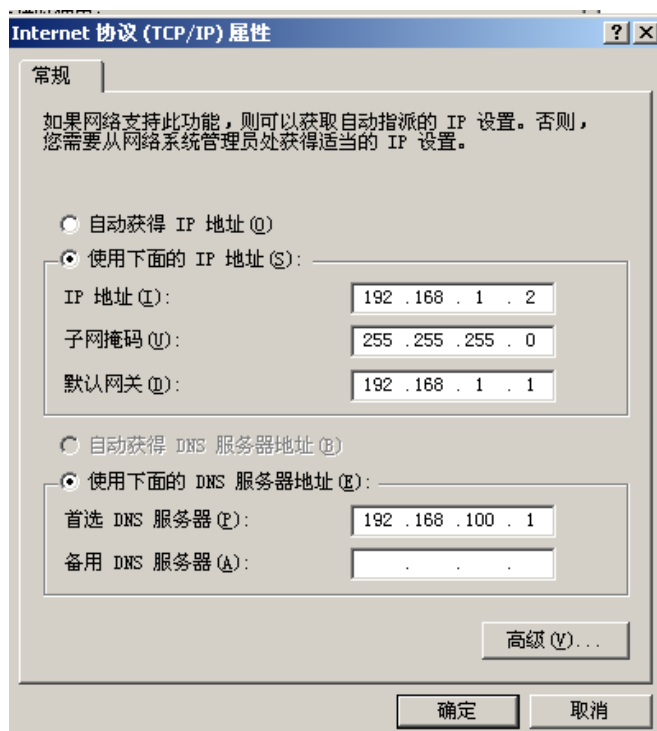


图 3.5 TCP/IP 属性窗口

步骤 2.2 这里交换机具有 2 层交换功能，不需要配置。

步骤 3.连通性测试和包传输路径跟踪测试。

步骤 3.1 以 PC0 到 PC1 的连通性测试为例。单击拓扑图中的 PC0 图标。在弹出的配置界面中，选择 Desktop 标签，选择 Command Prompt，键入 ping 命令。

PC>ping 192.168.1.3

注意：模拟环境与实际环境不同。Ping 命令的结果不能自动生成。模拟环境下使用 Ping 命令时，ICMP 数据报的传输路径可以在仿真环境中 Simulation 模式下察看到，点击右下角 Simulation 模式图标，在 Event List 中便可看到 Ping 事件，在工作区便会看到传输的包，然后点击 Auto Capture 按钮，可以看到包在设备间传输，同时便可看到 Ping 的结果。如图 3.6。

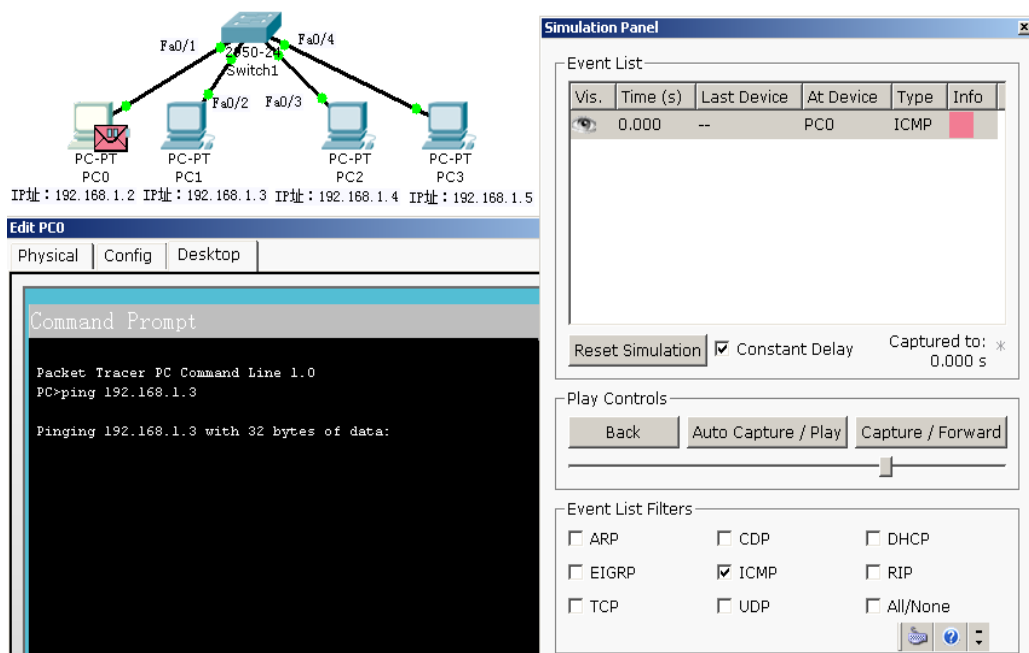


图 3.6 Ping 命令在模拟模式下的界面

查看结果，如果 Ping 通则网络正常，Ping 不通，则就要进行故障排查。

步骤 3.2 实际相邻的 PC 机间的连通性测试。实际环境中是 192.168.134.0 网段，测 192.168.134.51 到 192.168.134.71 的连通性。（如图 3.7 所示）

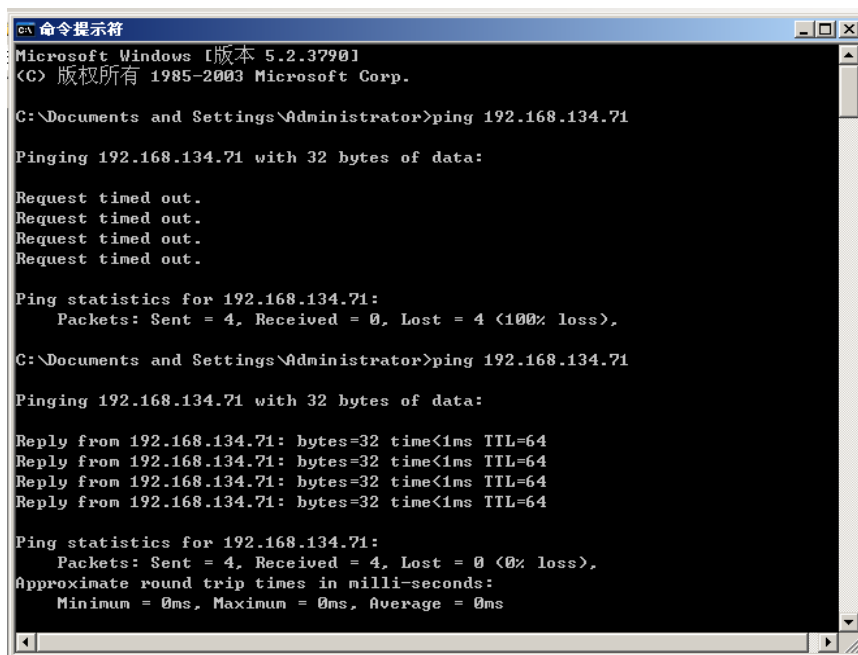


图 3.7 实际环境中 Ping 命令视图

注意：这里第一次 Ping 时不通，是因为有防火墙的阻挡。第二次 Ping 时，禁用防火墙，则 PC 机之间连通。

步骤 3.3 包传输路径跟踪测试。

交换机上数据报的二层分析。由 PC0 发送的 ICMP 数据报传送到交换机 Switch 1 时，Switch 1 的 Fa0/1 接口接收数据。然后查看数据中的源 MAC 地址和目的 MAC 地址，如果交换机知道源 MAC 地址和目的 MAC 地址在一个网段内，会将数据报丢弃，无需传送（称为过滤）；如果数据报的目的 MAC 地址不在交换机的 MAC 地址表中，交换机不知道目的网段，就会将数据报传送到除源网段以外的所有网段（称为泛洪）；如果数据报的目的 MAC 地址在交换机的 MAC 地址表中，交换机就会将数据报传送到相应网段的出口（称为转发）。这是交换机的二层功能。在这里，Switch 1 知道数据报的目的 MAC 地址在交换机的 MAC 地址表中，Switch 1 就会将数据报转发到相应网段的出口 Fa0/2。

步骤 3.3.1 如上图 3.6 所示，当 ICMP 包传输到 Switch 1 时，可以单击 Event List 中右侧的 Info 框在弹出的 PDU 信息界面中就可以查看包在 Switch 1 上的处理过程，也可以直接单击工作区中处于 Switch 1 上的包进入 PDU 信息界面。如图 3.8 所示：

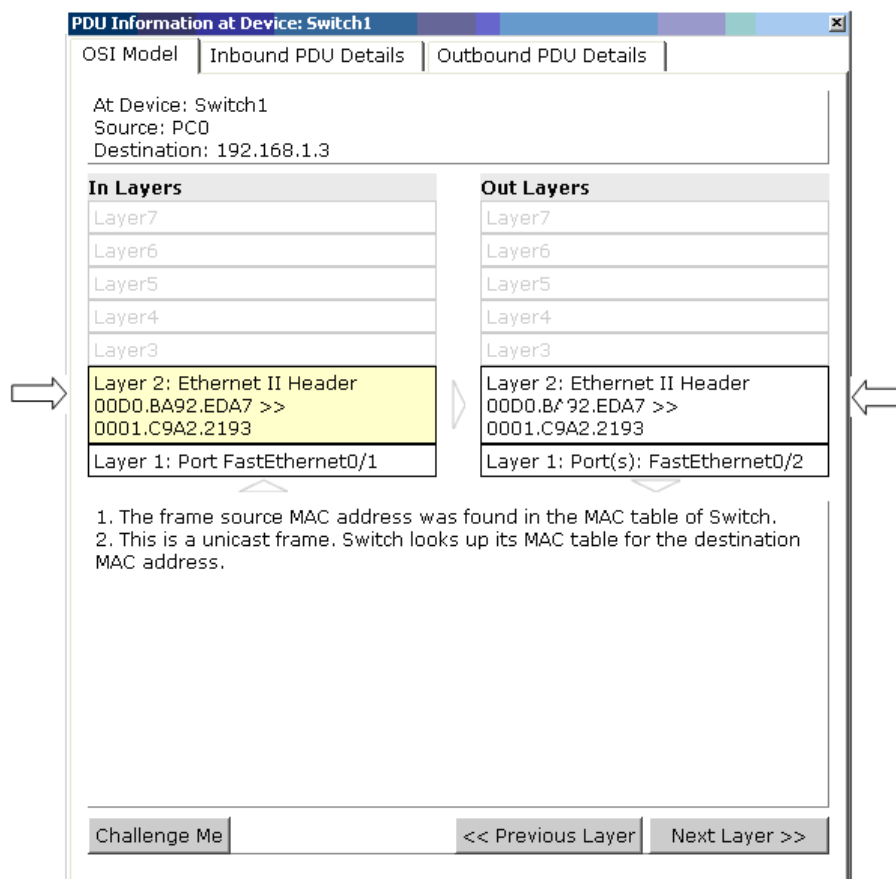


图 3.8 PDU 信息界面

从图 3.8 中, 可以看到一些信息。在图中左侧的 In Layers, layer1Fa0/1 是接收包的端口。Layer2 显示的是以太网帧的源 MAC 地址和目的 MAC 地址, 在这一层 Switch1 查看数据中的源 MAC 地址和目的 MAC 地址, 发现目的 MAC 地址在交换机的 MAC 地址表中。则在图中右侧的 Out Layers 的 layer2 中决定将帧从 FastEthernet0/2 端口进行转发, layer1 则在 Fa0/2 端口中发送数据报。

步骤 3.3.2 在图 3.8 中选择 Inbound PDU Details 标签, 便可查看进入 Switch1 数据报细节如图 3.9 所示。在 Ethernet II 中可以看到以太网帧的源 MAC 地址 00D0.BA92.EDA7 和目的 MAC 地址 0001.C9A2.2193; 在 IP 中可以看到源 IP 地址 192.168.1.2 和目的 IP 地址 192.168.1.3。ICMP 显示了一个 ICMP 数据帧。

同样在图 3.8 中选择 Outbound PDU Details 标签, 便可查看出 Switch1 数据报细节如图 3.10 所示。在图中同样可查看 MAC 地址和 IP 地址等信息。因为交换机依据目的 MAC 地址转发数据帧, 图 3.9 与图 3.10 并没有什么区别。

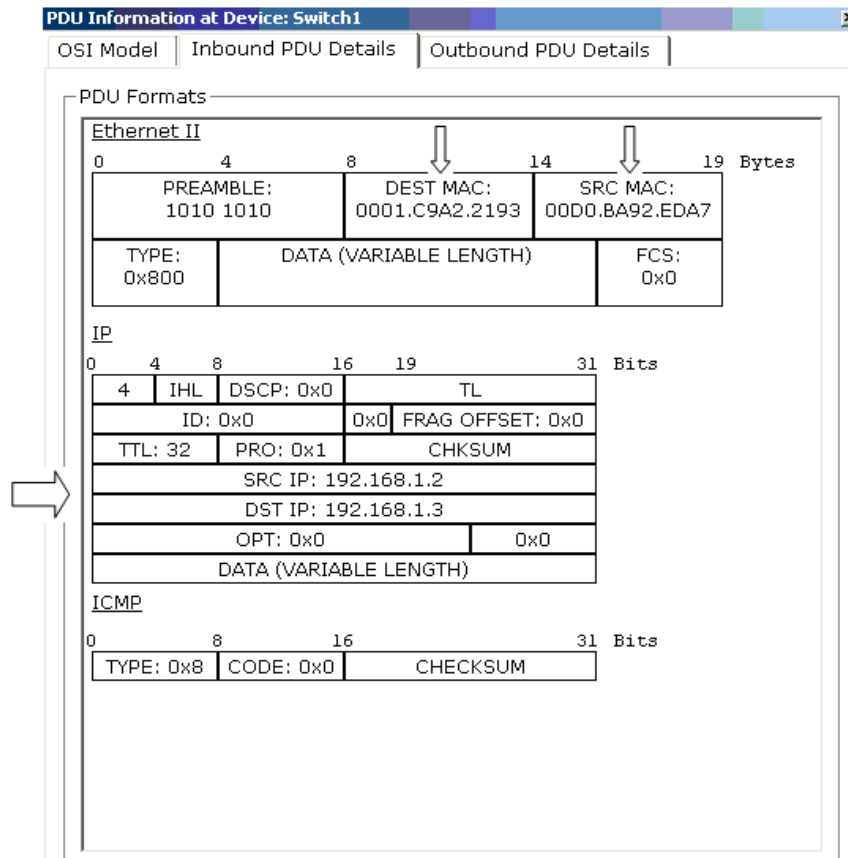


图 3.9 Inbound PDU Details 标签界面

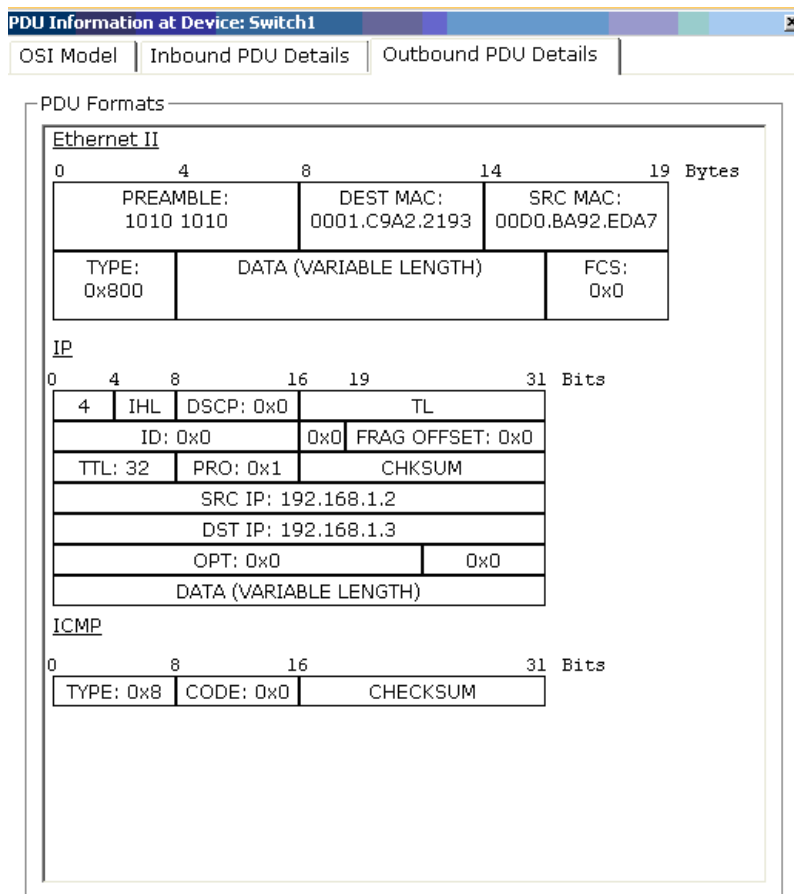


图 3.10 Outbound PDU Details 标签界面

【注意事项】

- 1、注意接口的选择以及连线所使用的线缆类型。
- 2、路由器间串口的配置时，不要漏掉时钟的设计。

【实验思考】

- 1、交换机的第一层功能是什么？
- 2、描述你在实验中的网络设备的规格和性能？
- 3、默认网关的作用是什么？
- 4、参考拓扑图中 PC 机的默认网关是否可以不设置？为什么？

实验四 交换机配置方式及基本命令的熟悉

【实验目的】

通过对交换机设备的几种配置手段、配置模式和基本配置命令的认识,获得交换机的基本使用能力。

【实验任务】

- 1、认识交换机的配置方式。
- 2、按照给出的参考拓扑图构建逻辑拓扑图。
- 3、按照给出的配置参数表配置各个设备。
- 4、练习交换机的一些基本命令。

建议实验学时: 2 学时。

【实验背景】

在前面的实验中我们已经接触了 Cisco 的路由器运行的 Cisco 互联网络操作系统 (ISO, Internetwork Operating System),熟悉了 Cisco IOS 软件内置的命令行界面 (CLI, command-line interface)。同样,交换机可以通过一个菜单驱动程序的界面,或者通过命令行界面 (CLI),或者在交换机配置了 IP 地址后通过 Telnet 远程登录、web 登录的方式对交换机来进行配置。

交换机除了可以通过 Console 端口与计算机直接连接外,还可以通过交换机的普通端口进行连接。如果是堆叠型的,也可以把几台交换机一起进行配置,因为实际上这个时候它们是一个整体,这时通过普通端口对交换机进行管理时,就不再使用超级终端了,而是以 Telnet 虚拟终端或 Web 浏览器的方式实现与被管理交换机的通信。前提是在本地配置方式中已为交换机配置好了 IP 地址,我们可通过 IP 地址与交换机进行通信,不过要注意,只有是网管型的交换机才具有这种管理功能。实际上最常用的 Catalyst 交换机 OS 被称为 Catalyst OS、CatOS,其最大的特点是基于 set 命令。但我们常用的是与路由器的 IOS 相类似的基于 IOS 的 Catalyst OS。下面简单介绍交换机的各种命令模式以及各种常用的命令。

表 4.1 交换机的各种命令模式的访问方式、提示符、退出方法及其描述

模式	访问方式	提示符	退出方法	描述
用户 EXEC (User EXEC)	在交换机上启动一个会话	Switch>	输入 Logout 或 quit	使用该模式完成基本的测试和系统显示功能
特权 EXEC (Privileged EXEC)	在用户 EXEC 模式下,输入 enable 命令	Switch#	输入 disable 或 exit	使用该模式来检验所输入的命令。一些配置命令也可以使用。可以用口令来保护对此模式的访问
VLAN 配置 (VLAN)	在特权 EXEC 模式下,输入 vlan	Switch(vlan)#	要退回到特权 EXEC 模式输入	使用该模式完成 vlan 各项参

configuration)	database 命令		入 exit	数的配置
全局配置 (Global configuration)	在特权 EXEC 模式下, 输入 configure 命令	Switch(config)#	要退回到特权 EXEC 模式输入 exit、end 或按下 ctr-z	使用该模式配置用于整个交换机的参数
接口配置 (Interface configuration)	在全局配置模式下, 输入 interface 命令以及特定端口号	Switch(config-if)#	要退回到全局配置模式, 输入 exit。要退回到特权 EXEC 模式, 按下 ctr-z 或输入 end	采用此模式为以太网接口配置参数
连接配置(Line configuration)	在全局配置模式下, 使用 line vty 或 line console 命令, 并指定连接编号	Switch(config-line)#	要退回到全局配置模式, 输入 exit。要退回到特权 EXEC 模式, 按下 ctr-z 或输入 end	使用该模式配置针对终端连接或 console 连接的参数

表 4.2 常用的命令及其完成的任务

命令	任务
Switch >enable	由用户模式进入特权模式
? (特权或者用户模式)	显示常用的命令的列表
Switch # show version	查看版本及引导信息
Switch # show running-config	查看运行设置
Switch # show startup-config	查看开机设置
Switch # show history	查看曾经键入过的命令的历史记录
Switch # show interface type slot/number	显示端口信息
Switch # copy running-config startup-config	将 RAM 中的当前配置保存到 NVRAM 中
Switch # copy startup-config running-config	加载来自 NVRAM 的配置信息
Switch # show vlan	显示虚拟局域网信息
Switch(config)#hostname	修改交换机的名称
Switch(config)#interface interface-number	对端口进行配置
Switch(config-if)#duplex full	将端口设置为全双工模式
Switch(config-if) #speed	设置端口的速度

【实验设备】

Catalyst2950, 运行终端仿真程序的 PC、Console 扁平线缆和相应的 DB-9 或 DB-25 适配器, 直通线。(本实验在 packet tracer 4.0 环境下完成)

【实验拓扑】

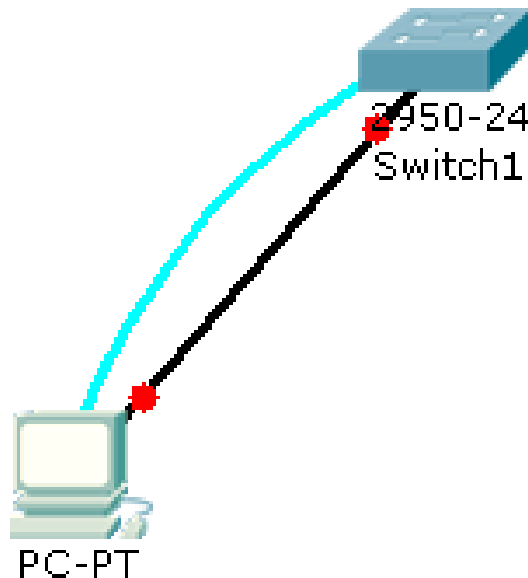


图 4.1

【实验步骤】

步骤 1 按照上述拓扑（在 packet tracer 4.0 中）将 PC 机与交换机连接好，双击 PC 机选择进入 Desktop->terminal 中,对交换机参数进行配置，进入命令行界面。使用 show version 命令来查看一下交换机的版本信息。

```
switch>show version
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE
SOFTWARE(fc1) //交换机所使用的操作系统版本号是 Version 12.1(22)EA4,
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba
Image text-base: 0x80010000, data-base: 0x80562000
ROM: Bootstrap program is is C2950 boot loader
Switch uptime is 49 minutes, 37 seconds
System returned to ROM by power-on
System image file is "flash:/c2950-i6q4l2-mz.121-22.EA4.bin" //该映像文件的名字是
c2950-i6q4l2-mz.121-22.EA4.bin
Cisco WS-C2950-24 (RC32300) processor (revision C0) with 21039K bytes of memory.
//交换机上安装了 21039K bytes 主存
Processor board ID FHK0610Z0WC
Last reset from system-reset
```

Running Standard Image

24 FastEthernet/IEEE 802.3 interface(s) //交换机上有 24 个快速以太网接口

32K bytes of flash-simulated non-volatile configuration memory. //非易失性存储器的容量是 32K bytes。

Base ethernet MAC Address: 0004.9A9B.D116

Motherboard assembly number: 73-5781-09

Power supply part number: 34-0965-01

Motherboard serial number: FOC061004SZ

Power supply serial number: DAB0609127D

Model revision number: C0

Motherboard revision number: A0

Model number: WS-C2950-24

System serial number: FHK0610Z0WC

Configuration register is 0xF //配置寄存器的值是 0xF

步骤 2 进入特权命令状态 enable；使用 show history 查看前面所输入的命令（不管是错误的还是正确的）；使用 show interface 端口号 来查看端口信息；使用 disable 退出特权命令状态。

```
Switch>enable
```

```
Switch#
```

```
switch#show history
```

```
show flash
```

```
enable
```

```
show flash
```

```
show history
```

```
show flash
```

```
show history
```

```
switch#show interface fas0/1
```

FastEthernet0/1 is up, line protocol is up (connected) //接口是启用的，线路协议是启用的

Hardware is Lance, address is 00d0.ba9e.6ba6 (bia 00d0.ba9e.6ba6) //显示接口的 MAC 地址

MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec, //最大数据传输单元为 1500bytes 带宽为 100000kbit/s,时延为 1000 秒

reliability 255/255, txload 1/255, rxload 1/255 //可靠性是 100%，收发的负载比。

Encapsulation ARPA, loopback not set

Keepalive set (10 sec)

Full-duplex, 100Mb/s //该接口是全双工的以 100Mb/s 来收发数据

input flow-control is off, output flow-control is off

ARP type: ARPA, ARP Timeout 04:00:00

Last input 00:00:08, output 00:00:05, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec //显示在前 5 分钟通过接口发送和接收的平

均位数和平均分组数。

```
956 packets input, 193351 bytes, 0 no buffer
  Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 watchdog, 0 multicast, 0 pause input
  0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
  0 output errors, 0 collisions, 10 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
```

0 output buffer failures, 0 output buffers swapped out//首先表示路由器接收的无错误分组的总数量。其次，它还表示路由器接收的无错误分组的总字节数。有无缓冲,接口所接收的广播或多播分组的总数量。

Switch#disable

步骤 3 从特权模式进入全局设置状态 configure terminal，将交换机的名字改为 SWI，

Switch#

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname SWI

步骤 4 设置进入特权状态的密码(secret)，此密文在设置以后不会以明文方式显示：

SWI(config)#enable secret catalyst

再次进入特权状态时要求输入口令。

SWI>enable

Password: //在此密码不会以明文的形式出现

SWI#

步骤 5 从全局配置模式进入 Fas0/1 端口配置模式，对端口进行配置：使用 duplex full 命令将端口设置为全双工模式，使用 speed 100 将其速率设为 100bps 使用 no shutdown 将端口状态设置为开。

SWI(config)#interface fas0/1

SWI(config-if)#duplex full

SWI(config-if)#speed 100

SWI(config-if)#no shutdown

SWI(config-if)#

步骤 6 使用 copy running-config startup-config 将配置从 running-config 保存到 startup-config 中，并使用 show running-config, show startup-config 查看其中的内容是否一致。

SWI#copy running-config startup-config

SWI#show running-config

【注意事项】

以上提供的常用命令只是针对于 packet tracer4.0 中的 2950 交换机而言，在其它交换机上不一定适用。

【思考题】

- 1、交换机和路由器上的功能和命令集是一样的吗？
- 2、远程配置交换机的硬软件条件是什么？

- 3、Encapsulation HAPA 是何意？
- 4、给出指定交换机的硬软件信息。

实验五 VLAN 构建与配置

【实验目的】

通过该实验理解 VLAN 的基本概念，掌握在二层交换机上创建 VLAN 的方法。

【实验任务】

- 1、按照给出的参考拓扑图构建逻辑拓扑图。
- 2、按照给出的配置参数表配置各个设备。
- 3、在二层交换机上构建 VLAN。
- 4、测试同一 VLAN 中的连通性。
- 5、利用三层路由器实现 VLAN 间通信。（进阶）

建议实验学时：4 学时；

【实验背景】

虚拟局域网 VLAN 是一组逻辑上的设备和用户，这些设备和用户并不受物理网段的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样，由此得名虚拟局域网。一个 VLAN 就是一个广播域，VLAN 之间的通信是通过第 3 层的路由器来完成的。与传统的局域网技术相比较，VLAN 技术更加灵活，它具有以下优点：

- 1) 减少网络设备的移动、添加和修改的管理开销；
- 2) 可以控制广播活动；
- 3) 可提高网络的安全性。

在实际应用中，假设某企业有 3 个主要部门：销售部，技术部和后勤部。这些部门的计算机分散连到 2 台交换机上，如要实现部门之间能相互通信，部门之间不能访问的需求就需要配置 Vlan。

【实验拓扑与配置参数】

实验的参考拓扑图和参考配置参数如图所示。

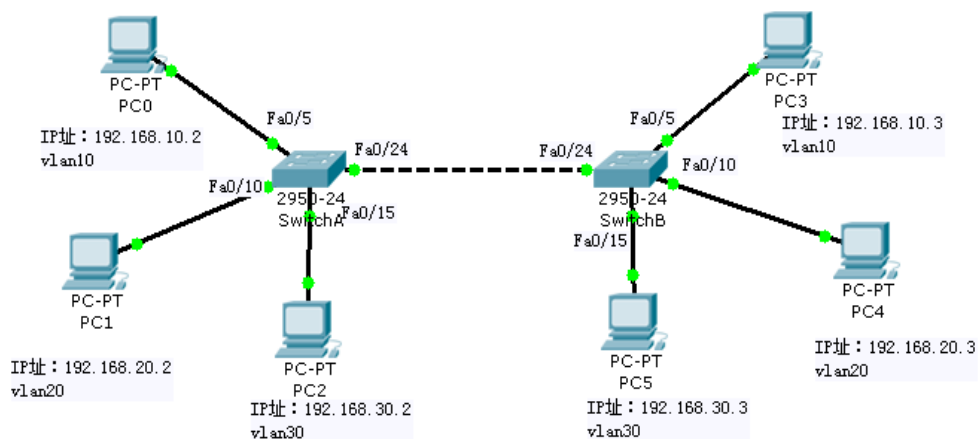


图 5.1 参考拓扑图

表 5.1 配置参数表

交换机信息				
交换机名称	类型	接口	所属 VLAN	
Switch A	2950-24	Fa0/5	Vlan 10	
		F a0/10	Vlan 20	
		Fa0/15	Vlan 30	
		Fa0/24	中继端口	
Switch B	2950-24	Fa0/5	Vlan 10	
		Fa0/10	Vlan 20	
		Fa0/15	Vlan 30	
		Fa0/24	中继端口	
PCS 信息 (子网掩码均为 255.255.255.0)				
主机名	IP 地址	缺省网关	所属网段	与 Switch 相连端口
PC0	192.168.10.2	192.168.10.1	192.168.10.0	SwitchA Fa0/5
PC1	192.168.20.2	192.168.20.1	192.168.20.0	SwitchA Fa0/10
PC2	192.168.30.2	192.168.30.1	192.168.30.0	SwitchA Fa0/15
PC3	192.168.10.3	192.168.10.1	192.168.10.0	Switch B Fa0/5
PC4	192.168.20.3	192.168.20.1	192.168.20.0	SwitchB Fa0/10
PC5	192.168.30.3	192.168.30.1	192.168.30.0	SwitchB Fa0/15

【实验设备】

两台 2950 交换机, PC 机 6 台, 直通线缆 6 根, 交叉线缆 1 根。(本实验在 packet tracer 4.0 环境下完成)

【实验步骤】

步骤 1 参考附录中 PackeTracer4.0 的使用方法, 按照图 5.1 参考拓扑图构建逻辑拓扑图。并按照表 5.1 参数配置表配置各个设备。

步骤 2 在交换机 Switch A 上创建三个 vlan(vlan10, 20, 30)并分别命名(v10,v20,v30)。(以交换机 Switch A 为例, 同样配置 Switch B)

步骤 2.1 创建 Vlan 10 并命名为 v10:

```
Switch# configure terminal
```

```
Switch(config) #hostname SwitchA           // 交换机改名
```

```
SwitchA(config)# vlan 10
```

```
SwitchA(config-vlan)# name v10           // 创建 Vlan 并命名为 v10
```

步骤 2.2 创建 Vlan 20 并命名为 v20:

```
SwitchA(config)#vlan 20
```

```
Switch A(config-vlan)#name v20           // 创建 Vlan 并命名为 v20
```

步骤 2.3 创建 Vlan 30 并命名为 v30:

```
SwitchA(config)#vlan 30
```

```
SwitchA(config-vlan)#name v30           // 创建 Vlan 并命名为 v10
```

步骤 3 把端口划分到 VLAN 中去。

(端口 Fa0/5 划到 v10, 端口 Fa0/10 划到 v20, 端口 Fa0/15 划到 v30,)

步骤 3.1 将 0/5 端口划分到 Vlan 10

```
SwitchA(config)#interface FastEthernet0/5
```

```
SwitchA(config-if)# switchport access vlan 10    // 将 0/5 端口划分到 Vlan 10
```

步骤 3.2 将 0/10 端口划分到 Vlan 20

```
SwitchA(config)#interface FastEthernet0/10
```

```
SwitchA(config-if)# switchport access vlan 20    // 将 0/10 端口划分到 Vlan 20
```

步骤 3.3 将 0/15 端口划分到 Vlan 30

```
SwitchA(config)#interface FastEthernet0/15
```

```
SwitchA(config-if)# switchport access vlan 30    // 将 0/15 端口划分到 Vlan 30
```

步骤 4.验证已创建的 VLAN。

```
SwitchA# show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24
10 v10	active	Fa0/5
20 v20	active	Fa0/10
30 v30	active	Fa0/15
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

步骤 5 按例给出交换机 Switch B 的配置。

步骤 6 设置交换机 Switch A 上与 Switch B 相连的端口（Fa0/24）。

Switch A 上与 Switch B 相连的端口 Fa0/24 的模式设置为 Trunk 模式。Trunk 是端口汇聚的意思，Trunk（干道）是一种封装技术，它是一条点到点的链路，主要功能就是仅通过一条链路就可以连接多个交换机从而扩展已配置的多个 VLAN。

步骤 6.1 交换机 Switch A 的 Fa0/24 的配置。

```
SwitchA(config)#interface FastEthernet0/24
```

```
SwitchA(config-if)# switchport mode trunk    // 将 Fa0/24 设为 Trunk 模式
```

步骤 6.2 按例给出交换机 Switch B 的 Fa0/24 的配置。

步骤 7 验证 PC0 和 PC3, PC1 和 PC4, PC2 和 PC5 能相互通信，说明同一 Vlan 内的主机能相互连通。而 PC0 和 PC4, PC5 不能相互通信，说明了不同 Vlan 间不能通信。

步骤 7.1 验证 PC0 和 PC3 能相互通信。（同样可验证 PC1 和 PC4, PC2 和 PC5 能连通）

各主机按照参数表中的 IP 地址和网关设置进行配置，并按照参数表要求与交换机相应的端口用直通线连接起来。

单击拓扑图中的 PC0 图标。在弹出的配置界面中，选择 Desktop 标签，选择 Command Prompt，键入 ping 192.168.10.3 命令。

```
PC>ping 192.168.10.3
```

Ping 命令的结果不能自动生成。模拟环境下使用 Ping 命令时，ICMP 数据报的传输路径可以在仿真环境中 Simulation 模式下看到，点击右下角 Simulation 模式图标，在 Event

List 中便可看到 Ping 事件, 在工作区便会看到传输的包, 然后点击 Auto Capture 按钮, 可以看到包在设备间传输, 同时便可看到 Ping 的结果。如图 5.2。

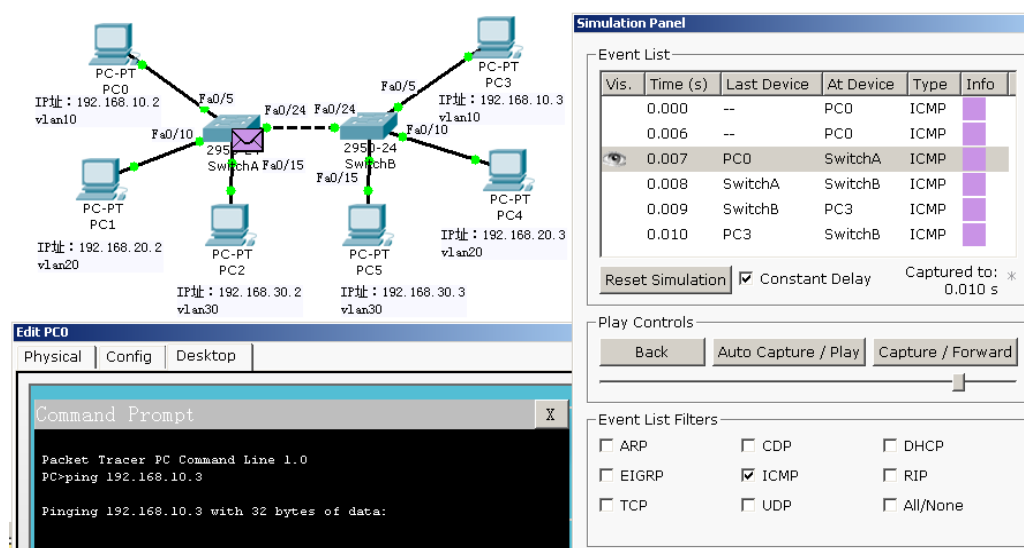


图 5.2 Ping 命令视图

查看结果, 如果 Ping 通则网络正常, Ping 不通, 则就要进行故障排查。

步骤 7.2 验证 PC0 和 PC4 不能相互通信。(其他可作同样验证)

在 PC0 的 Command Prompt 中输入 ping 192.168.20.3

PC>ping 192.168.20.3

查看结果, 如果 Ping 不通则网络正常, Ping 通, 则就要进行故障排查。

步骤 8. 交换机上数据报的传输跟踪。

以 PC0 和 PC3 的连通性测试时发送的 ICMP 数据报为例。

步骤 8.1 由 PC0 发送的 ICMP 数据报传送到交换机 Switch A 时, Switch A 的 Fa0/5 接口接收数据, 连接到 Fa0/5 的 PC 机则属于 Vlan10, 从这个端口流出的数据只能在 Vlan10 中流通。然后查看数据中的源 MAC 地址和目的 MAC 地址, 如果交换机知道源 MAC 地址和目的 MAC 地址在一个网段内, 会将数据报丢弃, 无需传送 (称为过滤); 如果数据报的目的 MAC 地址不在交换机的 MAC 地址表中, 交换机不知道目的网段, 就会将数据报传送到除源网段以外的所有网段 (称为泛洪); 如果数据报的目的 MAC 地址在交换机的 MAC 地址表中, 交换机就会将数据报传送到相应网段的出口 (称为转发)。这是交换机的二层功能。在这里, Switch A 知道数据报的目的 MAC 地址在交换机的 MAC 地址表中, Switch A 就会将数据报转发到相应网段的出口 Fa0/24。而 FastEthernet0/24 端口是一个 Trunk 端口, 所有 Vlan 都允许进入此端口并进行转发, 则将帧用 802.1q 进行标记, 802.1q 协议可对帧所属 VLAN 作标识, 标记它属于哪个 Vlan 的数据。从而保证同一 Vlan 的数据进行传输。

步骤 8.1.1 如上图 5.2 所示, 当 ICMP 包传输到 Switch A 时, 可以单击 Event List 中右侧的 Info 框在弹出的 PDU 信息界面中就可以查看包在 Switch 1 上的处理过程, 也可以直接单击工作区中处于 Switch A 上的包进入 PDU 信息界面。如图 5.3 所示:

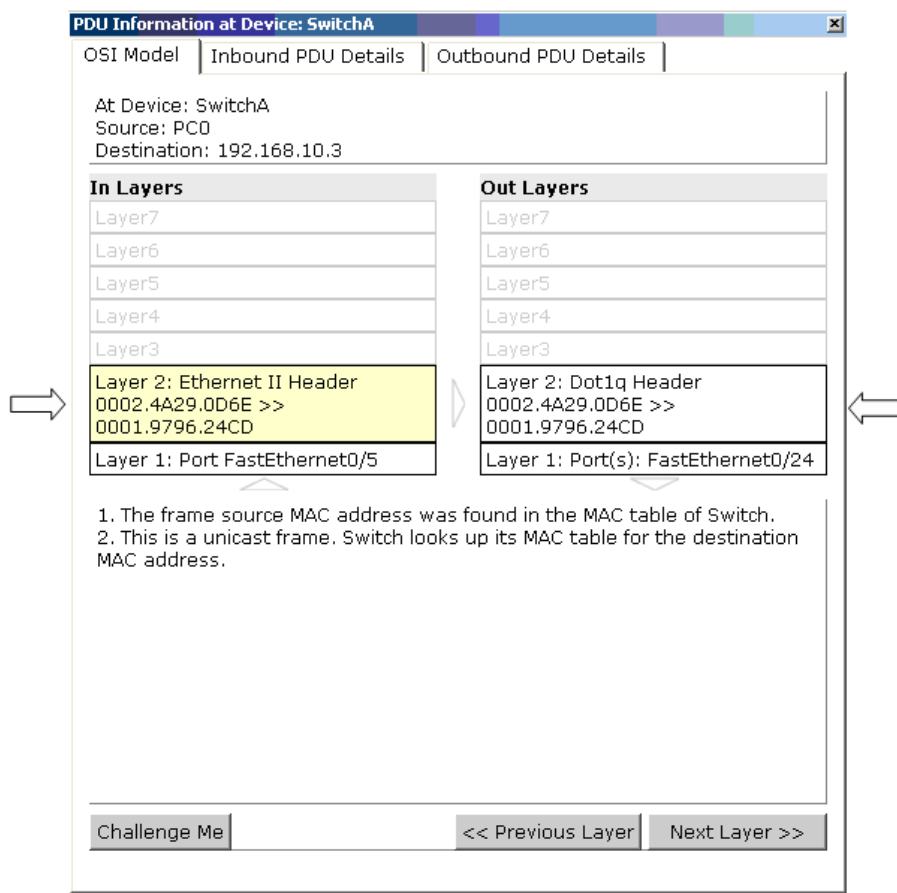


图 5.3 PDU 信息界面

从图 5.3 中, 可以看到一些信息。在图中左侧的 In Layers, layer1Fa0/5 是接收包的端口, 连接到 Fa0/5 的 PC 机则属于 Vlan10。Layer2 显示的是以太网帧的源 MAC 地址和目的 MAC 地址, 在这一层 Switch1 查看数据中的源 MAC 地址和目的 MAC 地址, 发现目的 MAC 地址在交换机的 MAC 地址表中。则在图中右侧的 Out Layers 的 layer2 中, 决定将帧从 FastEthernet0/24 端口进行转发, 而 FastEthernet0/24 端口是一个 Trunk 端口, 所有 Vlan 都允许进入此端口并进行转发, 图中的 Dot1q 是帧标记, 标记它属于哪个 Vlan 的数据。layer1 则在 Fa0/24 端口中发送数据报。

步骤 8.1.2 在图 5.3 中选择 Inbound PDU Details 标签, 便可查看进入 SwitchA 数据报细节如图 5.4 所示。在 Ethernet II 中可以看到以太网帧的源 MAC 地址 0002.4A29.0D6E 和目的 MAC 地址 0001.9796.24CD; 在 IP 中可以看到源 IP 地址 192.168.10.2 和目的 IP 地址 192.168.10.3。ICMP 显示了是一个 ICMP 数据帧。

同样在图 5.3 中选择 Outbound PDU Details 标签, 便可查看出 SwitchA 数据报细节如图 5.5 所示。在图中同样可查看 MAC 地址和 IP 地址等信息。图 5.4 与图 5.5 的区别是帧的格式不同, 流出 Switch A 的帧要进行标记, Dot1q 是帧标记, 标记它属于哪个 Vlan 的数据。

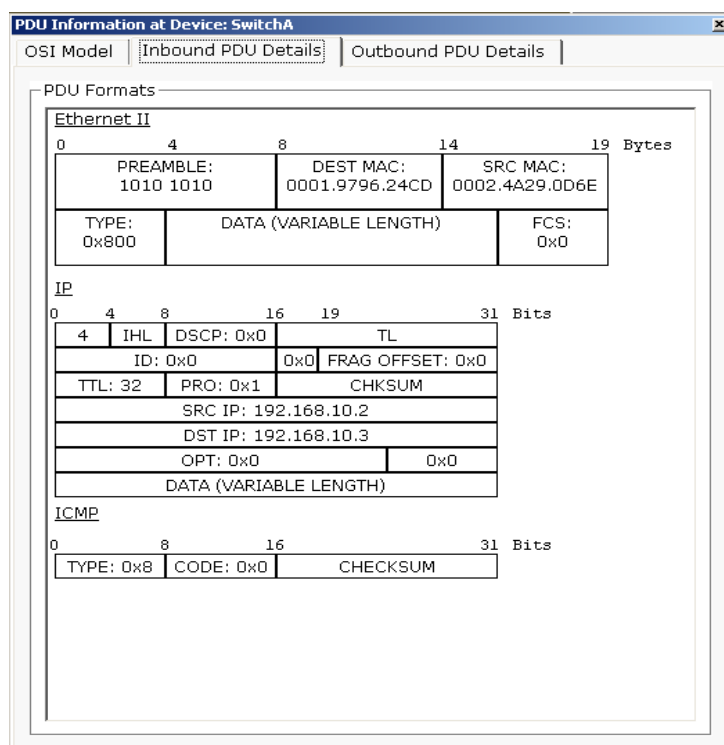


图 5.4 Inbound PDU Details 界面

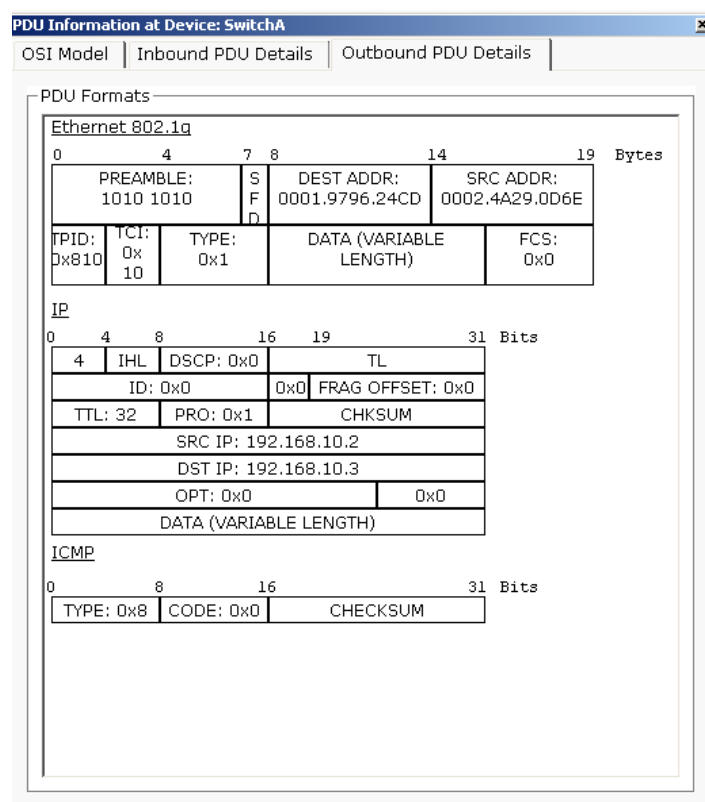


图 5.5 Outbound PDU Details 界面

步骤 8.2 由 PC0 发送的 ICMP 数据报传送到交换机 Switch B 时，Switch B 的 Fa0/24 接

口接收数据，FastEthernet0/24 端口是一个 Trunk 端口，发现进入此端口的帧是进行了 Dot1q 帧标记，属于 Vlan10 的数据。Switch B 去除帧标记，然后查看数据中的源 MAC 地址和目的 MAC 地址，如果交换机知道数据报的目的 MAC 地址在交换机的 MAC 地址表中，并且相应网段的出口 Fa0/5 属于 Vlan10，交换机就会将数据封装成以太网帧后传送到相应网段的出口。

【注意事项】

两台交换机之间相连的端口应该设置为 Trunk 模式。

【参考配置】

```
SwitchA# show running-config
version 12.1
hostname SwitchA
interface FastEthernet0/5
    switchport access vlan 10
    switchport mode access
interface FastEthernet0/10
    switchport access vlan 20
    switchport mode access
interface FastEthernet0/15
    switchport access vlan 30
    switchport mode access
interface FastEthernet0/24
    switchport mode trunk
interface Vlan1
    no ip address
    shutdown
line con 0
end
SwitchB# show running-config
version 12.1
hostname SwitchB
interface FastEthernet0/5
    switchport access vlan 10
    switchport mode access
interface FastEthernet0/10
    switchport access vlan 20
    switchport mode access
interface FastEthernet0/15
    switchport access vlan 30
    switchport mode access
interface FastEthernet0/24
    switchport mode trunk
```

```
interface Vlan1
  no ip address
  shutdown
  line con 0
end
```

【实验思考】

- 1、S2950 是否具有三层交换功能？若要 Vlan 间能够通信，交换机应具有什么层次要求？还可以加入什么设备使 Vlan 间能够通信？
- 2、端口 Access 和 Trunk 模式的含义是什么？
- 3、交换机是如何感知周围网络环境的变化（如计算机增加，减少等）？
- 4、三层交换技术产生的原因和技术特点？

进阶实验 二层交换机+路由器实现 VLAN 间通信

【实验目的】

进一步理解 VLAN 概念，掌握解决 VLAN 间通信的方法。

【实验任务】

- 1、按照给出的参考拓扑图构建逻辑拓扑图。
- 2、按照给出的配置参数表配置各个设备。
- 3、在路由器上创建子接口，选择 VLAN 封装格式，并激活路由选择协议。
- 4、在交换机中创建 VLAN，向 VLAN 中添加交换机端口，配置 Trunk 端口。
- 5、测试 VLAN 间相互通信。

【实验设备】

交换机 2950 1 台，路由器 2621 1 台，PC 2 台。（在模拟软件 PacketTracer4.0 环境下完成）

【实验背景】

在前面的应用案例中，若各个部门之间也需要通信，就需要配置 Vlan 间通信。

【实验拓扑与配置参数】

实验的参考拓扑图和参考配置参数如图所示。

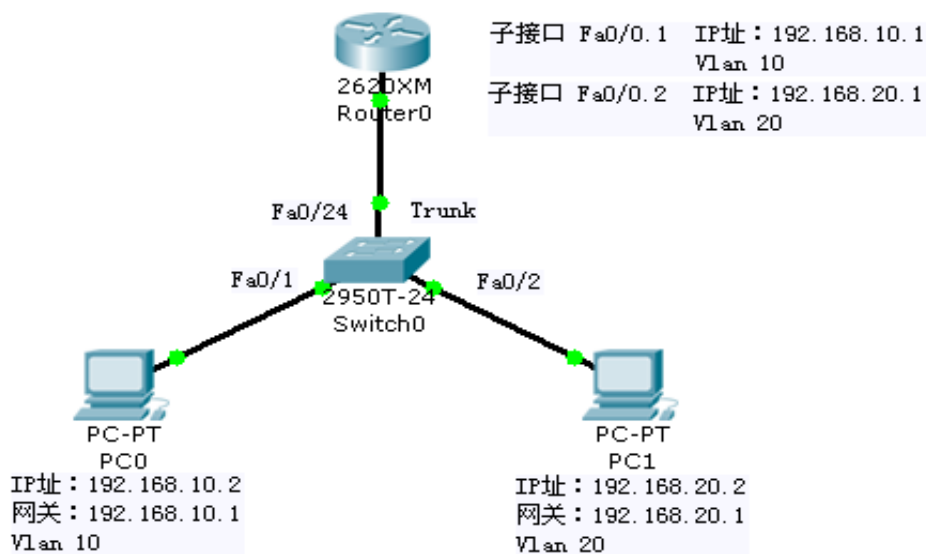


图 5.6 参考拓扑图

表 5.2 配置参数表

交换机信息				
交换机名称	类型	接口	所属 VLAN	
Switch 1	2950T-24	Fa0/1	Vlan 10	
		Fa0/2	Vlan 20	
		Fa0/24	中继端口	
PC 信息 (子网掩码均为 255.255.255.0)				
主机名	IP 地址	缺省网关	所属网段	与 Switch 相连端口
PC0	192.168.10.2	192.168.10.1	192.168.10.0	Switch1 Fa0/1
PC1	192.168.20.2	192.168.20.1	192.168.20.0	Switch1 Fa0/2
路由器信息				
路由器名称	类型	子接口	IP 地址	所属 VLAN
Router 0	2620XM	Fa0/0.1	192.168.10.1	Vlan 10
		Fa0/0.2	192.168.20.1	Vlan 20

【实验步骤】

步骤 1 参考附录中 PacketTracer4.0 的使用方法,按照图 5.6 参考拓扑图构建逻辑拓扑图。并按照表 5.2 参数配置表配置各个设备。

步骤 2 在 2950 上创建 vlan10, 20

```
Switch# configure terminal
```

```
Switch(config)#vlan 10
```

```
Switch(config-vlan)#name v10
```

```
Switch(config-vlan)#exit
```

```
Switch(config)#vlan 20
```

```
Switch(config-vlan)#name v20
```

步骤 3 把交换机端口分配给 vlan 。(Fa0/1 划给 vlan10, Fa0/2 划给 vlan20)

```
Switch(config)#interface FastEthernet0/1
```

```
Switch(config-if)#switchport access vlan 10
```

```
Switch(config)#interface FastEthernet0/2
```

```
Switch(config-if)#switchport access vlan 20
```

步骤 4 在 Fa0/24 端口设置 Trunk。

```
Switch(config)#interface FastEthernet0/24
```

```
Switch(config-if)#switchport mode trunk
```

注意: Cisco 2950 只支持 802.1Q 协议, 所以在这里不用专门来指定封装协议。若要指定协议使用命令: Switch(config-if)#switchport trunk encapsulation dot1q
(仿真环境不能使用, 因此这里就不必配置)

步骤 5 配置路由器子接口

```
Router(config)#interface fastethernet 0/0.1
```

```
Router(config-subif)#encapsulation dot1q 10
```

//配置封装模式为 IEEE802.1Q, 对应 VLAN 号为 10

```
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
```

```
Router(config)#interface fastethernet 0/0.2
```

```
Router(config-subif)#encapsulation dot1q 20
```

```
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
```

步骤 6 测试 PC0 到 PC1 的连通性。

单击拓扑图中的 PC0 图标。在弹出的配置界面中, 选择 Desktop 标签, 选择 Command Prompt, 键入 ping 192.168.20.2 命令。

```
PC>ping 192.168.20.2
```

Ping 命令的结果不能自动生成。模拟环境下使用 Ping 命令时, ICMP 数据报的传输路径可以在仿真环境中 Simulation 模式下察看到, 点击右下角 Simulation 模式图标, 在 Event List 中便可看到 Ping 事件, 在工作区便会看到传输的包, 然后点击 Auto Capture 按钮, 可以看到包在设备间传输, 同时便可看到 Ping 的结果。如图 5.7。

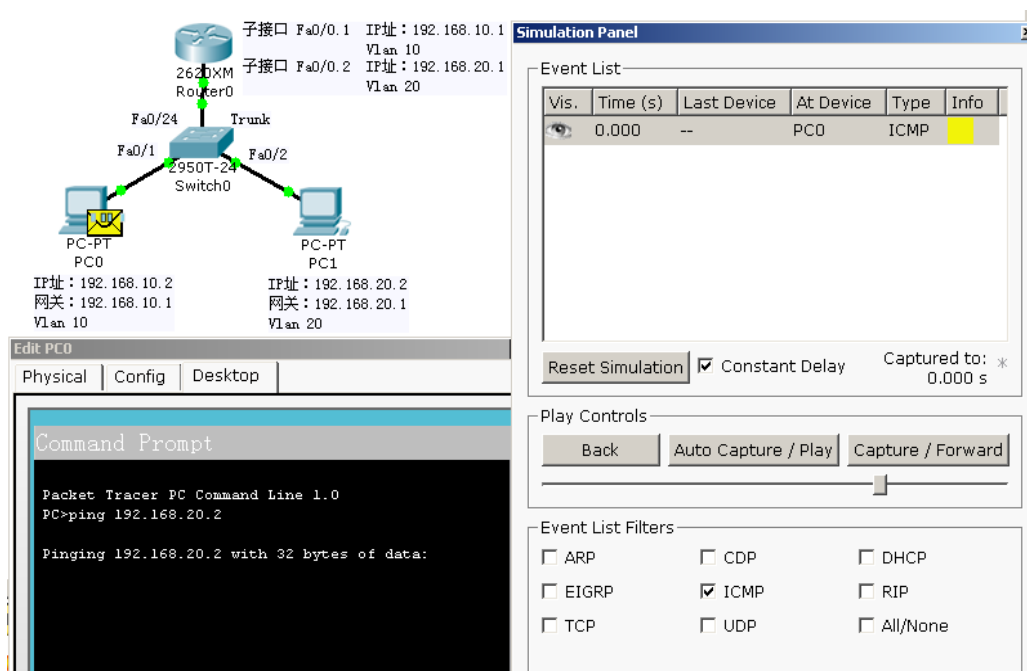


图 5.7 Ping 命令视图

查看结果，如果 Ping 通则网络正常，Ping 不通，则就要进行故障排查。

【参考配置】

```
Router#show running-config
version 12.2
hostname Router
interface FastEthernet0/0
  no ip address
  duplex auto
  speed auto
interface FastEthernet0/0.1
  encapsulation dot1Q 10
  ip address 192.168.10.1 255.255.255.0
interface FastEthernet0/0.2
  encapsulation dot1Q 20
  ip address 192.168.20.1 255.255.255.0
ip classless
line con 0
end
```

【注意事项】

- 1、因为与 Trunk 相连的路由器端口同时能够与两个 Vlan 连通，所以设置两个子接口（Fa0/0.1 和 Fa0/0.2），分别分配到两个 Vlan 中，并分别为这两个子接口分配 IP 地址，使之可以同时属于两个网段。
- 2、可以命令 ip routing 启动 IP 路由选择，这一命令通常在默认情况下是启动的。

【实验思考】

- 1、子接口是物理接口还是逻辑接口？为什么？
- 2、何为三层交换机？Cisco 的哪个系列交换机是三层交换机？
- 3、路由器可以配置的带 802.1Q 封装的子接口数最多有多少？
- 4、中继两端的封装为什么必须一致？Isl 与 Dot1.q 封装有什么不同？

实验六 多网段网络组建与静态路由配置

【实验目的】

通过设计有两个路由器的网络及静态路由的配置理解静态路由原理。

【实验任务】

- 1、按照给出的参考拓扑图构建逻辑拓扑图。
 - 2、按照给出的配置参数表配置各个设备。
 - 3、练习静态路由的配置。
 - 4、完成连通性测试和包传输路径跟踪测试。
- 建议实验学时：2 学时。

【实验背景】

静态路由是指由网络管理员手工给出的路由信息，建立路由表。静态路由适合在规模较小、不经常改变的网络。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手工去修改路由表中相关的静态路由信息。静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。

静态路由选择有许多优点：

- 1、不需要动态路由选择协议，这减少了路由器的计算和带宽开销。
- 2、在小型互连网络上很容易配置。
- 3、可以控制路由选择。

【实验拓扑与配置参数】

实验的参考拓扑图和参考配置参数如图所示。

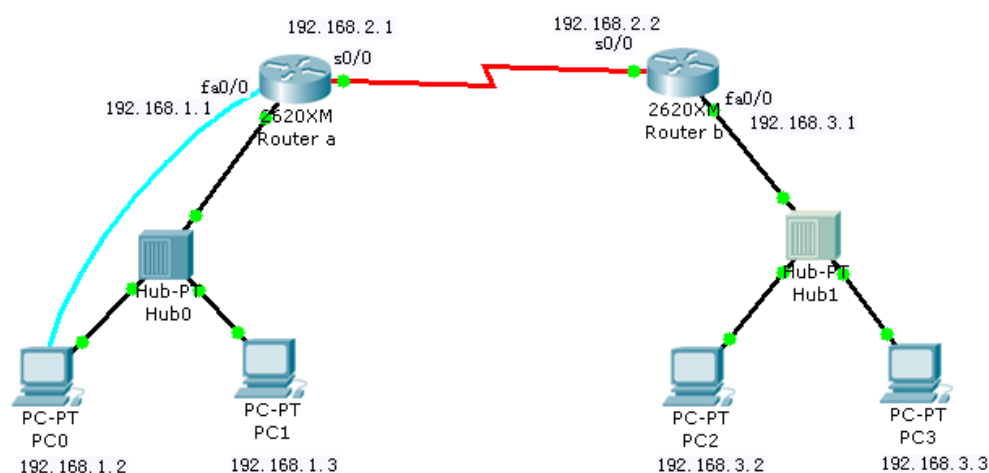


图 6.1 参考拓扑图

表 6.1 配置参数表

路由器信息(子网掩码均为 255.255.255.0)			
路由器名称	类型	IP 地址	时钟频率
Router a	2620XM	Fa0/0: 192.168.1.1 S0/0: 192.168.2.1	56000
Router b	2620XM	Fa0/0: 192.168.3.1 S0/0: 192.168.2.2	
PC 信息(子网掩码均为 255.255.255.0)			
主机名	IP 地址	缺省网关	所属网段
PC0	192.168.1.2	192.168.1.1	192.168.1.0
PC1	192.168.1.3	192.168.1.1	192.168.1.0
PC2	192.168.3.2	192.168.3.1	192.168.3.0
PC3	192.168.3.3	192.168.3.1	192.168.3.0
Hub 信息			
Hub 名称	类型	所属网段	
Hub 0	Hub-PT	192.168.1.0	
Hub 1	Hub-PT	192.168.3.0	

【实验设备】

PC 机 4 台；Cisco 路由器 2620XM 2 台；反转线 1 根；串行线缆 1 对；HUB 2 台，直通线 6 根。（本实验在 packet tracer 4.0 环境下完成）

【实验步骤】

步骤 1 参考附录中 PackeTracer4.0 的使用方法，按照图 6.1 参考拓扑图将设备连接起来，并按照表 6.1 参数配置表配置各个设备。

步骤 1.1 以 Router a 和 192.168.1.0 网络设备的配置为例

步骤 1.1.1 Router a 的配置

1. 配置以太网端口

```
Route#configure terminal
```

```
Router(config)# hostname Ra （改名为 Ra）
```

```
Ra (config)# interface FastEthernet0/0
```

```
Ra (config-if)# ip address 192.168.1.1 255.255.255.0
```

```
Ra (config-if)# no shutdown
```

2.配置串行端口

```
Ra(config)# interface Serial0/0
```

```
Ra(config-if)# bandwidth 56 （串行线两端都需要设定带宽）
```

```
Ra(config-if)# clock rate 56000 （串行线中 DCE 端需设定时钟，DTE 端则不需要）
```

```
Ra(config-if)# ip address 192.168.2.1 255.255.255.0
```

```
Ra(config-if) #no shutdown
```

步骤 1.1.2 192.168.1.0 网络中 PC0 和 PC1 的配置。

主机的 IP 址和网关根据配置参数表分配好的地址进行设计即可。192.168.1.0 网络中的 Hub 不需要进行配置。

单击拓扑图中的 PC0 图标。在弹出的配置界面中，选择 Desktop 标签，在选择 IP Configuration，便可配置主机 IP 址和网关。同样可配置 PC1。

步骤 1.2 按例给出 Router b 和 192.168.3.0 网络设备的配置。

步骤 2 配置静态路由。

步骤 2.1 以 Router a 中静态路由配置为例。

(Router a 上需配置到达所有网段的路由信息，才能与各个网段连通，因为参考拓扑比较简单，192.168.1.0 网段和 192.168.2.0 网段是直连的网段，所以只需要配置到 192.168.3.0 网段的路由信息。)

步骤 2.1.1 登陆到路由器 Router a 的 CLI。

步骤 2.1.2 进入全局模式，键入命令：

Ra (config) # ip route 192.168.3.0 255.255.255.0 192.168.2.2

步骤 2.1.3 检查配置的路由信息是否在路由表中。用 show ip route 命令。

Ra# show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, FastEthernet0/0 //指示 192.168.1.0 是 Router a 的直连网络

C 192.168.2.0/24 is directly connected, Serial0/0

S 192.168.3.0/24 [1/0] via 192.168.2.2 //指示这条路由信息是静态配置而来，192.168.3.0 网络是静态配置而得。

步骤 2.1.4 在特权配置模式下输入：Ra # copy running-config startup-config 将运行的配置文件保存一下。

步骤 2.2 按例给出 Router b 到达网络 192.168.1.0 的静态路由。

步骤 3 连通性和包传输路径的跟踪测试；

步骤 3.1 连通性测试。

步骤 3.1.1 主机间连通性测试。

以 PC0 到 PC2 的连通性测试为例。单击拓扑图中的 PC0 图标。在弹出的配置界面中，选择 Desktop 标签，选择 Command Prompt，键入 ping 命令。

PC> ping 192.168.3.2

注意：模拟环境不同与实际环境。Ping 命令的结果不能自动生成。模拟环境下使用 Ping 命令时，ICMP 数据报的传输路径可以在仿真环境中 Simulation 模式下察看到，点击右下角 Simulation 模式图标，在 Event List 中便可看到 Ping 事件，在工作区便会看到传输的包，然后点击 Auto Capture 按钮，可以看到包在设备间传输，同时便可看到 Ping 的结果。如图 6.2。

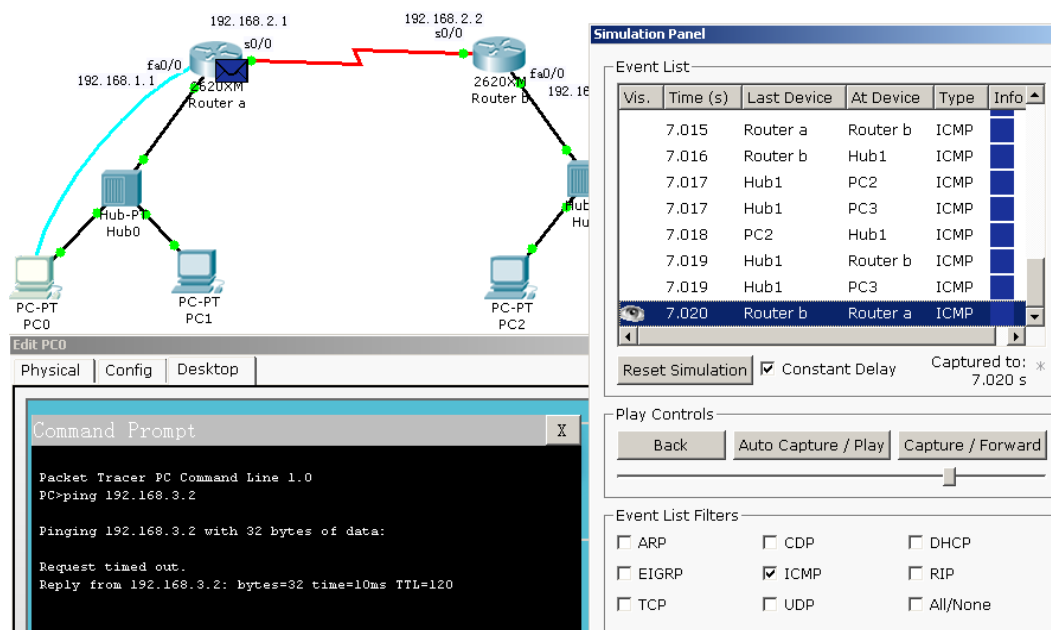


图 6.2 Ping 命令视图

查看结果，如果 Ping 通则网络正常，Ping 不通，则就要进行故障排查。

步骤 3.1.2 按例完成其他主机间连通性测试。

步骤 3.1.3 路由器间连通性测试。

以 Router a 到 Router b 的连通性测试为例。在 Router a 的命令行界面中输入以下命令：

Ra# ping 192.168.3.1

查看结果，如果 Ping 通则网络正常，Ping 不通，则就要进行故障排查。

步骤 3.2 包传输路径跟踪测试。

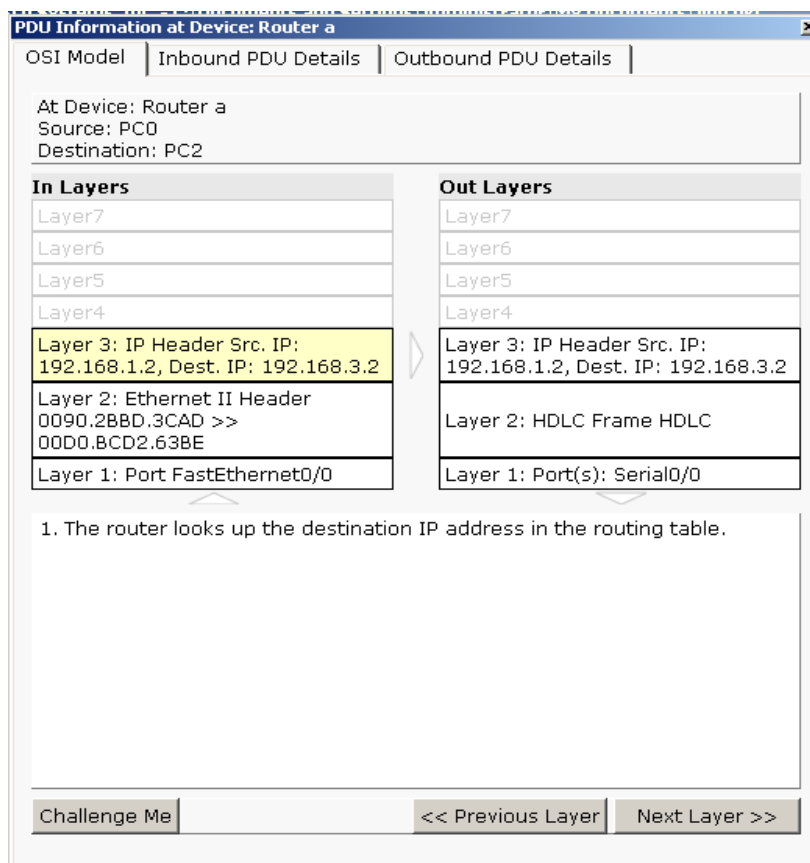
数据在三层的处理过程，可以以 PC0 到 PC2 的连通性测试时发送的 ICMP 数据报在路由器上的处理为例。

路由器工作在 OSI 模型中的第三层，即网络层。路由器利用网络层定义的“逻辑”上的网络地址（即 IP 地址）来区别不同的网络，实现网络的互连和隔离，保持各个网络的独立性。路由器不转发广播消息，而把广播消息限制在各自的网络内部。发送到其他网络的数据先被送到路由器，再由路由器转发出去。路由器转发 IP 分组时，只根据 IP 分组目的 IP 地址的网络号部分，选择合适的端口，把 IP 分组送出去。同主机一样，路由器也要判定端口所接的是否是目的子网，如果是，就直接把分组通过端口送到网络上，否则，也要选择下一个路由器来传送分组。如果没有到达目的网络的路由信息时，会将收到的数据发送到默认网关。

由 PC0 发送的 ICMP 数据报传送到路由器 Router a 时，Router a 的 Fa0/0 端口接收数据。然后对数据向上进行解封装，到第三层时，查看目的 IP 地址，并查看目的 IP 地址是否在路由选择表中，如果在路由表中就转发到相应的端口 s0/0 中。

在 PC1 的命令模式中键入 ping 192.168.3.2 命令，同样会在 Simulation 模式下的 Event List 中会看到 Ping 事件，在工作区便会看到传输的包。如上图 6.2 所示。

步骤 3.2.1 当 ICMP 包传输到 Router a 时，可以单击图 6.2 中 Event List 右侧的 Info 框在弹出的 PDU 信息界面中就可以查看包在 Router a 上的处理过程，也可以直接单击工作区中处于 Router a 上的包进入 PDU 信息界面。如图 6.3 所示：



如图 6.3 PDU 信息界面

从图 6.3 中, 可以看到一些信息。在图中左侧的 In Layers, layer1 的 Fa0/0 是接收包的端口。Layer2 显示的是以太网帧的源 MAC 地址和目的 MAC 地址, 在这一层 Router a 查看数据中的目的 MAC 地址与接收端口的 MAC 地址是否匹配, 然后进行解封装。在 Layer3, Router0 查看目的 IP 与端口的 IP 是否匹配, 然后查看目的 IP 地址是否在路由选择表中, 发现有目的 IP 址的路由信息, 此路由信息是静态配置而得。则在图中右侧的 Out Layers 的 layer3 中决定转发, 在 Layer2 用源 MAC 和目的 Mac 址对数据进行封装, 封装成 HDLC 帧。layer1 则将数据从 S0/0 端口中发送出去。

步骤 3.2.2 在图 6.3 中选择 Inbound PDU Details 标签, 便可查看进入 Router a 数据报细节, 如图 6.4 所示。在 Ethernet II 中可以看到以太网帧的源 MAC 地址 0090.4208.BCD2.3CAD 和目的 MAC 地址 00D0.BCD2.63BE; 在 IP 中可以看到源 IP 地址 192.168.1.2 和目的 IP 地址 192.168.3.2。

同样在图 6.3 中选择 Outbound PDU Details 标签, 便可查看出 Router a 数据报细节, 如图 6.5 所示。在图中同样可查看帧格式和 IP 地址等信息。图 6.4 与图 6.5 区别是帧的格式不同。因为数据从路由器流出时是要进行串行传输, 要使用 HDLC 帧, 而不在是以太网帧的格式。

PDU Information at Device: Router a

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 1010 1010		DEST MAC: 00D0.BCD2.63BE		SRC MAC: 0090.2BBD.3CAD	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL			
ID: 0x0		0x0		FRAG OFFSET: 0x0		
TTL: 32		PRO: 0x1		CHKSUM		
SRC IP: 192.168.1.2						
DST IP: 192.168.3.2						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

ICMP

0	8	16	31	Bits
TYPE: 0x8		CODE: 0x0		CHECKSUM

图 6.4 Inbound PDU Details 界面

PDU Information at Device: Router a

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

HDLC

0	8	16	32	32+x	40+x	48+x	Bits
FLG: 0111 1110		ADR: 0x8f		CONTROL: 0x0		DATA: (VARIABLE LENGTH)	
FCS: 0x0		FLG: 0111 1110					

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL			
ID: 0x0		0x0		FRAG OFFSET: 0x0		
TTL: 31		PRO: 0x1		CHKSUM		
SRC IP: 192.168.1.2						
DST IP: 192.168.3.2						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

ICMP

0	8	16	31	Bits
TYPE: 0x8		CODE: 0x0		CHECKSUM

图 6.5 Outbound PDU Details 界面

步骤 3.2.3 当 ICMP 数据报传输到 Router 上的时候, 路由器第一层功能是接受数据位串, 第二层功能将 HDLC 进行解封装, 第三层查看目的 IP 信息是否再自己的路由选择表中, 发现有目的 IP 的信息, 属于 Router b 的直连网络。然后对将数据封装成以太网帧, 从端口 Fa0/0 中转发出去。具体包跟踪可按照上面的分析给出。

【注意事项】

- 1、静态路由信息在缺省情况下是私有的, 不会传递给其他的路由器。
- 2、在默认情况下, 静态路由的出口方式指定优先级会比下一跳地址高, 但是我们这里建议网络管理者使用下一跳地址做为静态路由, 因为如果出口是在关闭状态下, 那么这条静态路由便不会被装载到路由表中。
- 3、静态路由的另一个作用是作动态路由的备份路由选项, 如果我们已经配置了动态路由, 可以手动的更改静态路由的优先级, 当动态路由出现问题的时候路由器便可以选择这条静态路由来转发数据包。

【参考配置】

Ra#show running //Router a 的运行配置

```
version 12.2
hostname Ra
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0
 ip address 192.168.2.1 255.255.255.0
 clock rate 56000
interface Serial0/1
 no ip address
 shutdown
router rip
 ip classless
 ip route 192.168.3.0 255.255.255.0 192.168.2.2
 line con 0
end
```

Rb#show running //Router b 的运行配置

```
version 12.2
hostname Rb
interface FastEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0
 ip address 192.168.2.2 255.255.255.0
interface Serial0/1
```



```
no ip address
shutdown
router rip
ip classless
ip route 192.168.1.0 255.255.255.0 192.168.2.1
line con 0
end
```

【实验思考】

1、路由选择表获取信息的方式有两种：以静态路由表项的方式手工输入和通过动态路由选择协议自动获取信息。静态路由和动态路由的优先级别那个高，是绝对的吗？那么优先级是由什么来决定的呢？

2、静态路由的管理距离是多少？管理距离有何作用？

3、为何有时需要配置默认路由？默认路由的作用是什么？

4、如何配置默认路由？（自己设计一个实验）

实验七 多网段网络组建与动态路由配置

【实验目的】

- 1、理解 RIP 动态路由原理。
- 2、练习动态路由配置。
- 3、掌握对路由器有关状态获取和分析的方法。

【实验任务】

- 1、按照拓扑构建一个小型局域网。
- 2、配置 PC 机的 IP 地址及网关。
- 3、配置路由器的各个接口、RIP 路由协议。
- 4、完成连通性和包传输路径基本测试。

建议实验学时：2 学时。

【实验背景】

动态路由协议可以允许网络快速的更新和适应于变化，大多数网络采用动态路由，因为它能使网络自动适应变化。其缺点是会增加网络的开销。在本实验中，将使用 RIP 作为路由选择协议，RIP 设计用于工作在中等大小的局域网中，并不适用于更复杂的环境。

RIP 经过若干年的发展，从一个有类路由选择协议 RIP 版本 1 改进到了无路由选择协议 RIP 版本 2，RIP2 除了具有 RIPV2 的所有功能还具有以下增强特性：支持身份验证、支持无类别子网掩码、使用路由标记、使用 D 类地址 244.0.0.9 组播传送路由选择更新信息。

【实验拓扑与参数配置】

本次实验的拓扑图和参数配置表。（本实验在 packet tracer 4.0 环境下完成）

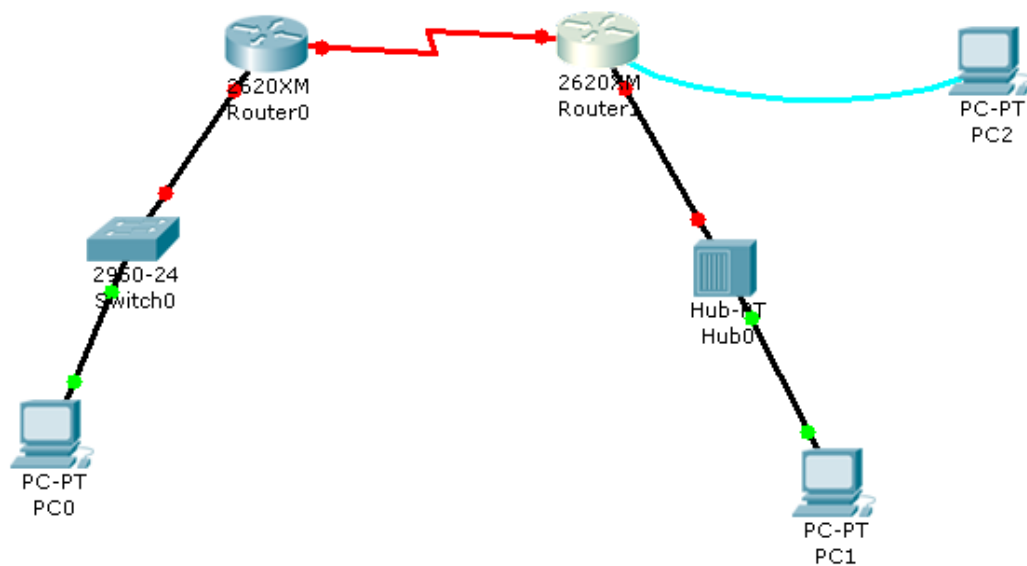


图 7.1 实验的拓扑图

表 7.1 参数配置表

路由器信息（子网掩码均为 255.255.255.0）				
主机名	类型	IP 地址	RIP 路由网络	时钟频率
Router1	2620XM	Fa0/0:192.168.1.1 Ser0/0: 192.168.2.1	192.168.1.0 192.168.2.0	56000
Router2	2620XM	Fa0/0:192.168.3.1 Ser0/0:192.168.2.2	192.168.2.0 192.168. 3.0	
PC 信息（子网掩码均为 255.255.255.0）				
主机名		IP 地址	默认网关	
PC0		192.168.1.2	192.168.1.1	
PC1		192.168.3.3	192.168.3.1	
交换机和 HUB 信息				
主机名		类型		
Hub 0		Hub-PT		
Switch 0		2950-24		

【实验设备】

两台 2620XM 的路由器，三台 PC 机，一台 2950-24 的交换机，一台 HUB-PT 的集线器，DCE/DTE Cable 一条，直通线四条、反转线一条。

【实验步骤】

步骤 1 对路由器进行配置。

步骤 1.1 先进入全局配置模式，执行命令“`erase startup-config`”，清除缓存的配置文件。使用“`reload`”命令重启路由器。

```
Router>enable
```

```
Router#erase startup-config
```

```
Router#reload
```

开始对路由器的名字进行配置。

```
Router>enable
```

```
Router#config terminal
```

```
Router(config)#hostname Router1
```

```
Router(config)#hostname Router2
```

步骤 1.2 接下来进入接口配置模式对路由器的接口进行配置，包括 IP 地址，开启接口，对 DCE 进行时钟设置。

```
Router1 (config)#interface fas0/0
```

```
Router1 (config-if)#ip address 192.168.1.1 255.255.255.0
```

```
Router1 (config-if)#no shutdown
```

```
Router1 (config)#interface serial 0/0
```

```
Router1 (config-if)#ip address 192.168.2.1 255.255.255.0
```

```
Router1 (config-if)#clock rate 5600
```

```
Router1 (config-if)#no shutdown
```

```

Router2 (config)#int ser2/0
Router2 (config-if)#ip address 192.168.2.2 255.255.255.0
Router2 (config-if)#no shutdown
Router2 (config-if)#exit
Router2 (config)#int fas0/0
Router2 (config-if)#ip address 192.168.3.1 255.255.255.0
Router2 (config-if)#no shutdown
Router2 (config-if)#end
Router2 #

```

步骤 2 对各主机按以上拓扑所规定的 IP 地址子网掩码以及缺省网关进行配置。在各主机上可以通过“ping 网关的 IP 地址”即：PC0>ping 192.168.1.1，PC1>ping 192.168.1.2，PC0>ping 192.168.3.2 分别来测试与网关的连通，测试 PC0 和 PC1 之间是否连通，若返回 ping 包信息则连通，若没有则检查它们之间的连接线缆及其接口配置。

步骤 3 路由器的全局模式使用“router rip”进入路由器配置，对各路由器使用“network 端口所在的网络地址”进行 RIP 路由协议配置，使用命令返回到全局模式。

步骤 3.1 对 Router1 进行 RIP 路由配置。

```

Router1 (config)#router rip
Router1 (config-router)#network 192.168.1.0
Router1 (config-router)#network 192.168.2.0
Router1 (config-router)#exit
Router1 (config)#end

```

步骤 3.2 对 Router2 进行 RIP 路由配置。

```

Router2 (config)#router rip
Router2 (config-router)#network 192.168.2.0
Router2 (config-router)#network 192.168.3.0
Router2 (config-router)#end

```

步骤 3.3 使用“copy running-config startup-config”将配置从 running-config 保存到 startup-config。

```

Router2 #copy running-config startup-config
Router1 #copy running-config startup-config

```

然后在各主机上使用 ping 命令从 PC0 与 PC1 进行测试，看看是否是连通的。若没有则检查配置信息。

步骤 4 检查路由器的基本配置。以路由器 Router1 为例，使用“show ip protocol”命令来看一下路由协议是否为 rip 即 Routing protocol is RIP。

```

Router1#show ip protocol
Routing Protocol is "rip"//路由协议为 rip

```

Sending updates every 30 seconds, next due in 24 seconds//路由选择的更新每 30s 广播，下一次更新在 24s 后发生。

Invalid after 180 seconds, hold down 180, flushed after 240//失效定时器的值为 180s，抑制定时器的值为 180s，刷新定时器的值为 240s。

```

Outgoing update filter list for all interfaces is not set

```

Incoming update filter list for all interfaces is not set //所有的接口都没有设置进出路由器的过滤表。

```

Redistributing: rip

```

Default version control: send version 1, receive any version

Interface	Send	Recv	Triggered RIP	Key-chain
FastEthernet0/0	1	2	1	
Serial0/0	1	2	1	

Automatic network summarization is in effect

Maximum path: 4

Routing for Networks:

192.168.1.0

192.168.2.0//路由器可以为去往这两个网络的包提供路由。

Passive Interface(s):

Routing Information Sources:

Gateway	Distance	Last Update
192.168.2.2	120	

Distance: (default is 120)

使用“show ip route”命令来列出路由器直达的以及可到达的网络和端口号。

Router1#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set//缺省网关没有配置

C 192.168.1.0/24 is directly connected, FastEthernet0/0

C 192.168.2.0/24 is directly connected, Serial0/0//这两个网络是直达的

R 192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:23, Serial0/0->192.168.3.0//这个网络是通过 192.168.2.2 这个接口可达的。

步骤 5 观察 RIP 路由的更新。在 ROUTER1 使用“debug ip rip”命令，来观察一下路由器的接口把更新发送给 ROUTER2。

Router1#debug ip rip

RIP protocol debugging is on

ROUTER1#RIP: received v1 update from 192.168.2.2 on Serial0/0

192.168.3.0 in 1 hops ->路由器从接口 192.168.2.2 接收到更新信息：到达 192.168.3.0 网络只需要一跳。

RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (192.168.1.1)//路由器从接口 192.168.1.1 发送更新信息。

RIP: build update entries

network 192.168.2.0 metric 1

network 192.168.3.0 metric 2//路由器到达网络 192.168.2.0 的度量值（跳数）是 1，路由器到达网络 192.168.3.0 的度量值（跳数）是 2。

RIP: sending v1 update to 255.255.255.255 via Serial0/0 (192.168.2.1)

RIP: build update entries

network 192.168.1.0 metric 1

```
ROUTER1#RIP: received v1 update from 192.168.2.2 on Serial0/0
```

```
192.168.3.0 in 1 hops
```

```
RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (192.168.1.1)
```

```
RIP: build update entries
```

```
network 192.168.2.0 metric 1
```

```
network 192.168.3.0 metric 2
```

```
RIP: sending v1 update to 255.255.255.255 via Serial0/0 (192.168.2.1)
```

```
RIP: build update entries
```

```
network 192.168.1.0 metric 1//路由器到达网络 192.168.1.0 的度量值（跳数）是 1。
```

```
Router1#undebg all
```

```
RIP protocol debugging is off
```

```
All possible debugging has been turned off
```

我们还可以练习使用其它的 debug 命令: “debug ip rip events”、“debug ip rip trigger”、“debug ip rip database”.最后如果要关闭当前的 debug 命令, 在其命令之前加 no 如: “no debug ip rip”, 如果要关闭所有的 debug 命令则使用 “undebg all”.

```
Router1#undebg all
```

```
RIP protocol debugging is off
```

```
All possible debugging has been turned off
```

【注意事项】

debug 命令不要使用的太多, 在一个繁忙网络中的实时调试将严重减慢网速, 不要一直打开调试, 在诊断出问题后要及时使用 undebg 命令关闭调试。在 RAM 较小的路由器上过多的调试会造成该路由器的重新启动。

【参考配置】

```
ROUTER1#show running-config
```

```
version 12.2
```

```
hostname ROUTER1
```

```
interface FastEthernet0/0
```

```
ip address 192.168.1.1 255.255.255.0
```

```
duplex auto
```

```
speed auto
```

```
interface Serial0/0
```

```
ip address 192.168.2.1 255.255.255.0
```

```
clock rate 56000
```

```
interface Serial0/1
```

```
no ip address
```

```
shutdown
```

```
interface Serial0/2
```

```
no ip address
```

```
shutdown
```

```
interface Serial0/3
```

```
no ip address
```

```
shutdown
router rip
network 192.168.1.0
network 192.168.2.0
ip classless
line con 0
end
ROUTER2 #show running-config
version 12.2
hostname ROUTER2
interface FastEthernet0/0
ip address 192.168.3.1 255.255.255.0
duplex auto
speed auto
interface FastEthernet1/0
no ip address
duplex auto
speed auto
shutdown
interface Serial0/0
ip address 192.168.2.2 255.255.255.0
interface Serial3/0
no ip address
shutdown
interface FastEthernet4/0
no ip address
shutdown
interface FastEthernet5/0
no ip address
shutdown
router rip
network 192.168.2.0
network 192.168.3.0
ip classless
line con 0
End
```

【实验思考】

- 1、在步骤 2 中主机 PC0 到主机 PC1 能 ping 通吗？在步骤 3 中呢？为什么？
- 2、动态路由如何与静态路由结合使用？
- 3、练习使用本实验中提到的所有 debug 命令，观察其输出结果有什么异同？
- 4、使用 debug 命令如何排错？

实验八 网络访问控制与基本包过滤配置

【实验目的】

通过本实验理解基于 IP 源地址的包过滤原理和应用方法。掌握标准访问控制列表的设计、配置和测试。

【实验任务】

- 1、参照拓扑图建立网络拓扑。
- 2、配置路由器和 PC，确保网络拓扑的连通性。
- 3、配置标准访问控制列表满足应用需求。

建议实验学时：2 学时。

【背景描述】

在本次实验中我们首先组建一个简易的校园网，在此基础上利用标准访问控制列表实施访问控制。扩展包过滤实验和 NAT/PAT 实验做为后续实验仍然使用该拓扑，并在本次实验的基础上不断加强访问控制，最后形成一个基于路由器包过滤和地址转换技术的相对安全的校园网。

本次实验中我们在 Packet Tracer4.0 的仿真环境中实现如下应用需求：教学网段和宿舍网段不能访问行政网段，管理网段中只允许 PC1 访问行政网段，行政网段可以访问 DMZ 中的 WWW、FTP、SMTP 服务器。

实验之前大家应该理解标准访问控制列表的基本特点，工作原理和应用的方法，熟练掌握其基本语法和配置步骤。会使用 Show running-config、Show access-lists 等命令查看访问控制列表是否配置成功、以及在仿真环境中测试是否达到预期结果。

- 标准访问控制列表的基本语法如下：

Access-list access-list-number {deny | permit} source [source-wildcard] [log]

access-list 命令参数的含义如下：

- (1) access-list-number:访问控制列表号,标准访问控制列表的号码范围是 1~99。
- (2) deny:如果满足条件,数据包被拒绝从该入口通过。
- (3) permit:如果满足条件,数据包允许从该入口通过。
- (4) source:数据包的源网络地址,源网络地址可以是具体的地址或 any(任意),如果源地址是单个 IP 地址时,将"source"改成"host",后再写 IP 地址即可。
- (5) Source-wildcard:源地址通配符掩码,可选项。通配符掩码是一个 32 比特位的数字字符串,使用 1 或 0 来表示,它被用"."分成 4 组,每组 8 位。在通配符掩码位中,0 表示"检查相应的位",而 1 表示不检查相应位。通配符掩码相当于子网掩码的反码。

- (6) Log:可选项,生成日志信息,记录匹配 permit 或 deny 语句的包。

可以通过在"access-list"命令前加"no"的形式,来删除一个已经建立的标准 ACL。

- 关键字 any 和 host 的用法

(1)any 指定对允许所有的 IP 地址作为源地址。这样,当某环境下允许访问任何目的地址时,我们就不用输入 source 位为"0.0.0.0",再输入通配符掩码为"255.255.255.255"了,直接使用"any"就可以了。下面两行指令是等价的。

```
access-list 1 permit 0.0.0.0 255.255.255.255
```


access-list 1 permit any

(2)host 用在访问表中指定通配符掩码是 0.0.0.0 这样某环境下要输入单个的地址,如 172.16.8.1,就不用输入 172.16.8.1 和通配符掩码 0.0.0.0 了,直接在地址前加 host 就可以了。

ACL 的使用

在创建了一个访问控制列表并分配了表号之后,为了让该访问控制列表起作用,用户必须把它配置到一个接口上且指明数据流方向。

其语法是: **ip access-group access-list-number {in|out}**

(1) Ip: 定义所用的协议。

(2) access-list-number: 访问控制列表的号码。

(3) in |out: 定义 ACL 是被应用到接口的流入方向(in),还是接口的流出方向(out)。

【实验拓扑和配置参数】

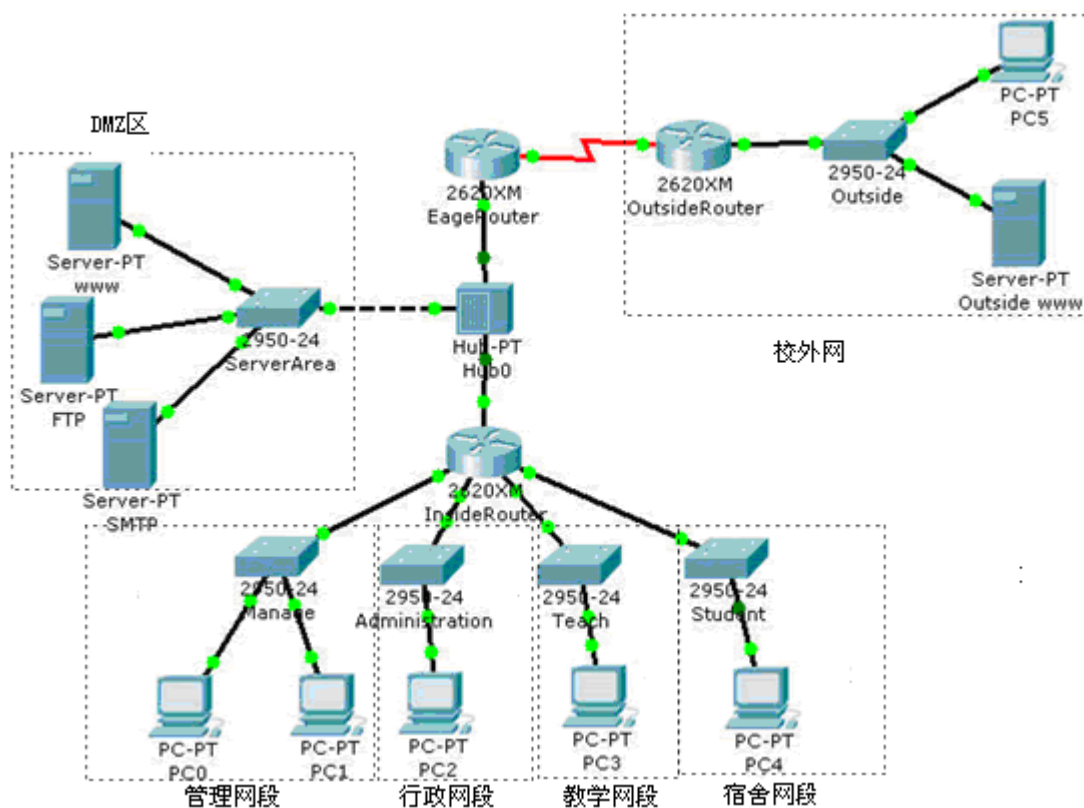


图 8.1 实验拓扑

表 8.1 实验配置参数

路由器配置信息（子网掩码均为 255.255.255.0）				
主机名	类型	IP 地址	RIP 路由网络	时钟频率
InsideRouter	2620XM	Fa0/0: 192.168.1.2	192.168.1.0	
		Eth1/0: 192.168.2.1	192.168.2.0	
		Eth1/1: 192.168.3.1	192.168.3.0	
		Eth1/2: 192.168.4.1	192.168.4.0	
		Eth1/3: 192.168.5.1	192.168.5.0	
EageRouter	2620XM	Fa0/0: 192.168.1.1	192.168.1.0	
		Ser0/0: 218.58.59.91	218.58.59.0	
OutsideRouter	2620XM	Fa0/0: 218.58.100.1	218.58.59.0	9600
		Ser0/0: 218.58.59.90	218.58.100.0	
PC 和 Server 配置信息（子网掩码均为 255.255.255.0）				
主机名		IP 地址	默认网关	所属网段
PC0		192.168.2.2	192.168.2.1	192.168.2.0
PC1		192.168.2.3	192.168.2.1	192.168.2.0
PC2		192.168.3.2	192.168.3.1	192.168.3.0
PC3		192.168.4.2	192.168.4.1	192.168.4.0
PC4		192.168.5.2	192.168.5.1	192.168.5.0
PC5		218.58.100.2	218.58.100.1	218.58.100.0
WWW		192.168.1.3	192.168.1.1	192.168.1.0
FTP		192.168.1.4	192.168.1.1	192.168.1.0
SMTP		192.168.1.5	192.168.1.1	192.168.1.0
Outside WWW		218.58.100.3	218.58.100.1	218.58.100.0
交换机和 Hub 配置信息				
主机名	类型	所属网段	备注	
Manage	2950-24	192.168.2.0	所属校园网管理网段	
Administration	2950-24	192.168.3.0	所属校园网行政网段	
Teach	2950-24	192.168.4.0	所属校园网教学网段	
Student	2950-24	192.168.5.0	所属校园网宿舍网段	
Server Area	2950-24	192.168.1.0	DMZ 区	
Outside	2950-24	218.58.100.0	所属校外网	
Hub 0	Hub-PT	Hub-PT		

【实验设备】

Cisco Router	2620XM	3 台
Catalyst Switch	2950-24	6 台
Hub	Hub-PT	1 台
PC	PC-PT	5 台
Server	Server-PT	4 台

【实验步骤】

步骤 1 建立网络拓扑并确保其连通性

参照拓扑图和配置信息表在 Packet Tracer 中建立网络拓扑、进行配置。测试连通性，确保网络中的任何两个设备间能相互访问（能 Ping 通）。然后保存该拓扑的一个复本，以备后用。

步骤 2 配置标准访问控制列表满足应用需求**步骤 2.1.**

我们在 InsideRouter 上创建标准访问控制列表 access-list 1, 将其应用到 InsideRouter 的 Eth1/1 端口上，配置命令如下：

```
InsideRouter>en
InsideRouter#config t
InsideRouter(config)#access-list 1 permit 192.168.1.0 0.0.0.255
InsideRouter(config)#access-list 1 permit host 192.168.2.3
InsideRouter(config)#exit
InsideRouter#config t
InsideRouter(config)#interface e1/1
InsideRouter(config-if)#ip access-group 1 out
InsideRouter(config-if)#end
```

步骤 2.2 我们查看一下刚刚建立的访问控制列表。

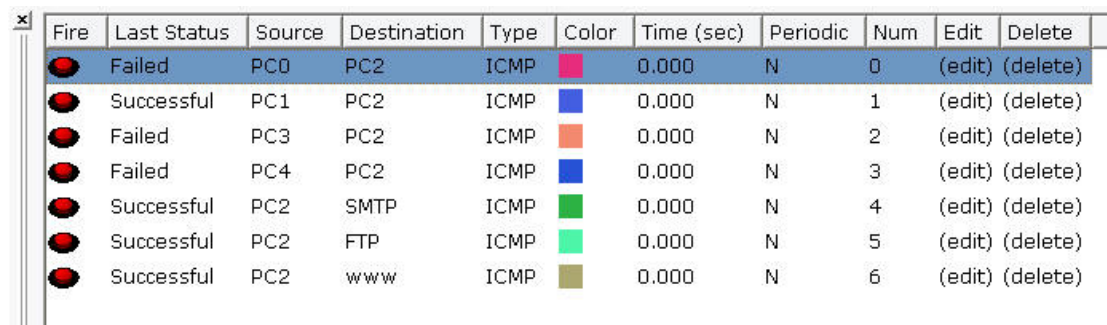
```
InsideRouter#show access-lists
```

会有如下信息：

```
Standard IP access list 1
    permit 192.168.1.0 0.0.0.255
    permit host 192.168.2.3
```

显示信息表明访问控制列表已建立，接下来我们进行测试。

点击“Toggle PDU List Window”使其显示在 Workspace 的下方，然后添加多个 Simple PDU 进行测试。结果如图 8.2 所示：



Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete
	Failed	PC0	PC2	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC1	PC2	ICMP		0.000	N	1	(edit)	(delete)
	Failed	PC3	PC2	ICMP		0.000	N	2	(edit)	(delete)
	Failed	PC4	PC2	ICMP		0.000	N	3	(edit)	(delete)
	Successful	PC2	SMTP	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC2	FTP	ICMP		0.000	N	5	(edit)	(delete)
	Successful	PC2	www	ICMP		0.000	N	6	(edit)	(delete)

图 8.2 标准访问控制列表测试结果

步骤 2.3 实验结果分析

0 号 PDU 的 Failed 状态和 1 号 PDU 的 Successful 状态说明管理网段中只有 PC1 访问行政网段。2 号 PDU 和 3 号 PDU 的 Failed 状态说明教学网段和宿舍网段不能访问行政网段。4 号、5 号和 6 号 PDU 的 Successful 状态说明行政网段可以访问 DMZ 中的 WWW、FTP、SMTP 服务器。

在这个实验中我们暂时不考虑对外网的访问控制，这部分内容我们将在以后的实验中

逐步完善。

【注意事项】

- 1、使用 Packet Tracer 4.0 进行连通性测试时，有时候在理论上连通的路径上添加第一个 Simple PDU 时其 Last Status 显示 Failed，等添加第二个或第三个 Simple PDU 时便可显示正确的 Last Status。
- 2、每一个访问控制列表最后一项都有一个默认的 deny any 语句。因此如果其他的控制语句都是 deny ×××最后一定不要忘记添加 permit any。
- 3、数据包一旦匹配控制语句中的某一条则不会继续匹配之后的控制语句，因此控制语句的顺序对实验的结果有直接的影响，请注意。
- 4、将本次实验的正确配置保存一个副本，以备后用。

【参考配置】

```
OutsideRouter#show run
version 12.2
hostname OutsideRouter
interface FastEthernet0/0
 ip address 218.58.100.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0
 ip address 218.58.59.90 255.255.255.0
 clock rate 9600
interface Serial0/1
 no ip address
 shutdown
router rip
 network 218.58.59.0
 network 218.58.100.0
 ip classless
 line con 0
end
EageRouter#show run
version 12.2
hostname EageRouter
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
interface Serial0/0
 ip address 218.58.59.91 255.255.255.0
interface Serial0/1
 no ip address
```

```
shutdown
interface FastEthernet1/0
  no ip address
  shutdown!
router rip
  network 192.168.1.0
  network 218.58.59.0
ip classless
line con 0
end
InsideRouter#show run
version 12.2
hostname InsideRouter
interface FastEthernet0/0
  ip address 192.168.1.2 255.255.255.0
  duplex auto
  speed auto
interface Ethernet1/0
  ip address 192.168.2.1 255.255.255.0
  duplex auto
  speed auto
interface Ethernet1/1
  ip address 192.168.3.1 255.255.255.0
  ip access-group 1 out
  duplex auto
  speed auto
interface Ethernet1/2
  ip address 192.168.4.1 255.255.255.0
  duplex auto
  speed auto
interface Ethernet1/3
  ip address 192.168.5.1 255.255.255.0
  duplex auto
  speed auto
router rip
  network 192.168.1.0
  network 192.168.2.0
  network 192.168.3.0
  network 192.168.4.0
  network 192.168.5.0
ip classless
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit host 192.168.2.3
line con 0
```

end

【实验思考】

- 1、解释一下在 Step2.1 中为什么 PC1 到 PC4 的 Simple PDU 的 Last Status 是 Failed?
- 2、标准访问控制列表依据什么实现访问控制的，有什么样的优点和不足？
- 3、标准访问控制列表的配置一般包括哪几步？
- 4、标准访问控制列表有什么样的应用原则？

实验九 网络访问控制与扩展包过滤配置

【实验目的】

通过本实验理解基于 IP 地址、协议和端口的包过滤原理和应用方法,掌握扩展访问控制列表的设计、配置和测试。

【实验任务】

在实验八的基础上,配置扩展访问控制列表满足应用需求。

建议实验学时:4 学时。

【实验背景】

在基本包过滤的实验中我们在一个简易的校园网拓扑上通过配置标准访问控制列表,加强了对行政网段的访问控制。在本节的实验中我们继续通过配置扩展访问控制列表加强对 DMZ 区和内外网之间的访问控制。

本次实验中我们有如下的应用需求:

禁止宿舍网段和校外网访问 FTP 服务器上。

外网可以访问 www 服务器和 SMTP 服务器。

所有的计算机都可以访问外网中 outside www 服务器。

实验之前大家应该理解扩展访问控制列表的基本特点,工作原理和应用的原则,熟练掌握其基本语法和配置步骤。会使用 Show running-config、Show access-lists 等命令查看访问控制列表是否配置成功,以及在仿真环境中测试是否达到预期结果。

- 扩展访问控制列表的语法

扩展 ACL 也是在全局配置模式下进行设计的,其命令"access-list"的语法格式为:

```
access-list access-list-number {deny|permit} protocol source[source-wildmask] destination
[destination-wildmask] [operator operand] [established]
```

命令参数的含义如下:

- (1) access-list-number: 访问控制列表号,范围为 100-199。
- (2) deny: 如果满足条件,数据包被拒绝通过。
- (3) permit: 如果满足条件,数据包允许通过。
- (4) protocol: 指定协议类型,如 IP/TCP/UDP/ICMP 等。
- (5) source: 源地址。
- (6) destination: 目的地址。
- (7) source-mask: 源通配符掩码。
- (8) destination-mask: 目的通配符掩码。
- (9) operator operand: 可为 <|>|=|<|>|,分别表示"小于|大于|等于|不等于"端口号。
- (10) established: 可选项,表示连接的状态。

- 协议及协议的端口号

可以使用扩展 ACL 来做到针对协议及其参数的更精细的包过滤,如 TCP,UDP,ICMP 和 IP。在扩展 ACL 中,要指定上层 TCP 或 UDP 端口号,从而选择允许或拒绝的协议。常见的端口号及其对应协议为: FTP 20/21; Telnet 23; SMTP 25; TFTP 69; DNS 53; Http 80 等。

扩展 ACL 的 IP 地址和通配符掩码的使用,同标准 ACL,此处不再详述。

【实验拓扑和配置参数表】

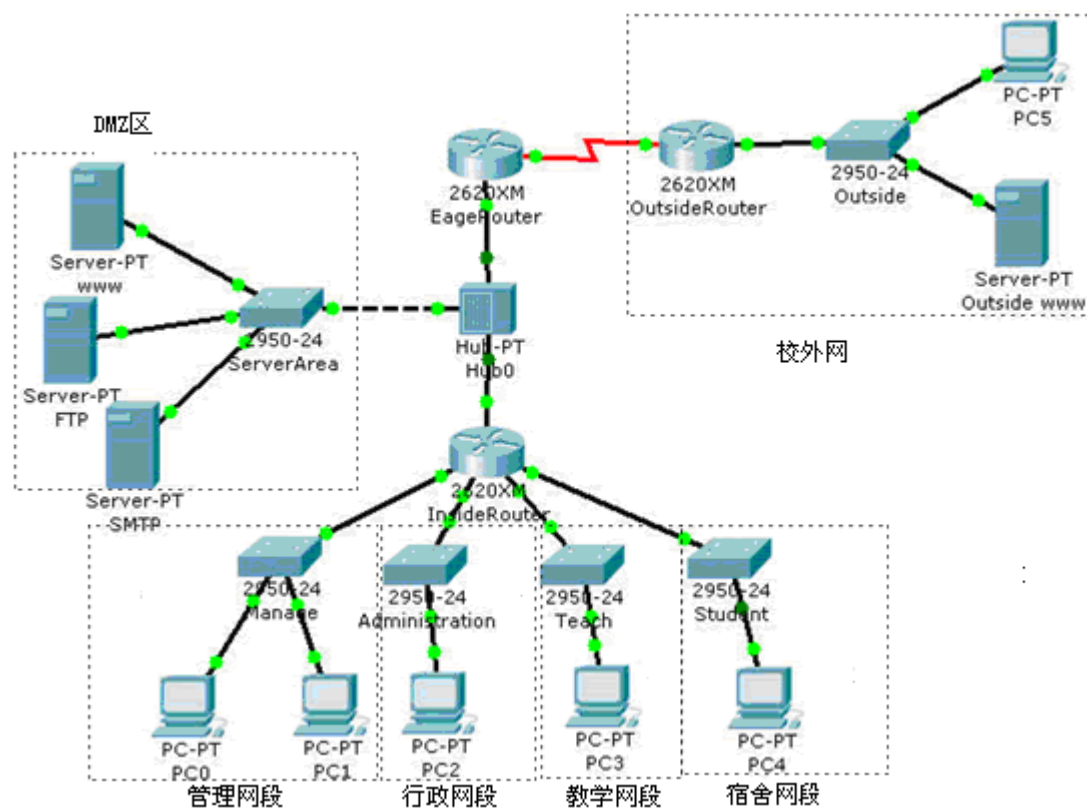


图 9.1 实验拓扑

表 9.1 实验配置参数

路由器配置信息（子网掩码均为 255.255.255.0）				
主机名	类型	IP 地址	RIP 路由网络	时钟频率
InsideRouter	2620XM	Fa0/0: 192.168.1.2 Eth1/0: 192.168.2.1 Eth1/1: 192.168.3.1 Eth1/2: 192.168.4.1 Eth1/3: 192.168.5.1	192.168.1.0 192.168.2.0 192.168.3.0 192.168.4.0 192.168.5.0	
EageRouter	2620XM	Fa0/0: 192.168.1.1 Ser0/0: 218.58.59.91	192.168.1.0 218.58.59.0	
OutsideRouter	2620XM	Fa0/0: 218.58.100.1 Ser0/0: 218.58.59.90	218.58.59.0 218.58.100.0	9600
PC 和 Server 配置信息（子网掩码均为 255.255.255.0）				
主机名		IP 地址	默认网关	所属网段
PC0		192.168.2.2	192.168.2.1	192.168.2.0
PC1		192.168.2.3	192.168.2.1	192.168.2.0
PC2		192.168.3.2	192.168.3.1	192.168.3.0
PC3		192.168.4.2	192.168.4.1	192.168.4.0
PC4		192.168.5.2	192.168.5.1	192.168.5.0
PC5		218.58.100.2	218.58.100.1	218.58.100.0
WWW		192.168.1.3	192.168.1.1	192.168.1.0
FTP		192.168.1.4	192.168.1.1	192.168.1.0
SMTP		192.168.1.5	192.168.1.1	192.168.1.0
Outside WWW		218.58.100.3	218.58.100.1	218.58.100.0
交换机和 Hub 配置信息				
主机名	类型	所属网段	备注	
Manage	2950-24	192.168.2.0	所属校园网管理网段	
Administration	2950-24	192.168.3.0	所属校园网行政网段	
Teach	2950-24	192.168.4.0	所属校园网教学网段	
Student	2950-24	192.168.5.0	所属校园网宿舍网段	
Server Area	2950-24	192.168.1.0	DMZ 区	
Outside	2950-24	218.58.100.0	所属校外网	
Hub 0	Hub-PT	Hub-PT		

【实验设备】

Cisco Router	2620XM	3 台
Catalyst Switch	2950-24	6 台
Hub	Hub-PT	1 台
PC	PC-PT	5 台
Server	Server-PT	4 台

【实验步骤】

我们利用上节实验最后保存的拓扑和配置信息，实验步骤如下：

步骤 1

步骤 1.1 首先我们配置扩展访问控制列表满足禁止宿舍网段访问 FTP 服务器上的 ftp 资源的应用需求。

我们创建扩展访问控制列表 access-list 100，将其应用到 InsideRouter 的 Fa0/0 端口上。

```
InsideRouter#config t
```

```
InsideRouter(config)# access-list 100 deny tcp 192.168.5.0 0.0.0.255 host 192.168.1.4 eq 21
```

```
InsideRouter(config)# access-list 100 permit ip any any
```

```
InsideRouter(config)#exit
```

```
InsideRouter#config t
```

```
InsideRouter(config)#interface fa0/0
```

```
InsideRouter(config-if)#ip access-group 100 out
```

步骤 1.2 下面我们查看一下刚刚建立的访问控制列表

```
InsideRouter#show ip access-lists
```

```
Standard IP access list 1
```

```
    permit 192.168.1.0 0.0.0.255
```

```
    permit host 192.168.2.3
```

```
Extended IP access list 100
```

```
    deny tcp 192.168.5.0 0.0.0.255 host 192.168.1.4 eq 21
```

```
    permit ip any any
```

显示信息表明访问控制列表已建立，接下来我们进行测试。

点击“Toggle PDU List Window”使其显示在 Workspace 的下方，然后添加多个 Complex PDU 进行测试。

添加 Complex PDU 时 Select Application 根据数据包的类型做出相应的选择，Source Port 可以设置为 1024~65536 的任意值，其他内容使用默认值。各个 Complex PDU 设置如下：

Create Complex PDU

Source Settings

Source Device: PC4

Outgoing Port: FastEthernet ☒ Auto Select Port

PDU Settings

Select Application: FTP

Destination IP Address: 192.168.1.4

TTL: 32

Source Port: 1026

Destination Port: 21

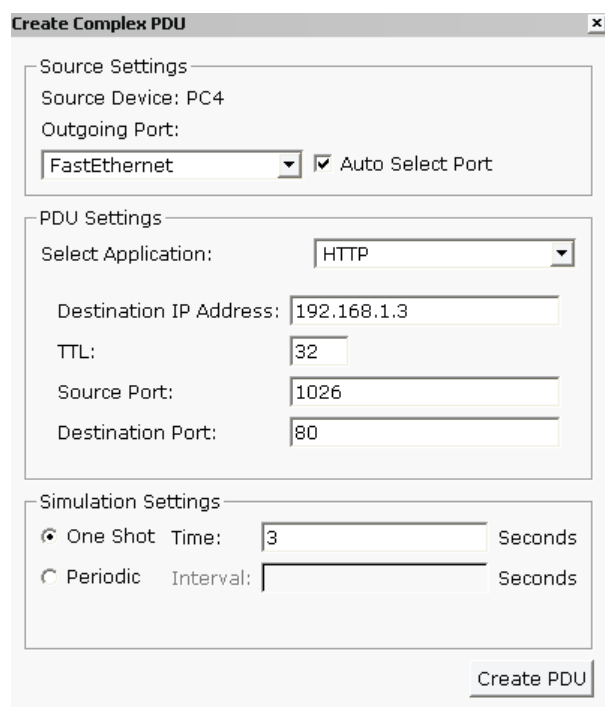
Simulation Settings

☒ One Shot Time: 3 Seconds

☐ Periodic Interval: Seconds

Create PDU

图 9.2 PC4 到 FTP 服务器的 FTP PDU 设置

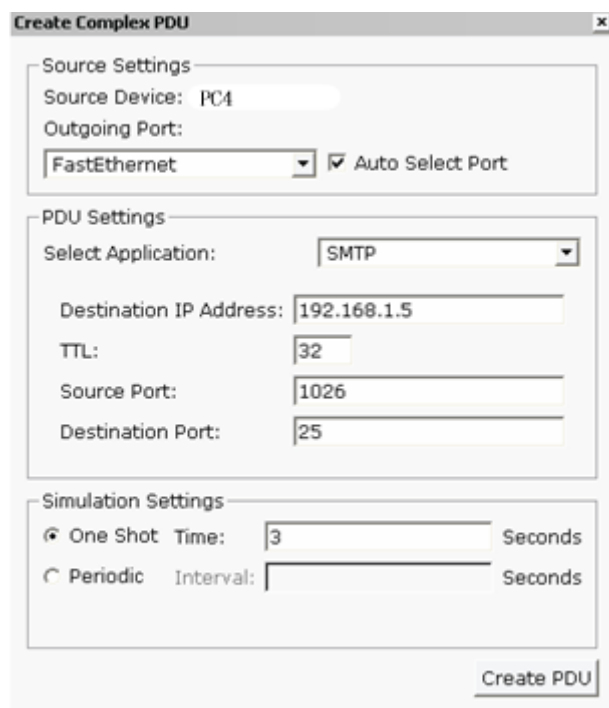


The 'Create Complex PDU' dialog box is shown with the following settings:

- Source Settings:**
 - Source Device: PC4
 - Outgoing Port: FastEthernet (dropdown menu)
 - ☒ Auto Select Port
- PDU Settings:**
 - Select Application: HTTP (dropdown menu)
 - Destination IP Address: 192.168.1.3
 - TTL: 32
 - Source Port: 1026
 - Destination Port: 80
- Simulation Settings:**
 - ☒ One Shot Time: 3 Seconds
 - ☐ Periodic Interval: (empty field) Seconds

At the bottom right is a 'Create PDU' button.

图 9.3 PC4 到 HTTP 服务器的 HTTP PDU 设置



The 'Create Complex PDU' dialog box is shown with the following settings:

- Source Settings:**
 - Source Device: PC4
 - Outgoing Port: FastEthernet (dropdown menu)
 - ☒ Auto Select Port
- PDU Settings:**
 - Select Application: SMTP (dropdown menu)
 - Destination IP Address: 192.168.1.5
 - TTL: 32
 - Source Port: 1026
 - Destination Port: 25
- Simulation Settings:**
 - ☒ One Shot Time: 3 Seconds
 - ☐ Periodic Interval: (empty field) Seconds

At the bottom right is a 'Create PDU' button.

图 9.4 PC4 到 SMTP 服务器的 SMTP PDU 设置

结果如下图所示:

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete
	Failed	PC4	192.168.1.4	TCP		3.000	N	0	(edit)	(delete)
	Successful	PC4	192.168.1.3	TCP		3.000	N	1	(edit)	(delete)
	Successful	PC4	192.168.1.5	TCP		3.000	N	2	(edit)	(delete)

图 9.5 扩展访问控制列表测试结果

步骤 1.3 实验结果分析

0 号 PDU Failed 状态说明宿舍网段无法访问 FTP 服务器。

1 号 PDU Successful 状态说明宿舍网段可以访问 WWW 服务器。

2 号 PDU Successful 状态说明宿舍网段可以访问 FTP 服务器。

步骤 2

步骤 2.1 我们创建扩展访问控制列表 access-list 101，将其应用到 EageRouter 的 Fa0/0 端口上，以满足其他的应用需求。

```
EageRouter#config t
```

```
EageRouter(config)#ip access-list extend 101
```

```
EageRouter(config)#access-list 101 deny tcp 218.58.100.0 0.0.0.255 host 192.168.1.4 eq 21
```

```
EageRouter(config)#access-list 101 permit tcp 218.58.100.0 0.0.0.255 host 192.168.1.3 eq 80
```

```
EageRouter(config)#access-list 101 permit tcp 218.58.100.0 0.0.0.255 host 192.168.1.5 eq 25
```

```
EageRouter(config)#access-list 101 permit tcp host 218.58.100.3 eq 80 any
```

```
EageRouter(config)#exit
```

```
EageRouter#config t
```

```
EageRouter(config)#interface fa0/0
```

```
EageRouter(config-if)#ip access-group 101 out
```

```
EageRouter(config-if)#end
```

步骤 2.2 下面我们查看一下刚刚建立的访问控制列表

```
EageRouter#show access-lists
```

```
Extended IP access list 101
```

```
deny tcp 218.58.100.0 0.0.0.255 host 192.168.1.4 eq 21
```

```
permit tcp 218.58.100.0 0.0.0.255 host 192.168.1.3 eq 80
```

```
permit tcp 218.58.100.0 0.0.0.255 host 192.168.1.5 eq 25
```

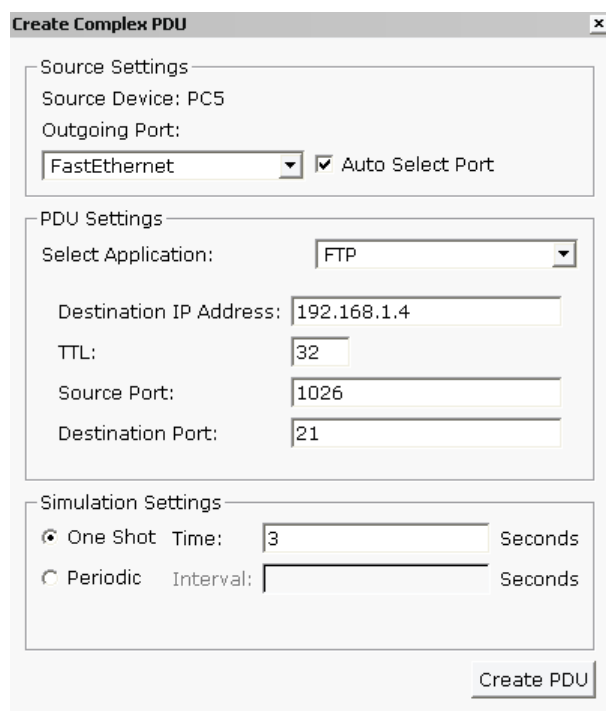
```
permit tcp host 218.58.100.3 eq 80 any
```

```
permit ip 192.168.0.0 0.0.255.255 any
```

显示信息表明访问控制列表已建立，接下来我们进行测试。

点击“Toggle PDU List Window”使其显示在 Workspace 的下方，然后添加多个 Complex PDU 进行测试。

添加 Complex PDU 时 Select Application 根据数据包的类型做出相应的选择，Source Port 可以设置为 1024~65536 的任意值，其他内容使用默认值。各个 Complex PDU 设置如下：

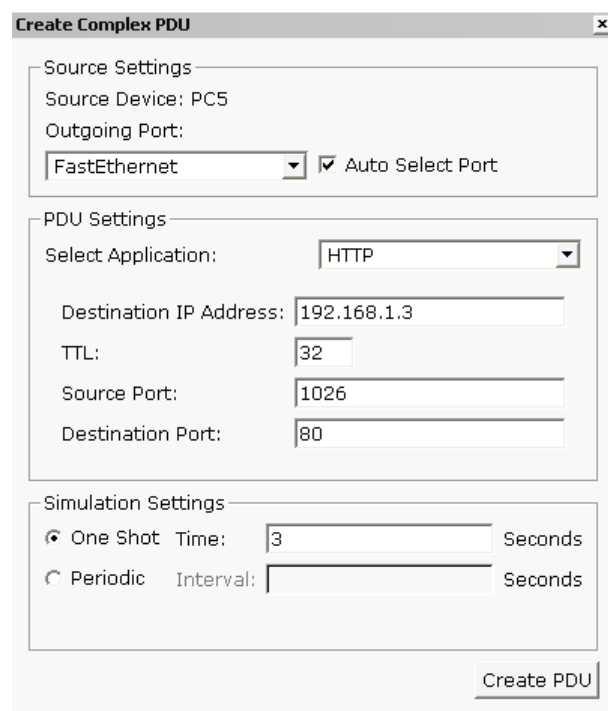


The 'Create Complex PDU' dialog box is shown with the following settings:

- Source Settings:**
 - Source Device: PC5
 - Outgoing Port: FastEthernet (dropdown menu)
 - ☒ Auto Select Port
- PDU Settings:**
 - Select Application: FTP (dropdown menu)
 - Destination IP Address: 192.168.1.4
 - TTL: 32
 - Source Port: 1026
 - Destination Port: 21
- Simulation Settings:**
 - ☒ One Shot Time: 3 Seconds
 - ☐ Periodic Interval: (empty field) Seconds

At the bottom right is a 'Create PDU' button.

图 9.6 PC5 到 FTP 服务器的 FTP PDU 设置

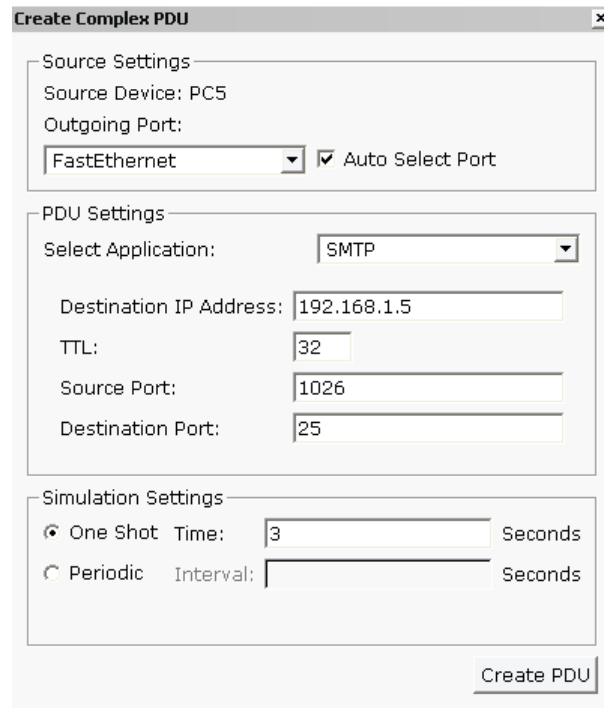


The 'Create Complex PDU' dialog box is shown with the following settings:

- Source Settings:**
 - Source Device: PC5
 - Outgoing Port: FastEthernet (dropdown menu)
 - ☒ Auto Select Port
- PDU Settings:**
 - Select Application: HTTP (dropdown menu)
 - Destination IP Address: 192.168.1.3
 - TTL: 32
 - Source Port: 1026
 - Destination Port: 80
- Simulation Settings:**
 - ☒ One Shot Time: 3 Seconds
 - ☐ Periodic Interval: (empty field) Seconds

At the bottom right is a 'Create PDU' button.

图 9.7 PC5 到内网 WWW 服务器的 HTTP PDU 设置

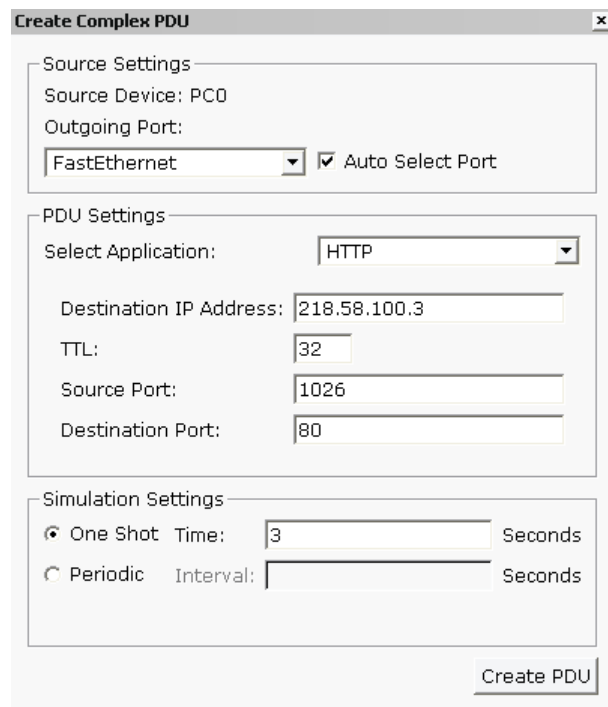


The 'Create Complex PDU' dialog box is shown with the following settings:

- Source Settings:**
 - Source Device: PC5
 - Outgoing Port: FastEthernet (dropdown menu)
 - ☒ Auto Select Port
- PDU Settings:**
 - Select Application: SMTP (dropdown menu)
 - Destination IP Address: 192.168.1.5
 - TTL: 32
 - Source Port: 1026
 - Destination Port: 25
- Simulation Settings:**
 - ☒ One Shot Time: 3 Seconds
 - ☐ Periodic Interval: (empty field) Seconds

At the bottom right is a 'Create PDU' button.

图 9.8 PC5 到 SMTP 服务器的 SMTP PDU 设置



The 'Create Complex PDU' dialog box is shown with the following settings:

- Source Settings:**
 - Source Device: PC0
 - Outgoing Port: FastEthernet (dropdown menu)
 - ☒ Auto Select Port
- PDU Settings:**
 - Select Application: HTTP (dropdown menu)
 - Destination IP Address: 218.58.100.3
 - TTL: 32
 - Source Port: 1026
 - Destination Port: 80
- Simulation Settings:**
 - ☒ One Shot Time: 3 Seconds
 - ☐ Periodic Interval: (empty field) Seconds

At the bottom right is a 'Create PDU' button.

图 9.9 PC0 到 Outside WWW 服务器的 HTTP PDU 设置

PC1、PC2、PC3、PC4 到 Outside WWW 服务器的 Complex PDU 设置和 PC0 到 Outside WWW 服务器的 Complex PDU 设置一样，在此不再重复。

测试结果如下图所示：

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete	
	Failed	PC5	192.168.1.4	TCP		3.000	N	0	(edit)	(delete)	
	Successful	PC5	192.168.1.3	TCP		3.000	N	1	(edit)	(delete)	
	Successful	PC5	192.168.1.5	TCP		3.000	N	2	(edit)	(delete)	
	Successful	PC0	218.58.100.3	TCP		3.000	N	3	(edit)	(delete)	
	Successful	PC4	218.58.100.3	TCP		3.000	N	4	(edit)	(delete)	
	Successful	PC2	218.58.100.3	TCP		3.000	N	5	(edit)	(delete)	
	Successful	PC1	218.58.100.3	TCP		3.000	N	6	(edit)	(delete)	
	Successful	PC3	218.58.100.3	TCP		3.000	N	7	(edit)	(delete)	

图 9.10 扩展访问控制列表测试结果 2

步骤 2.3 实验结果分析

0 号 PDU 的 Failed 状态说明外网不能访问内网的 FTP 服务器。

1 号 PDU 的 Successful 状态说明外网能访问内网的 WWW 服务器。

2 号 PDU 的 Successful 状态说明外网能访问内网的 SMTP 服务器。

3 号 PDU 的 Successful 状态说明管理网段能访问外网的 Outside WWW 服务器。

4 号 PDU 的 Successful 状态说明行政网段能访问外网的 Outside WWW 服务器。

5 号 PDU 的 Successful 状态说明教学网段能访问外网的 Outside WWW 服务器。

6 号 PDU 的 Successful 状态说明宿舍网段能访问外网的 Outside WWW 服务器。

至此应用需求已经全部满足实验结束。

【注意事项】

在测试的过程中，仍然会出现第一次测试不成功，第二次测试成功的现象，实验中要注意，不要为此得出错误的结论。

在 Simulation 模式下跟踪数据包时，数据包到达目的地时可能显示一个闪烁的 X，但是 PDU List Window 中 Last status 却是 successful。我们可以点击带闪烁的 PDU，在 PDU Information —— OSI model 选项卡中我们点击 next layer 或者 previous layer 我们可以找到出现 X 的原因，这仍然不能否定我们正确的设置了访问控制列表，并且它起到了预期的结果。

【参考配置】

```

InsideRouter#show run
version 12.2
hostname InsideRouter
interface FastEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 ip access-group 100 out
 duplex auto
 speed auto
interface Ethernet1/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
interface Ethernet1/1
 ip address 192.168.3.1 255.255.255.0

```

```
ip access-group 1 out
duplex auto
speed auto
interface Ethernet1/2
ip address 192.168.4.1 255.255.255.0
duplex auto
speed auto
interface Ethernet1/3
ip address 192.168.5.1 255.255.255.0
duplex auto
speed auto
router rip
network 192.168.1.0
network 192.168.2.0
network 192.168.3.0
network 192.168.4.0
network 192.168.5.0
ip classless
access-list 1 deny 192.168.5.0 0.0.0.255
access-list 1 deny 192.168.4.0 0.0.0.255
access-list 1 permit host 192.168.2.3
access-list 1 deny 192.168.2.0 0.0.0.255
access-list 1 permit any
access-list 100 deny tcp 192.168.5.0 0.0.0.255 host 192.168.1.4 eq 21
access-list 100 permit ip any any
line con 0
end
EageRouter#show run
version 12.2
hostname EageRouter
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip access-group 101 out
duplex auto
speed auto
interface Serial0/0
ip address 218.58.59.91 255.255.255.0
interface Serial0/1
no ip address
shutdown
interface FastEthernet1/0
no ip address
shutdown
router rip
```



```
network 192.168.1.0
network 218.58.59.0
ip classless
access-list 101 deny tcp 218.58.100.0 0.0.0.255 host 192.168.1.4 eq 21
access-list 101 permit tcp 218.58.100.0 0.0.0.255 host 192.168.1.3 eq 80
access-list 101 permit tcp 218.58.100.0 0.0.0.255 host 192.168.1.5 eq 25
access-list 101 permit tcp host 218.58.100.3 eq 80 any
line con 0
end
```

【实验思考】

- 1、思考扩展访问控制列表的进行访问控制的依据有那些？
- 2、有人说在同一个 Router 上同一个端口的同一个方向上不能绑定多个访问控制列表，在同一个 Router 上同一个端口的两个不同方向（inside、outside）能分别绑定一个访问控制列表，这个说法对吗？请做实验验证。
- 3、扩展访问控制列表的配置一般包括哪几步？
- 4、扩展访问控制列表有什么样的应用原则？

实验十 内外网结构下的网络地址转换（NAT/PAT）

【实验目的】

通过本实验理解网络地址转换的原理和技术，掌握扩展 NAT/PAT 设计、配置和测试。

【实验任务】

- 1、配置静态网络地址转换并完成相应的测试。
 - 2、配置动态网络地址转换并完成相应的测试。
 - 3、配置端口地址转换（PAT）并完成相应的测试。
- 建议实验学时：4 学时。

【实验背景】

本次实验在前两次实验的基础上，利用 NAT 和 PAT 技术实现私有地址和公有地址的相互转换，进一步增强校园网的安全性。另外 NAT 和 PAT 也是解决 IP 地址不足的一个有效方法。

本次实验中我们有如下的应用需求：

- 1、将 192.168.1.3 静态 NAT 到 218.58.59.93。
- 2、将 192.168.1.5 静态 NAT 到 218.58.59.94。
- 3、将管理网段、行政网段的内部私有 IP 动态 NAT 到 218.58.59.95 和 218.58.59.96。
- 4、将教学网段、宿舍网段的内部私有 IP 动态 PAT 到 218.58.59.97。

学生在实验之前要理解网络地址转换的原理。会使用 Show running-config、Show ip nat translation 等命令查看访问控制列表是否配置成功，以及在仿真环境中测试是否达到预期结果。

● 静态 NAT 的配置。

- 1、Router (config) #ip nat inside source static local-ip global -ip

参数说明：

local-ip：内部本地地址。被转换的地址。

global-ip：内部全球地址。用来转换内部本地地址的地址。

- 2、指定内外部接口，命令格式如下：

Router (config) #interface type slot#/port#

Router (config-if) #ip nat inside

Router (config) #interface type slot#/port#

Router (config-if) #ip nat outside

● 动态 NAT 的配置。

- 1、定义一个可以根据需要进行分配的全球地址池。

Router (config) #ip nat pool name start-ip end-ip {netmask netmask| prefix-length prefix-length}

参数说明：

name：地址池名称。

start-ip：地址池中地址范围的起始 IP 地址。

end-ip：地址池中地址范围的结束 IP 地址。

netmask：网络掩码。

prefix-length：网络掩码中有多少位是 1，规定地址池所属的网络的网络掩码。

- 2、定义一个标准访问控制列表。

Router(config) #access-list access-list-number permit source [source-wildcard]

3、建立动态地址转换，它引用 2 中定义的访问控制列表。

```
Router(config)#ip nat inside source list { access-list-number |name} pool name
```

4、指定内外部接口，命令格式如下：

```
Router (config) #interface type number
```

```
Router (config-if) #ip nat inside
```

```
Router (config) #interface type number
```

```
Router (config-if) #ip nat outside
```

- PAT 的配置。

1、Router (config) #ip nat inside source static local-ip global -ip overload

2、指定内外部接口，命令格式如下：

```
Router (config) #interface type number
```

```
Router (config-if) #ip nat inside
```

```
Router (config) #interface type number
```

```
Router (config-if) #ip nat outside
```

- 内部地址和外部地址的说明。

对于网络地址转换的理解核心在于搞清楚 NAT 术语中所提到的四个地址。

inside local(内部本地地址): 在自有网络中（归自己管理，进行 IP 规划的网络）分配给私有主机的地址，一般情况下该地址是 RFC1918 中定义的私有地址。

inside global(内部全局地址): 私有主机使用的非自有网络的地址，通常情况下 inside global 地址是从合法的全球统一可寻址空间中分配的地址，也就是通常所说的公有 IP。

outside local(外部本地地址): 非私有主机在自有网络内表现出来的 IP 地址。该地址是自有网络的管理员为本网络以外的设备所准备的用于在自有网络内使用的 IP 地址。outside local 地址的特点是只会出现在自有网络内但是是供给非私有主机使用的。

outside global(外部全局地址): 非私有主机在自有网络以外的区域使用的 IP 地址，是非私有主机所在网络的管理员负责管理其分配的。outside global 地址的特点是不会出现在自有网络中而且不是给私有主机使用，不归自有网络的管理员负责。

【实验拓扑和配置参数】

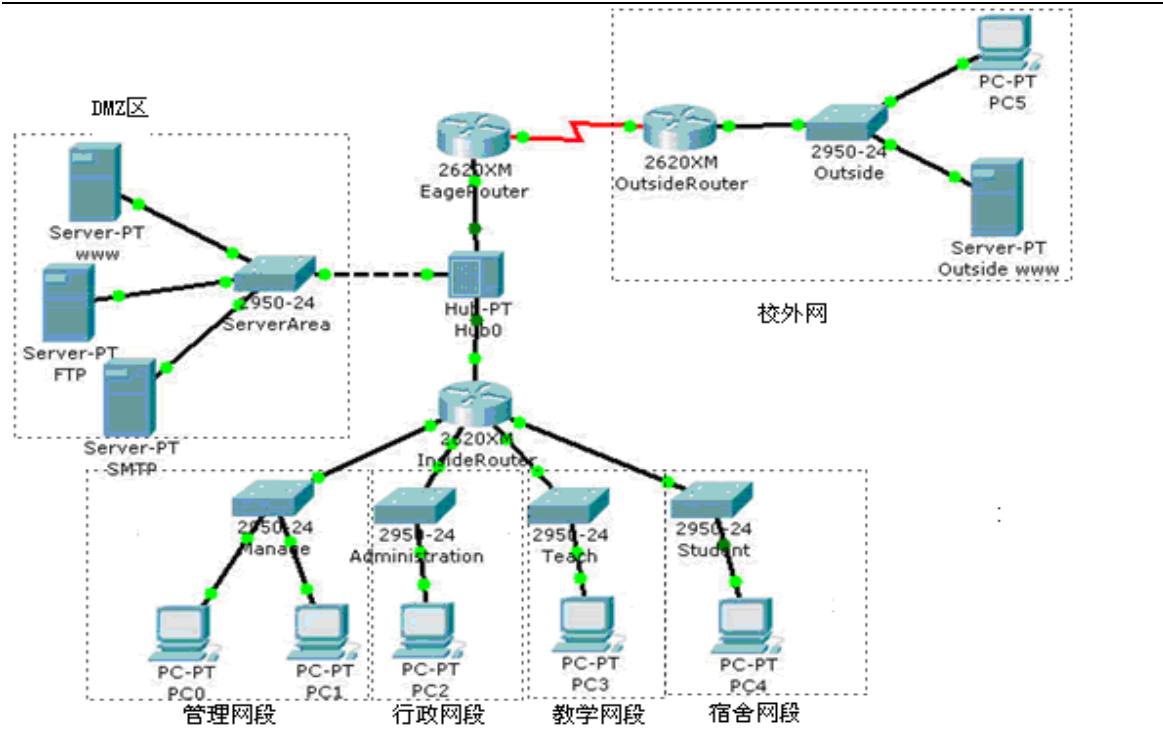


图 10.1 实验拓扑
表 10.1 实验配置参数

路由器配置信息（子网掩码均为 255.255.255.0）				
主机名	类型	IP 地址	RIP 路由网络	时钟频率
InsideRouter	2620XM	Fa0/0: 192.168.1.2	192.168.1.0	
		Eth1/0: 192.168.2.1	192.168.2.0	
		Eth1/1: 192.168.3.1	192.168.3.0	
		Eth1/2: 192.168.4.1	192.168.4.0	
		Eth1/3: 192.168.5.1	192.168.5.0	
EageRouter	2620XM	Fa0/0: 192.168.1.1	192.168.1.0	
		Ser0/0: 218.58.59.91	218.58.59.0	
OutsideRouter	2620XM	Fa0/0: 218.58.100.1	218.58.59.0	9600
		Ser0/0: 218.58.59.90	218.58.100.0	
PC 和 Server 配置信息（子网掩码均为 255.255.255.0）				
主机名		IP 地址	默认网关	所属网段
PC0		192.168.2.2	192.168.2.1	192.168.2.0
PC1		192.168.2.3	192.168.2.1	192.168.2.0
PC2		192.168.3.2	192.168.3.1	192.168.3.0
PC3		192.168.4.2	192.168.4.1	192.168.4.0
PC4		192.168.5.2	192.168.5.1	192.168.5.0
PC5		218.58.100.2	218.58.100.1	218.58.100.0
WWW		192.168.1.3	192.168.1.1	192.168.1.0
FTP		192.168.1.4	192.168.1.1	192.168.1.0
SMTP		192.168.1.5	192.168.1.1	192.168.1.0
Outside WWW		218.58.100.3	218.58.100.1	218.58.100.0
交换机和 Hub 配置信息				

主机名	类型	所属网段	备注
Manage	2950-24	192.168.2.0	所属校园网管理网段
Administration	2950-24	192.168.3.0	所属校园网行政网段
Teach	2950-24	192.168.4.0	所属校园网教学网段
Student	2950-24	192.168.5.0	所属校园网宿舍网段
Server Area	2950-24	192.168.1.0	DMZ 区
Outside	2950-24	218.58.100.0	所属校外网
Hub 0	Hub-PT	Hub-PT	

【实验设备】

Cisco Router	2620XM	3 台
Catalyst Switch	2950-24	6 台
Hub	Hub-PT	1 台
PC	PC-PT	5 台
Server	Server-PT	4 台

【实验步骤】

步骤 1

步骤 1.1 我们首先将 192.168.1.3 静态转换到 218.58.59.93，配置过程如下：

```
EageRouter#config t
EageRouter(config)#ip nat inside source static 192.168.1.3 218.58.59.93
EageRouter(config)#interface fa0/0
EageRouter(config-if)#ip nat inside
EageRouter(config-if)#interface s0/0
EageRouter(config-if)#ip nat outside
EageRouter(config-if)#end
```

步骤 1.2 我们来查看一下刚才的配置。

```
EageRouter#show ip nat translations
Pro  Inside global    Inside local    Outside local    Outside global
---  218.58.59.93       192.168.1.3    ---              ---
```

以上显示信息说明配置已建立。

接下来我们进行测试，添加一个由 PC5 到 218.58.59.93 的 Complex PDU 格式如图 10.2:

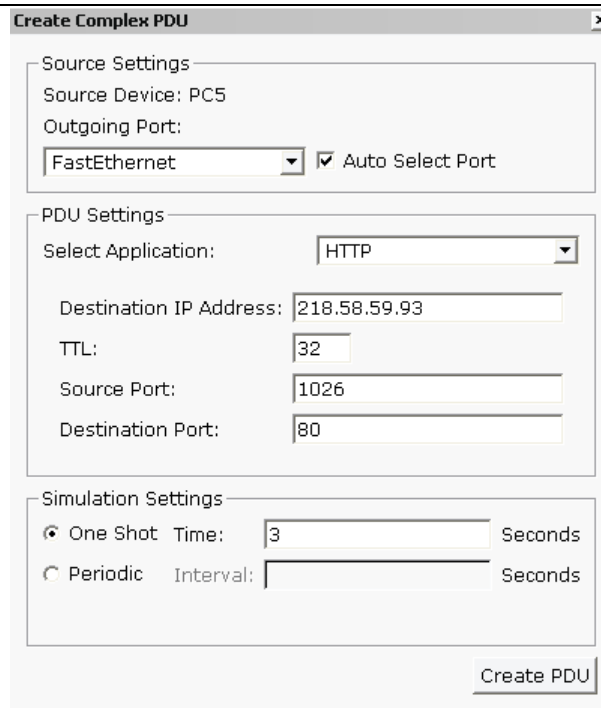


图 10.2 PC5 到 218.58.59.93 的 HTTP Complex PDU 设置
在 Simulation 模式下我们跟踪该 PDU 如图 10.3 所示:

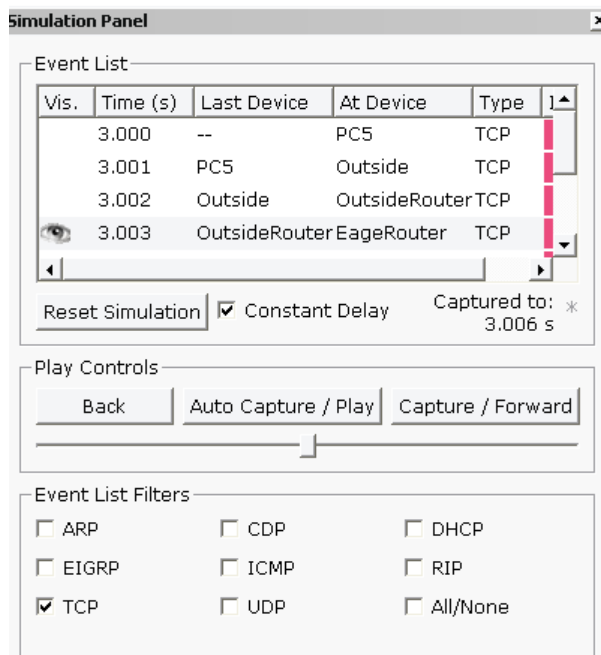


图 10.3 Simulation 模式下跟踪 PC5 到 218.58.59.93 的 HTTP PDU



Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Pi
	Successful	PC5	218.58.59.93	TCP		3.000	N

图 10.4 PC5 到 218.58.59.93 的 HTTP PDU 实验结果

图 10.4 中 PDU 的 Successful 状态说明外网网段可以访问 218.58.59.93 上的 HTTP 资源。

步骤 1.3 实验结果分析

我们在 Logical 视图中单击 EageRouter 上的 PDU，调出 PDU Information 对话框，在 OSI Model 选项卡中我们可以清楚的看到 IP 地址的转换过程，OSI Model 下方的英文信息说明这一点。如图 10.5 所示：

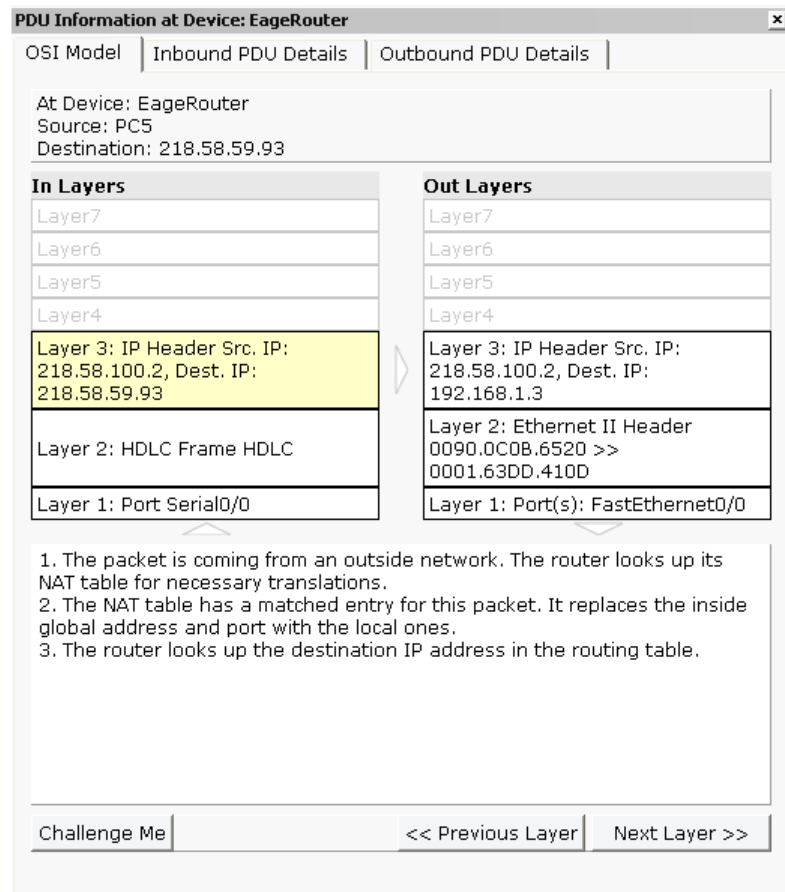


图 10.5 EageRoute 上 PC5 到 218.58.59.93 HTTP PDU 的 IP 地址转换过程

步骤 2

步骤 2.1 首先将 192.168.1.5 静态转换到 218.58.59.94，配置过程如下：

```
EageRouter#config t
EageRouter(config)#ip nat inside source static 192.168.1.5 218.58.59.94
EageRouter(config)#interface fa0/0
EageRouter(config-if)#ip nat inside
EageRouter(config-if)#interface s0/0
EageRouter(config-if)#ip nat outside
```

EageRouter(config-if)#end

步骤 2.2 我们来查看一下刚才的配置。

EageRouter#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	218.58.59.93	192.168.1.3	---	---
---	218.58.59.94	192.168.1.5	---	---

以上显示信息说明配置完成。

接下来我们进行测试，添加一个由 PC5 到 218.58.59.94 的 Complex PDU 格式如下：

Create Complex PDU

Source Settings

Source Device: PC5
Outgoing Port:
FastEthernet ☐ Auto Select Port

PDU Settings

Select Application: SMTP
Destination IP Address: 218.58.59.94
TTL: 32
Source Port: 1026
Destination Port: 25

Simulation Settings

☒ One Shot Time: 3 Seconds
☐ Periodic Interval: Seconds

Create PDU

图 10.6 PC5 到 218.58.59.94 的 SMTP Complex PDU 设置

在 Simulation 模式下我们跟踪该 PDU 如图 10.7 所示：

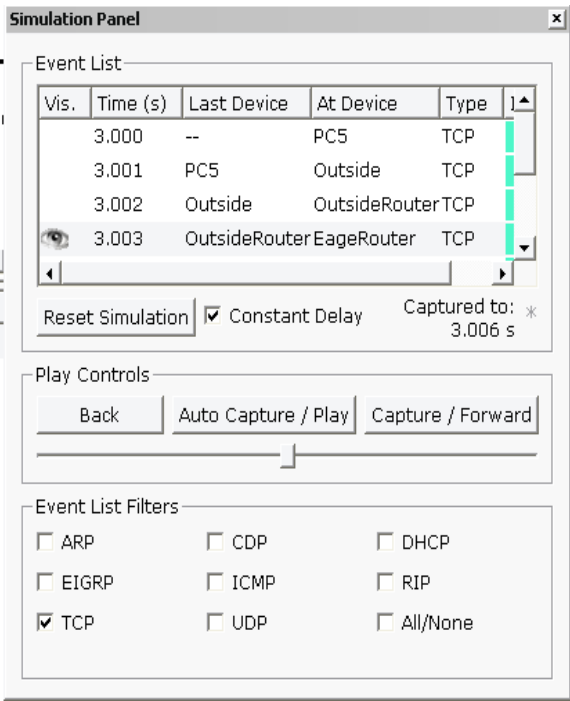


图 10.7 Simulation 模式下跟踪 PC5 到 218.58.59.94 的 SMTP PDU

Fire	Last Status	Source	Destination	Type	Color	Time (sec)
	Successful	PC5	218.58.59.94	TCP		3.000

图 10.8 PC5 到 218.58.59.94 的 SMTP PDU 实验结果

步骤 2.3 实验结果分析。

我们单击 EageRouter 上的 PDU，调出 PDU Information 对话框，在 OSI Model 选项卡中我们可以清楚的看到 IP 地址的转换过程，OSI Model 下方的英文信息说明这一点。如图 10.9 所示：

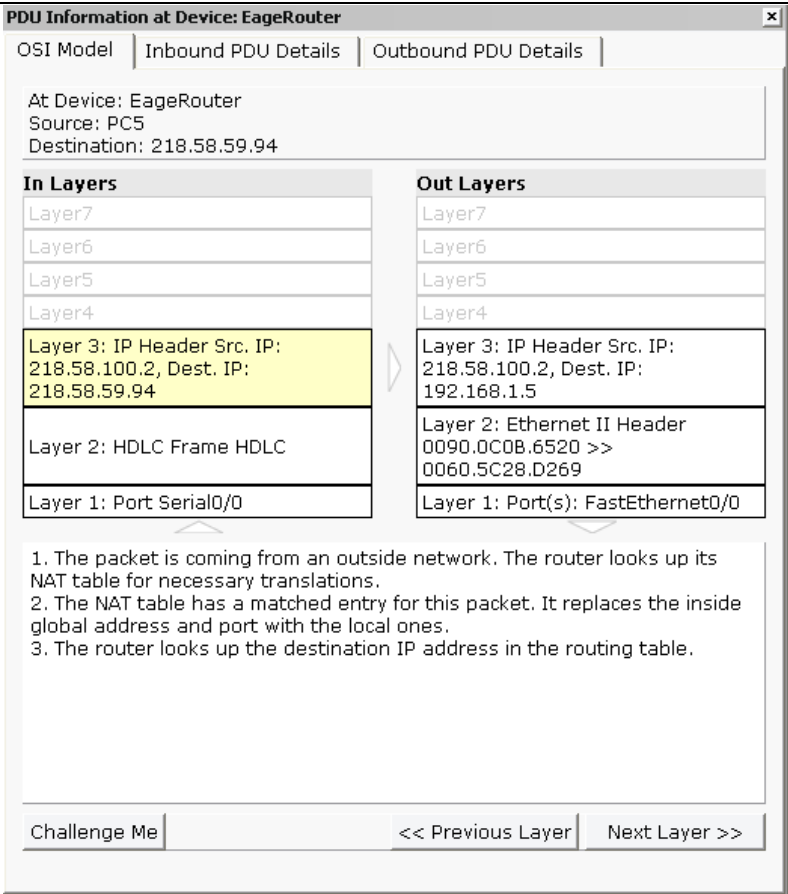


图 10.9 EageRoute 上 PC5 到 218.58.59.93 SMTP PDU 的 IP 地址转换过程

步骤 3

步骤 3.1 下面我们将管理网段（192.168.2.0）、行政网段（192.168.3.0）的内部私有 IP 动态转换到 218.58.59.95 和 218.58.59.96。配置命令如下：

```
EageRouter#config t
EageRouter(config)# access-list 1 permit 192.168.3.0 0.0.0.255
EageRouter(config)# access-list 1 permit 192.168.2.0 0.0.0.255
EageRouter(config)#exit
EageRouter(config)#ip nat pool mypool 218.58.59.95 218.58.59.96 netmask 255.255.255.0
EageRouter(config)#ip nat inside source list 1 pool mypool
EageRouter(config)#interface fa0/0
EageRouter(config-if)#ip nat inside
EageRouter(config-if)#interface s0/0
EageRouter(config-if)#ip nat outside
```

步骤 3.2 我们来测试一下刚才的配置。

我们建立两个 Complex PDU 格式如下图所示：

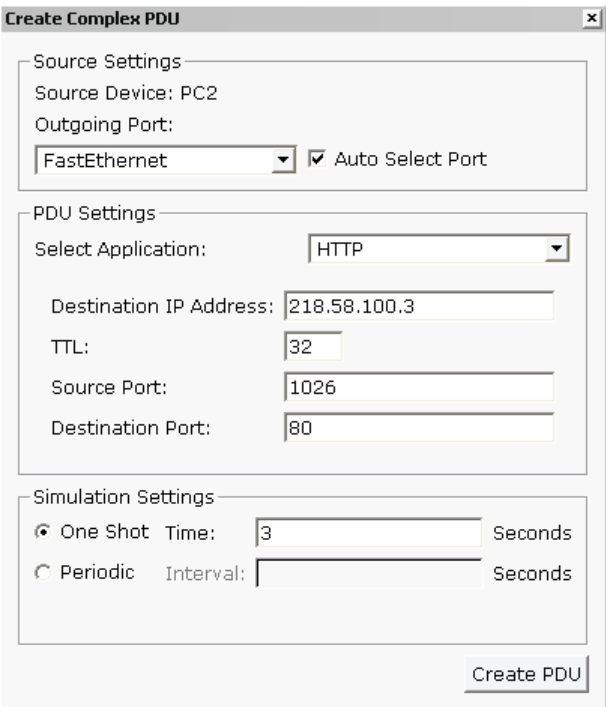


图 10.10 PC2 到 218.58.100.3 的 HTTP Complex PDU 设置

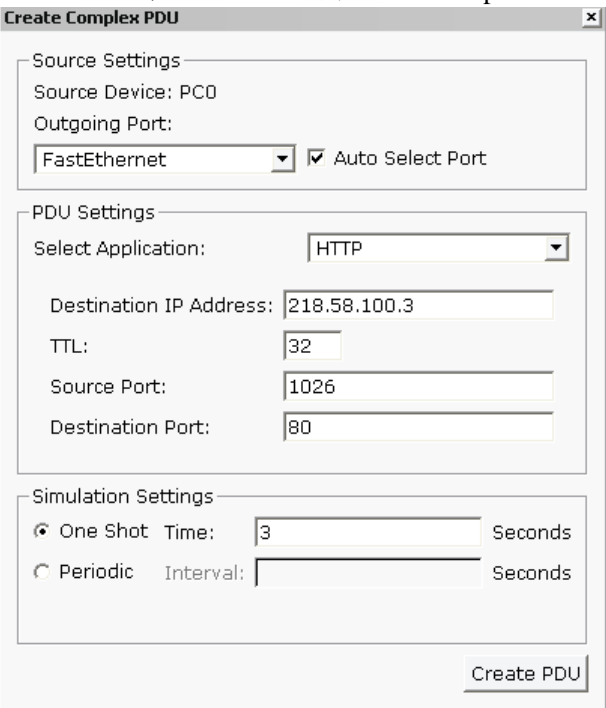


图 10.11 PC0 到 218.58.100.3 的 HTTP Complex PDU 设置

结果如下图所示

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete
	Successful	PC0	218.58.100.3	TCP		3.000	N	0	(edit)	(delete)
	Successful	PC2	218.58.100.3	TCP		3.000	N	1	(edit)	(delete)

图 10.12 PC0、PC2 分别到 218.58.100.3 的 HTTP PDU 实验结果

图 10.12 中 0 号 PDU 和 1 号 PDU 的 Successful 状态分别说明管理网段和行政网段可以访问 218.58.59.100.3 上的 HTTP 资源。

此时我们用如下命令做进一步的验证。

EageRouter#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	218.58.59.93	192.168.1.3	---	---
---	218.58.59.94	192.168.1.5	---	---
---	218.58.59.95	192.168.2.2	---	---
---	218.58.59.96	192.168.3.2	---	---

信息显示又增加了两个条目，正好是刚才进行的 NAT 地址转换。

步骤 3.3 实验结果分析。

我们分别调出两个数据包在 EageRouter 上的 PDU Information 面板，在各自 OSI Model 选项卡中我们可以清楚的看到各自的 Ip 地址的转换过程，OSI Model 下方的英文信息说明这一点。如图 10.13 和 10.14 所示：

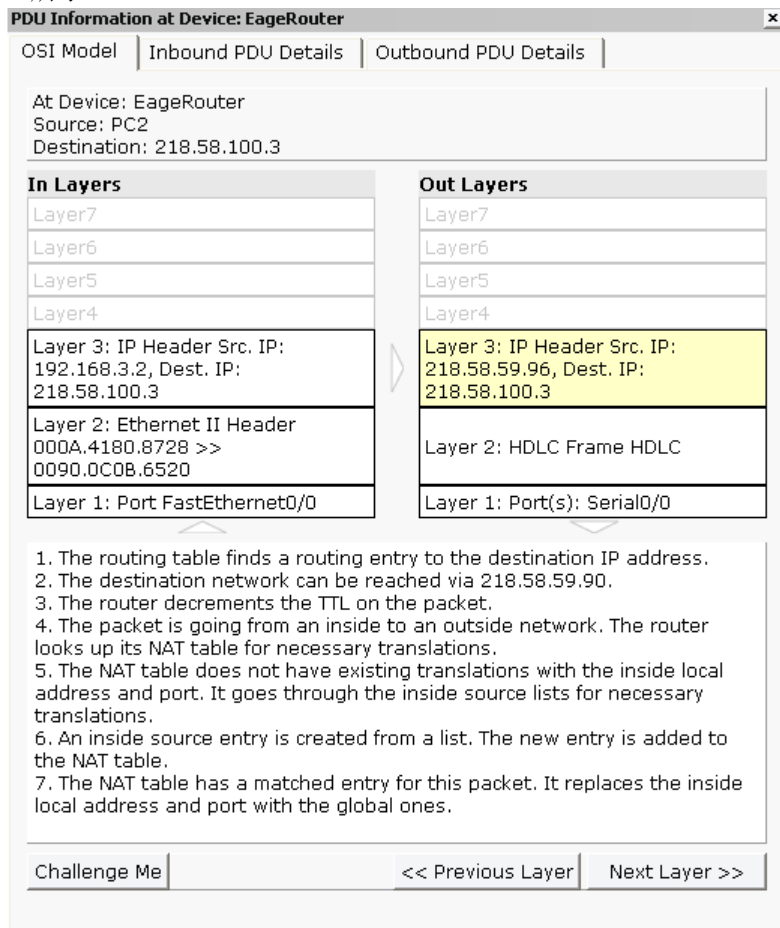


图 10.13 EageRoute 上 PC2 到 218.58.100.3 HTTP PDU 的 IP 地址转换过程

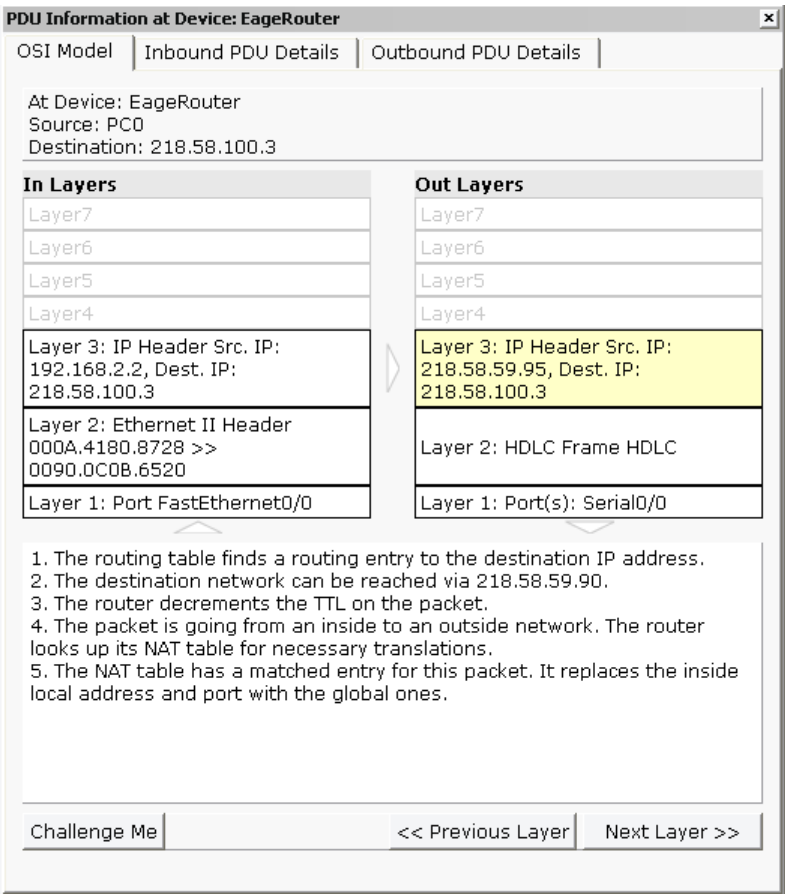


图 10.14 EgeRoute 上 PC0 到 218.58.100.3 HTTP PDU 的 IP 地址转换过程

我们看到 192.168.2.2 NAT 到了 218.58.59.95，而 192.168.3.2NAT 到了 218.58.59.96。达到了预期的效果。那么 192.168.2.3 NAT 到哪个 IP 地址呢？

我们创建一个 Complex PDU 如图 10.15 所示：

Create Complex PDU

Source Settings

Source Device: PC1

Outgoing Port: FastEthernet ☒ Auto Select Port

PDU Settings

Select Application: HTTP

Destination IP Address: 218.58.100.3

TTL: 32

Source Port: 1026

Destination Port: 80

Simulation Settings

☒ One Shot Time: 3 Seconds

☐ Periodic Interval: Seconds

Create PDU

图 10.15 PC1 到 218.58.100.3 的 HTTP Complex PDU 设置

我们调出该数据包在 EageRouter 上的 PDU Information 面板，在各自 OSI Model 选项卡中我们可以清楚的看到数据包被丢弃了。下方的英文信息说明这一点，如图所示：

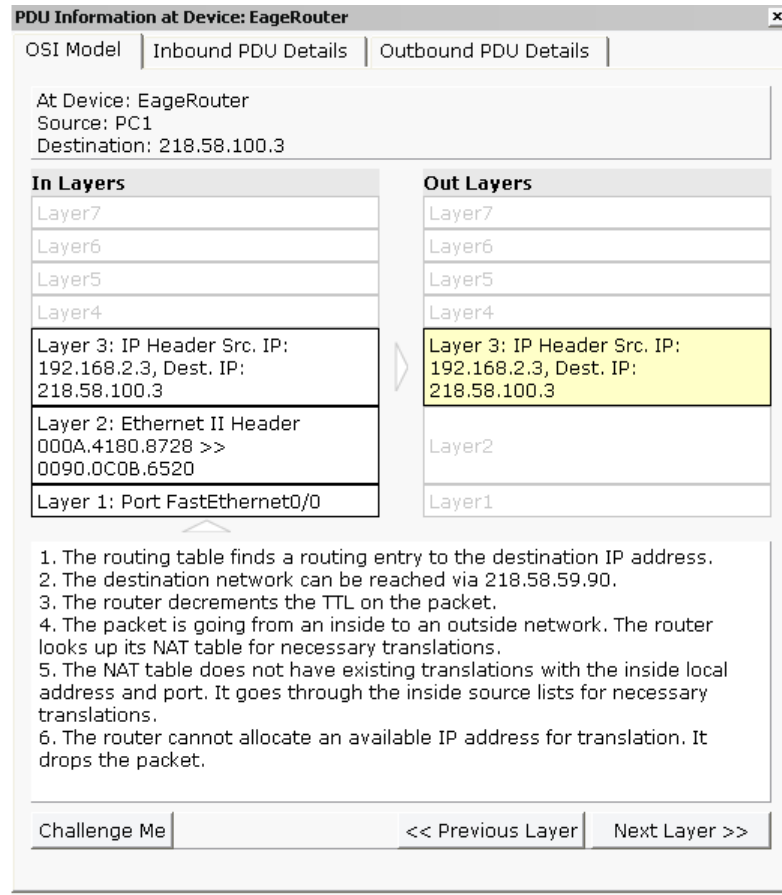


图 10.16 EageRoute 上 PC1 到 218.58.100.3 HTTP PDU 的丢包过程

我们说这也是正常的，大家可以思考一下为什么。

步骤 4

步骤 4.1 我们将教学网段（192.168.4.0）、宿舍网段（192.168.5.0）的内部私有 IP 通过端口地址转换转换到 218.58.59.97，配置命令如下：

```
EageRouter#config t
EageRouter(config)# access-list 2 permit 192.168.4.0 0.0.0.255
EageRouter(config)# access-list 2 permit 192.168.5.0 0.0.0.255
EageRouter(config-std-nacl)#exit
EageRouter(config)#ip nat pool mypool1 218.58.59.97 218.58.59.97 netmask 255.255.255.0
EageRouter(config)#ip nat inside source list 2 pool mypool1 overload
EageRouter(config)#interface fa0/0
EageRouter(config-if)#ip nat inside
EageRouter(config-if)#interface s0/0
EageRouter(config-if)#ip nat outside
EageRouter(config)#end
```

我们建立两个 Complex PDU 格式如下图所示：

步骤 4.2 我们来测试一下刚才的配置。

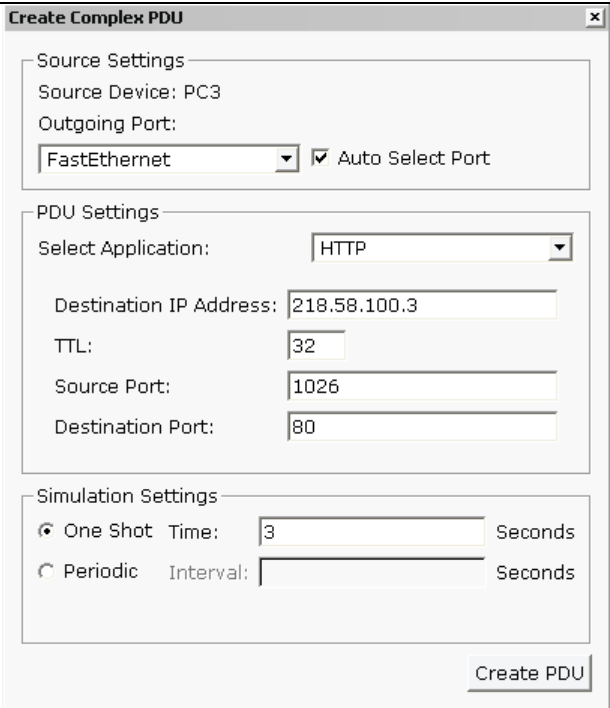


图 10.17 PC3 到 218.58.100.3 的 HTTP Complex PDU 设置

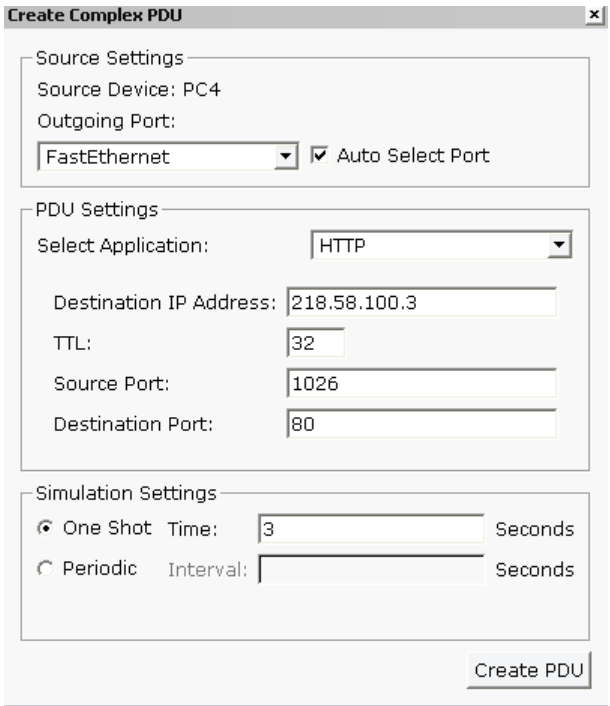


图 10.18 PC4 到 218.58.100.3 的 HTTP Complex PDU 设置

结果如图 10.19 所示

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete
	Successful	PC3	218.58.100.3	TCP		3.000	N	0	(edit)	(delete)
	Successful	PC4	218.58.100.3	TCP		3.000	N	1	(edit)	(delete)

图 10.19 PC3、PC4 分别到 218.58.100.3 的 HTTP PDU 实验结果

图 10.19 中 0 号 PDU 和 1 号 PDU 的 Successful 状态分别说明教学网段和宿舍网段可以访问 218.58.59.100.3 上的 HTTP 资源。

此时我们用如下命令做进一步的验证。

EageRouter#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	218.58.59.93	192.168.1.3	---	---
---	218.58.59.94	192.168.1.5	---	---
---	218.58.59.95	192.168.2.2	---	---
---	218.58.59.96	192.168.3.2	---	---
tcp	218.58.59.97:1026	192.168.4.2:1026	218.58.100.3:80	218.58.100.3:1026
tcp	218.58.59.97:1024	192.168.5.2:1026	218.58.100.3:80	218.58.100.3:1024

黑体部分就是我们刚才 PAT 的结果。

步骤 4.3 实验结果分析。

我们分别调出两个数据包在 EageRouter 上的 PDU Information 面板，在各自 OSI Model 选项卡中我们可以清楚的看到各自的 IP 地址的转换过程。下方的英文信息说明这一点，如图 10.20 所示：

PDU Information at Device: EageRouter

OSI Model

Inbound PDU Details

Outbound PDU Details

At Device: EageRouter

Source: PC4

Destination: 218.58.100.3

In Layers

Layer7

Layer6

Layer5

Layer4

Layer 3: IP Header Src. IP: 192.168.5.2, Dest. IP: 218.58.100.3

Layer 2: Ethernet II Header 000A.4180.8728 >> 0090.0C0B.6520

Layer 1: Port FastEthernet0/0

Out Layers

Layer7

Layer6

Layer5

Layer4

Layer 3: IP Header Src. IP: 218.58.59.97, Dest. IP: 218.58.100.3

Layer 2: HDLC Frame HDLC

Layer 1: Port(s): Serial0/0

1. The routing table finds a routing entry to the destination IP address.

2. The destination network can be reached via 218.58.59.90.

3. The router decrements the TTL on the packet.

4. The packet is going from an inside to an outside network. The router looks up its NAT table for necessary translations.

5. The NAT table has a matched entry for this packet. It replaces the inside local address and port with the global ones.

Challenge Me

<< Previous Layer

Next Layer >>

图 10.20 EageRoute 上 PC4 到 218.58.100.3 HTTP PDU 的 IP 地址转换过程

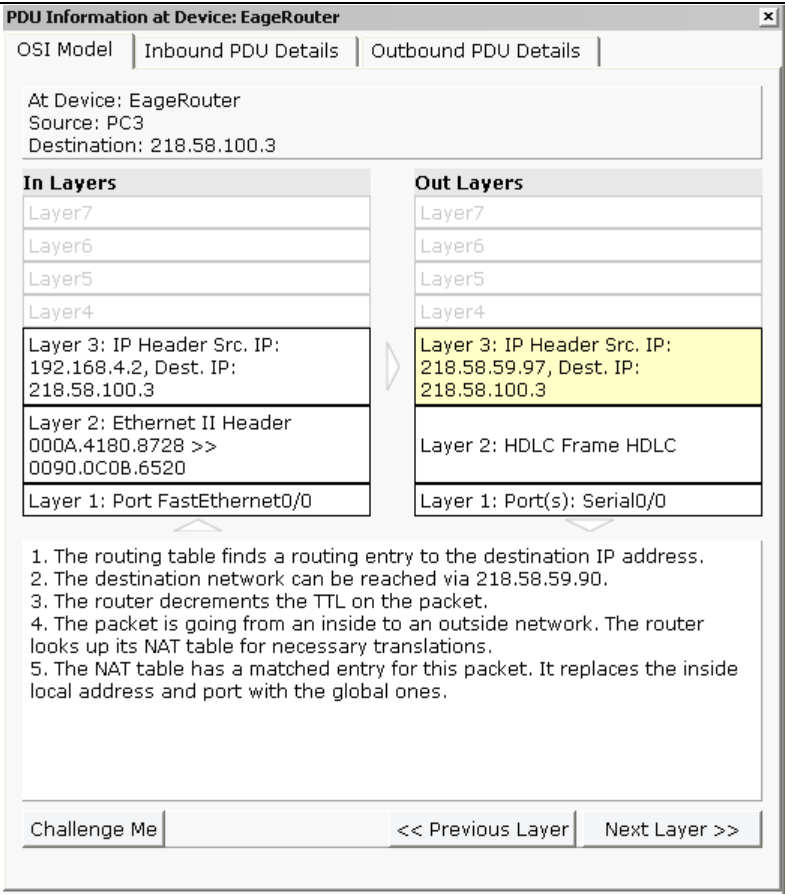


图 10.21 EageRoute 上 PC3 到 218.58.100.3 HTTP PDU 的 IP 地址转换过程至此实验内容全部结束。本次实验内容较多，希望大家理清头绪，好好总结。

【参考配置】

```
EageRouter#show run
version 12.2
hostname EageRouter
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip access-group 101 out
ip nat inside
duplex auto
speed auto
interface Serial0/0
ip address 218.58.59.91 255.255.255.0
ip nat outside
interface Serial0/1
no ip address
shutdown
interface FastEthernet1/0
no ip address
shutdown
```

```
router rip
  network 192.168.1.0
  network 218.58.59.0
ip nat pool mypool 218.58.59.95 218.58.59.96 netmask 255.255.255.0
ip nat pool mypool1 218.58.59.97 218.58.59.97 netmask 255.255.255.0
ip nat inside source list 1 pool mypool
ip nat inside source list 2 pool mypool1 overload
ip nat inside source static 192.168.1.3 218.58.59.93
ip nat inside source static 192.168.1.5 218.58.59.94
ip classless
access-list 101 deny tcp 218.58.100.0 0.0.0.255 host 192.168.1.4 eq 21
access-list 101 permit tcp 218.58.100.0 0.0.0.255 host 192.168.1.3 eq 80
access-list 101 permit tcp 218.58.100.0 0.0.0.255 host 192.168.1.5 eq 25
access-list 101 permit tcp host 218.58.100.3 eq 80 any
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 2 permit 192.168.4.0 0.0.0.255
access-list 2 permit 192.168.5.0 0.0.0.255
line con 0
end
```

```
OutsideRouter#show run
version 12.2
hostname OutsideRouter
interface FastEthernet0/0
  ip address 218.58.100.1 255.255.255.0
  duplex auto
  speed auto
interface Serial0/0
  ip address 218.58.59.90 255.255.255.0
  clock rate 9600
interface Serial0/1
  no ip address
  shutdown
router rip
  network 218.58.59.0
  network 218.58.100.0
ip classless
line con 0
end
```

```
InsideRouter#show run
version 12.2
hostname InsideRouter
interface FastEthernet0/0
  ip address 192.168.1.2 255.255.255.0
  ip access-group 100 out
  duplex auto
  speed auto
interface Ethernet1/0
  ip address 192.168.2.1 255.255.255.0
  duplex auto
  speed auto
```

```
interface Ethernet1/1
 ip address 192.168.3.1 255.255.255.0
 ip access-group 1 out
 duplex auto
 speed auto
interface Ethernet1/2
 ip address 192.168.4.1 255.255.255.0
 duplex auto
 speed auto
interface Ethernet1/3
 ip address 192.168.5.1 255.255.255.0
 duplex auto
 speed auto
router rip
 network 192.168.1.0
 network 192.168.2.0
 network 192.168.3.0
 network 192.168.4.0
 network 192.168.5.0
ip classless
access-list 1 deny 192.168.5.0 0.0.0.255
access-list 1 deny 192.168.4.0 0.0.0.255
access-list 1 permit host 192.168.2.3
access-list 1 deny 192.168.2.0 0.0.0.255
access-list 1 permit any
access-list 100 deny tcp 192.168.5.0 0.0.0.255 host 192.168.1.4 eq 21
access-list 100 permit ip any any
line con 0
end
```

【实验思考】

- 1、总结一下 NAT 和 PAT 的应用场景和配置步骤。
- 2、思考一下图 10.16 中 PC1 到 218.58.100.3 HTTP PDU 为什么被丢弃。
- 3、在 Simulation 模式下跟踪数据包时，数据包到达目的地时可能显示一个闪烁的 X，但是 PDU List Window 中 Last status 却是 successful。你能解释一下原因吗？

附录一 路由器和交换机产品简介

(一) 路由器

思科公司的产品被网络用户广泛的使用, 对它们的典型产品及其特性的了解可对网络设备有一定大致的认识, 以下主要对 Cisco1800 系列、Cisco2600 系列、Cisco 2800 系列、Cisco 3700 系列模块化和固定配置的路由器产品进行简单介绍。

首先以“S26C-12007XK”, “CD26-BHP-12.0.7=”这两个产品型号为例介绍一下 Cisco 产品型号名的字母含义:

前缀: S -- 预装机箱,无独立介质包装、SF -- 预装机箱,无独立介质包装、SW -- 软盘介质、CD -- 光盘介质。

中间: A -- Enterprise 版本、B -- 包含 IP/IPX/Apple Talk/DecNet 协议、C -- IP Only 版本、D -- Desktop 版本, 包含 IP/IPX、E -- Remote Access Server 版本, 配合多口拨号访问服务、H -- 防火墙特性版本、P -- IP PLUS 特性,如:Easy IP, Multicast Routing, DLSw+、L -- IPSEC 56 位加密版本、K2 -- IPSEC 3DES 加密, 此项技术目前对中国禁止出口,因此不能定购和升级、N -- APPN 特性版本、R1 -- SNA 特性版本、U -- 支持 H.323 数据流压缩特性版本、W -- IPSEC 40 位加密版本、HY -- 具备 IPSEC 56 位加密的防火墙特性版本。

后缀: T -- 有修改(patch)的版本、(旧) XK -- 有修改(patch)的版本(新)、FL26-C-B= Cisco IOS 的升级协议. 具备此协议的软件升级是合法的. 注意: 如果同时支持多个特性集, 则相应应有多个字母, 如 CD26-BHP-12.0.7=。

1、Cisco 1800 系列

Cisco 1800 系列集成多业务路由器是 Cisco 1700 系列模块化和固定配置路由器的下一代产品。Cisco 1801、1802、1803、1811 和 1812 集成路由器(如图 1 所示)采用了固定的配置, 而 Cisco 1841 集成路由器则采用了模块化的配置。与上一代的 Cisco 1700 系列路由器相比, 固定配置路由器专为宽带、城域以太网和无线的安全连接而设计, 可以提供显著的性能提升、功能改进、丰富的用途和更高的价值。Cisco 1800 系列固定配置路由器可以为分支机构和小型办公室提供安全的宽带接入和多种并发服务, 提供集成化 ISDN 基本速率接口(BRI)、模拟调制解调器, 或者用于冗余 WAN 链路和负载平衡的以太网备用端口, 利用多个天线为同时进行的 802.11a/b/g 操作提供安全的无线 LAN。提供高级安全功能, 包括: 状态化检测防火墙、IP 安全(IPSec) VPN(三重数据加密标准[3DES]或者高级加密标准[AES])、入侵防范系统(IPS)、通过实施网络准入控制(NAC)和安全访问策略, 提供支持 VLAN 和可选的以太网供电(PoE)的 8 端口 10 兆/100 兆可管理交换机, 通过基于 Web 的工具和 Cisco IOS 软件提供简便的部署和远程管理功能。



图 1 Cisco 1800 系列固定配置路由器

Cisco 1801、1802 和 1803 路由器可以通过基于基本电话服务的非对称 DSL(ADSL)(Cisco 1801)基于 ISDN 的 ADSL(Cisco 1802)或者对称高速 DSL(G.SHDSL)(Cisco 1803),提供高速 DSL 宽带接入, 同时利用集成的备用 ISDN S/T BRI 确保可靠的网络连接。Cisco 1811 和

1812 不仅可以通过两个 10/100 BASE-T 快速以太网端口提供高速宽带或者以太网接入,还能够通过一个 V.92 模拟调制解调器 (Cisco 1811) 或者 ISDN S/T BRI 接口 (Cisco 1812) 提供集成的备用 WAN 连接。

Cisco 1800 系列固定配置路由器可以为中小企业 SMB (SMB-SmallMediumBusiness) 和企业小型分支机构提供功能强大的网络基础设施。它们可以提供对互联网、企业网络或者其他远程办公室的访问,同时利用集成的 Cisco IOS 软件安全特性和功能保护关键的数据。它们还让企业可以用同一个设备提供多种过去通常由多个设备分别执行的服务 (集成化路由器可以提供冗余连接、LAN 交换机、防火墙、VPN、IPS、无线技术和服务质量[QoS]),从而大幅度地降低成本。Cisco IOS 软件为这种灵活性提供了有力的支持。它可以利用公认的、标准的互联网和专用 WAN 联网软件,提供业界安全性最高、扩展能力最强和功能最丰富的网络支持。

2、Cisco 2600 系列

Cisco 系统有限公司的 Cisco 2600 模块化访问路由器系列,为远程分支机构提供新的通用性、集成性和强大功能。



图 2 Cisco2600 系列固定配置路由器

Cisco 2600 系列可使用 Cisco 1600 和 Cisco 3600 系列的接口模块,提供了高效率、低成本的解决方案,以满足当今远程分支机构的需求,同时可支持以下应用:多业务语音/数据集成、办公室拨号服务、企业外部网/VPN 访问。

随着新的业务和应用推陈出新,网络技术在不断地变化。Cisco 2600 系列的模块化体系结构具有适应此种变化所需要的通用性。Cisco 2600 系列使用功能强大的 RISC 处理器,其超强的功能可支持当今远程分支机构需要的高级服务质量、安全性和网络集成特性等。Cisco 2600 系列具有单或双以太网局域网接口,两个 Cisco 广域网接口卡插槽、一个 Cisco 网络模块插槽以及一个新型高级集成模块 (AIM) 插槽。

Cisco 1600、Cisco 2600 和 Cisco 3600 系列路由器所使用的广域网接口卡支持各种串行口、综合业务数字网基本速率接口 (ISDN BRI) 以及综合信道服务设备/数据服务设备 (CSU/DSU) 等可选项,以实现主、备广域网连接。Cisco 2600 和 Cisco 3600 系列使用的网络模块支持高密度串行口,拨号池以及多业务语音/数据集成等多种可选项。

Cisco 2600 系列具有以下优点,支持 Cisco 网络端到端解决方案。

(1) 多业务集成。Cisco 2600 系列将 Cisco 2500 系列的通用性、集成性和强大功能进一步扩展到较小的远程分支机构。

(2) 投资保护。Cisco 2600 系列支持对模块组件进行现场投资升级,所以客户能轻而易举

地更新他们的网络接口，而无需对整个远程分支机构进行全面升级。

(3) 降低了成本。Cisco 2600 系列将 CSU/DSU, ISDN 网络终端 (NTI) 设备以及远程分支机构布线室中的其它设备集成到一台很小的设备中，提供一种节省空间的解决方案，使用网络管理软件（比如 Cisco Works 和 Cisco View）可对此方案进行远程管理。

(4) Cisco 2600 系列是 Cisco 端到端解决方案的一部分，它允许企业将高效低成本的无缝网络基础结构扩充到远程分机构。

3、Cisco 2800 系列集成多业务路由器

模块化 Cisco2800 系列集成多业务路由器（参见图 1）是思科公司推出的一个全新的集成多业务路由器系列，它进行了专门的优化，可安全、线速地同时提供数据、语音和视频服务，重新定义了最佳大型企业和中小型企业路由。Cisco 2800 系列的独特集成系统架构提供了最高业务灵活性和投资保护。



图 3 Cisco 2800 系列

Cisco 2800 系列由四个新平台组成（参见图 1）：Cisco 2801、Cisco 2811、Cisco 2821 和 Cisco 2851。与相似价位的前几代思科路由器相比，Cisco 2800 系列的性能提高了五倍、安全性和话音性能提高了十倍、具有全新内嵌服务选项，且大大提高了插槽性能和密度，同时保持了对目前 Cisco 1700 系列和 Cisco 2600 系列中现有 90 多种模块中大多数模块的支持，从而提供了极大的性能优势。

Cisco 2800 系列能以线速为多条 T1/E1/xDSL 连接提供多种高质量并发服务。这些路由器提供了内嵌加密加速和主板话音数字信号处理器 (DSP) 插槽；入侵保护和防火墙功能；集成化呼叫处理和语音留言；用于多种连接需求的高密度接口；以及充足的性能和插槽密度，以用于未来网络扩展和高级应用。

(1) 用于数据、语音和视频的安全网络连接。安全已成为网络的基本构建块。路由器在网络防御战略中起重要作用，因为安全性需内嵌于整个网络之中。Cisco 2800 系列具有先进、集成的端到端安全性，以用于提供融合服务和应用。

(2) 融合 IP 通信。Cisco 2800 系列可满足中小企业和企业分支机构的 IP 通信需求，同时在单一路由平台中提供业界领先的安全性。Cisco CallManager Express (CME) 是一个内嵌于 Cisco IOS 软件的可选解决方案，为思科 IP 电话提供了呼叫处理。此解决方案适用于有数据连接需求、对于为多达 72 部电话部署一个融合 IP 电话解决方案感兴趣的客户。

(3) 集成化服务。凭借 Cisco 2800 系列独特的集成化服务架构，客户现可用传统 IP 路由安全地部署 IP 通信，并为更多的高级服务预留接口和模块插槽。

4、Cisco 3700 系列应用服务路由器

Cisco 3700 系列应用服务路由器 (Application Service Router) 是一系列全新的模块化路由器，可实现新的电子商务应用在集成化分支机构访问平台中的灵活、可扩展的部署。Cisco 3700 系列支持 Cisco AVVID (语音、视频和集成数据体系结构)，而 Cisco AVVID 则是一种覆盖整个企业的、基于各种标准的网络体系结构，它可为将各种商业和技术战略组合成一个聚合模型奠

定基础。



图 4 Cisco 3700 系列应用服务路由器

总之，Cisco 3700 系列提供了一个针对分支机构应用和服务的模块化集成和整合而优化的访问平台。模块化 Cisco 3700 系列应用服务路由器充分利用了 Cisco 1700、2600 和 3600 系列路由器针对 WAN 访问、语音网关和拨号应用等而配备的可选的网络模块(NM)、WAN 接口卡(WIC)和高级集成模块(AIM)。此外，Cisco 3725 和 Cisco 3745 这两个 Cisco 3700 平台引进一种新的、可提供更广泛接口的高密度服务模块 (HDSM)。配备四个 NM 插槽的 Cisco 3745 路由器取消了在每一对相邻 NM 插槽之间的中心导轨，因此可以采用两个 HDSM，而不是四个 NM。配备两个 NM 插槽的 Cisco 3725 路由器可在它所配备的两个 NM 插槽之一中采用一个 HDSM，并仍可在剩余的 NM 插槽内采用一个 NM。采用新的 HDSM 之后，Cisco 3700 系列路由器就能够集成更高端口密度和新的高性能服务了。

Cisco 3700 系列的另一新增功能是，它能够在用于 IP 电话和/或 Aironet 无线 LAN 应用的可选 10/100 交换模块上支持集成化在线供电 (In-Line Power)。Cisco 3700 系列在基本机箱通过插槽和端口集成，可使这些 NM 插槽能在较小的占地面积上集成更多服务。这两种 Cisco 3700 平台均可提供更高的闪存和 DRAM 默认内存，可加快并简化未来增加服务和功能的过程。此外，Cisco 3745 路由器还提供了其他一些在高密度、多服务配置中所必要的可用性功能。

Cisco 3725 和 3745 主要特点：

- (1) 两个集成化 10/100 LAN 端口
- (2) 两个集成化高级集成模块 (AIM) 插槽
- (3) 三个集成化 WAN 接口卡 (WIC) 插槽
- (4) 两个 (Cisco 3725) 或四个 (Cisco 3745) 网络模块 (NM) 插槽
- (5) 一个 (Cisco 3725) 或两个 (Cisco 3745) 高密度服务模块 (HDSM) 功能插槽
- (6) 32MBFlash/128MB DRAM (默认)
- (7) 针对 16-端口 EtherSwitch NM 和 36-端口 EtherSwitch HDSM 的可选在线供电 (In-Line Power)
- (8) 可支持所有主要的 WAN 协议和传输介质：LL、FR、ISDN、X.25、ATM、部分 T1/E1、T1/E1、xDSL、T3/E3、HSSI
- (9) 可支持 Cisco 1700、2600 和 3600 系列中所配备的某些 NM、WIC、和 AIM
- (10) 两个 RU (Cisco 3725) 或三个 RU (Cisco 3745) 机架安装式机箱

Cisco 3745 的其他主要特点：

- (1) 可在现场更换的母板、I/O 板和风扇托架
- (2) 无源背板
- (3) 可选内置备用电源 (RPS --- 系统和在线供电电源)
- (4) NM 和 RPS 热插拔 (OIR)

(二) 交换机

Cisco 的交换机产品以“Catalyst”为商标, 包含 1900、2800、2900、3500、4000、5000、5500、6000、8500 等十多个系列。总的来说, 这些交换机可以分为两类: 一类是固定配置交换机, 包括 3500 及以下的大部分型号, 比如 1924 是 24 口 10Mbps 以太网交换机, 带两个 100Mbps 上行端口。除了有限的软件升级之外, 这些交换机不能扩展; 另一类是模块化交换机, 主要指 4000 及以上的机型, 网络设计者可以根据网络需求, 选择不同数目和型号的接口板、电源模块及相应的软件。

选择设备时, 许多人对长长的产品型号十分头疼。其实, Cisco 对产品的命名有一定之规。就 Catalyst 交换机来说, 产品命名的格式如下:

Catalyst NNXX [-C] [-M] [-A/-EN]

其中, NN 是交换机的系列号, XX 对于固定配置的交换机来说是端口数, 对于模块化交换机来说是插槽数, 有 -C 标志表明带光纤接口, -M 表示模块化, -A 和 -EN 分别是指交换机软件是标准板或企业版。

目前, 网络集成项目中常见的 Cisco 交换机有以下几个系列, 1900/2900 系列、3500 系列、6500 系列。他们分别使用在网络的低端、中端和高端。下面分别介绍一下这几个系列的产品:

1、低端产品

先说一下低端的产品, 1900 和 2900 是低端产品的典型。其实在低端交换机市场上, Cisco 并不占特别的优势, 因为 3Com、Dlink 等公司的产品具有更好的性能价格比。

1900 交换机适用于网络末端的桌面计算机接入, 是一款典型的低端产品。它提供 12 或 24 个 10Mbps 端口及 2 个 100Mbps 端口, 其中 100Mbps 端口支持全双工通讯, 可提供高达 200Mbps 的端口带宽。机器的背板带宽是 320Mbps。

带企业版软件的 1900 还支持 VLAN 和 ISL Trunking, 最多 4 个 VLAN, 但一般情况下, 低端的产品对这项功能的要求不多。某些型号的 1900 带 100BaseFX 光纤接口。如 C1912C、C1924C 带一个百兆 Tx 口和一个百兆 Fx 口, C1924F 带两个 100BaseFX 接口。1900 系列的主要型号如下:

C1912: 12 口 10BaseTx, 2 口 100BaseTx, 1 个 AUI 口

C1912C: 12 口 10BaseTx, 1 口 100BaseTx, 1 个 AUI 口, 1 个 100BaseFx 口

C1924: 24 口 10BaseTx, 2 口 100BaseTx, 1 个 AUI 口

C1924C: 24 口 10BaseTx, 1 口 100BaseTx, 1 个 AUI 口, 1 个 100BaseFx 口

C1924F: 24 口 10BaseTx, 1 个 AUI 口, 1 个 100BaseFx 口

如果在你的网络中, 有些桌面计算机是 100Mbps 的, 那么 2900 系列可能更加适合。与 1900 相比, 2900 最大的特点是速度增加, 它的背板速度最高达 3.2G, 最多 24 个 10/100Mbps 自适应端口, 所有端口均支持全双工通讯, 使桌面接入的速度大大提高。除了端口的速率之外, 2900 的其他许多性能也比 1900 系列有了显著的提高。比如, 2900 的 MAC 地址表容量是 16K, 可以划分 1024 个 VLAN, 支持 ISL Trunking 协议等等。

2900 系列的产品线很长。其中, 有些是普通 10/100BaseTx 交换机, 如 C2912、C2924 等; 有些是带光纤接口的, 如 C2924C 带两个 100BaseFx 口; 有些是模块化的, 如 C2924M 带两个扩展槽。扩展槽的插卡可以放置 100BaseTx 模块、100baseFx 模块, 甚至可以插 ATM 模块和千兆以太网接口卡(GBIC)。详细情况如下:

C2912-XL: 12 口 10/100BaseTx 自适应

C2912MF-XL: 2 个扩展槽, 12 口 100BaseFX

C2924-XL: 24 口 10/100BaseTX 自适应

C2924C-XL: 22 口 10/100BaseTX 自适应, 2 口 100BaseFX

C2924M-XL: 2 个扩展槽, 24 口 10/100BaseTx 自适应

在 2900 系列中, 有两款产品比较独特, 一是 C2948G, 二是 C2948G-L3。2948G 的性能价格比还不错, 它使用的软件和 Catalyst 5000/5500 一样, 有 48 个 10/100Mbps 自适应以太网端口和 2 个千兆以太网端口, 24G 背板带宽, 带可热插拔的冗余电源, 有一系列容错特征和网管特性。C2948G-L3 在 C2948G 的基础上增加了三层交换的能力, 最大三层数据包吞吐量可达

10Mpps。不过,总的来说,2900 系列交换机一般用在网络的低端,千兆和路由的能力并不是很重要,所以两款 2948 在实际项目中使用得不多。

2、中端产品

再来看中端产品,中端产品中 3500 系列使用广泛,很有代表性。C3500 系列交换机的基本特性包括背板带宽高达 10Gbps,转发速率 7.5Mpps,它支持 250 个 VLAN,支持 IEEE 802.1Q 和 ISL Trunking,可选冗余电源等等。不过 C3500 的最大特性在于管理和千兆。

管理特性方面,C3500 实现了 Cisco 的交换集群技术,可以将 16 个 C3500, C2900, C1900 系列的交换机互联,并通过一个 IP 地址进行管理。利用 C3500 内的 Cisco Visual Switch Manager (CVSM) 软件还可以方便地通过浏览器对交换机进行设置和管理。

千兆特性方面,C3500 全面支持千兆接口卡 (GBIC)。目前 GBIC 有三种 1000BaseSx,适用于多模光纤,最长距离 550m; 1000BaseLX/LH,多模/单模光纤都适用,最长距离 10km; 1000BaseZX 适用于单模光纤,最长距离 100km。

C3500 主要有 4 种型号:

Catalyst 3508G XL: 8 口 GBIC 插槽

Catalyst 3512 XL: 12 口 10/100M 自适应, 2 口 GBIC 插槽

Catalyst 3524 XL: 24 口 10/100M 自适应, 2 口 GBIC 插槽

Catalyst 3548 XL: 48 口 10/100M 自适应, 2 口 GBIC 插槽

3、高端产品

最后,介绍一下高端的产品。对于企业数据网来说,C6000 系列替代了原有的 C5000 系列,是最常用的产品。

Catalyst 6000 系列交换机为园区网提供了高性能、多层交换的解决方案,专门为需要千兆扩展、可用性高、多层交换的应用环境设计,主要面向园区骨干连接等场合。Catalyst 6000 系列是由 Catalyst 6000 和 Catalyst 6500 两种型号的交换机构成,都包含 6 个或 9 个插槽型号,分别为 6006、6009、6506 和 6509,其中,尤以 6509 使用最为广泛。所有型号支持相同的超级引擎、相同的接口模块,保护了用户的投资。这一系列的特性主要包括:

(1)端口密度大。支持多达 384 个 10/100BaseTx 自适应以太网口,192 个 100BaseFX 光纤快速以太网口,以及 130 个千兆以太网端口 (GBIC 插槽)。

(2)速度快。C6500 的交换背板可扩展到 256 Gbps,多层交换速度可扩展到 150 Mpps。C6000 的交换背板带宽 32 Gbps,多层交换速率 30 Mpps。支持多达 8 个快速/千兆以太网口利用以太网通道技术 (Fast EtherChannel, FEC 或 Gigabit EtherChannel, GEC) 连接,在逻辑上实现了 16 Gbps 的端口速率,还可以跨模块进行端口聚合实现。

(3)多层交换。C6000 系列的多层交换模块可以进行线速的 IP, IPX 和 and IP-multicast 路由。

(4)容错性能好。C6000 系列带有冗余超级引擎,冗余负载均衡电源,冗余风扇,冗余系统时钟,冗余上连,冗余的交换背板 (仅对 C6500 系列),实现了系统的高可用性。

(三)思科路由器和交换机所使用的协议

下面从网络、路由、数据链路、网络安全技术等 4 个方面对思科的路由器和交换机所使用的协议进行了分类和特点介绍。

1、思科网络路由协议 网络/路由 (Network/Routing)

CGMP: 思科组管理协议 (CGMP: Cisco Group Management Protocol)

EIGRP: 增强的内部网关路由选择协议 (EIGRP: Enhanced Interior Gateway Routing Protocol)

IGRP: 内部网关路由协议 (IGRP: Interior Gateway Routing Protocol)

HSRP: 热备份路由器协议 (HSRP: Hot Standby Routing Protocol)

RGMP: Cisco Router Port Group Management Protocol

2、思科数据链路协议 数据链路 (Data Link)

CDP: 思科发现协议 (CDP: Cisco Discovery Protocol)

DTP: 思科动态中继协议 (DTP: Dynamic Trunk Protocol)

ISL & DISL: 思科交换链路内协议和动态 ISL 协议 (ISL: Inter-Switch Link Protocol)

VTP: 思科 VLAN 中继协议 (VTP: VLAN Trunking Protocol)

3、思科网络安全技术协议 网络安全技术 (Security/VPN)

L2F: 第二层转发协议 (Layer 2 Forwarding Protocol)

TACACS: 终端访问控制器访问控制系统 (TACACS: Terminal Access Controller Access Control System)

4 思科其他协议

SCCP: 信令连接控制协议

SCCP: Skinny Client Control Protocol

附录二 Packet Tracer 4.0 使用简介

Packet Tracer 是 Cisco 公司为思科网络技术学院开发的一款模拟软件,可以用来模拟 CCNA 的实验。我们也以 Packet Tracer 4.0 做为模拟软件来进行我们的实验。

下面按四个方面对该软件做简单介绍。

- 1、基本界面。
- 2、选择设备,为设备选择所需模块并且选用合适的线型互连设备。
- 3、配置不同设备。
- 4、测试设备的连通性,并在 simulation 模式下跟踪数据包,查看数据包的详细信息。

1、首先我们认识一下 Packet Tracer4.0 的基本界面

打开 Packet Tracer 4.0 时界面如下图所示:

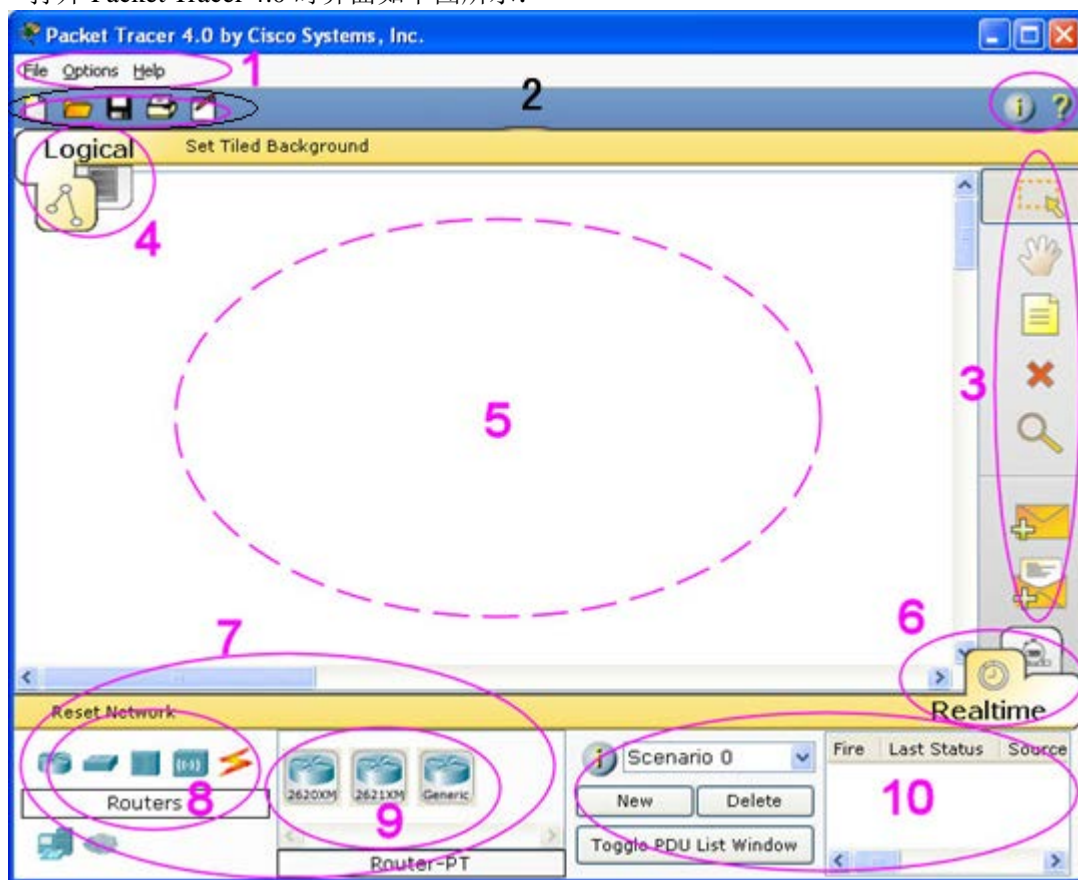


图1 Packet Tracer 4.0 基本界面

表 1 Packet Tracer 4.0 基本界面介绍

1	菜单栏	此栏中有文件、选项和帮助按钮，我们在此可以找到一些基本的命令如打开、保存、打印和选项设置，还可以访问活动向导。
2	主工具栏	此栏提供了文件按钮中命令的快捷方式，我们还可以点击右边的网络信息按钮，为当前网络添加说明信息。
3	常用工具栏	此栏提供了常用的工作区工具包括：选择、整体移动、备注、删除、查看、添加简单数据包和添加复杂数据包等。
4	逻辑/物理工作区转换栏	我们可以通过此栏中的按钮完成逻辑工作区和物理工作区之间转换。
5	工作区	此区域中我们可以创建网络拓扑，监视模拟过程查看各种信息和统计数据。
6	实时/模拟转换栏	我们可以通过此栏中的按钮完成实时模式和模拟模式之间转换。
7	网络设备库	该库包括设备类型库和特定设备库。
8	设备类型库	此库包含不同类型的设备如路由器、交换机、HUB、无线设备、连线、终端设备和网云等。
9	特定设备库	此库包含不同设备类型中不同型号的设备，它随着设备类型库的选择级联显示。
10	用户数据包窗口	此窗口管理用户添加的数据包。

2、选择设备，为设备选择所需模块并且选用合适的线型互连设备

我们在工作区中添加一个 2600 XM 路由器。首先我们在设备类型库中选择路由器，特定设备库中单击 2600 XM 路由器，然后在工作区中单击一下就可以把 2600 XM 路由器添加到工作区中了。我们用同样的方式再添加一个 2950-24 交换机和两台 PC。注意我们可以按住 Ctrl 键再单击相应设备以连续添加设备。如图 2.2 所示：

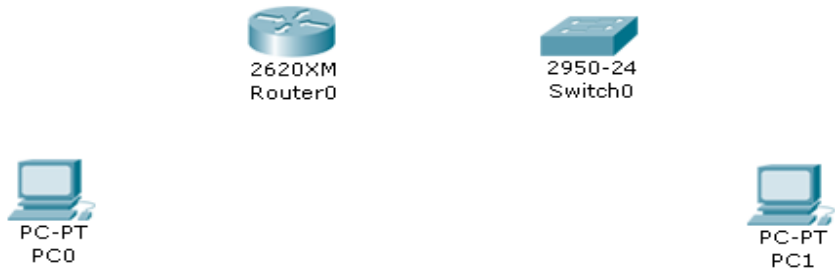


图 2 设备添加

接下来我们要选取合适的线型将设备连接起来。我们可以根据设备间的不同接口选择特定

的线型来连接，当然如果我们只是想快速的建立网络拓扑而不考虑线型选择时我们可以选择自动连线，如图 3 所示：

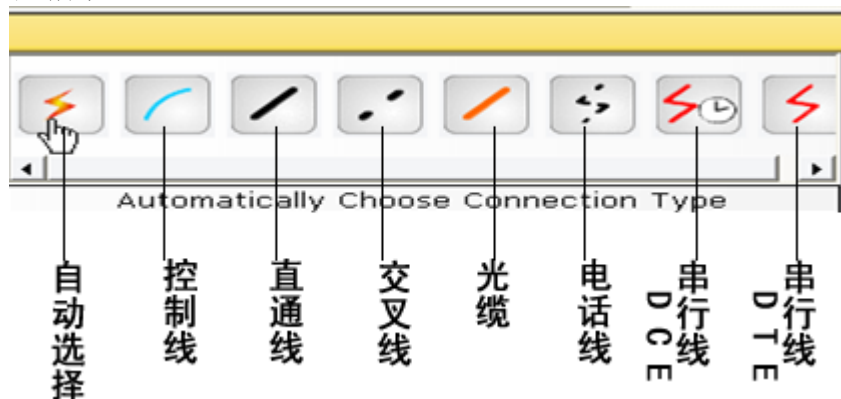


图 3 线型介绍

在正常连接 Router0 和 PC0 后，我们再连接 Router0 和 Switch 0，提示出错了，如下图：

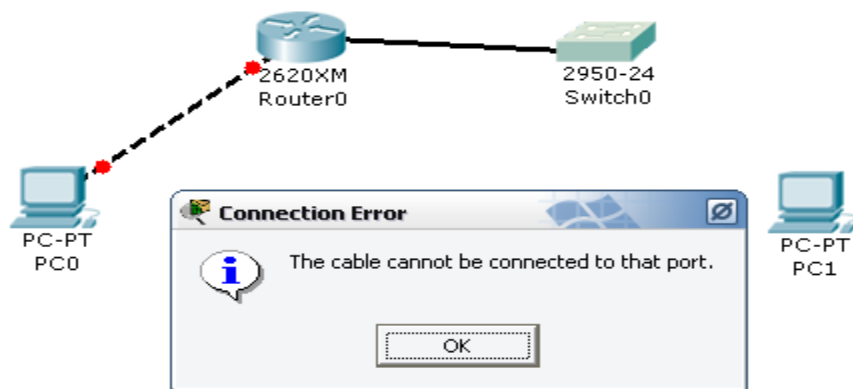


图 4 出错信息

出错的原因是 Router 上没有合适的端口。如图所示：



图 5 Cisco2620 XM 的接口面板

默认的 2600 XM 有三个端口，刚才连接 PC0 已经被占去了 ETHERNET 0/0, Console 口和 AUX 口自然不是连接交换机的所以会出错，所以我们在设备互连前要添加所需的模块（添加模块时注意要关闭电源）。我们为 Router 0 添加 NM-4E 模块（将模块添加到空缺处即可，删除模块时将模块拖回到原处即可）。模块化的特点增强了 Cisco 设备的可扩展性。我们继续完成连

接。

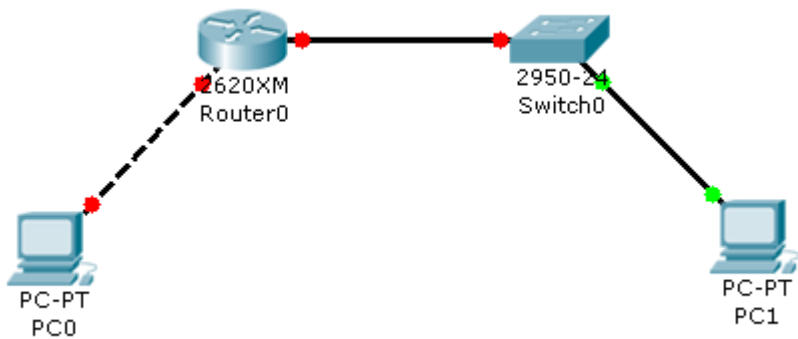


图 6 设备连接

我们看到各线缆两端有不同颜色的圆点，它们分别表示什么样的含义呢？

表 2 线缆两端亮点含义

链路圆点的状态	含义
亮绿色	物理连接准备就绪，还没有 Line Protocol status 的指示
闪烁的绿色	连接激活
红色	物理连接不通，没有信号
黄色	交换机端口处于“阻塞”状态

线缆两端圆点的不同颜色来将有助于我们进行连通性的故障排除。

3、配置不同设备。

我们配置一下 Router0，在 Router0 上单击打开设备配置对话框。如图 7 所示：

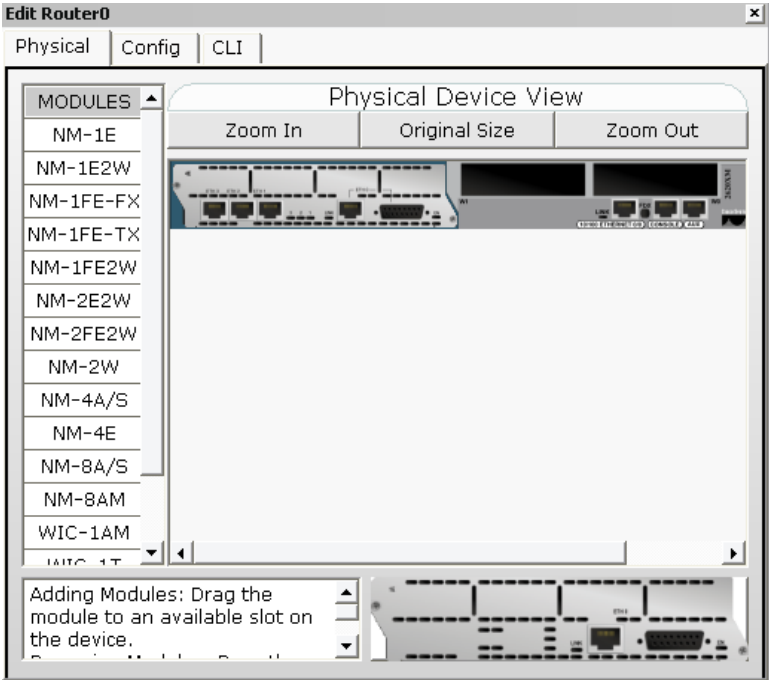


图 7 Router0 的 Physical 配置选项卡

Physical 选项卡用于添加端口模块，刚刚我们已经介绍过了，至于各模块的详细信息，大家可以参考帮助文件。

我们主要介绍一下 Config 选项卡和 CLI 选项卡。

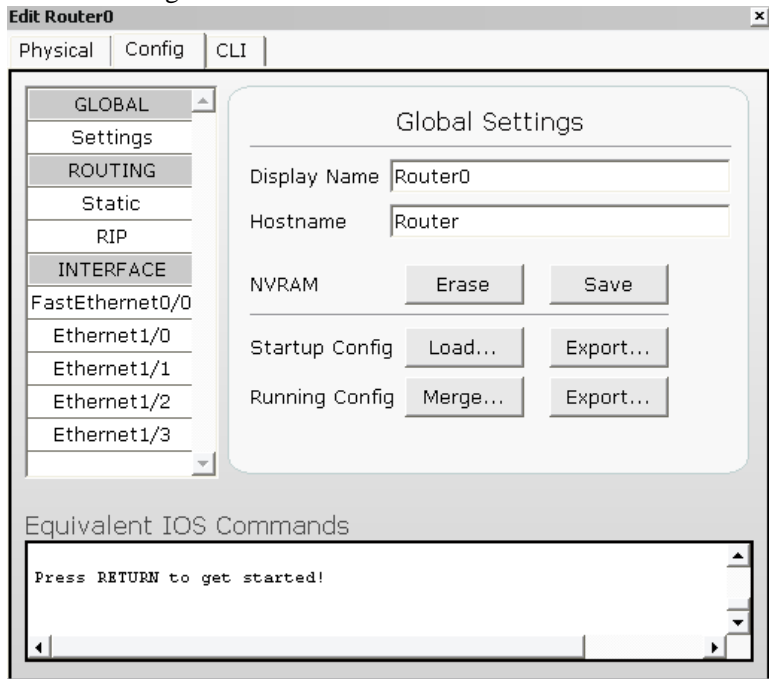


图 7 Router0 的 Config 和 CLI 配置选项卡

Config 选项卡给我们提供了简单配置路由器的图形化界面，在这里我们可以全局信息，路由信息和端口信息。当你进行某项配置时下面会显示相应的命令。这是 Packer Tracer

中的快速配置方式，主要用于简单配置，将注意力集中在配置项和参数上，实际设备中没有这样的方式。

对应的 CLI 选项卡则是在命令行模式下对 Router0 进行配置，这种模式和实际路由器的配置环境相似。

我们配置一下 FastEthernt 0/0 端口，如图所示：

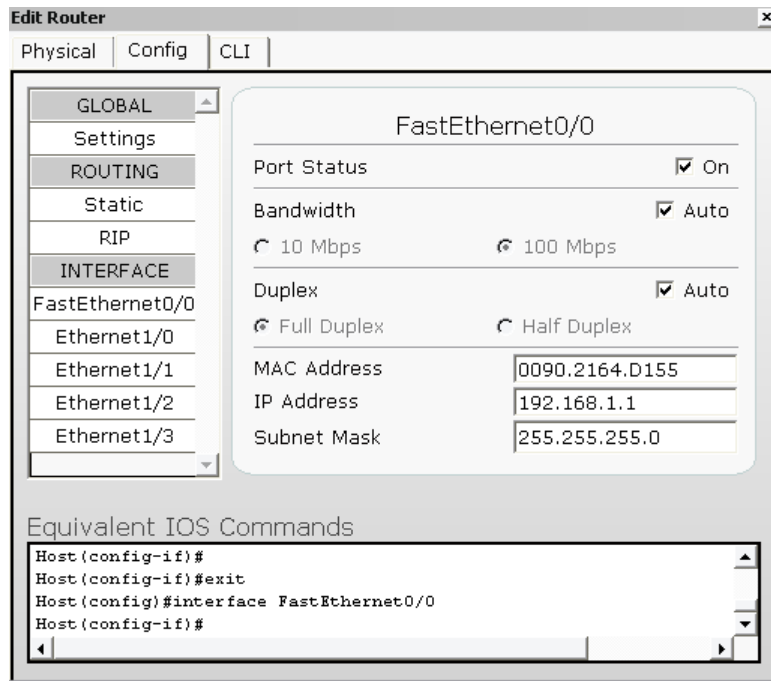


图 8 Config 选项卡中的端口配置

下面我们来看一下终端设备的配置，单击 PC0 打开配置对话框，在 Config 选项卡中配置默认网关和 IP 地址分别为 192.168.1.1，192.168.1.2 255.255.255.0

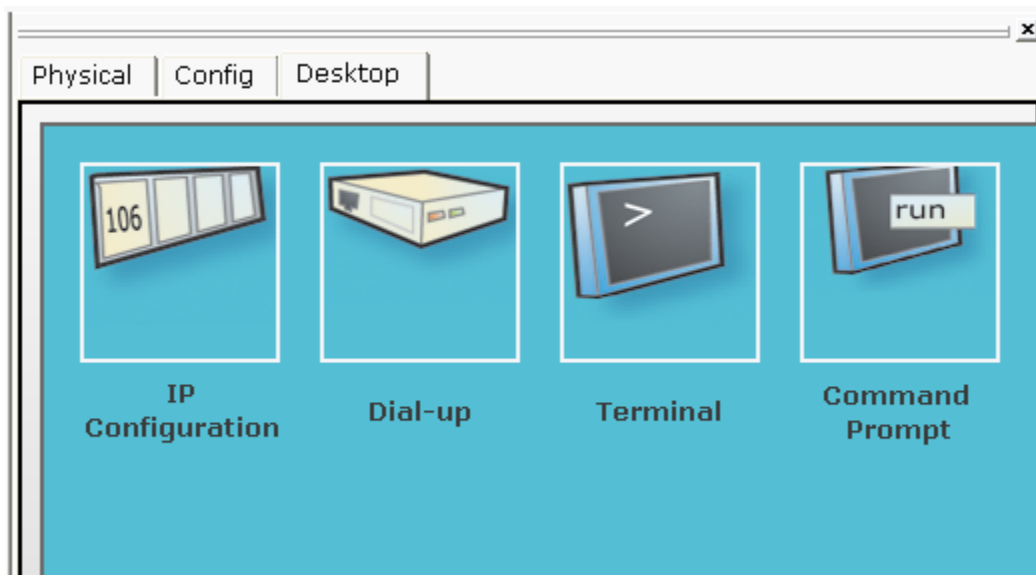


图 9 终端设备配置面板

Desktop 选项卡中的 IP Configuration 也可以完成默认网关和 IP 地址的设置。Terminal 选项模拟一个超级终端对路由器或者交换机进行配置。Command Prompt 相当于计算机中的命令窗口。

我们用相似的方法配置 Router0 上 Ethernet 1/0(192.168.2.1 255.255.255.0)和 PC1

(192.168.2.2 255.255.255.0 默认网关为 192.168.2.1)。
配置完成后我们发现所有的圆点已经变为闪烁的绿色。图 10：

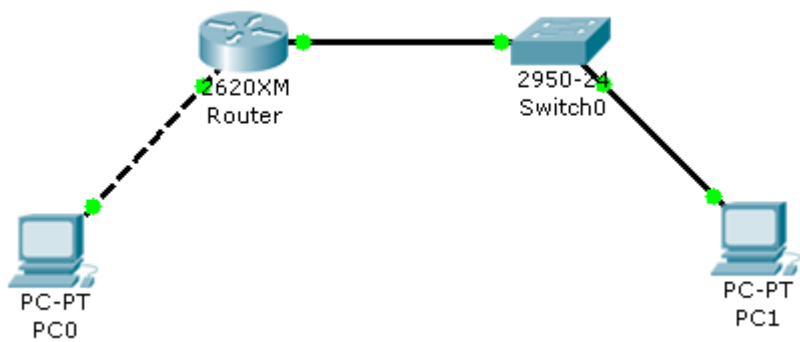


图 10

4、测试设备的连通性，并在 **simulation** 模式下跟踪数据包查看数据包的详细信息。
在 Realtime 模式下添加一个从 PC1——PC0 的简单数据包，结果如下图所示：

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete
	Successful	PC1	PC0	ICMP		0.000	N	0	(edit)	(delete)

图 11

Last Status 的状态是 Successful 说明 PC1 到 PC0 的链路是通的。
下面我们在 Simulation 模式下跟踪一下这个数据包，如图 12 所示：

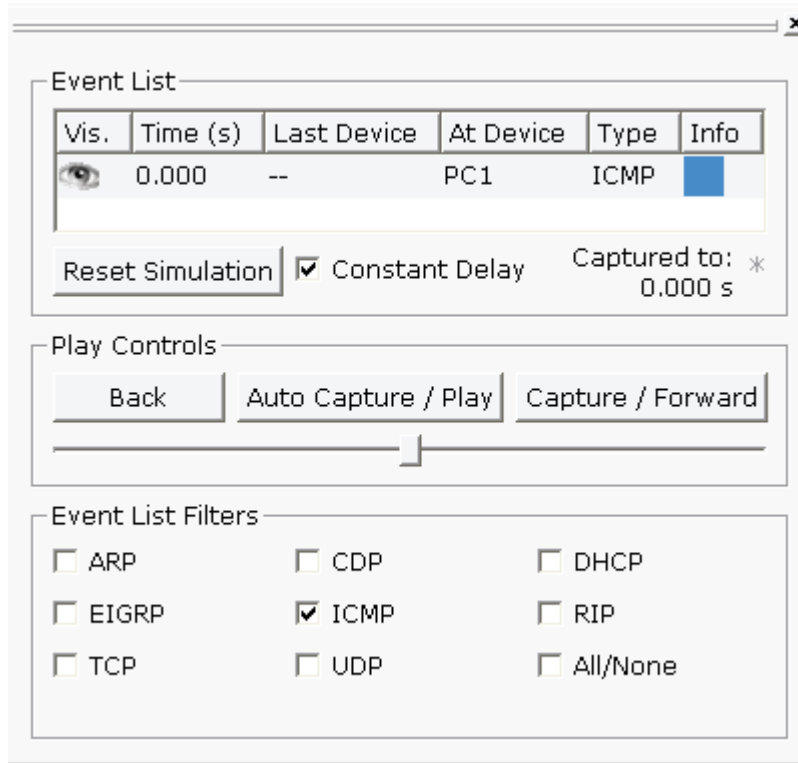


图 12

点击 Capture/Forward 会产生一系列的事件，这一系列的事件说明了数据包的传输路径。

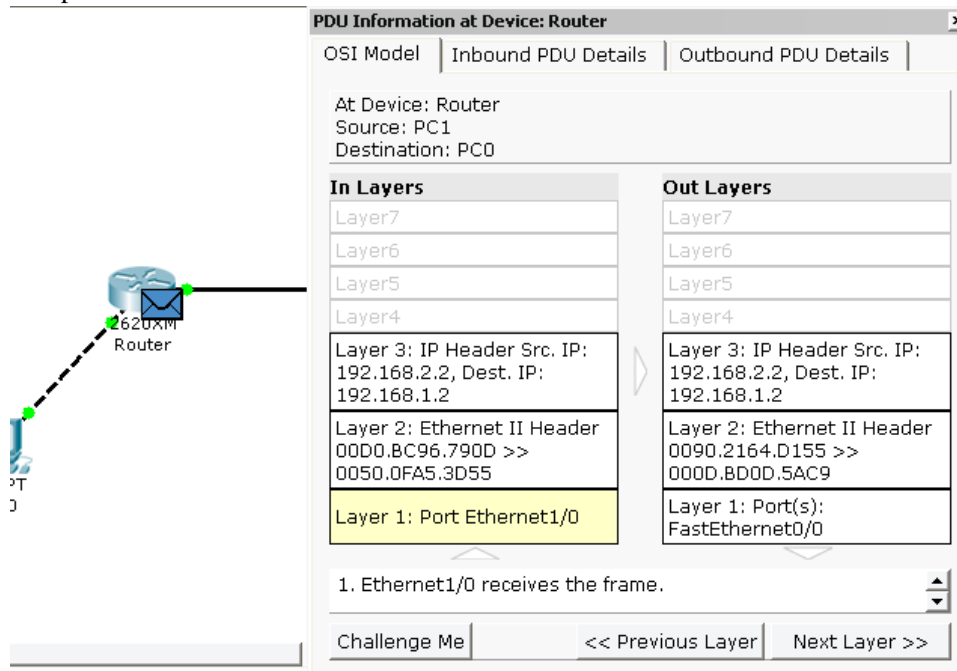


图 13

点击 Router0 上的数据包，可以打开 PDU Information 对话框，在这里我们可以看到数据包在进入设备和出设备时 OSI 模型上的变化，在 Inbound PDU Details 和 Outbound PDU Details 中我们可以看到数据包或帧格式的变化，这有助于我们对数据包做更细致的分析。

在这里我们简要介绍了以下使用 **Packet Tracer 4.0** 时进行的基本操作。大家可以在帮助文件中找到更详细的介绍。