[实验一 认识并熟悉计算机网络的硬件组成 2](#_Toc147825203)

[实验二 熟悉网络模拟软件的使用 7](#_Toc147825204)

[实验三 配置Cisco交换机 12](#_Toc147825205)

[实验四 配置VLAN 19](#_Toc147825206)

[实验五 CISCO路由器的配置 27](#_Toc147825207)

[实验六 配置静态路由 34](#_Toc147825208)

[实验七 配置动态路由RIP 38](#_Toc147825209)

[实验八 综合协议分析 42](#_Toc147825210)

# 实验一 认识并熟悉计算机网络的硬件组成

一、实验目的

认识PC硬件设备，网卡，网线，集线器，交换机，路由器等网络设备。

二、实验内容

1、 对PC机的认识。

2、认识网卡，了解网卡的基本构造，网卡与网线的连接，网卡的参数设置，各种网卡的数据传输率。网卡又叫做网络适配器，如图1-1所示，是连接计算机和网络硬件的设备, 它一般插在计算机的主板扩展槽中。它的标准是由IEEE来定义的。网卡工作于OSI的最低层，也就是物理层。网卡的类型不同，与之对应的网线或者其他网络设备也不同，不能盲目混合使用。软件工作于数据链路层，支持协议。

集成网卡和独立网卡的区别为：性质不同、CPU占用率不同、功能不同。

一、性质不同

1、集成网卡：集成网卡是集成在主板上的网络解码芯片。

2、独立网卡：独立网卡是作为扩展卡插到计算机总线上的。

二、CPU占用率不同

1、集成网卡：集成网卡的CPU占用率比独立网卡大，宽带分配更冗余。

2、独立网卡：独立网卡的CPU占用率比集成网卡小，宽带分配更合理。

三、功能不同

1、集成网卡：主板使用一块通过PCI (或者更新的PCI-Express总线)连接到主板上的集成网卡来集成以太网的功能。

2、独立网卡：独立网卡用于集成多接口或者使用其它种类的网络。

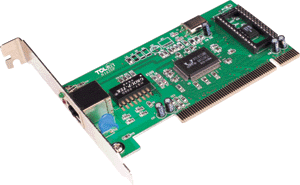


图1-1  网卡

网卡的工作原理为：整理计算机上要发往网线上的数据，并将数据分解为适当大小的数据包之后向网络上发送出去。每块网卡都有一个唯一的网络节点地址，它是网卡生产厂家在生产时烧入ROM中的，且保证唯一。网卡地址又称为MAC地址。

1. 认识网线（主要是双绞线）。双绞线是将一对或一对以上的双绞线封装在一个绝缘外套中而形成的一种传输介质(如图1-2所示)，是目前局域网最常用的一种布线材料。从图中我们可以看出双绞线中的每一对都是由两根绝缘铜导线相互缠绕而成的，这是为了降低信号的干扰程度而采取的措施。双绞线一般用于星型网络的布线连接，两端安装有RJ-45头(接口)，连接网卡与集线器，最大网线长度为100米，如果要加大网络的范围，在两段双绞线之间可安装中继器，最多可安装4个中继器，如安装4个中继器连5个网段，最大传输范围可达500米，网络中不能出现环路（10M以太网配置规则）。

http://www.long163.net/Article/UploadFiles/200511/20051102073505717.jpg

图1-2  双绞线

双绞线由8根铜导线组成，这8根铜导线的顺序分别橙白—1，橙—2，绿白—3，蓝—4，蓝白—5，绿—6，棕白—7，棕—8，如图1-3所示。10BASE-T和100BASE-TX规定，以太网上的各站点分别将1、2线作为自己的发送线，3、6线作为自己的接收线。



图1-3  双绞线的顺序

4、认识HUB。集线器(HUB)应用很广泛，它不仅使用于局域网、企业网、校园网，还可以使用于广域网。大多数小型局域网使用带有RJ-45接头的双绞线组成的星型局域网，这种网络经常要使用到集线器。集线器的功能就是分配带宽，将局域网内各自独立的计算机连接在一起并能互相通信，如图1-4所示。集线器用在物理层扩展以太网，进行多借口转发，不进行碰撞检测。分类，如图1-5所示。

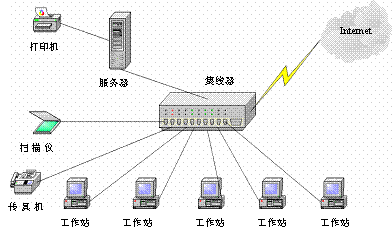


图1-4  集线器

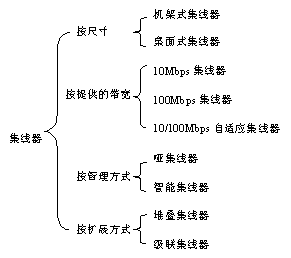


图1-5  集线器的分类

5、认识交换机。交换机也叫交换式集线器（多接口网桥），是局域网中的一种重要设备。它可将用户收到的数据包根据目的地址转发到相应的端口。它与一般集线器的不同之处是：集线器是将数据转发到所有的集线器端口，既同一网段的计算机共享固有的带宽，传输通过碰撞检测进行，同一网段计算机越多，传输碰撞也越多，传输速率会变慢；而交换机每个端口为固定带宽，有独特的传输方式，传输速率不受计算机台数增加影响，所以它更优秀。交换机的分类如图1-6所示。

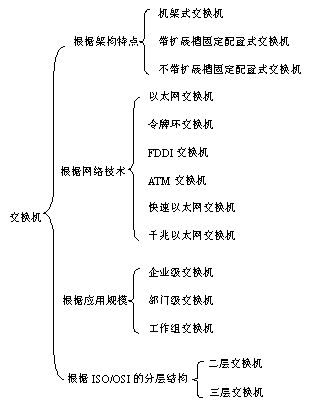


图1-6  交换机的分类

6、路由器的认识。路由器(Router)是一种多端口的网络设备，它能够连接多个不同网络或网段，并能将不同网络或网段之间的数据信息进行传输，从而构成一个更大的网络，如图1-8所示。从计算机网络模型角度来看，路由器的行为是发生在OSI的第3层(网络层)。路由器主要用于异种网络互联或多个子网互联。

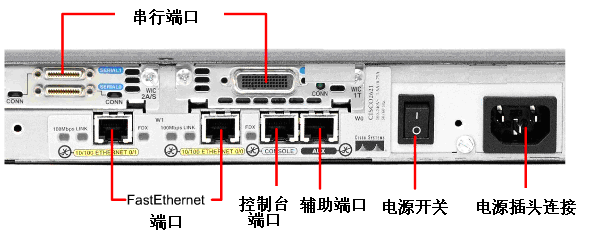


图1-7 路由器

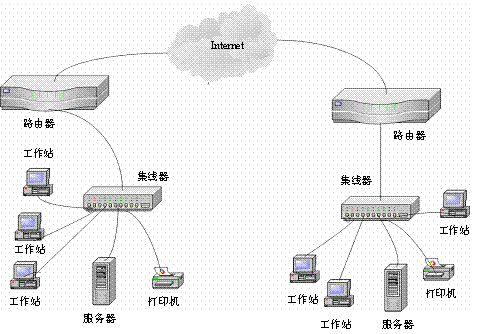


图1-8  由路由器构成的网络

三、实验报告要求

1.填写本人上机过程所调试程序的步骤和程序的执行结果，以及自己的实验体会和收获。

2.实验报告要自己独立填写完成，页面要工整，并注意保存好，按照教师规定日期准时提交，作为平时成绩的重要依据和期末考试的参考。

# 实验二 熟悉网络模拟软件的使用

一、实验目的

能够熟练使用网络模拟软件

二、实验内容

⒈熟悉界面

（1）设备的选择与连接

在界面的左下角一块区域，这里有许多种类的硬件设备，从左至右，从上到下依次为路由器、交换机、集线器、无线设备、设备之间的连线（Connections）、终端设备、仿真广域网、Custom Made Devices（自定义设备）下面着重讲一下“Connections”，用鼠标点一下它之后，在右边会出现各种类型的线，依次为Automatically Choose Connection Type（自动选线）、控制线、直通线、交叉线、光纤、电话线、同轴电缆、DCE、DTE。其中DCE和DTE是用于路由器之间的连线，实际当中需要把DCE和一台路由器相连，DTE和另一台设备相连。而在这里只需选一根就是了，若选了DCE这一根线，则和这根线先连的路由器为DCE，配置该路由器时需配置时钟。交叉线只在路由器和电脑直接相连，或交换机和交换机之间相连时才会用到。

注：Custom Made Devices设备是做什么的呢？通过实验发现用鼠标单击不放开左键把位于第一行的第一个设备也就是Router中的任意一个拖到工作区，然后再拖一个，尝试用串行线Serial DTE连接两个路由器时发现，他们之间是不会正常连接的，原因是这两个设备初始化时都是模块化的，但是没有添加，比如多个串口等等。那么，这个Custom Made Devices设备就比较好了，他会自动添加一些“必须设备的”，在实验环境下每次选择设备就不用手动添加所需设备了，使用起来很方便，除非想添加“用户自定义设备”里没有的设备再添加也不迟。

当需要用哪个设备的时候，先用鼠标单击一下它，然后在中央的工作区域点一下就OK了，或者直接用鼠标摁住这个设备把它拖上去。选中一种线，然后就在要连接的线的设备上点一下，选接口，再点另一设备，选接口就OK了。注意，接口不能乱选。连接好线后，可以把鼠标指针移到该连线上，就会出现线两端的接口类型和名称，配置的时候要用到它。

（2）、对设备进行编辑在右边有一个区域，如图2-1所示，从上到下依次为选定/取消、移动（总体移动，移动某一设备，直接拖动它就可以了）、Place Note（先选中）、删除、Inspect（选中后，在路由器、PC机上可看到各种表，如路由表等）、simple PPD、complex。

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

注意到软件界面的最右下角有两个切换模式，分别是Realtime mode(实时模式)和Simulation mode（模拟模式），实时模式顾名思意即时模式，也就是说是真实模式。举个例子，两台主机通过直通双绞线连接并将他们设为同一个网段，那么A主机PingB主机时，瞬间可以完成，对吗？这就是实时模式。而模拟模式呢，切换到模拟模式后主机A的CMD里将不会立即显示ICMP信息，而是软件正在模拟这个瞬间的过程，以人类能够理解的方式展现出来。

1)有趣的Flash动画。点击Auto Capture（自动捕获），那么直观、生动的Flash动画即显示了网络数据包的来龙去脉……这是该软件的一大闪光点，随后会举例详细介绍的。

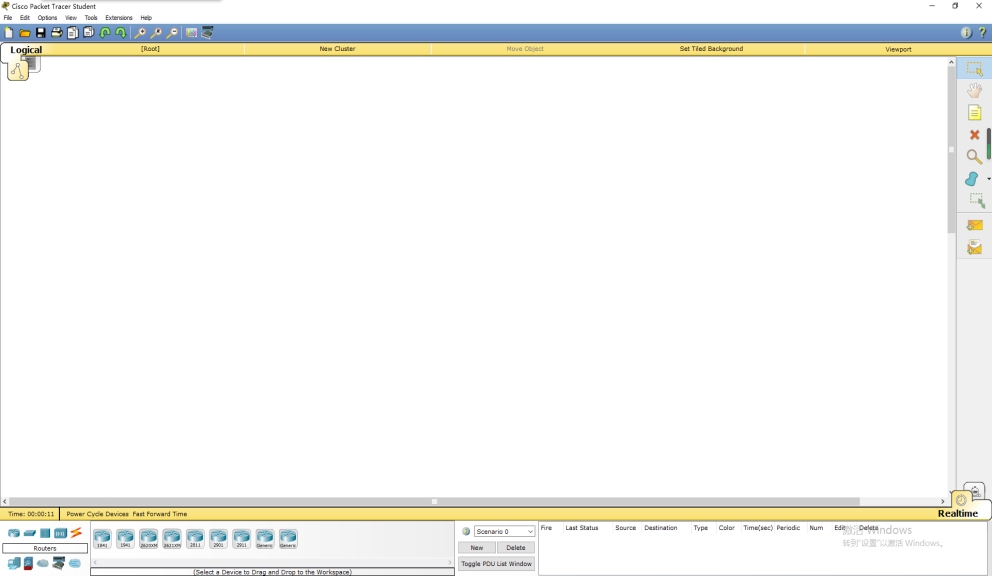


图2-1 设备编辑界面

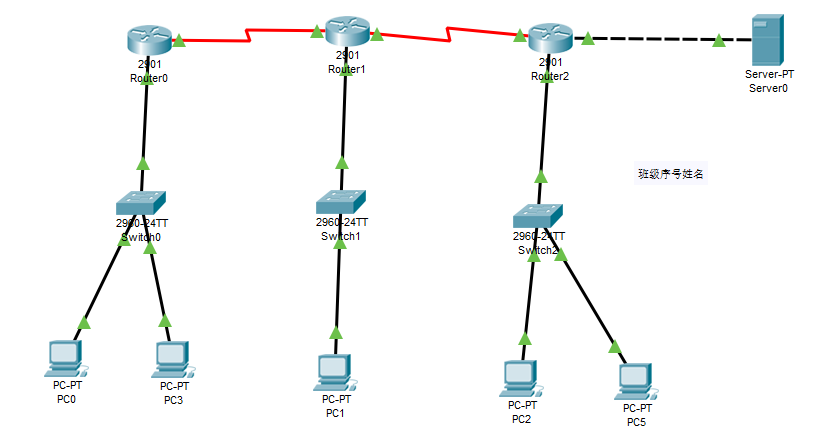


图2-2第一个拓扑图

2)单击Simulate mode会出现Event List对话框，该对话框显示当前捕获到的数据包的详细信息，包括持续时间、源设备、目的设备、协议类型和协议详细信息，非常直观！

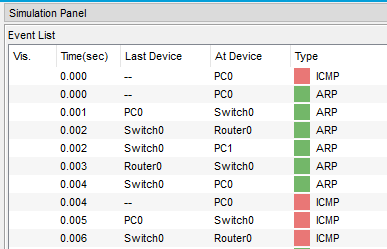


图2-3 Event List 对话框

3）要了解协议的详细信息，请单击显示不用颜色的协议类型信息Info，这个功能非常强大：很详细的OSI模型信息和各层PDU。

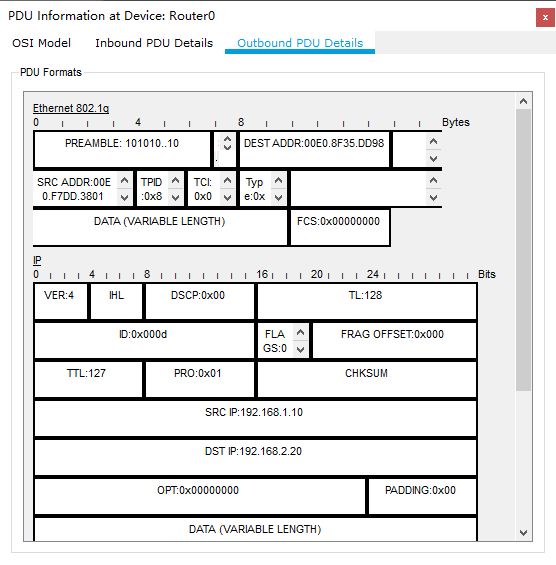


图2-4 PDU详情

⒉设备管理

Packet Tracer 5.0提供了很多典型的网络设备，它们有各自迥然不同的功能，管理界面和使用方式也不同。这里详细介绍一下PC机和路由器这两个设备的设备管理方法。

（1）、PC机

一般情况下，PC机不像路由器有CLI(command-line interface，命令行界面)，它只需要在图形界面下简单地配置一下就行了。一般通过Desktop选项卡下面的IP Configuation就行实现简单的IP地址、子网、网关和DNS的配置。此外还提供了拨号、终端、命令行（只能执行一般的网络命令）、Web浏览器和无线网络功能。如果要设置PC机自动获取IP地址，可以在Config选项卡里的Global Settings设置。

（2）、路由器

选好设备，连好线后就可以直接进行配置了，然而有些设备，如某些路由器需添加一些模块才能用。直接点一下设备，就进入了其属性配置界面。

有Physical、config、CLI三个选项，在Physical中，MODULES（模块）下有许多模块，最常用的有WIC-1T（WAN Interface Card）和WIC-2T。在最下面的左边是该对该模块的文字描述，最下面的右边是该模块的图。

在模块的右边是该路由器的图。可看它的上面有许多现成的接口，在图的矩形框中。也有许多空槽，图中用椭圆标出，在空槽上可添加模块，如WIC-1T，WIC-2T，用鼠标左键按住该模块不放，拖到想放的插槽中即可添加，不过这样肯定不会成功，因为还没有关闭电源。电源位置如图所示，就是带绿点的那个东西。绿色表示开，路由器默认情况下电源是开的。用鼠标点一下绿点那里，它就会关闭。添加模块后重新打开电源，这是路由器又重新启动了。如果你没有添加WIC-1T或WIC-2T这一模块，当使用DTE或DCE线连接两台路由器（Router PT除外）时，会发觉根本连不了，因为它还没有Serial 这一接口。

在Config中，可以设置路由器的显示名称、查看和配置路由协议与接口，会发现这里有Serial口了。CLI是命令行配置界面（也称现金行接口）——属于CCNA展现技能的舞台。

三、实验报告要求

1.填写本人上机过程所调试程序的步骤和程序的执行结果，以及自己的实验体会和收获。

2.实验报告要自己独立填写完成，字迹要工整，并注意保存好，按照教师规定日期准时提交，作为平时成绩的重要依据和期末考试的参考。

# 实验三 配置Cisco交换机

一、实验目的

熟悉IOS命令及相关的知识

二、实验内容

（1）、几种配置命令模式

switch>这种提示符表示是在用户命令模式，只能使用一些查看命令。

switch#这种提示符表示是在特权命令模式。

switch(config)#这种提示符表示是全局配置模式

switch(config-if)#端口配置命令模式

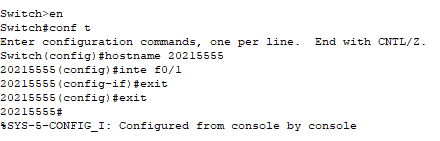


图3-1几种命令模式

（2）、检查、查看命令

这些命令是查看当前配置状况，通常是以show(sh)为开始的命令。Show version查看IOS的版本、show flash查看flash内存使用状况、show mac-address-table查看MAC地址列表。

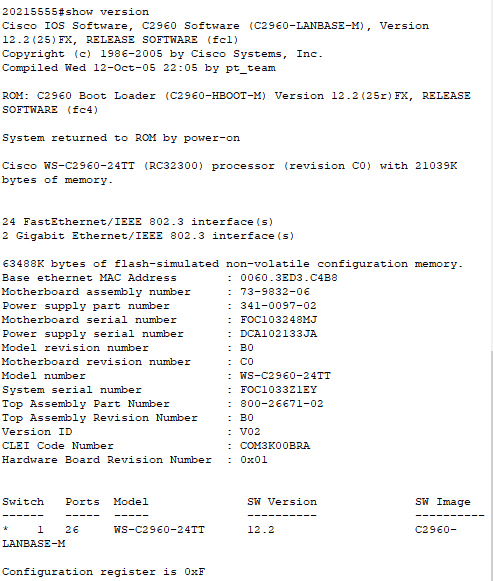


图3-2 检查、查看版本

![C:\Users\Administrator\AppData\Roaming\Tencent\Users\5651643\QQ\WinTemp\RichOle\I{C5J($]DO](~8]81[9M%E3.png](data:image/png;base64,)

图3-3检查、查看flash

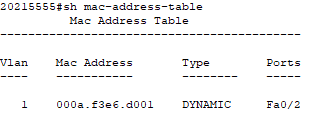


图3-4 查看MAC地址

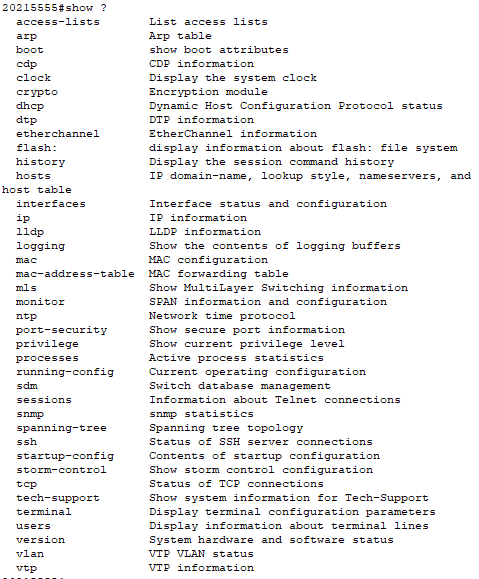


图3-5 Show ?帮助命令显示当前所有的查看命令

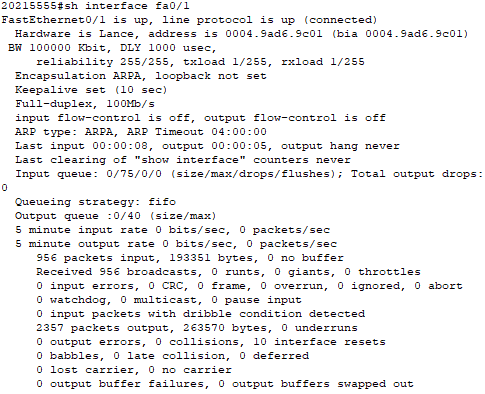


图3-6 查看端口状态信息

（3）、密码设置命令

Cisco交换机、路由器中有很多密码，设置好这些密码可以有效地提高设备的安全性。

switch(config)#enable password设置进入特权模式进的密码

switch(config-line)#可以设置通过console端口连接设备及telnet远程登录时所需要的密码

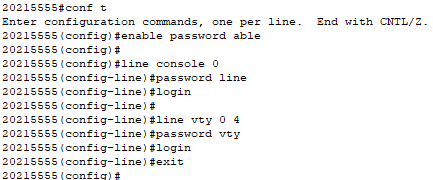


图3-7 设置交换机的各种密码

C:\Users\Administrator\AppData\Roaming\Tencent\Users\5651643\QQ\WinTemp\RichOle\(~FZVR{Q]}UP4BU8ENSRD}E.png默认情况下，这些密码都是以明文的形式存储，所以很容易查看到。为了避免这种情况，我们可以以密文的形式存储各种密码:service password-encryption

图3-8 密文密码

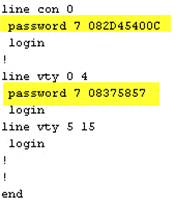


图3-9 密码以密文的形式存储

（4）、配置IP地址及默认网关

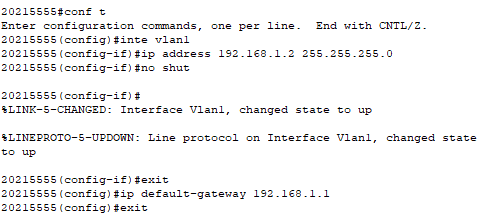


图3-10 配置IP及默认网关

（5）、管理MAC地址表

switch#show mac-address-table显示MAC地址列表

switch#clear mac-address-table dynamic清除动态MAC地址列表

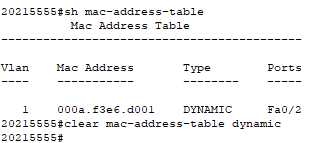


图3-11 显示MAC地址

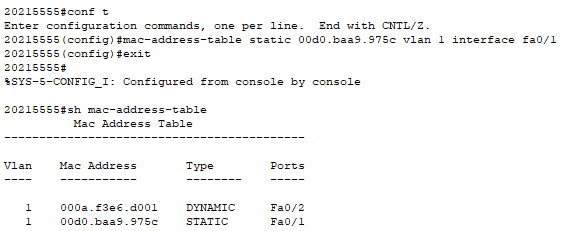


图3-12 设置静态MAC地址

（6）、配置端口安全

switch(config-if)switchport port-security

在此我们通过输入最基本的命令来配置端口安全，接受了只答应一个MAC地址的默认设置，这就决定了只有第一个设备的MAC地址可以与这个端口通信；假如另一MAC地址试图通过此端口通信，交换机会关闭此端口。

假如用户有一个4端口的集线器连接到交换机的此端口，就需要4个MAC：switchport port-security maximum 4 /答应此端口通过的最大MAC地址数目为4。

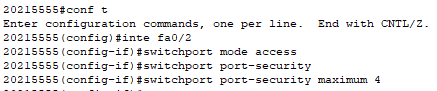


图3-13 端口通过的最大MAC地址数为4

switchport port-security violation [protect|restrict|shutdown]:此命令告诉交换机当端口上MAC地址数超过了最大数量之后交换机应该怎么做，一共三个参数：protect，restrict和shutdown，默认是关闭端口(shutdown)。我们可以选择使用restrict来警告网络管理员，也可以选择protect来答应通过安全端口通信并丢弃来自其它MAC地址的数据包。

C:\Users\Administrator\AppData\Roaming\Tencent\Users\5651643\QQ\WinTemp\RichOle\@PJ$R0UO(QRW7E}(7J9JD~H.png

图3-14 关闭端口

（7）、实例拓扑图

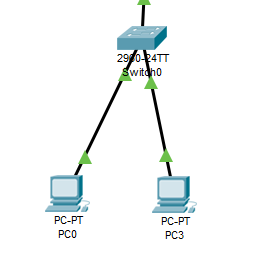


图3-15 实例拓扑图\*

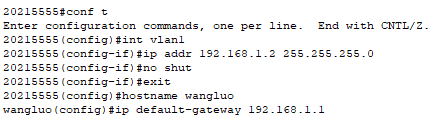


图3-16 配置实例中的交换机fa0/1端口

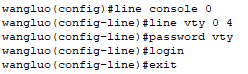


图3-17 配置密码

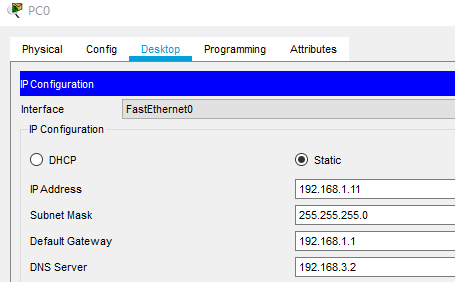


图3-18 PC0的配置

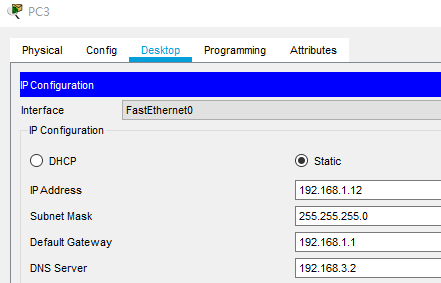


图3-19 PC3的配置

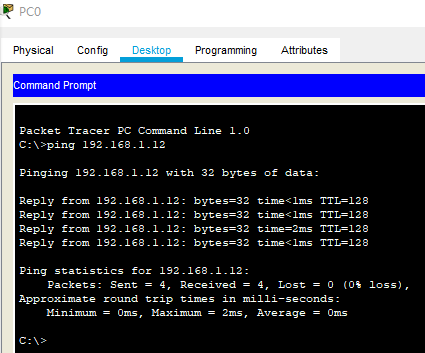


图3-20 测试局域网连通状况\*

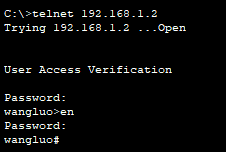


图3-21 实现对交换机的远程管理\*

三、填写实验报告要求

1. 记录本人上机过程所调试程序的步骤和程序的执行结果，以及自己的实验体会和收获。

2. 实验报告要自己独立完成，并注意保存好，按照教师规定日期准时提交，作为平时成绩的重要依据和期末考试的参考。

# 实验四 配置VLAN

一、实验目的

1．掌握VLAN的基本概念和原理

2．掌握VLAN配置与管理方法

二、实验内容

1.配置VLAN

（1）、实例拓扑图

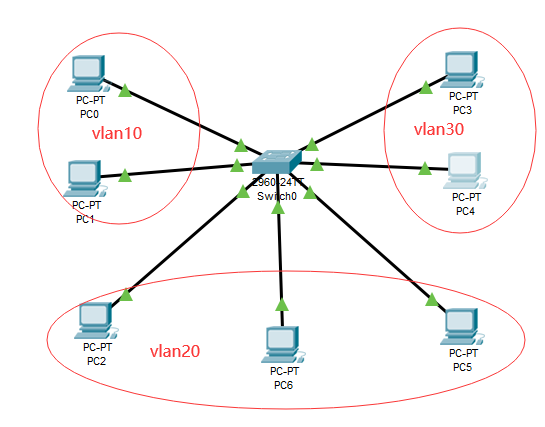


图4-1 划分vlan\*

（2）、创建VLAN

在Cisco IOS中有两种方式创建vlan，在全局配置模式下使用vlan vlanid命令，如switch(config)#vlan 10；在vlan database下创建vlan，如switch(vlan)#vlan 20。

0,4095：保留，仅限系统使用。用户不能查看。

　1：CISCO默认VLAN，不能删除。

　2－1001：用于以太网的VLAN，用户可自己创建的VLAN

　1002－1005：用于FDDI和令牌环的默认VLAN，不能删除。

　1006－1024：保留，仅限系统使用。用户不能查看。

　1025－4094：仅用于以太网的VLAN. 扩展的VLAN，只有3550以上的交换机才能配，且必须将VTP模式设为透明模式。

（3）、把端口划分给vlan(基于端口的vlan)

switch(config)#interface fastethernet0/1进入端口配置模式

switch(config-if)#switchport mode access配置端口为access模式

switch(config-if)#switchport access vlan 10把端口划分到vlan 10

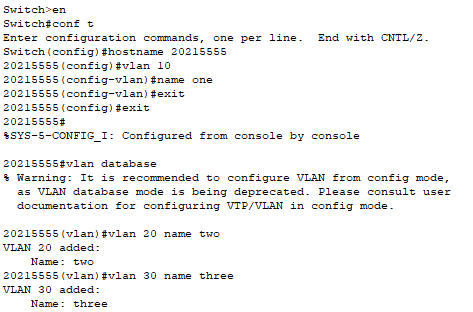


图4-2 创建vlan

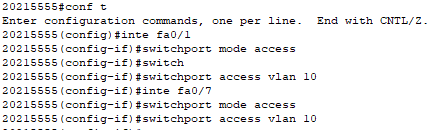


图4-3 端口划分

如果一次把多个端口划分给某个vlan可以使用interface range命令。

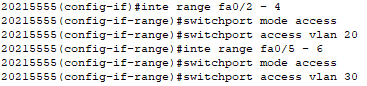


图4-4 多个端口划分

（4）、查看vlan信息

switch#show vlan

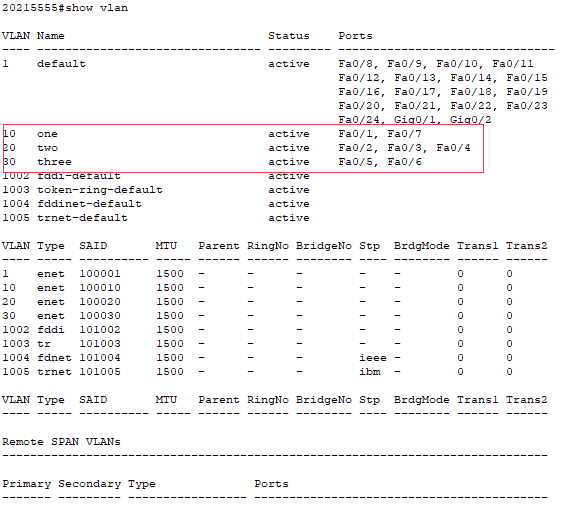


图4-5 show VLAN\*

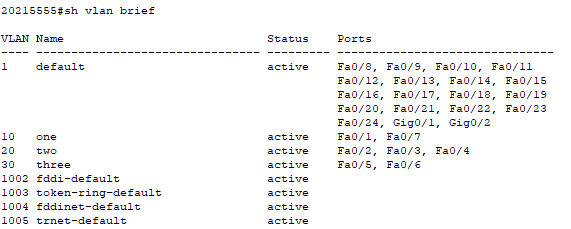


图4-6 查看vlan简明信息

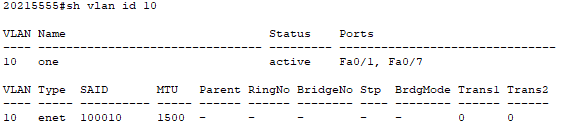


图4-7 查看id为10的vlan

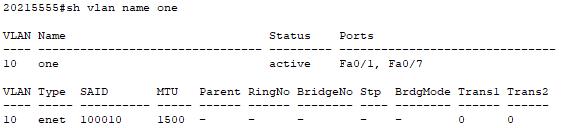


图4-8 通过vlan的名字查看vlan

（5）、删除配置

先删端口后删模块。

C:\Users\Administrator\AppData\Roaming\Tencent\Users\5651643\QQ\WinTemp\RichOle\A]JT]2B]V9%1{6HXV{C`[5Y.png

图4-9 把第0个模块中的第9个端口从vlan 50中删除

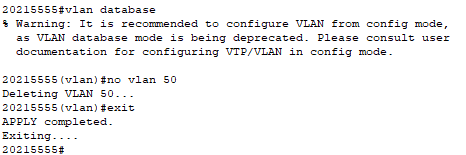


图4-10 删除vlan 50

（6）、PC配置

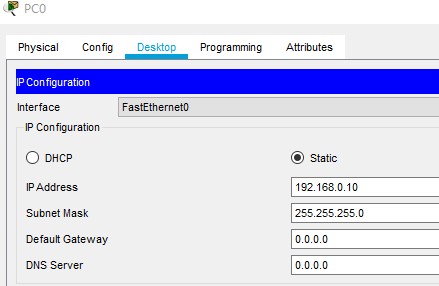


图4-11 PC参数

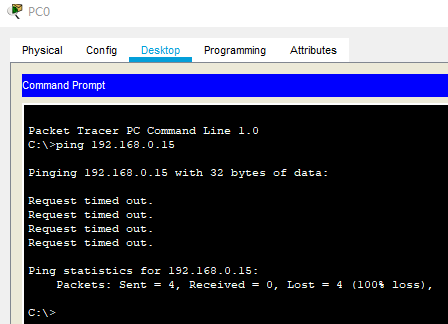


图4-12 测试不同vlan间的隔离通信\*

2. 路由器实现Vlan间通信

（1）、实例拓扑图

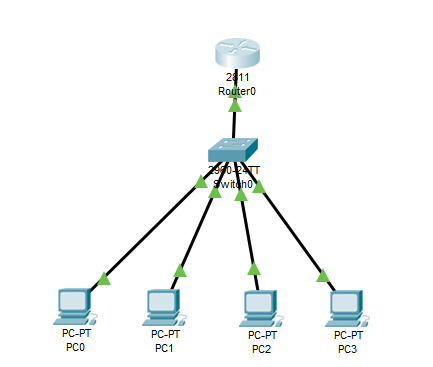


图4-13 路由器：Cisco 2811，交换机：Cisco 2960\*

（1）、创建Vlan

switch#vlan databae

switch (vlan)#vlan 10 name one

switch (vlan)#vlan 20 name two

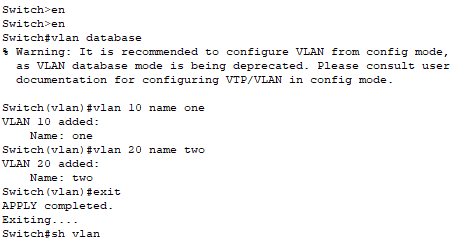


图4-14 创建VLAN

（2）、把交换机端口分配给Vlan

switch #conf t

switch (config)#int range fa0/2 – 3

switch (config-if-range)#switchport mode access

switch (config-if-range)#switchport access vlan 10

switch (config-if-range)#int range fa0/4 – 5

switch (config-if-range)#switchport mode access

switch (config-if-range)#switchport access vlan 20

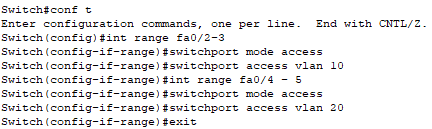


图4-15 分配端口

（3）、配置交换机trunk端口

使用Trunk可以使一条物理链路上可以传送多个VLAN数据，Trunk使用特殊的标识来区分不同的VLAN，帧标记（tag）。

switch(config)#int fa0/1

switch(config-if)#switchport mode trunk

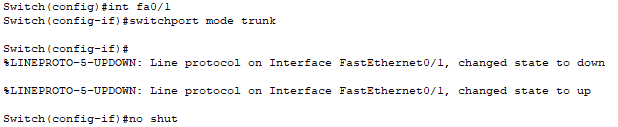


图4-16 端口trunk模式

（4）、配置路由器子接口

Router#conf t

Router(config)#int fa0/0.1

Router(config-subif)#encapsulation dot1q 10

Router(config-subif)#ip address 192.168.1.1 255.255.255.0

Router(config-subif)#int fa0/0.2

Router(config-subif)#encapsulation dot1q 20

Router(config-subif)#ip address 192.168.2.1 255.255.255.0

Router(config-subif)#int fa0/0

Router(config-if)#no shut

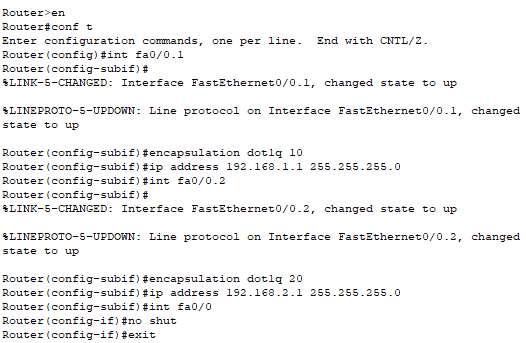


图4-17 端口封装

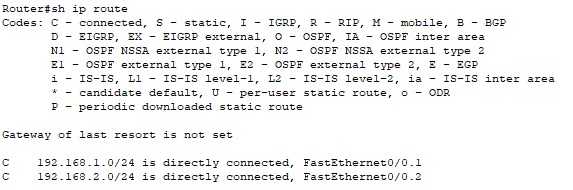


图4-18 查看路由器中的路由表\*

（5）、配置计算机，测试

在本次实验中，pc0与pc1同处于vlan 10 网段192.168.1.1；pc2与pc3同处于Vlan 20 网段192.168.2.1。

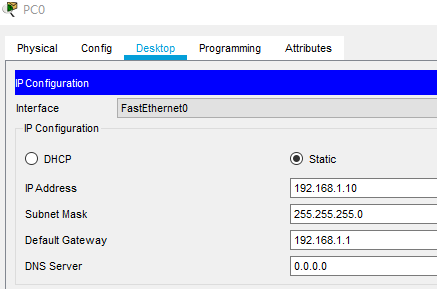


图4-19 PC0参数设置

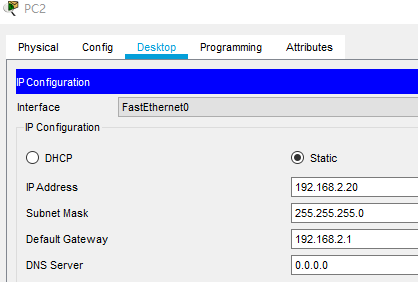


图4-20 PC2参数设置

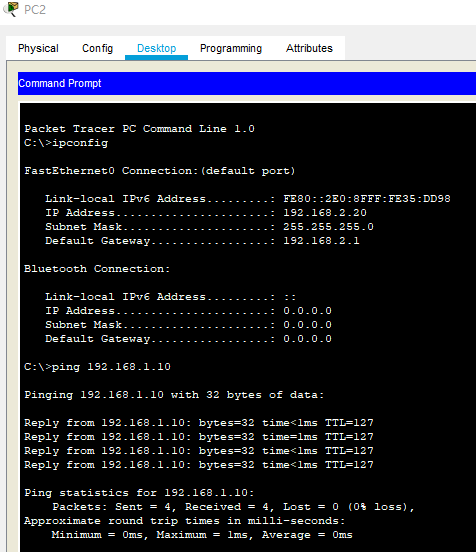


图4-21 不同网段中的计算机完全可以ping 通\*

三、填写实验报告要求

1. 记录本人上机过程所调试程序的步骤和程序的执行结果，以及自己的实验体会和收获。

2. 实验报告要自己独立完成，并注意保存好，按照教师规定日期准时提交，作为平时成绩的重要依据和期末考试的参考。

# 实验五 CISCO路由器的配置

一、实验目的

了解思科网络设备的配置基本特点及IOS命令基本操作方法

二、实验内容

（1）、实验环境搭建

添加一个模块化的路由器，单击Packet Tracer 5.0的工作区中刚添加的路由器，在弹出的配置窗口上添加一些模块：

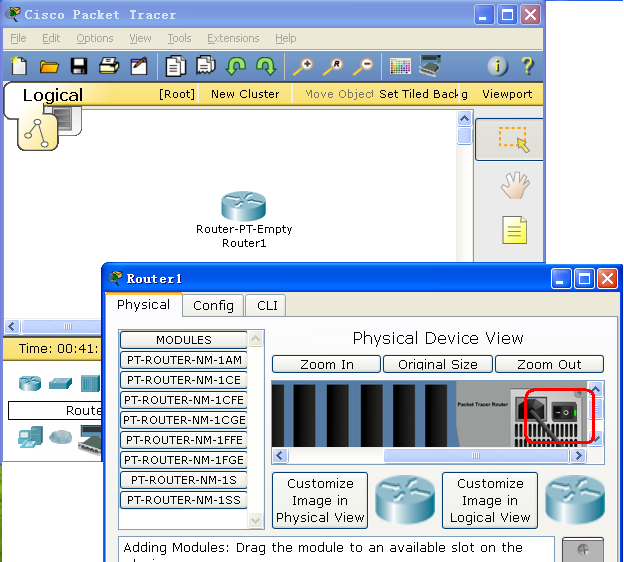


图5-1 路由器

默认情况下，路由器的电源是打开的，添加模块时需要关闭路由器的电源，单击图5-1箭头所指的电源开关，将其关闭，路由器的电源关闭后绿色的电源指示灯也将变暗。

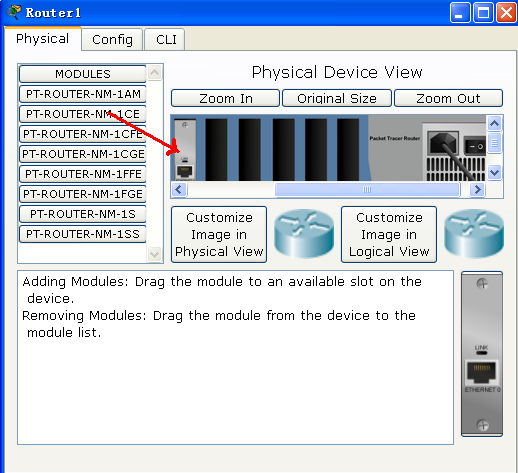


图5-2 添加所需要的模块

在“MODULES”下寻找所需要的模块，选中某个模块时会在下方显示该模块的信息。然后拖到路由器的空插槽上即可。

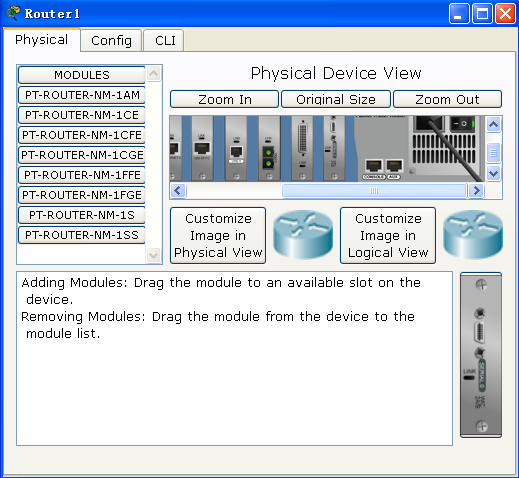


图5-3 各种模块添加完成，打开路由器的电源

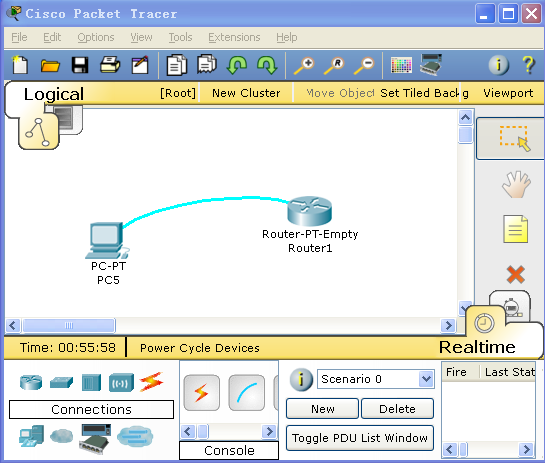


图5-4 添加一计算机，其RS-232与路由器的Console端口相连

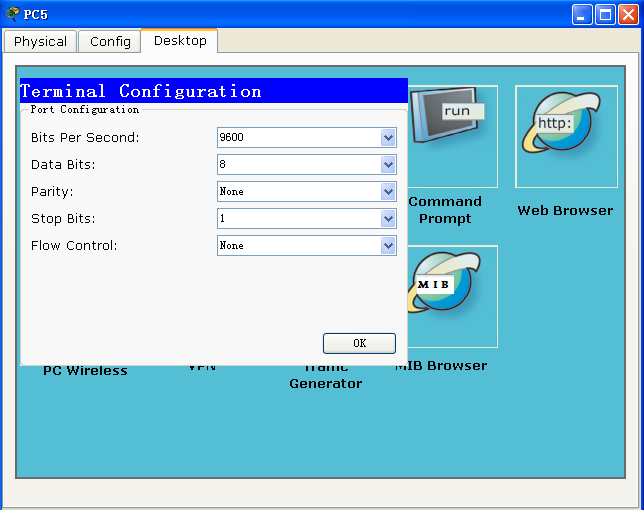


图5-5 用计算机的终端连接路由器

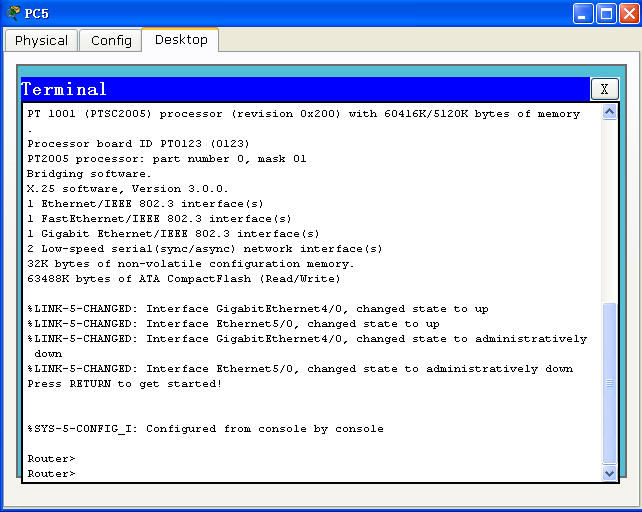


图5-6 实验环境搭建完成

（2）、配置单个的路由器

路由器的几种模式：User mode(用户模式)、Privileged mode（特权模式）、Global configuration mode(全局配置模式)、Interface mode(接口配置模式)、Subinterface mode(子接口配置模式)、Line mode、Router configuration mode（路由配置模式）。每种模式对应不同的提示符。

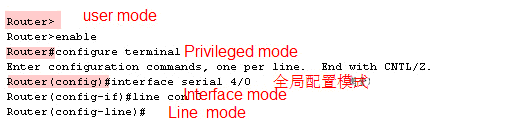


图5-7 几各配置命令提示符

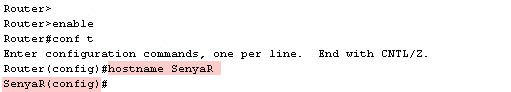


图5-8 配置路由器的名字

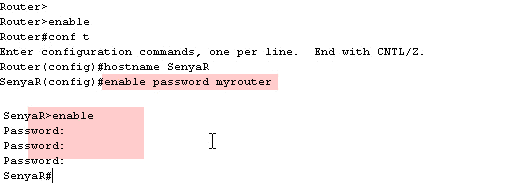


图5-9 配置enable密码

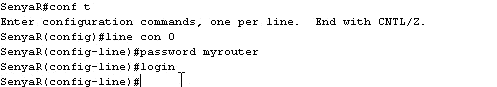


图5-10 配置Console登录时的密码

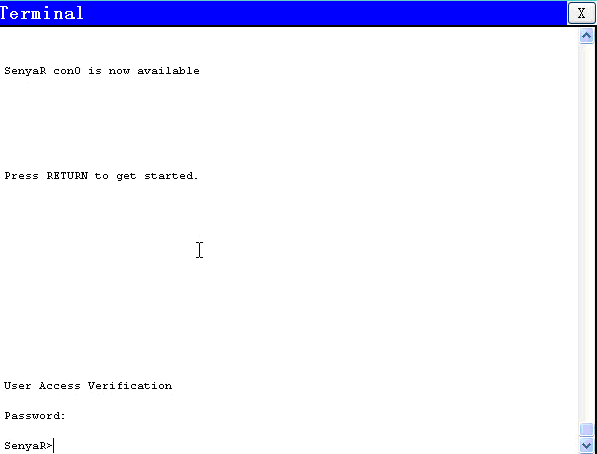


图5-11 通过Console端口登录到路由器需要输入密码

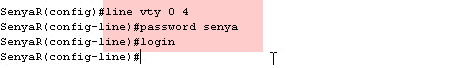


图5-12 配置终端登录方式的密码

默认情况下路由器中的各种密码以明文形式保存。在全局配置模式下使用service password-encryption命令加密口令。

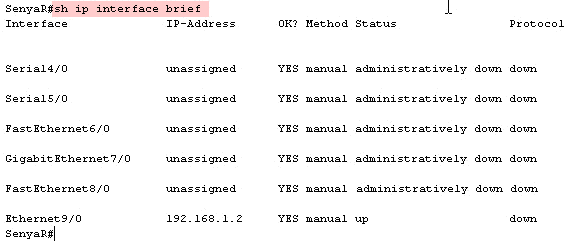


图5-13 查看路由器接口的IP配置信息

首先要明白接口名称表示方式：接口类型 接口数字标识/插槽数字标识，如Serial 4/0表示该接口为串口，第一个插槽的第4个接口。插槽的数字标识是从零开始的。

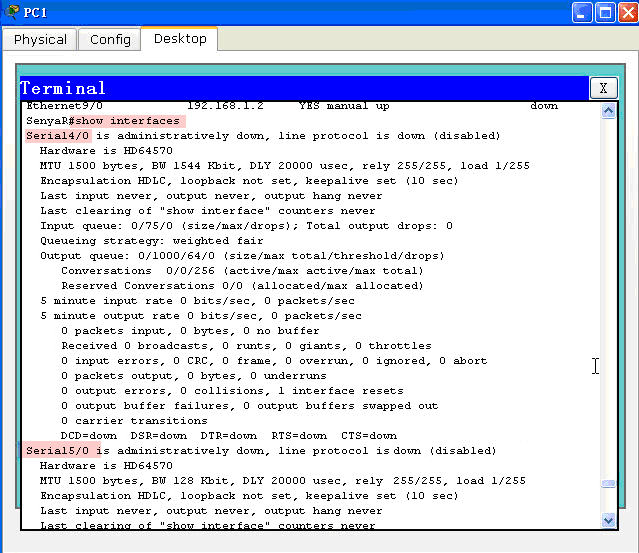


图5-14 显示所有接口的详细信息

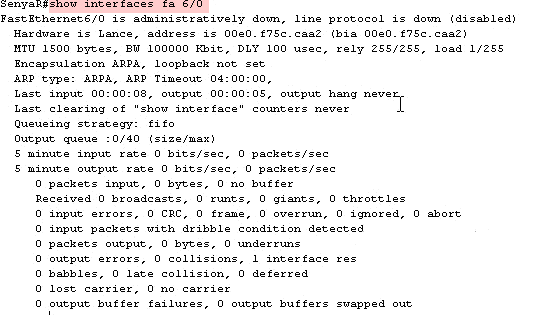


图5-15 显示某个指定端口的详细信息



图5-16 配置登录时的欢迎信息

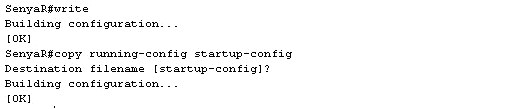


图5-17 保存配置信息

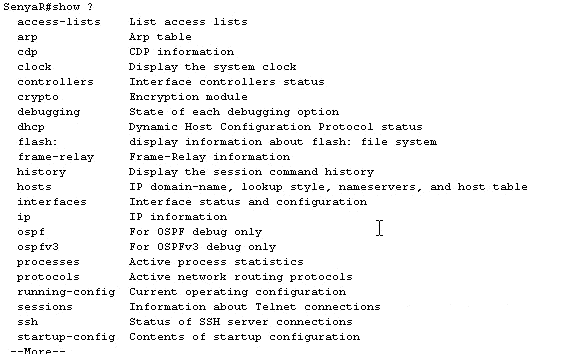


图5-18 各显示显示信息的命令

思科的IOS命令非常庞大，不同的硬件，不同的版本，它们的命令是不同的。只有多练习才能掌握。

三、填写实验报告要求

1. 记录本人上机过程所调试程序的步骤和程序的执行结果，以及自己的实验体会和收获。

2. 实验报告要自己独立完成，并注意保存好，按照教师规定日期准时提交，作为平时成绩的重要依据和期末考试的参考。

# 实验六 配置静态路由

一、实验目的

掌握静态路由配制方法。静态路由是非自适应性路由计算协议，是由管理人员手动配置的，不能够根据网络拓扑的变化而改变。因此，静态路由非常简单，适用于非常简单的网络。

二、实验内容

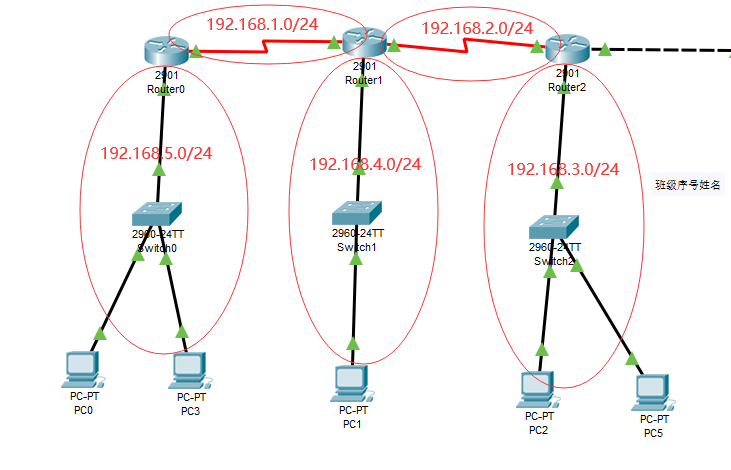


图6-1 拓扑图\*

网络拓扑图说明：路由器的串口是背对背的直接连接，因此，有一个串口要配置时钟速率，使用clock rate命令进行配置，配置时钟速率的一串口为DCE端。

（１）、基本配置

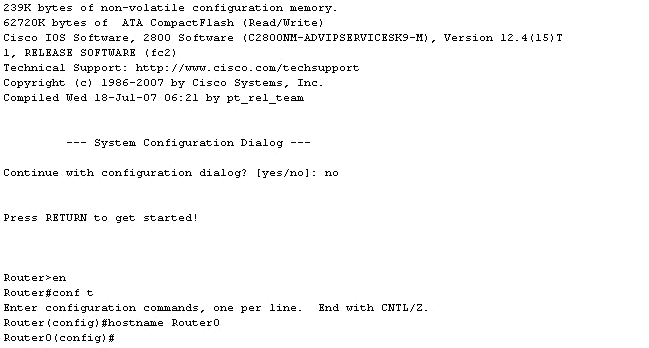


图6-2 配置路由器、交换机的名字

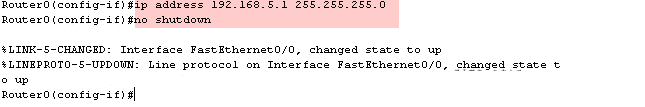


图6-3 配置路由器FastEthernet接口IP地址

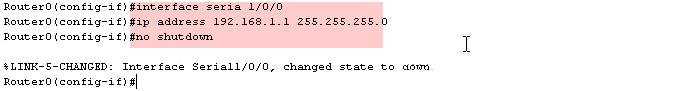


图6-4 配置路由器Serial口ip地址



图6-5 设置串口时钟速率(DCE)

由于实验环境中的路由器是背对背连接（直接连接）因此把两个背对背连接的串口其中一个设置为DCE。

（２）、配置各个路由器上的静态路由

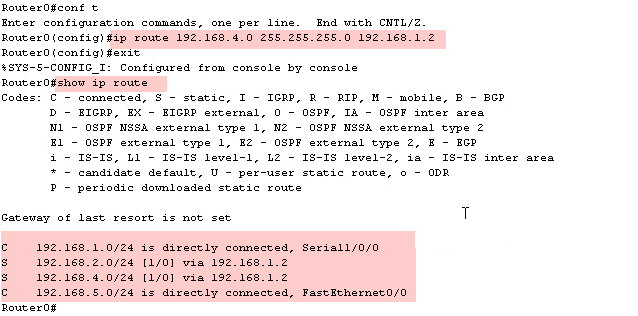


图6-6 配置Router0的静态路由，并查看路由表\*



图6-7 删除一条静态路由表

图6-8 配置默认路由

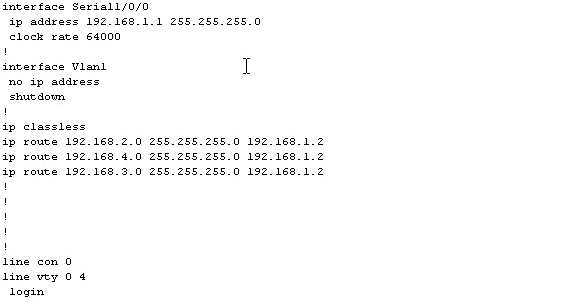


图6-9 本实验环境中Router0的静态路由配置



图6-10 本实验环境中Router１的静态路由配置



图6-11 本实验环境中Router３的默认路由配置

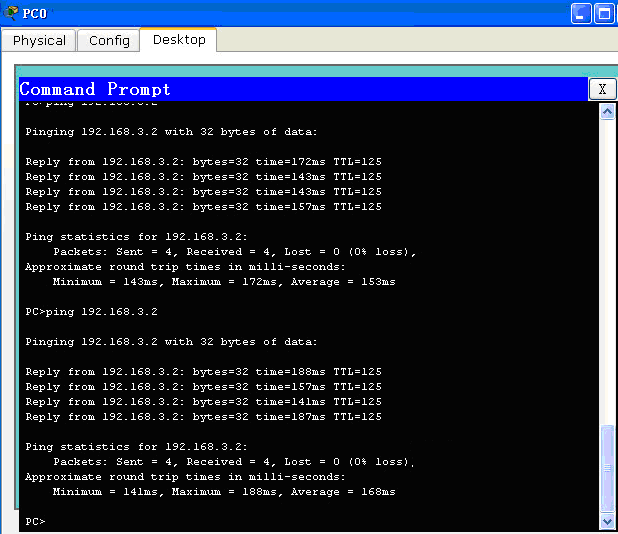


图6-12 PC0 ping通 PC5，验证配置\*

虽然说静态路由简单，不常使用，随着互联网用户、计算机的增加，路由表越来越庞大，配置默认路由往往也很重要。

三、填写实验报告要求

1. 记录本人上机过程所调试程序的步骤和程序的执行结果，以及自己的实验体会和收获。

2. 实验报告要自己独立完成，并注意保存好，按照教师规定日期准时提交，作为平时成绩的重要依据和期末考试的参考。

# 实验七 配置动态路由RIP

一、实验目的

掌握动态路由配置方法。动态路由协议采用自适应路由算法，能够根据网络拓扑的变化而重新计算机最佳路由。由于路由的复杂性，路由算法也是分层次的，通常把路由协议（算法）划分为自治系统(AS)内的(IGP,Interior Gateway Protocol)与自治系统之间(EGP,External Gateway Protocol)的路由协议。

RIP的全称是Routing Information Protocol，是IGP，采用Bellman-Ford算法。RFC1058是RIP version 1标准文件，RFC2453是RIP Version 2的标准文档。

二、实验内容

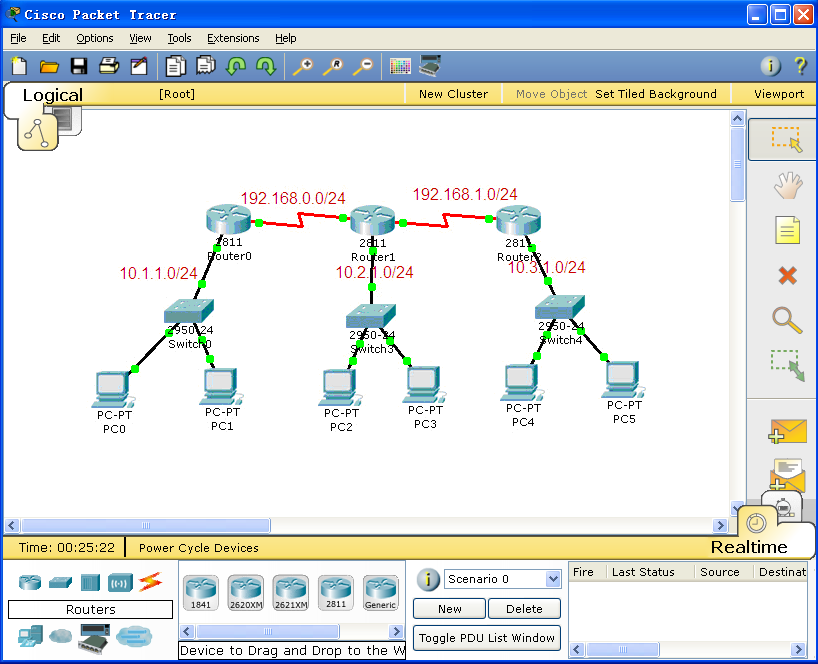


图7-1 拓扑图\*

实验环境中各个网段与路由器接口IP地址分配如上图所示。

RIP协议基本配置命令：

Router(config)#ip classless　让路由器支持无类编址，RIPv1是不支持无类IP编址的。

Router(config)#router rip

Router(config-router)#network w.x.y.z

可选的配置命令：

Router(config)#no router rip在路由器上关闭RIP协议

Router(config-router)#no network w.x.y.z从RIP协议中移除w.x.y.z网络

Router(config-router)#version 2RIP协议为第2版

Router(config-if)#ip rip send version 2该接口仅发送RIP ver 2报文

Router(config-if)#ip rip send version 1该接口仅发送RIP ver 1报文

Router(conifg-if)#ip rip send version 1 2该接口发送RIP ver 1报文和RIP ver 2报文

Router(config-if)#ip rip receive version 2该接口仅接收RIP ver 2报文

Router(config-router)#no auto-summary关闭路由协议的自动聚合功能

Router(config-router)#ip split-horizon配置水平分割，水平分割（split horizon）是一种避免路由环路的出现和加快路由汇聚的技术。由于路由器可能收到它自己发送的路由信息，而这种信息是无用的，水平分割技术不反向通告任何从终端收到的路由更新信息，而只通告那些不会由于计数到无穷而清除的路由。路由器从某个接口接收到的更新信息不允许再从这个接口发回去



图7-2 水平分割

首先根据实验需要配置好PC机及路由器各个接口的IP地址等参数。

（１）、三个路由器的基本配置

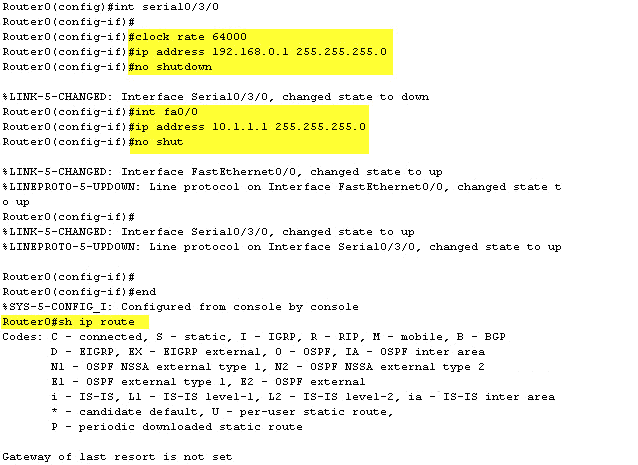


图7-3 基本配置

基本配置主要是配置路由器的名字，安全密码，各个端口的IP地址等。仅一个路由器配置为例，其余的路由器与该路由器配置相似。

（2）、RIP路由协议配置

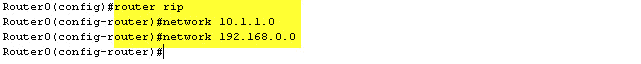


图7-4 配置RIP

Router0的配置；10.0.0.0是A类网络，前8bits是网络ID，在配置时应该是netwok 10.0.0.0

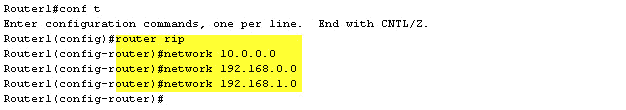


图7-5 Router1的配置

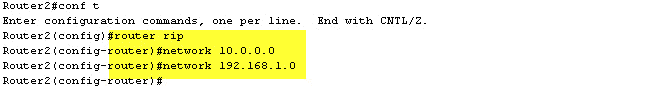


图7-6 Rotuer2的配置

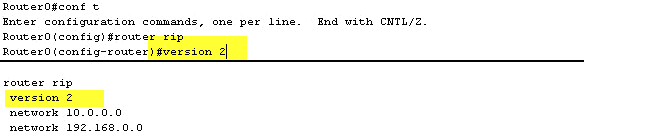


图7-7 给每个路由器RIP协议启用第二版

（3）、RIP路由协议的诊断与排错

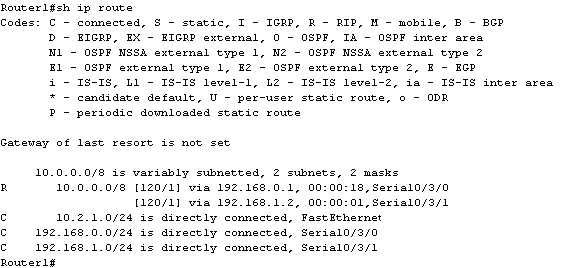


图7-8 查看路由表show ip route\*

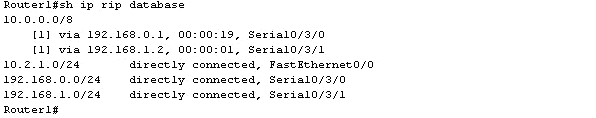


图7-9 show ip rip database

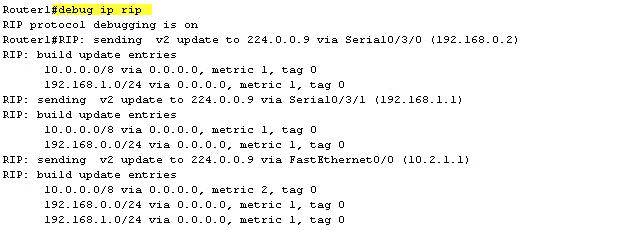
.

图7-10 debug ip rip开启RIP诊断，no debug ip rip 关闭RIP诊断

（4）、使用计算机不同网段互ping检查网络连通

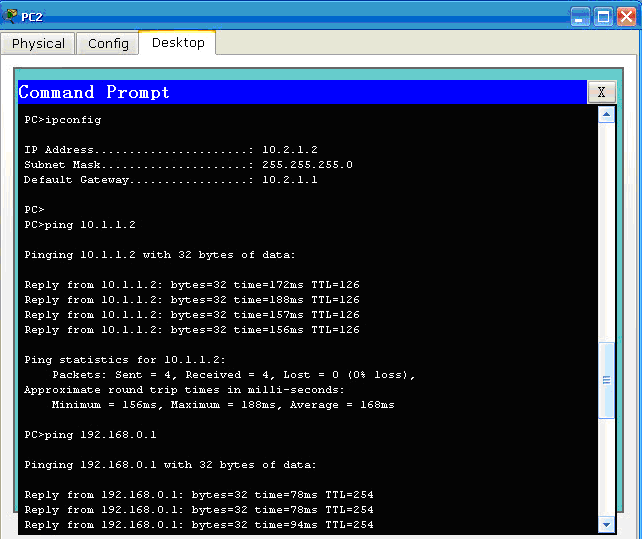


图7-11 pc2可以ping通所有的网段\*

三、填写实验报告要求

1. 记录本人上机过程所调试程序的步骤和程序的执行结果，以及自己的实验体会和收获。

2. 实验报告要自己独立完成，并注意保存好，按照教师规定日期准时提交，作为平时成绩的重要依据和期末考试的参考。

# 实验八 综合协议分析

**一、实验目的**

搭建一个小型互联网，模拟Internet的典型Web服务过程。通过该实验，可以进一步理解Internet的工作原理和协议过程，并提高综合知识的运用能力和分析能力。具体目标包括：

1、掌握网络拓扑的分析能力；

2、进一步理解路由协议的工作原理；

3、综合了解各种协议如何协同工作，完成Internet信息服务。

**二、实验设备**

1、计算机、局域网；

2、Cisco Packet Tracer模拟软件。

**三、相关准备知识**

（1）ADSL

ADSL（Asymmetric Digital Subscriber Line，ADSL，也称非对称数字用户线路）是一种能够通过普通电话线提供宽带数据业务的技术，是近年来最常见的Internet接入方式。它采用频分复用技术把普通的电话线分成了电话、上行和下行三个相对独立的信道，4kHz以下频段仍用于传送POTS（传统电话业务），从而避免了相互之间的干扰。ADSL采用DMT（离散多音频）技术，将40Khz以上的高端频带划分为256个4kHz左右的子频宽，其中25子信道用于上行通道，其余239个子信道用于下行通道。在更高的ADSL2+标准中，其下行速率最高可达16M bps，而上行速率可达800kbps。

（2）分组交换技术

Internet的通信方式是采用分组交换。源端首先将一个完整报文切割成多个适合传输的分组，沿途路由器采用存储-转发的机制接力传送这些分组，目的端接收到所有分组后再其重新组成一个完整报文。分组交换的最大好处是，较小的分组有利于路由器的并行传输，提高了通信效率，从而减少网络时延。分组交换又可进一步分为数据报交换和虚电路交换。

**四、实验步骤**

## 1．在PacketTracer中构建协议综合分析实验拓扑图

（1）网络拓扑图的构建。在PT的工作区构建如图8-1所示的网络拓扑图。其中模拟的Internet由四部分组成：家庭网络、ISP接入提供商、Internet核心交换网、网站。具体配置如下：

家庭网络：采用ADSL接入Internet，IP地址采用DHCP从ISP自动获取。

ISP：通过传统电话线将用户的家庭网络接入Internet核心网；并配备一个DNS服务器为用户提供DNS解析服务；通过路由器为用户提供DHCP服务可分配的IP地址池为：192.168.1.1~192.168.1.140。

Internet核心服务部分由三台路由器互联模拟组成，采用RIPv2动态了路由协议，实现IP数据包的分组交换。

网站：包含一台Web服务器，用于提供Web服务。

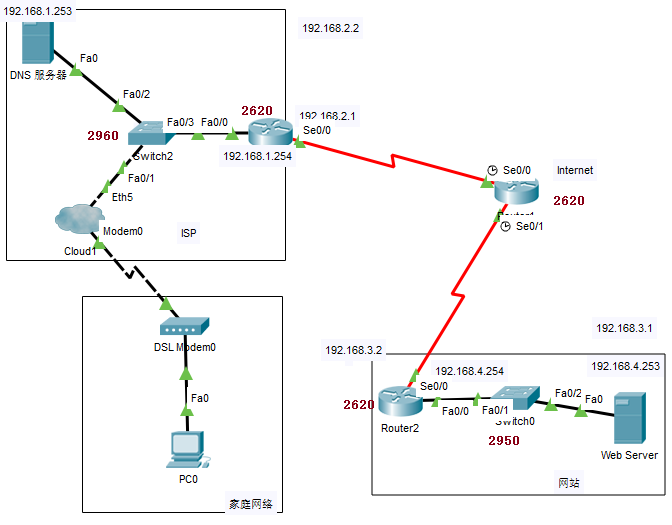


图8-1 综合网络拓扑图

（2）各设备的IP配置。如表8.1为该实验的地址分配。

表8.1 综合实验地址分配

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **设备** | **接口** | **IP地址** | **子网掩码** | **默认网关** |
| PC0 | Fa0 | DHCP获得  255.255.255.0 | | |
| DNSServer | Fa0 | 192.168.1.253 | 255.255.255.0 | 192.168.1.254 |
| Router0 | Fa0/0 | 192.168.1.254 | 255.255.255.0 | --- |
| Se0/0 | 192.168.2.1 | 255.255.255.0 | --- |
| Router1 | Se0/0 | 192.168.2.2 | 255.255.255.0 | --- |
| Se0/1 | 192.168.3.1 | 255.255.255.0 | --- |
| Router2 | Se0/0 | 192.168.3.2 | 255.255.255.0 | --- |
| Fa0/0 | 192.168.4.254 | 255.255.255.0 | --- |
| WebServer | Fa0 | 192.168.4.253 | 255.255.255.0 | 192.168.4.254 |

（3）路由器的主要配置。路由器Router0的配置如图8.2所示。其中红色框表示配置路由器的以太网口，蓝色框表示配置路由器的serial口，橙色框表示配置路由器的RIP路由，绿色框表示配置路由器的DHCP（动态主机配置协议）。



图8.2 配置路由器Router0

路由器Router1的配置如图10.3所示。

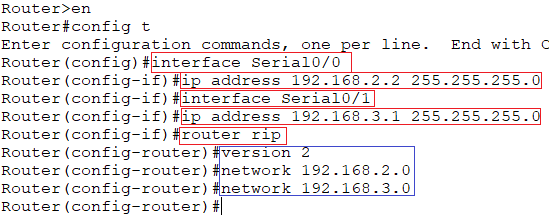


图8.3 配置路由器Router1

路由器Router2的配置如图8.4所示。

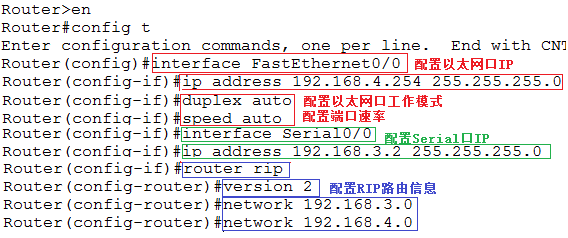
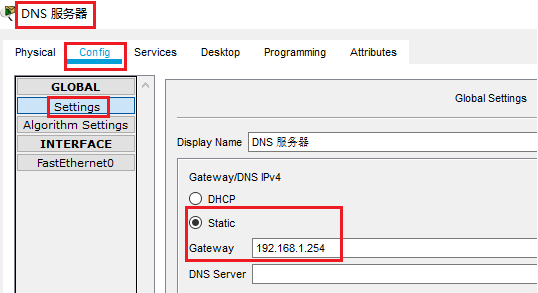


图8.4 配置路由器Router2

（4）DNS服务器的主要配置。该服务器需要开启DNS服务，并添加一条资源记录，将“www.姓名拼音.com”（[www.test.com](http://www.test.com)模拟网站的域名）解析成192.168.4.253，如图8.5所示。



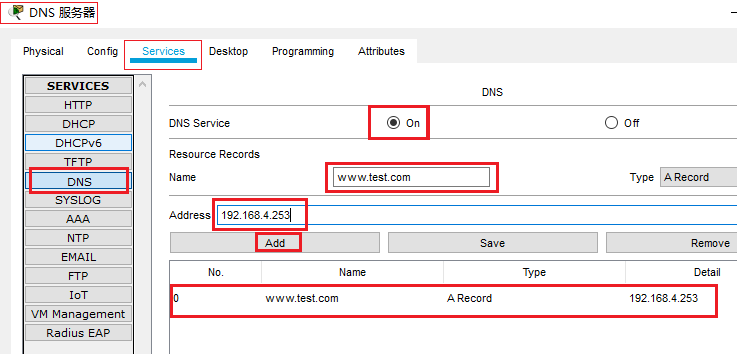
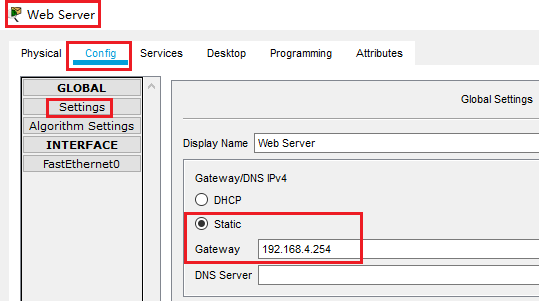


图8.5 配置DNS服务器

（5）Web服务器的主要配置。该服务器需要开启HTTP服务，默认的主页内容如图8.5所示。



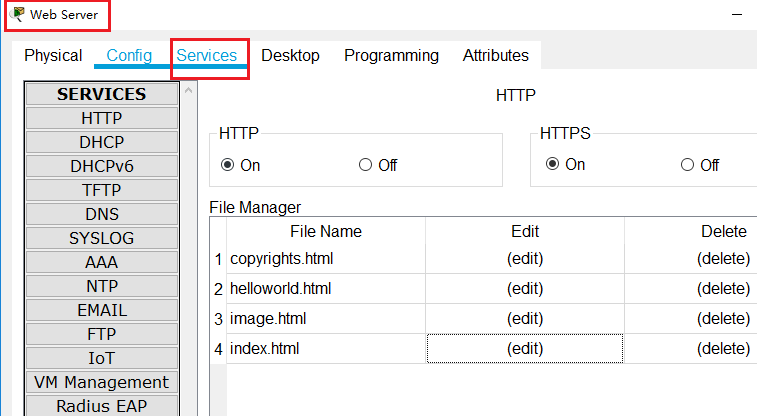
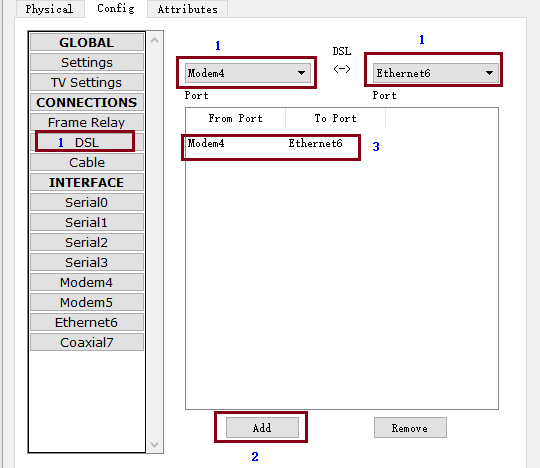


图8.5 配置Web服务器及服务器默认的主页内容

（6）调制解调器Modem0的主要配置。调制解调器的作用是模拟信号和数字信号的“翻译员”。电子信号分两种，一种是"模拟信号"，一种是"数字信号"。我们使用的电话线路传输的是模拟信号，而PC机之间传输的是数字信号。所以当通过电话线把自己的电脑连入Internet时，就必须使用调制解调器来"翻译"两种不同的信号。连入Internet后，当PC机向Internet发送信息时，由于电话线传输的是模拟信号，所以必须要用调制解调器来把数字信号"翻译"成模拟信号，才能传送到Internet上，这个过程叫做"调制"。当PC机从Internet获取信息时，由于通过电话线从Internet传来的信息都是模拟信号，所以PC机想要看懂它们，还必须借助调制解调器这个“翻译”，这个过程叫作“解调”。总的来说就称为“调制解调”。

如下图中DSL两端的端口取决于实际连接的端口名称。



## 2．综合检查整个实验的网络配置，测试拓扑

（1）熟悉网络拓扑以及IP地址编制。

使用Inspect检查工具打开各设备的端口状态汇总表（Port Status Summary Table），分别检查PC0、DNS服务器、Web服务器，以及各路由器物理接口的IP地址配置，熟悉本实验的**网络拓扑**和**IP编制方案**。完成该步骤后可知，组成模拟互联网的四个网络的IP编址分别为192.168.1.0~192.168.4.0。

（2）检查路由表，理解RIP动态路由协议的功能，测试网络拓扑。

分别打开Router0、Router1和Router2的路由表，可以发现各路由器的路由信息，完整的路由表应包含4个网络的路由信息。如图8.7所示给出了Router1的路由表，可以看出Router1上有两条直连路由（C），两条RIP路由，观察路由信息，理解其含义。在实时模式下，从PC0的桌面上打开Web浏览器，输入Web服务器的URL“www.姓名拼音.com”（“www.test.com”），按Enter键。成功访问网站，如图8.8所示。

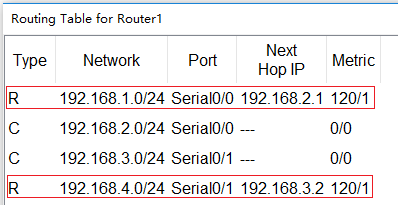


图8.7 Router1的路由表



图8.8 在PC0上成功访问Web服务器上的网站

## 3．理解DHCP协议的工作

观察PC0访问网站的过程，并综合运用所学到的计算机网络知识，分析该访问过程所涉及的DHCP协议事件，理解该协议是如何工作的。

（1）DHCP的工作过程。

DHCP（DynamicHostConfigurationProtocal，动态主机配置协议）主要作用是使客户机能够在TCP/IP网络上获得相关的配置信息，为客户机自动配置可用的网络地址。DHCP服务器和客户端之间的交互报文主要有5个：DHCPDISCOVER、DHCPOFFER、DHCPREQUEST、DHCPACK和DHCPRELEASE。DHCP客户端使用UDP的端口68，DHCP服务器使用UDP的端口67。其标准交互过程如图8.9所示：

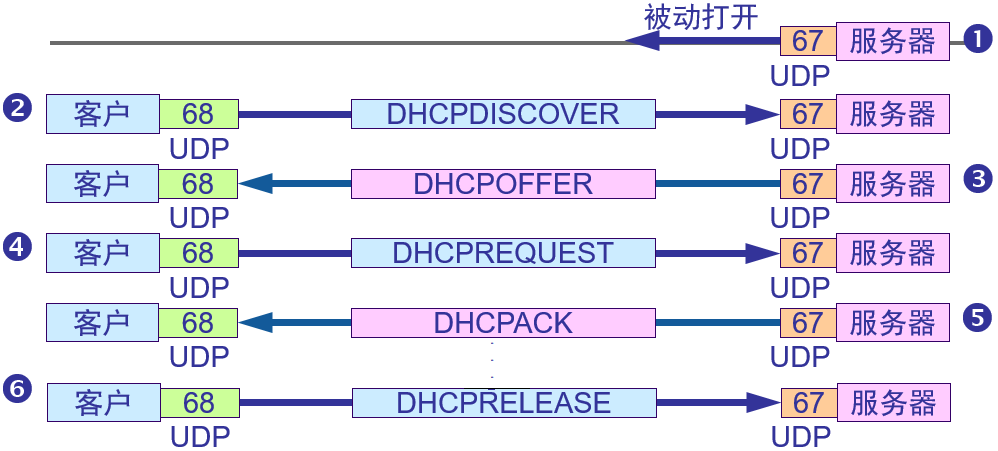


图8.9 DHCP服务器和客户端的标准交互过程

1）DHCP服务器被动打开UDP端口67，等待客户端发来的报文。

2）DHCP客户从UDP端口68发送DHCPDISCOVER报文（源地址为0.0.0.0，目的地址为：255.255.255.255）。

3）凡收到DHCPDISCOVER报文的DHCP服务器，就会从IP地址池中挑选一个尚未出租的IP地址，然后利用广播发出DHCPOFFER报文传送给DHCP客户机。这时候之所以用广播是因为客户还没有IP地址（源地址为DHCP服务器的静态IP地址，目的地址为：255.255.255.255）。

4）DHCP客户从几个DHCP服务器中选择其中的一个，并利用广播方式向所选择的DHCP服务器发送DHCPREQUEST报文。之所以用广播是因为客户机不只要通知所挑选的DHCP服务器，还要通知没有选中的DHCP服务器（源地址为：0.0.0.0，目的地址为：255.255.255.255）

5）被选择的DHCP服务器利用广播的方式发送确认报文DHCPACK给DHCP客户，进入已绑定状态，客户机可以开始使用得到的临时IP地址了。

6）DHCP客户可随时提前终止服务器所提供的租用期，这时只需向DHCP服务器发送释放报文DHCPRELEASE即可。

（2）观察DHCP动态主机配置过程

将上一步创建好的网络拓扑图从实时模式（Realtime）切换到模拟模式（Simulation），然后打开PC0的终端窗口，首先释放当前网卡获取的IP地址，然后为网卡重新从DHCP服务器上面获取新的IP地址，具体操作如图8.10所示。然后在EditFilters窗口设置为只显示DHCP，之后按下Play按钮，观察DHCP动态主机配置过程。当DHCP数据报在PC0和Router0之间有两次往返时，检查PC0的IP地址（可以通过多种方式查看），此时可以发现PC0已经获得了IP地址配置。如果BufferFull（缓冲区已满）窗口打开，单击ViewPreviousEvents按钮，可以查看以前的事件。

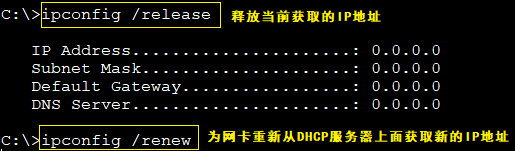


图8.10 释放与重新获取DHCPIP地址

## 4．理解ARP协议的工作

观察PC0访问网站的过程，并综合运用所学到的计算机网络知识，分析该访问过程所涉及的ARP协议事件，理解该协议是如何工作的。

仍然停留在模拟模式，并启用Router1的Serial0/1接口。

（1）检查设备的ARP缓存。

使用Inspect检查工具分别检查PC0、DNS服务器、Router1和Web服务器的ARP表，可发现所有的ARP缓存均为空，如图8.11所示。

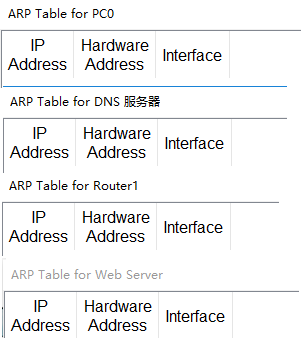


图8.11 ARPTable为空的设备

（2）观察ARP协议的执行情况

在EditFilters窗口设置为只显示ARP，然后在PC0的桌面打开Web浏览器，输入www.test.com，按回车键，接着按下Play按钮，观察ARP的执行过程。可以发现在PC0请求网页的过程中先后总共执行3次ARP之后打开网站首页，3次ARP分别是：

1）PC0查询DNS服务器192.168.1.253的MAC地址；

2）PC0查询网关路由器192.168.1.254的MAC地址；

3）Router2查询网站服务器192.168.4.253的MAC地址。

思考为什么执行三次ARP，完成课后思考题。

## 5．观察PC访问web网站的协议执行过程

单击Delete按钮，删除之前步骤中捕获的事件，在EditFilters窗口设置为显示DNS、UDP、HTTP和TCP。从PC0的桌面打开Web浏览器，重新输入www.test.com，按回车键，接着按下Play按钮，捕获DNS、UDP、HTTP与TCP的交互。

通过观察上述访问过程，可以发现在PC0访问网页的过程中，各协议事件的发生顺序依次如下。

（1）DNS查询过程：PC0通过DNS服务器获得www.test.com域名的IP地址。

DNS功能：将字符串形式的服务器域名地址解析为IP地址，如上网时在IE里输入www.neuq.edu.cn，系统要通过DNS转换成202.206.16.82。DNS服务器是维护DNS的分布式数据库系统的服务器，查询该系统以答复来自DNS客户机（本实验中PC0是DNS客户机）的查询请求。

DNS的查询过程：

1）在PC0的浏览器中输入www.test.com域名，操作系统会先检查PC0本地的hosts文件是否有这个网址映射关系，如果有，就先调用这个IP地址映射，完成域名解析。显然本实验中PC0的本地hosts文件中没有这个网址映射关系。

2）如果hosts里没有这个域名的映射，则查找本地（即PC0）DNS解析器缓存，是否有这个网址映射关系，如果有，直接返回，完成域名解析。

3）如果hosts与本地DNS解析器缓存都没有相应的网址映射关系，首先会找TCP/IP参数中设置的首选DNS服务器，在此我们叫它本地DNS服务器，此服务器收到查询时，如果要查询的域名，包含在本地配置区域资源中，则返回解析结果给客户机（即PC0），完成域名解析，此解析具有权威性。本实验到此为止，完成域名解析。以下为扩展部分。

4）如果要查询的域名，不由本地DNS服务器区域解析，但该服务器已缓存了此网址映射关系，则调用这个IP地址映射，完成域名解析，此解析不具有权威性。

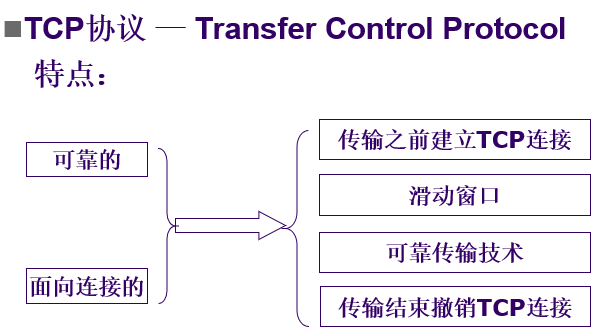
5）如果本地DNS服务器本地区域文件与缓存解析都失效，则根据本地DNS服务器的设置（是否设置转发器）进行查询，如果未用转发模式，本地DNS就把请求发至13台根DNS，根DNS服务器收到请求后会判断这个域名(.com)是谁来授权管理，并会返回一个负责该顶级域名服务器的一个IP。本地DNS服务器收到IP信息后，将会联系负责.com域的这台服务器。这台负责.com域的服务器收到请求后，如果自己无法解析，它就会找一个管理.com域的下一级DNS服务器地址(http://test.com)给本地DNS服务器。当本地DNS服务器收到这个地址后，就会找http://test.com域服务器，重复上面的动作，进行查询，直至找到www.test.com主机。

6）如果用的是转发模式，此DNS服务器就会把请求转发至上一级DNS服务器，由上一级服务器进行解析，上一级服务器如果不能解析，或找根DNS或把转请求转至上上级，以此循环。不管是本地DNS服务器用的是转发，还是根提示，最后都是把结果返回给本地DNS服务器，由此DNS服务器再返回给客户机。

从客户端到本地DNS服务器是属于递归查询，而DNS服务器之间的交互查询就是迭代查询。

（2）TCP建立连接过程：PC0与Web服务器通过三次握手建立TCP连接。

TCP（TransMIssion Control Protocol）网络传输控制协议，是一种面向连接的、可靠的、基于字节流的传输层通信协议，如图8.12所示。面向连接是指一次正常的TCP传输需要通过在TCP客户端和TCP服务端建立特定的虚电路连接来完成，该过程通常被称为“三次握手”。可靠性可以通过很多种方法来提供保证，在这里我们关心的是数据序列和确认。TCP通过数据分段(Segment)中的序列号保证所有传输的数据可以在远端按照正常的次序进行重组，而且通过确认保证数据传输的完整性。数据传输前建立连接的工作要经过“三次握手”，数据传输后断开连接的工作要经过“四次挥手”。



8.12 TCP协议特点

**三次握手，**如图8.13所示：

1）第一次握手：客户机将TCP标志位SYN置为1，并将随机产生的发送序号seq number X发送给服务器，服务器由SYN=1知道客户机要求建立联机。客户机进入SYN\_SENT状态，等待服务器确认；

2）第二次握手：服务器收到数据报文后由标志位SYN=1知道客户机请求建立连接，服务器将标志位SYN置为1，ACK置为X+1，并将随机产生的发送序号seq numberY发送给客户机以确认连接请求，服务器进入SYN\_RCVD状态；

3）第三次握手：客户机收到确认后，检查ACK是否正确，即第一次握手发送的seq numberX+1，以及SYN是否为1，如果正确则将标志位ACK置为Y+1，并将该数据包发送给服务器，服务器检查ACK是否为之前发送的seq numberY+1，如果正确则连接建立成功，客户机和服务器进入ESTABLISHED状态，完成三次握手，随后客户机和服务器之间可以开始传输数据了。

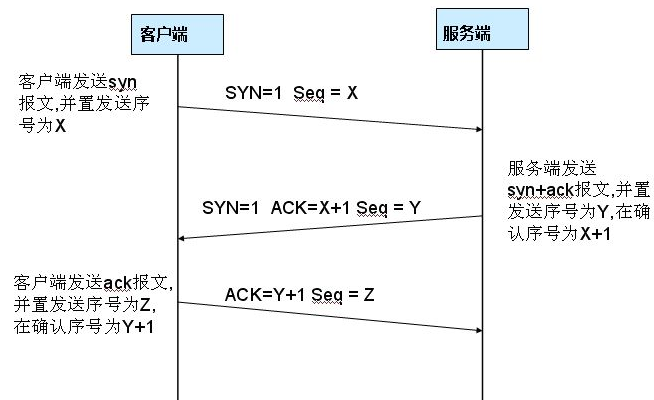


图8.13 TCP三次握手过程

（3）HTTP过程：PC0与Web服务器之间的HTTP请求与响应过程；

HTTP协议（HyperText Transfer Protocol，超文本传输协议）是用于从WWW服务器传输超文本到本地浏览器的传送协议。它可以使浏览器更加高效，使网络传输减少。它不仅保证计算机正确快速地传输超文本文档，还确定传输文档中的哪一部分，以及哪部分内容首先显示(如文本先于图形)等。

HTTP由请求和响应构成，是一个标准的客户端服务器模型（B/S）。HTTP协议永远都是客户端发起请求，服务器回送响应，如图8.14所示。

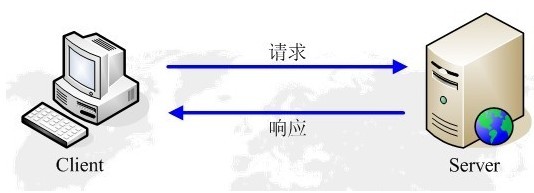


图8.14 HTTP请求响应模型

HTTP是一个无状态的协议。无状态是指客户机（Web浏览器）和服务器之间不需要建立持久的连接，这意味着当一个客户端向服务器端发出请求，然后服务器返回响应(Response)，连接就被关闭了，在服务器端不保留连接的有关信息。HTTP遵循请求(Request)/响应(Response)模型。客户机（浏览器）向服务器发送请求，服务器处理请求并返回适当的响应。所有HTTP连接都被构造成一套请求和响应。

一次HTTP操作称为一个事务，其工作整个过程如下：

1）地址解析，如用客户端浏览器请求这个页面：http:www.test.com；

2）封装HTTP请求数据包。把以上部分结合本机自己的信息，封装成一个HTTP请求数据包；

3）HTTP是比TCP更高层次的应用层协议，根据规则，只有低层协议建立之后才能，才能进行更层协议的连接，因此，首先要建立TCP连接。

4）客户机发送请求命令。建立连接后，客户机发送一个请求给服务器，请求的格式为：统一资源标识符（URL）、协议版本号，后边是MIME信息包括请求修饰符、客户机信息和可能的内容。

5）服务器响应。服务器接到请求后，给予相应的响应信息，其格式为一个状态行，包括信息的协议版本号、一个成功或错误的代码，后边是MIME信息包括服务器信息、实体信息和可能的内容。实体消息是服务器向浏览器发送头信息后，它会发送一个空白行来表示头信息的发送到此为结束，接着，它就以Content-Type应答头信息所描述的格式发送用户所请求的实际数据。

6）服务器关闭TCP连接。一般情况下，一旦Web服务器向浏览器发送了请求数据，它就要关闭TCP连接，然后如果浏览器或者服务器在其头信息加入了这行代码：Connection:keep-alive。TCP连接在发送后将仍然保持打开状态，于是，浏览器可以继续通过相同的连接发送请求。保持连接节省了为每个请求建立新连接所需的时间，还节约了网络带宽。

其中1）是步骤（1）DNS查询过程；3）是步骤（2）TCP建立连接过程；2）、4）和5）是该步骤的HTTP过程；6）是下面步骤（4）TCP拆除连接过程。

（4）TCP拆除连接过程：PC0与Web服务器通过四次挥手拆除TCP连接。

**四次挥手，**如图8.15所示：

1）第一次挥手：客户机发送一个FIN=1，并将随机产生的发送序号seq number X发送给服务器，用来关闭客户机到服务器的数据传送，客户机进入FIN\_WAIT\_1状态；

2）第二次挥手：服务器收到FIN=1后，知道客户机请求关闭连接，发送一个ACK=X+1给客户机，并将随机产生的发送序号seq numberZ发送给客户机以确认关闭连接请求，服务器进入CLOSE\_WAIT状态；

3）第三次挥手：服务器发送一个FIN=1，ACK=X以及随机产生的发送序号seq numberY用来关闭服务器到客户机的数据传送，服务器进入LAST\_ACK状态；

4）第四次挥手：客户机收到FIN=1后，客户机进入TIME\_WAIT状态，接着发送一个ACK=Y和发送序号seq numberX给服务器，服务器进入CLOSED状态。

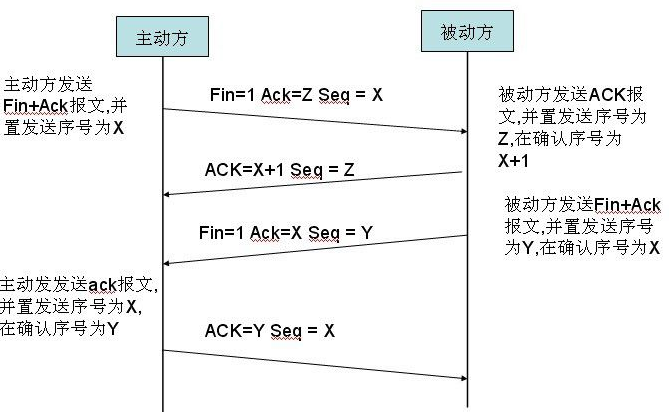


图8.15 TCP四次挥手过程

## 6．观察应用层数据单元的封装方式

可以通过两种方式检查数据包：当数据包信封在动画中显示时，单击它，或者当该数据包实例列在EventList中时，单击其Type列。

在EventList窗口中打开任意一个类型为DNS的数据包，可以发现DNS数据包的封装顺序自顶向下分别为：DNS数据包🡪UDP报文🡪IP分组🡪Ethernet数据帧，如图8.16所示。

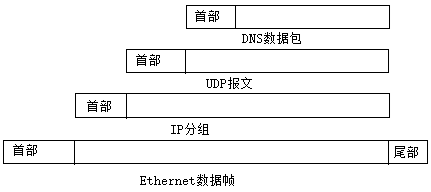


图8.16 DNS数据包的封装顺序

在Event List窗口中打开任意一个类型为HTTP并且Last Device为Router0的数据包。观察Inbound PDU Details（入站PDU详细数据）和Outbound PDU Details（出站PDU详细数据），可以发现HTTP数据包在链路层的封装会发生变化，一种方式为HTTP数据包🡪TCP段🡪IP分组🡪Ethernet数据帧，另一种方式为HTTP数据包🡪TCP段🡪IP分组🡪HDLC数据帧（PPP帧）。

首先Ethernet、IEEE802.3、PPP和HDLC都是数据链路层的协议，如图8.17所示。广域网中经常会使用串行链路来提供远距离的数据传输，高级数据链路控制HDLC（High-Level Data Link Control）和点对点协议PPP（ Point to Point Protocol）是两种典型的串口封装协议。PPP协议是一种点到点(一根链路两端只有两个接口)链路层协议，主要用于在全双工的同异步链路上进行点到点的数据传输。HDLC协议是一种面向比特的链路层协议，思科公司定义的协议。Cisco HDLC协议的帧首部有三个字段，地址字段、控制字段和协议字段。对比以太网的帧，没有目标MAC地址源MAC地址。

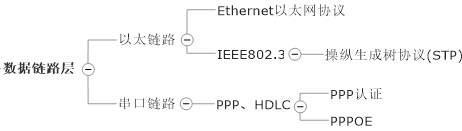


图8.17 数据链路层协议

通过观察数据单元的传输过程可以发现，无论涉及的是哪种应用协议和传输协议，在Inbound PDU Details（入站PDU详细数据）和Outbound PDU Details（出站PDU详细数据）视图中，它们都始终封装在IP数据包中。另外，IP分组在Internet网络的传输过程中，源目IP地址并没有发生变化，但是帧的封装及帧的MAC地址会根据实际物理网络发生改变。

**五、**填写实验报告要求

1. 记录本人上机过程所调试程序的步骤和程序的执行结果，以及自己的实验体会和收获。

2. 实验报告要自己独立完成，并注意保存好，按照教师规定日期准时提交，作为平时成绩的重要依据和期末考试的参考。