**《计算机网络基础》实验指导书**

**（信息学部）**

**主编：章曙光**

**北京城市学院**

**2024年 8月**

目 录

[实验项目一 VLAN划分 1](#_Toc175243081)

[实验项目二 路由配置及静态路由实现 18](#_Toc175243082)

[实验项目三 OSPF动态路由实现 27](#_Toc175243083)

[实验项目四 典型三层网络规划与实现 37](#_Toc175243084)

[实验项目五 数据包捕获与分析 38](#_Toc175243085)

[实验项目六 NAT技术 42](#_Toc175243086)

[实验项目七 基于服务器的网络应用搭建 47](#_Toc175243087)

**实验项目一 VLAN划分**

**一、实验目的**

1．掌握交换机的基本配置，熟悉交换机的配置模式和常用配置命令。

2．理解VLAN的工作原理。

3. 掌握基于端口划分VLAN的配置命令。

**二、实验内容**

利用Packet Tracer网络仿真软件配置Cisco 2960交换机，用基于端口技术划分VLAN，在一台交换机上划分多个虚拟局域网，提高局域网内的安全性能。

**三、实验设备与环境**

运行Windows 7或Windows 10操作系统的计算机1台， Packet Tracer 6.2网络仿真软件1套，仿真设备Cisco 2960交换机1台，仿真PC机4台，仿真连接线若干。

**四、实验原理**

如果一个局域网的规模较大，就很容易发生广播风暴，使网络流量剧增，导致局域网传输性能下降。另外，局域网内的计算机通常都能互相访问，增加了安全隐患。虚拟局域网（VLAN）就是为解决以太网的广播问题和安全性而提出的一种协议，它在以太网帧的基础上增加了VLAN头，用VLAN ID把用户划分为更小的工作组，限制不同工作组间的用户互访，每个工作组就是一个虚拟局域网。VLAN的优点是可以限制广播范围，并能够形成逻辑工作组，动态管理网络。VLAN技术可以在交换式网络基础上，根据网络上的终端设备属性划分成逻辑工作组，使各逻辑工作组在一定程度上进行隔离。VLAN的划分方法有很多种，如端口划分、MAC地址划分、网络层划分及IP组播划分等。

本实验采用基于端口技术划分VLAN，对一台交换机上的四个端口进行配置，分别划分到两个VLAN，将四台计算机配置到这两个逻辑工作组中。通过本实验，理解虚拟局域网技术的原理，并掌握基于端口划分VLAN的配置命令。

如果在交换机上要配置一个标号为5的VLAN，可在全局配置模式下输入以下命令：

vlan 5

然后就可将端口划分给这个VLAN，假设要把快速以太网口1划分给vlan 5，必须先进入此接口的配置模式，然后输入以下命令：

switchport access vlan 5

**五、实验步骤**

**（一）实验准备：熟悉交换机的基本配置**

1.启动Packet Tracer 6.2，从设备区选择Cisco 2960交换机，拖入工作区，如图1.1所示。

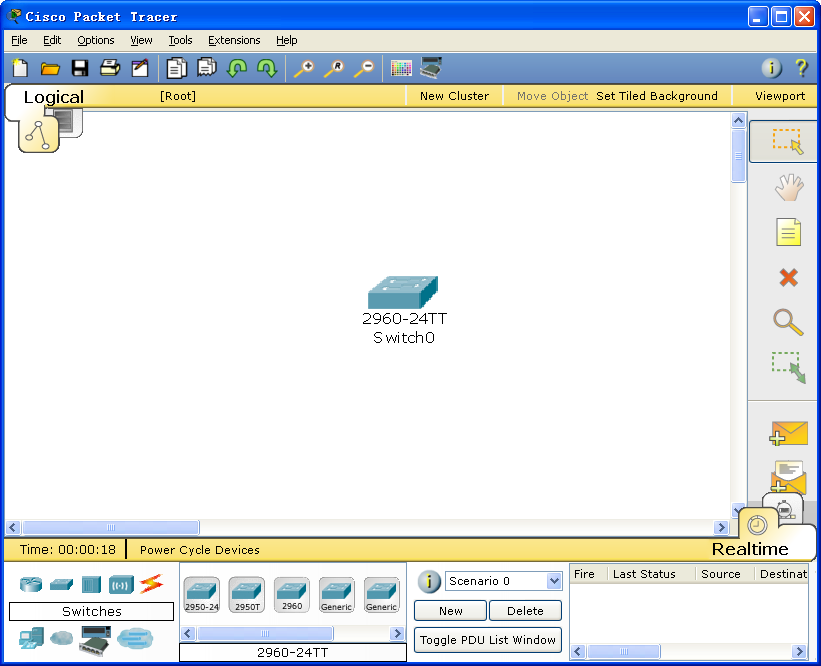


图1.1 Cisco 2960交换机

2．交换机配置模式的转换

交换机有用户模式、特权配置模式、全局配置模式、接口配置模式、线路配置模式等多个模式，要掌握交换机的配置就必须理解各个模式的作用，并熟练掌握这些模式之间的切换命令。

鼠标点击2960交换机，点击CLI命令行，敲击回车键后进入用户模式，输入以下命令，学习各个配置模式之间的切换命令。为了便于理解配置命令，在某些命令后用//加以注释，读者做实验时请勿输入这些注释。

Switch>enable // >为用户模式提示符，输入enable进入特权配置模式

Switch#configure terminal //进入全局配置模式命令，#为特权模式提示符

Switch(config)#hostname Switch2960 //为交换机取名为Switch2960

Switch2960(config)#interface Fastethernet 0/1 //进入接口配置模式

Switch2960(config-if)#exit //返回全局配置模式

Switch2960(config)#interface Fastethernet 0/2 //进入接口配置模式

Switch2960(config-if)#exit //返回全局配置模式

Switch2960(config)#end //返回特权配置模式

Switch2960#

命令截图如图1.2所示。

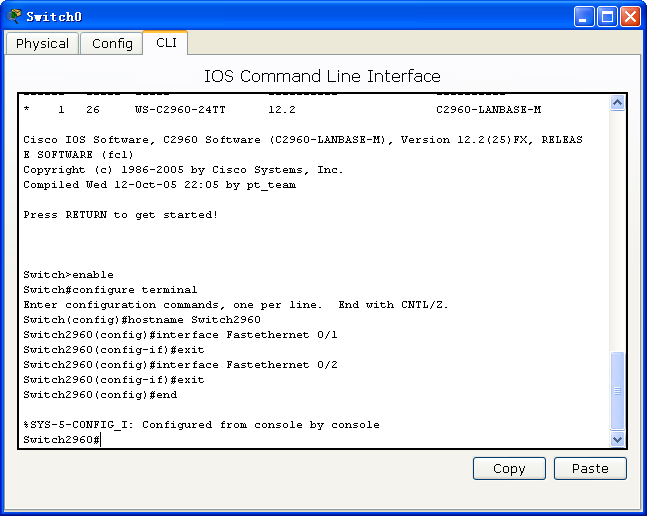


图1.2 交换机配置模式的切换

3．帮助信息的使用

在特权模式下输入exit命令返回用户模式。在用户模式下输入？，可以查询用户模式下可键入的命令。如图1.3所示。

Switch2960>?

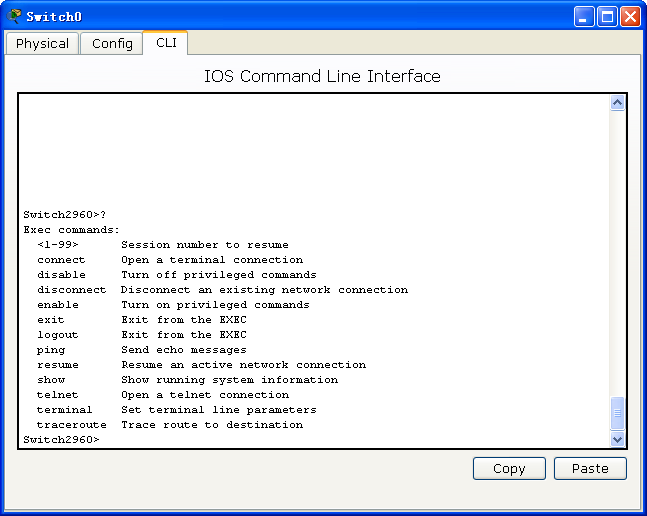


图1.3 查询用户模式下可用的命令

在不完整的命令后紧接着键入？可查询完整的命令，如en后键入？会显示enable命令。在show命令后键入空格和？可查询show命令的各项参数。

Switch2960>en？ //en后键入？查询完整命令，注意：en和？之间无空格

enable //自动显示enable完整命令

Switch2960>show ? // 注意：show和？之间有空格

如下图1.4所示。

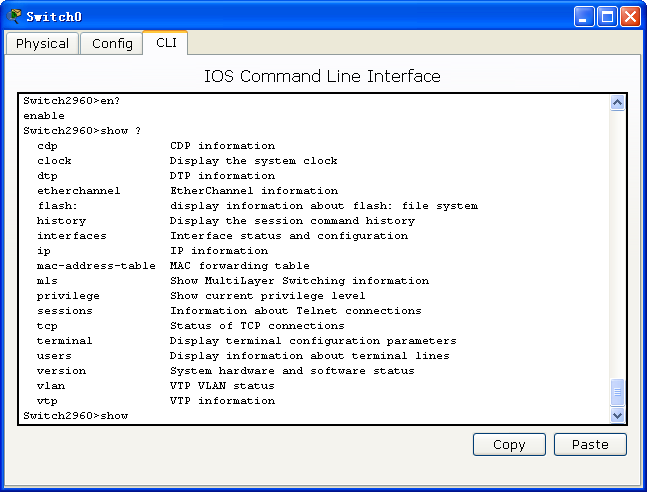


图1.4 帮助命令的应用

读者可在show命令后键入图中所列出的一些参数查询交换机的相关信息，如clock、version、vlan等参数。

4．配置命令的使用

交换机输入命令时比较智能化，有些命令如果记得不全，可以按Tab键，自动补齐该命令。如在特权模式下键入conf后按Tab键，则自动显示configure命令，接着再按Tab键则在configure后面自动补上terminal，成为一个完整的命令：configure terminal，如图1.5的最下面三行所示。

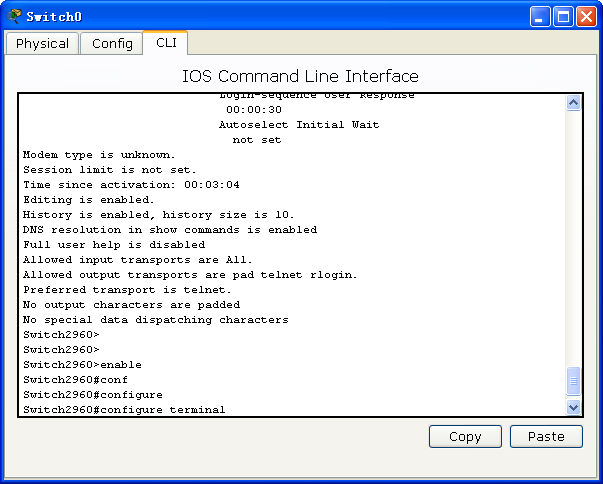


图1.5 Tab键的应用

为了方便，也可在不引起歧义的前提下输入不完整的命令，同输入完整命令的效果一样。在用户模式下分别输入以下命令，可达到与步骤2相同的结果：

Switch>en

Switch#conf ter

Switch(config)#host Switch2960

Switch2960(config)#int f0/1

Switch2960(config-if)#ex

Switch2960(config)#int f0/2

Switch2960(config-if)#ex

Switch2960(config)#end

Switch2960#

命令缩写的截图如图1.6所示。

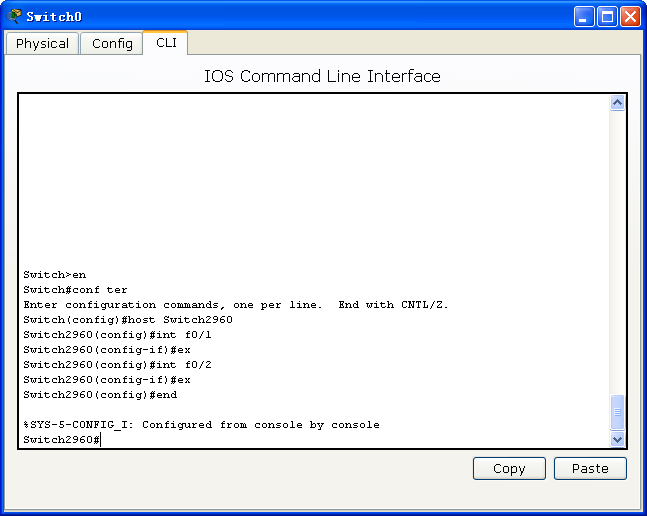


图1.6 命令缩写练习

5．配置接口传输速率和工作方式

在用户模式下输入以下命令，注意问号提示符？的应用。

SwithchA>enable

SwithchA#configure terminal

SwithchA(config)#interface f0/3

SwithchA(config-if)#speed ? //为端口f0/3设置速率，用？显示速率参数

10 Force 10 Mbps operation //可提供10Mbit/s的速率

100 Force 100 Mbps operation //可提供100Mbit/s的速率

auto Enable AUTO speed configuration //可提供10/100M自适应的速率

SwithchA(config-if)#speed 10 //选择10Mbit/s的速率，通常选auto

SwithchA(config-if)#duplex ? //为端口f0/3设置双工的工作方式

auto Enable AUTO duplex configuration //可提供自适应的双工方式

full Force full duplex operation //可提供全双工的工作方式

half Force half-duplex operation //可提供半双工的工作方式

SwithchA(config-if)#duplex half //此处选择半双工的工作方式，通常选auto

SwithchA(config-if)#no shutdown //激活接口

SwithchA(config-if)#end

命令截图如图1.7所示。

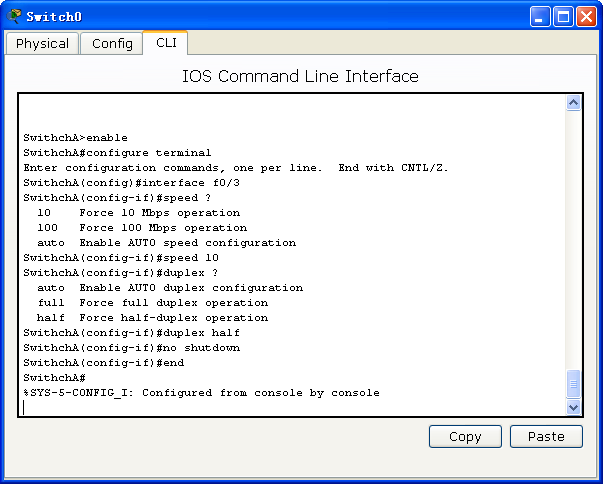


图1.7 利用问号帮助命令配置端口参数

输入查询端口配置命令：

SwithchA#show interface f0/3

端口查询结果如图1.8所示。

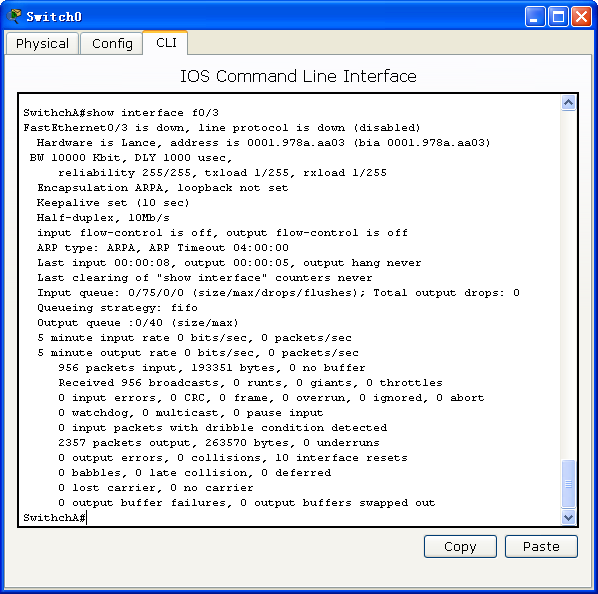


图1.8 查询端口参数

可以看到此端口的双工方式和端口速率，由于该端口未连接计算机，所以端口状态为down。

**（二）VLAN的划分与配置**

**1.** 用Packet Tracer 6.2构建网络拓扑

启动Packet Tracer 6.2，添加1台Cisco 2960交换机、4台PC机。用直连线将PC0-PC3计算机分别连接到交换机的Fastethernet 0/1-0/4端口上。网络拓扑图如下图1.9所示。

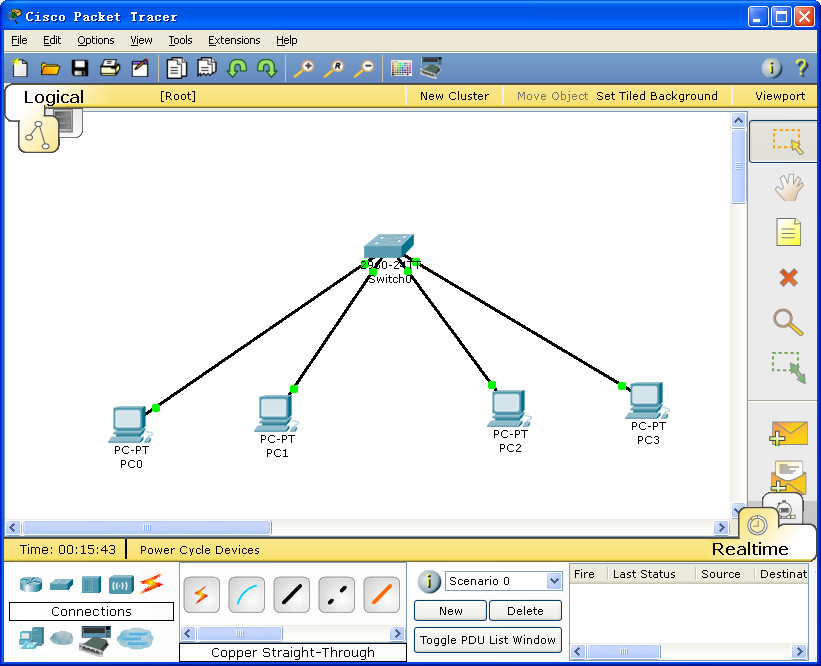


图1.9虚拟局域网配置拓扑图

**2.** 配置PC机的IP地址、子网掩码

鼠标点击网络拓扑图上的PC0，出现PC0的配置窗口，点击Desktop，点击IP Configuration，配置IP地址和子网掩码如下图1.10所示。

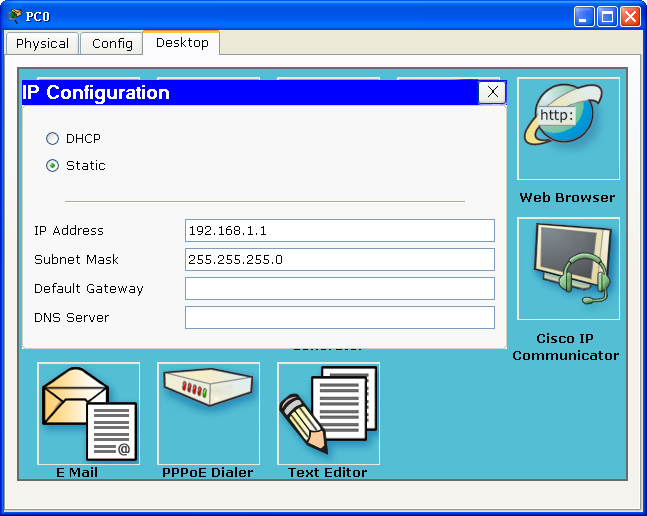


图1.10 PC0的IP地址配置

在拓扑图上分别点击另外三台计算机，分别配置IP地址和子网掩码，它们的IP地址分别配置为192.168.1.2，192.168.1.3，192.168.1.4**（学生做实验时，最后一个字段需修改为学号后2位或后3位，视情况而定，依次递增1，但不许大于254）**，子网掩码均设为255.255.255.0，默认网关和DNS服务器不设置。

**3.** 查询默认VLAN，并检验四台计算机的连通性

鼠标点击交换机Switch0，输入enable命令进入特权模式，然后输入show vlan查询VLAN，如下图1.11所示。

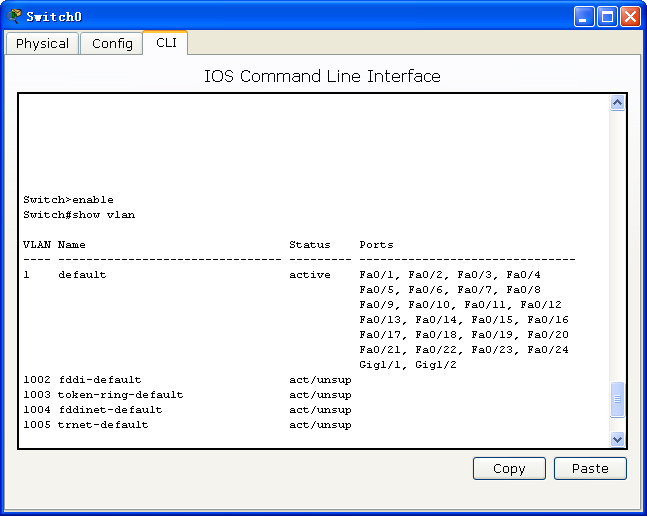
****

图1.11 VLAN划分前的默认VLAN

可以看到交换机的所有快速以太网端口和吉比特以太网端口都处于默认的虚拟局域网VLAN 1，并处于激活状态。鼠标点击PC0，选择Command Prompt进入命令行，输入ping命令，检验与另外三台计算机的连通性，发现四台计算机是互相连通的，如下图1.12所示。

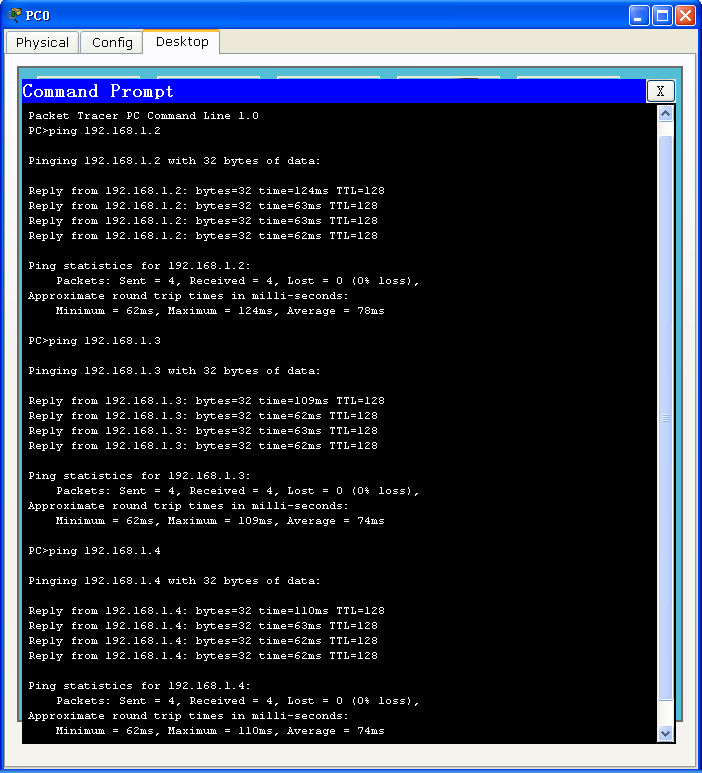
****

图1.12 VLAN划分前四台计算机的连通性测试

**4.** 划分VLAN，并查询VLAN的配置

鼠标点击交换机Switch0，输入以下命令新建两个VLAN，分别取名为VLAN10和VLAN20。为了便于理解配置命令，在某些命令后用//加以注释，读者做实验时请勿输入这些注释。

Switch>enable //进入特权配置模式

Switch#configure terminal //进入全局配置模式

Switch(config)#vlan 10 //创建虚拟局域网 10

Switch(config-vlan)#name vlan10 //给此虚拟局域网取名为VLAN10

Switch(config-vlan)#exit //返回全局配置模式

Switch(config)#vlan 20 //创建虚拟局域网 20

Switch(config-vlan)#name vlan20 //给此虚拟局域网取名为VLAN20

Switch(config-vlan)#end //返回特权配置模式

Switch#

输入以下命令，将与四台计算机相连的交换机端口分别划分给VLAN10和VLAN20。

Switch#configure terminal //进入全局配置模式

Switch(config)#interface fastethernet 0/1 //进入接口配置模式，对快速以太网口fa0/1进行配置

Switch(config-if)#switchport access vlan 10 //将此接口划分到VLAN 10

Switch(config-if)#exit //返回全局配置模式，也可不输入此命令

Switch(config)#interface fastethernet 0/2 //进入接口配置模式，配置fa0/2

Switch(config-if)#switchport access vlan 10 //将此接口也划分到VLAN 10

Switch(config-if)#exit

Switch(config)#interface fastethernet 0/3 //进入接口配置模式，配置fa0/3

Switch(config-if)#switchport access vlan 20 //将此接口也划分到VLAN 20

Switch(config-if)#exit

Switch(config)#interface fastethernet 0/4 //进入接口配置模式，配置fa0/4

Switch(config-if)#switchport access vlan 20 //将此接口也划分到VLAN 20

Switch(config-if)#end

Switch#

划分VLAN的配置过程如下图1.13所示。

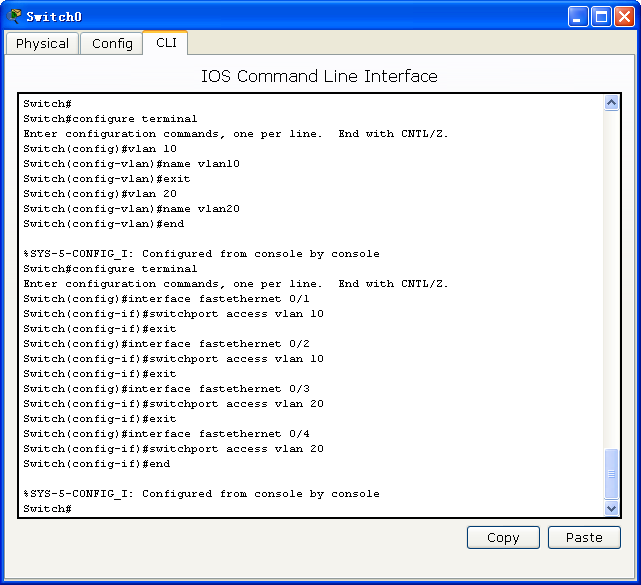
****

图1.13 划分VLAN的配置

以上配置命令将fa0/1和fa0/2划分到VLAN 10，将fa0/3和fa0/4划分到VLAN 20，可以输入show vlan命令查询VLAN划分的结果，如下图1.14所示。

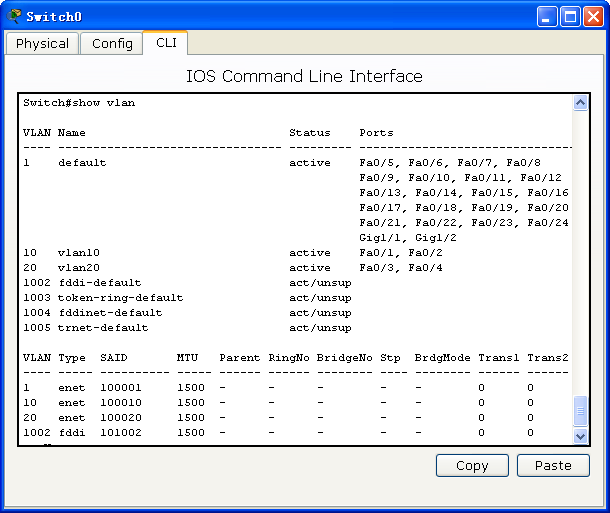
****

图1.14 划分VLAN后的查询结果

可以看到新增了两个VLAN，原来同在VLAN 1中的四个接口分别被配置到了VLAN 10和VLAN 20中。

**5.** 检验网络的连通性

鼠标点击PC0，选择Command Prompt进入命令行，输入ping命令后结果如下图1.15。

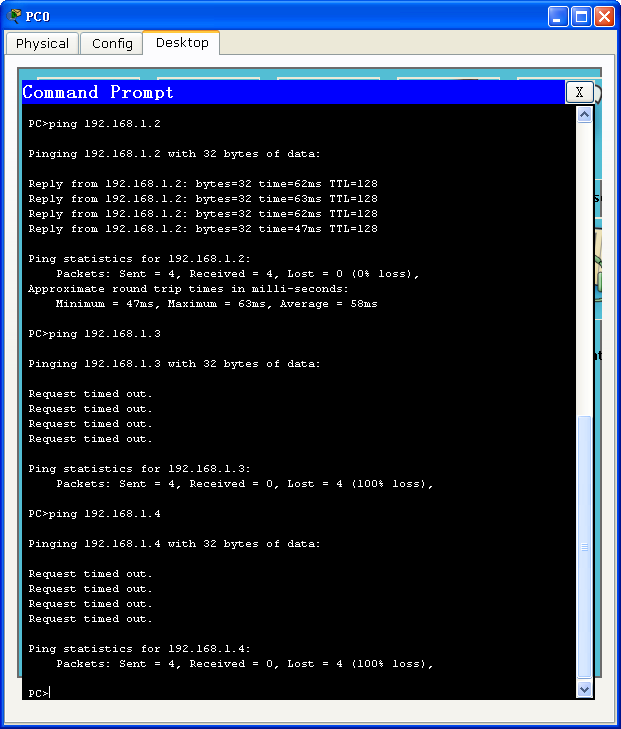
****

图1.15 划分VLAN后PC0与其他计算机的连通性测试

发现PC0与PC1是连通的，但PC0与PC2、PC3不连通。单击PC2，选择Command Prompt进入命令行，输入ping命令后结果如下图1.16所示。

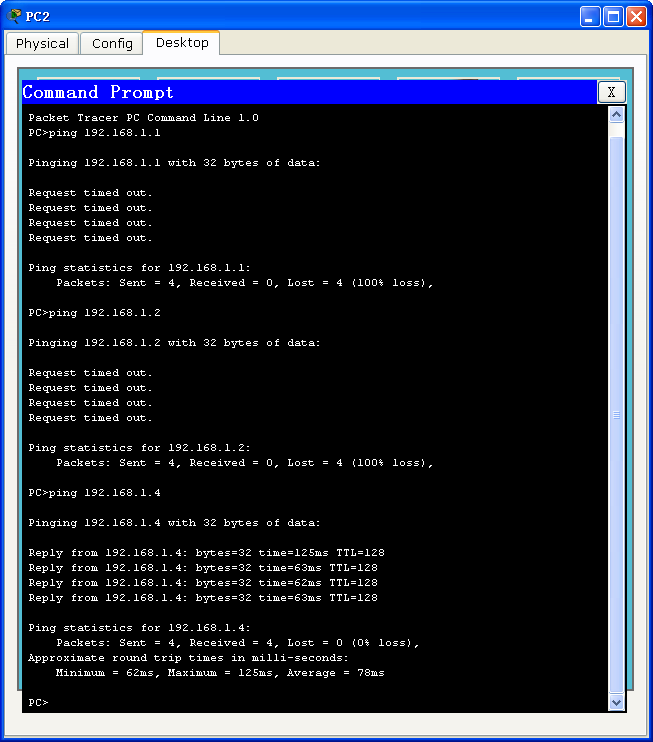
****

图1.16 划分VLAN后PC2与其他计算机的连通性测试

发现PC2与PC0、PC1不连通，但与PC3是连通的。从而可以看出交换机的四个端口被划分成了两个VLAN，PC0和PC1属于VLAN10，PC2和PC3属于VLAN20，这两个VLAN互相之间不能直接访问，但VLAN内部可以直接访问。

**六、实验注意事项**

配置交换机时必须使用命令行来配置，不能使用视窗界面配置。

**七、思考题**

1．怎样才能把一个VLAN的计算机划分到另一个VLAN？

2．如何使两个VLAN的计算机之间互相通信？

3．如果有两台交换机，怎么配置多个VLAN？

**八、实验考核要求**

1.撰写实验报告。

2.VLAN配置正确。

3.各PC机之间的连通性检测正确。

**实验项目二 路由配置及静态路由实现**

**一、实验目的**

1．掌握路由器的配置模式和基本配置命令。

2．理解静态路由的原理。

3. 掌握路由器的静态路由配置。

**二、实验内容**

利用Packet Tracer网络仿真软件构建两个局域网，分别用两台路由器连接，配置静态路由，实现两个局域网的互联。

**三、实验设备与环境**

运行Windows 7或Windows 10操作系统的计算机1台， Packet Tracer 6.2网络仿真软件1套，仿真设备路由器、交换机各2台、PC机4台、连接线路若干。

**四、实验原理**

IP协议是实现网络互联的核心协议，路由器（Router）则是实现网络互联的关键设备。作为不同网络之间互相连接的枢纽，路由器构成了基于TCP/IP 的国际互联网络Internet的主体脉络。路由器属于OSI模型的第三层（网络层），用于连接多个逻辑上分开的网络。路由器可以执行从一个网段到另一个网段的数据传输，也能执行从一种网络向另一种网络的数据传输。当数据从一个子网传输到另一个子网时，也可通过路由器来完成。因此，路由器具有判断网络地址和选择路径的功能，它可以按照静态路由方式或动态路由方式选择转发路径。

静态路由是最简单的路由形式，由管理员通过命令行设置非实时更新的路由表，管理员负责完成发现路由并通过网络传播路由的任务。静态路由使网络更加安全，因为在路由器中，它只定义了通常一条（也可多条）流进和流出网络的路由。但静态路由也有缺点，如网络发生问题或拓扑结构发生变化时，网络管理员就必须手工调整这些改变。因此，静态路由适用于小型网络。

做静态路由的配置一般是在全局配置模式下，其命令格式如下：

ip route 目的网络地址 目的网络掩码 下一跳路由器接口IP地址

或：ip route 目的网络地址 目的网络掩码 本路由器的转发接口标识

本实验是将两个局域网用两台路由连起来，通过配置静态路由实现互联互通。

**五、实验步骤**

**1.** 用Packet Tracer 6.2构建网络拓扑

启动Packet Tracer 6.2，添加2台路由器（Generic，Router-PT）、2台交换机（2960）、4台PC机。用串口线连接路由器1的Serial2/0口与路由器2的Serial2/0口，以路由器1的Serial2/0口为DCE侧（串口线上有时钟标志），敲入配置命令时需设置时钟频率；交换机与路由器以及交换机与PC机之间用直连双绞线连接。各端口及其IP地址如图2.1所示（学生实验时需修改IP地址最后一个字段为学生本人学号后2位或后3位相关，依次递,1）。

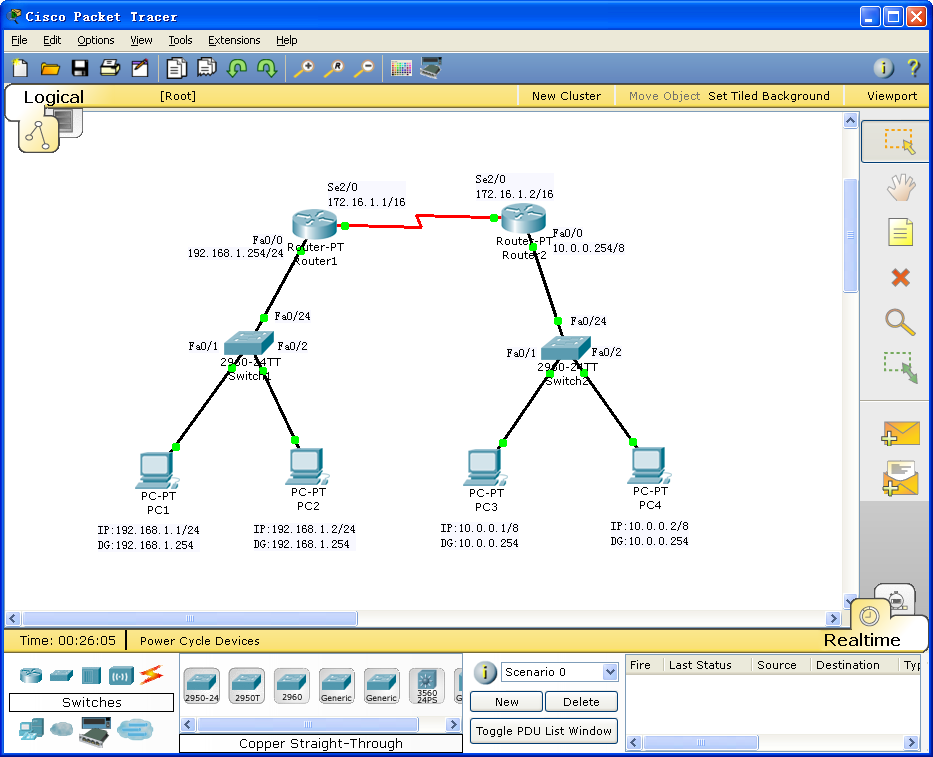


图2.1 静态路由配置网络拓扑图

**2.** 配置PC机的IP地址、子网掩码和默认网关地址

单击网络拓扑图上的PC1，出现PC1的配置窗口，点击Desktop，点击IP Configuration，按网络拓扑图上所给的IP地址及默认网关地址进行配置，子网掩码采用默认值，如图2.2所示。此处要注意的是，计算机的默认网关是与这台计算机相连的路由器接口的IP地址。其他机器的配置类似，此处略。

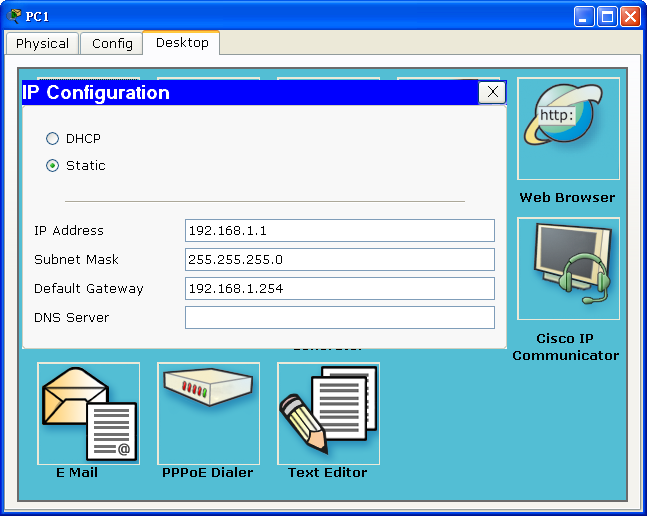


图2.2 PC1的IP配置

下面开始配置路由器。分别对2台路由器的快速以太网口Fa0/0和串口Se2/0配置IP地址，并激活。为了便于理解配置命令，在某些命令后用//加以注释，读者做实验时切勿将这些注释也敲进去。

**3.** 配置Router1接口的IP地址

单击网络拓扑图上的Router1，出现Router1的配置窗口，点击CLI（命令行）配置界面，路由器启动后询问“Continue with configuration dialog? [yes/no]:”，敲入no；随后配置界面提示“Press RETURN to get started!”，敲击回车键即可开始配置Router1。为路由器取名后，配置Fa0/0和串口Se2/0的IP地址，并激活，如图2.3所示。

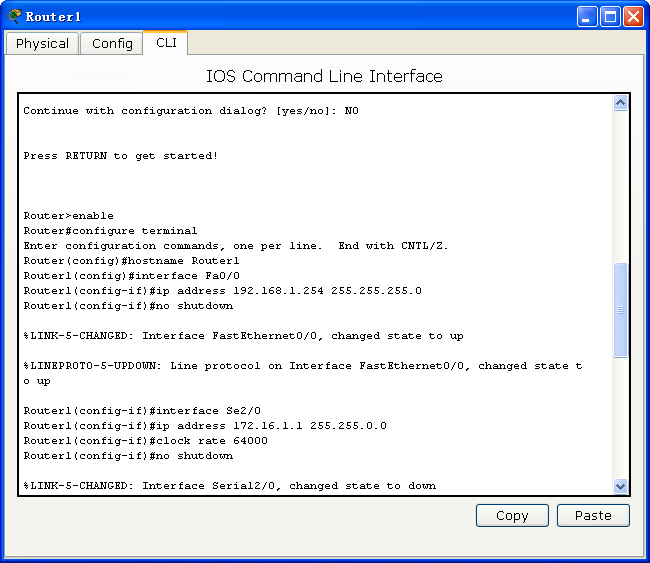


图2.3 Router1的接口配置

对Router1的配置命令如下：

Router>enable //进入特权配置模式

Router#configure terminal //进入全局配置模式

Router(config)#hostname Router1 //为路由器取名为Router1

Router1(config)#interface Fa0/0

//进入接口配置模式，以便对快速以太网口Fa0/0进行配置

Router1(config-if)#ip address 192.168.1.254 255.255.255.0

//为Fa0/0接口配置IP地址

Router1(config-if)#no shutdown //激活Fa0/0接口

Router1(config-if)#interface Serial2/0

//进入接口配置模式，以便对串口Serial2/0进行配置

Router1(config-if)#ip address 172.16.1.1 255.255.0.0 //为Se2/0串口配置IP地址

Router1(config-if)clock rate 64000 //DCE侧设备需设置时钟频率

Router1(config-if)#no shutdown //激活Serial2/0串口

**4.** 配置Router2接口的IP地址

与配置Router1接口的IP地址的步骤基本相同，开始配置Router2的接口IP地址，如图2.4所示。

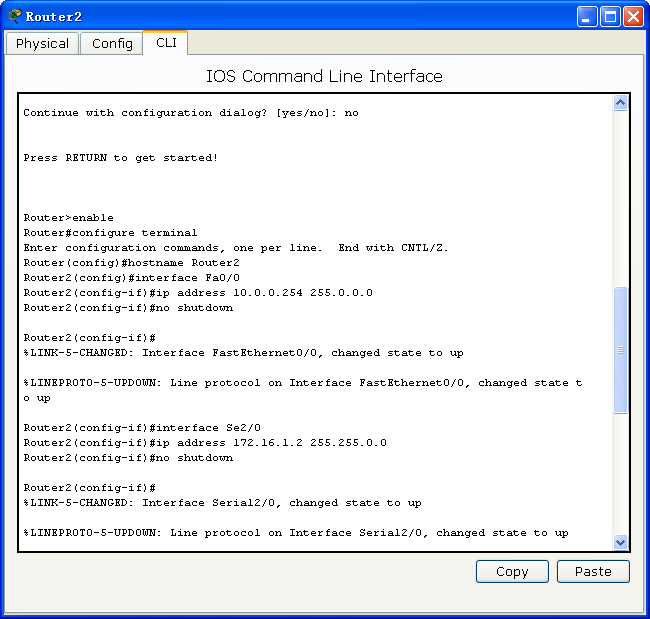


图2.4 Router2的接口配置

**5.** 配置静态路由**。**在全局配置模式下进行静态路由的配置

先使路由器Router1处于全局配置模式，配置Router1到目的网络10.0.0.0/8的静态路由，并用show ip route命令显示路由信息：

Router1(config)#ip route 10.0.0.0 255.0.0.0 172.16.1.2

//配置到目的网络10.0.0.0/8的静态路由

Router1(config)#exit //退回特权模式，以便查询路由信息

Router1#show ip route //查询路由信息

查询到三条路由信息，如图2.5所示。

S 10.0.0.0/8 [1/0] via 172.16.1.2

C 172.16.0.0/16 is directly connected, Serial2/0

C 192.168.1.0/24 is directly connected, FastEthernet0/0

其中S代表静态路由，10.0.0.0/8 [1/0] via 172.16.1.2表示Router1到目的网络10.0.0.0/8需经由IP地址为172.16.1.2的接口转发；

C代表直连路由，表示与路由器直接相连的网络。

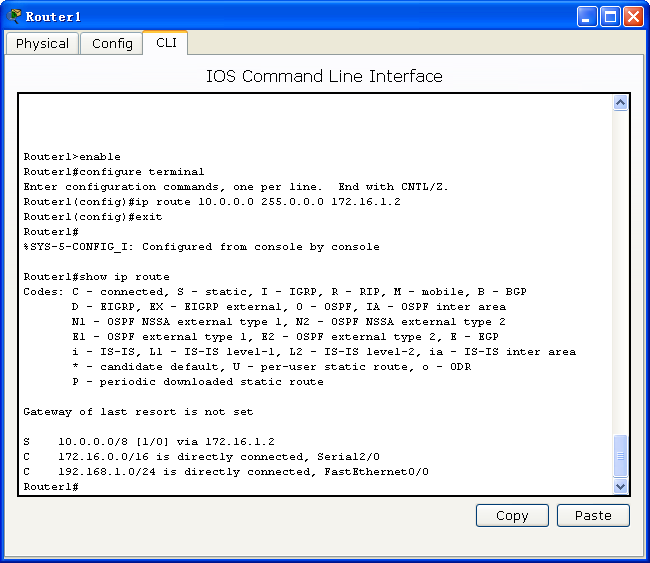


图2.5 Router1的静态路由配置及路由表信息

接着使路由器Router2处于全局配置模式，配置Router2到目的网络192.168.1.0/24的静态路由，并用show ip route命令显示路由信息：

Router2(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.1

//配置到目的网络192.168.1.0/24的静态路由

Router2(config)#exit //退回特权模式，以便查询路由信息

Router2#show ip route //查询路由信息

查询到三条路由信息，如图2.6所示。

C 10.0.0.0/8 is directly connected, FastEthernet0/0

C 172.16.0.0/16 is directly connected, Serial2/0

S 192.168.1.0/24 [1/0] via 172.16.1.1

其中S代表静态路由，192.168.1.0/24 [1/0] via 172.16.1.1表示Router2到目的网络192.168.1.0/24需经由172.16.1.1接口转发；C代表直连路由，表示与路由器直接相连的网络。

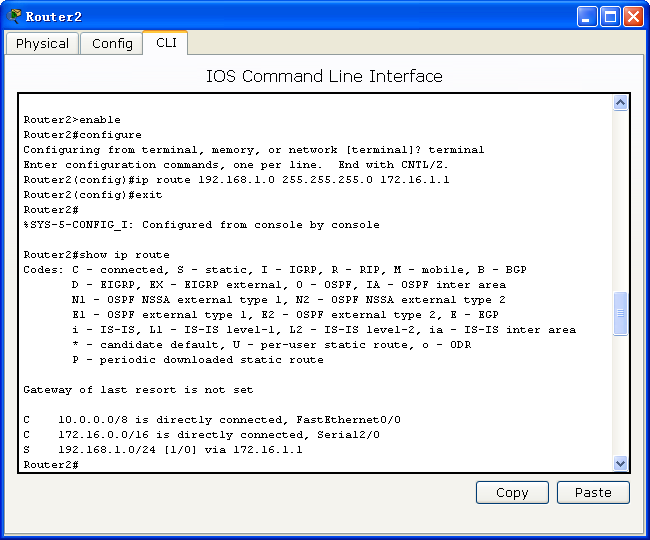


图2.6 Router2的静态路由配置及路由表信息

**6.** 验证网络的连通性

配置完静态路由后，可以检验各个网络之间的连通性。

以PC1为例，检验它与其他机器是否连通。鼠标点击PC1，选择Command Prompt进入命令行，输入ping 另外三台计算机的命令后结果如图2.7。第一个包超时是因为发出第一个ping包后，需发送arp包查询中间链路接口的MAC地址，获得MAC地址后再向目的主机发送ping包。如果已经知道沿途各接口的MAC地址，只要网络连通，就不会超时了。此后的包都有回应，证明PC1能与另外三台计算机连通。

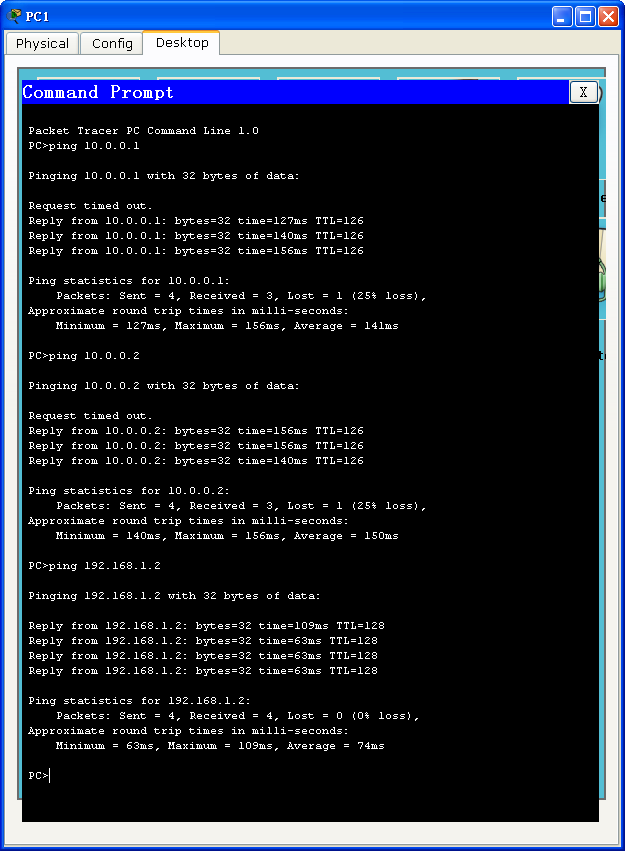


图2.7 验证PC1到其他三台计算机的连通性

**六、实验注意事项**

1．路由器到计算机之间的连线必须使用交叉线（黑色虚线），不能使用直连线。

2．在配置路由器串口时，务必在DCE侧配置时钟信号频率并激活，否则路由器之间的链路不能连通。

3．配置完毕后如果ping不通，则要查看路由是否正确，查看路由器的各接口是否有正确地址并已激活，或者查看计算机的IP地址及默认网关是否正确。

**七、思考题**

1．如何用命令行查询路由器的接口配置情况？

2. 如何采用默认路由进行本实验的配置？

**八、实验考核要求**

1.撰写实验报告。

2.路由器配置模式能随意切换。

3.修改IP地址后，能正确配置静态路由，实现网络互联互通。

**实验项目三 OSPF动态路由实现**

**一、实验目的**

1．理解动态路由的原理。

2．进一步掌握路由器的配置模式和基本配置命令。

3. 掌握OSPF动态路由协议的配置。

**二、实验内容**

利用Packet Tracer网络仿真软件构建三个局域网（此处用一台计算机代表一个局域网），每个局域网连接到一台路由器，三台路由器通过串口线相连，在三台路由器上配置OSPF动态路由协议，实现三个局域网的互联。

**三、实验设备与环境**

运行Windows 7或Windows 10操作系统的计算机1台，Packet Tracer 6.2网络仿真软件1套，仿真设备路由器3台、PC机3台、连接线路若干。

**四、实验原理**

动态路由是通过网络中路由器之间的相互通信来传递路由信息，利用接收到的路由信息自动更新路由表。路由器之间进行路由信息交换时所运行的协议称为路由协议，通常说的路由协议是指动态路由协议。动态路由是指按照一定的算法，发现、选择和更新路由，从其他路由器上学习有关路由信息，用来自动建立或维护自己的路由表的过程。

动态路由协议可以随着网络拓扑结构的变化，通过动态学习的方式，在较短时间内自动更新路由表，使网络达到收敛状态。OSPF（Open Shortest Path First 开放式最短路径优先）是一个内部网关协议（Interior Gateway Protocol，简称 IGP）， 用于在单一自治系统（Autonomous System，AS）内决策路由。OSPF 性能优于 RIP，是当前域内路由广泛使用的路由协议。

OSPF协议有五种包：

1. Hellow：发现邻居建立邻接关系

2. DBD：检查路由器的数据库之间是否同步

3. LSR：向另外一台设备请求特定的链路状态

4. LSU：发送链路状态信息

5. LSACK：确认多段的发送信息

OSPF协议有三张表：

1. 邻居列表：列出每台路由器全部已经建立邻接关系的邻居路由器

2. 链路状态数据库：列出网络中其他路由器的信息，由此显示了全网的网络拓扑

3. 路由表：列出通过SPF算法计算出到达每个相连网络的最佳路径

OSPF协议的特点：

1. 区域概念，有效减少路由条目对CPU和内存占用，将拓扑变动局限在本区域内，详细的LSA泛洪控制

2. 邻接关系。OSPF协议定义了一些路由器类型和网络类型，邻接关系的建立是有交换Hellow信息的路由器类型和交换Hellow信息的网络类型决定的

3. 每台收到从邻居路由器发出的LSA的路由器都会把这些LSA记录在它的LSDB中，并且发送一份LSA拷贝给这台路由器其他所有邻居。

4. 当这些路由器LSDB完全相同时，就以自身为根，使用SPF算法计算一条无环的最短路径拓扑图。从而构建自己的路由表。

配置OSPF协议之前，必须先把路由器接口的IP地址配好并激活，然后在全局配置模式下启用OSPF协议，进入路由配置模式后通告与此路由器相连的网络。

在全局配置模式下启用OSPF路由的命令为：router ospf 1，在配置模式下通告相连网络的命令是：network 路由器各接口所在的网络地址 反向掩码 area 区域号。

本实验是用三台路由器连接三个局域网，配置OSPF动态协议后实现互联互通。

**五、实验步骤**

**1.** 用Packet Tracer 6.2构建网络拓扑

启动Packet Tracer 6.2，添加3台路由器（Generic，Router-PT）、3台PC机。用串口线连接路由器1的Serial2/0口与路由器2的Serial2/0口，以路由器1的Serial2/0口为DCE侧（串口线上有时钟标志）；用串口线连接路由器2的Serial3/0口与路由器3的Serial3/0口，以路由器2的Serial3/0口为DCE侧（串口线上有时钟标志）；PC机与路由器用交叉双绞线连接，每台计算机代表一个以太网。各端口及其IP地址见图3.1所示，（学生实验时需修改IP地址最后一个字段为学生本人学号后2位或后3位相关，依次递增1）。

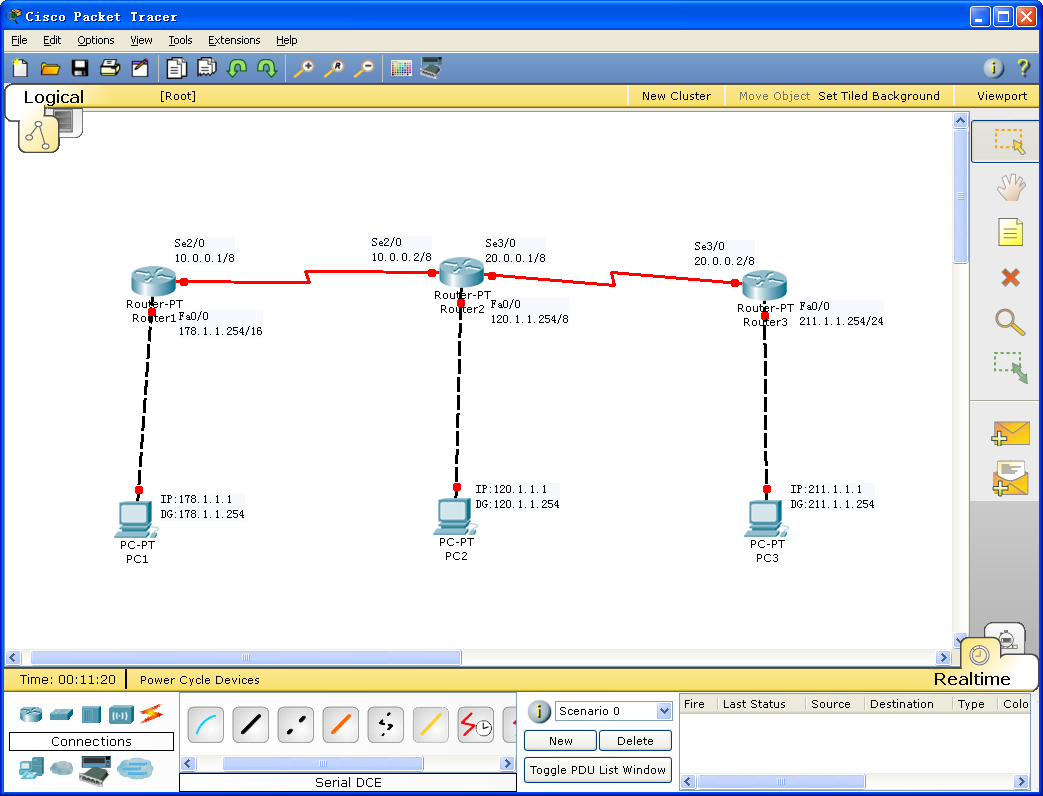


图3.1 OSPF动态路由配置网络拓扑图

**2.** 配置PC机的IP地址、子网掩码和默认网关地址

分别按拓扑图上的数据配置三台PC机的IP地址、子网掩码和默认网关地址，图3.2是PC1的配置图。配置默认网关时一定要注意，每台计算机的默认网关是与这台计算机相连的路由器接口的IP地址，其他机器的配置类似，此处略。



图3.2 PC1的IP配置

**3.** 配置路由器的接口

分别对3台路由器的快速以太网口和串口配置IP地址，并激活。

配置Router1的快速以太网接口和串口，见图3.3。

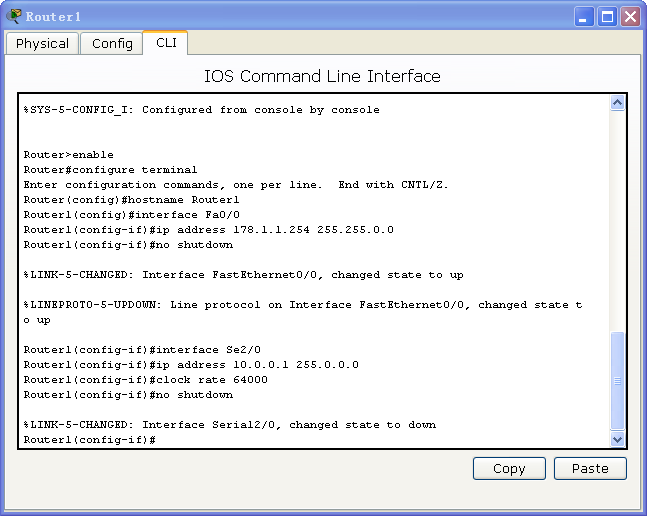


图3.3 Router1的接口配置

配置Router2的快速以太网接口和串口，见图3.4。

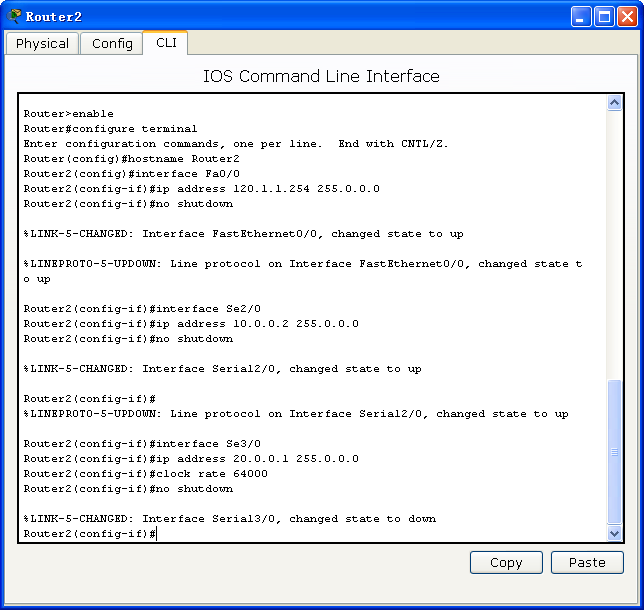


图3.4 Router2的接口配置

配置Router3的快速以太网接口和串口，见图3.5。

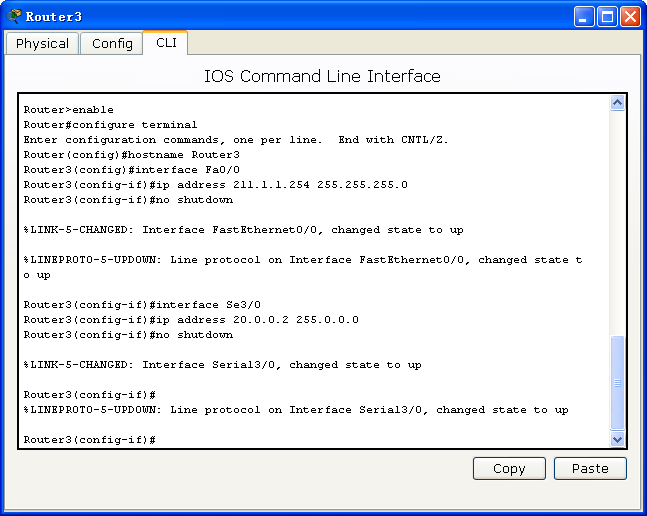


图3.5 Router3的接口配置

**4.**查询路由信息

在每台路由器的用户模式或特权模式下输入show ip route可以显示每台路由器的路由信息，Router1的路由信息如图3.6所示。

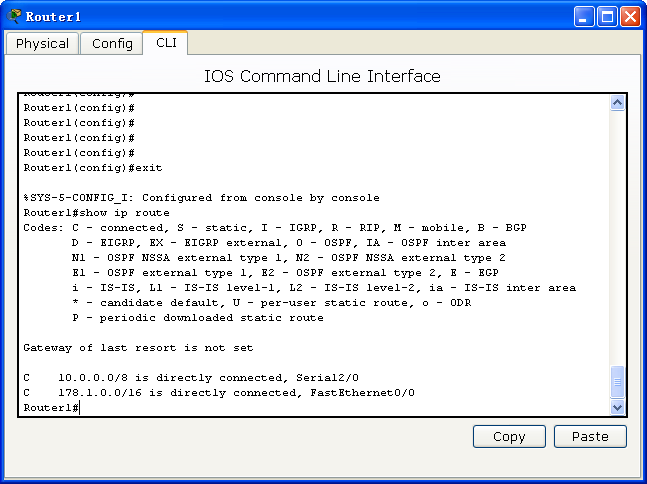


图3.6 Router1的路由信息

只有两条和Router1直接相连的直连路由信息，到其他网络没有路由。

C 10.0.0.0/8 is directly connected, Serial2/0 表示网络10.0.0.0/8通过串口Serial2/0与本路由器直接相连；

C 178.1.0.0/16 is directly connected, FastEthernet0/0表示网络178.1.0.0/16通过快速以太网接口FastEthernet0/0与本路由器直接相连。

Router2和Router3的路由信息也只有直连路由信息，读者可自行验证。

**5.**检验网络的连通性

在主机PC1的命令行分别输入ping PC2和PC3的IP地址的命令，如图3.7所示。结果均为超时，表明PC1与PC2、PC3尚未连通。

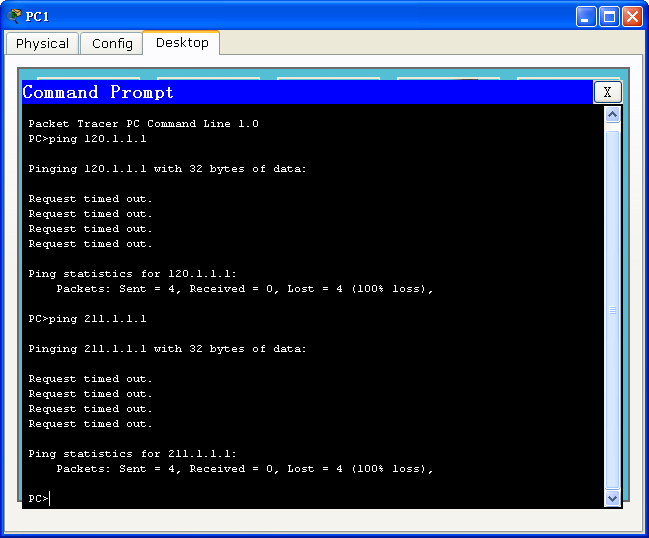


图3.7 用ping命令检测PC1至PC2和PC3的连通性

**6.** 配置OSPF动态路由协议

在全局配置模式下分别对每台路由器配置OSPF协议

Router1的配置命令如下：

Router1(config)#router ospf 1 //启用ospf动态路由协议

Router1(config-router)#network 178.1.0.0 0.0.255.255 area 0 //通告与自己直连的网络

Router1(config-router)#network 10.0.0.0 0.255.255.255 area 0 //通告与自己直连的网络

Router2的配置命令如下：

Router2(config)#router ospf 1 //启用ospf动态路由协议

Router2(config-router)#network 120.0.0.0 0.255.255.255 area 0 //通告与自己直连的网络

Router2(config-router)#network 10.0.0.0 0.255.255.255 area 0 //通告与自己直连的网络

Router2(config-router)#network 20.0.0.0 0.255.255.255 area 0 //通告与自己直连的网络

Router3的配置命令如下：

Router3(config)#router ospf 1 //启用ospf动态路由协议

Router3(config-router)#network 211.1.1.0 0.0.0.255 area 0 //通告与自己直连的网络

Router3(config-router)#network 20.0.0.0 0.255.255.255 area 0 //通告与自己直连的网络

**7.** 查询路由信息。

查询路由表

配置完三台路由器的动态路由以后，分别在每台路由器的用户模式或特权模式下输入show ip route可以显示每台路由器的路由信息，Router1的路由表如图3.8所示。

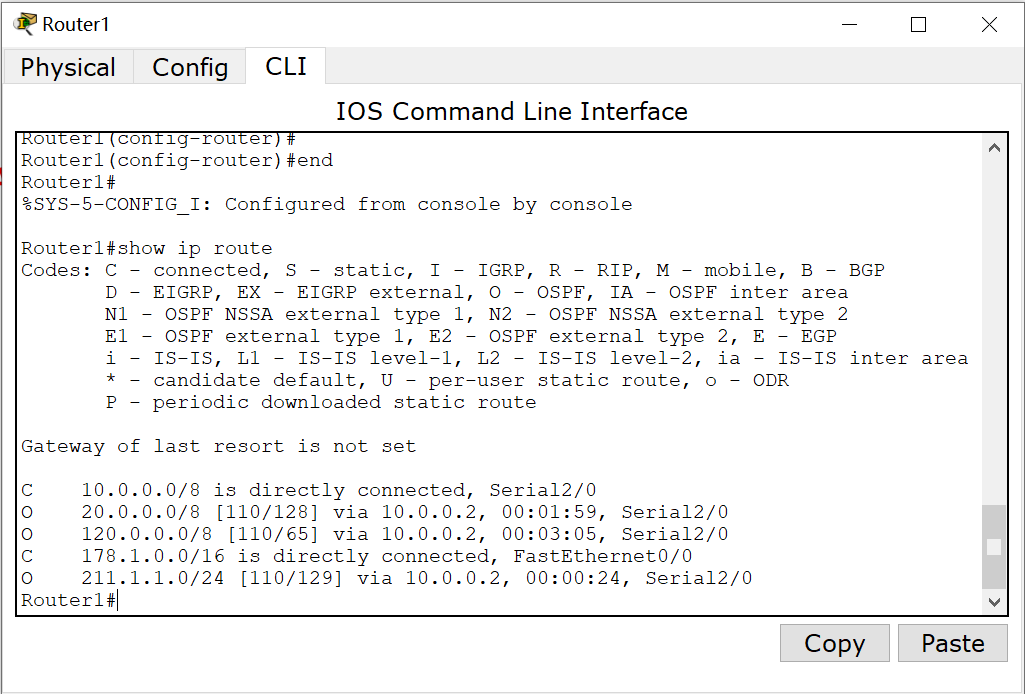


图3.8 配置完OSPF协议后的Router1的路由表信息

从图中可看出增加了三条以O为标志的路由记录，表明是通过OSPF协议动态获得的至其他三个网络的路由。

O 20.0.0.0/8 [110/128] via 10.0.0.2, 00:01:59, Serial2/0表示此路由表信息是通过OSPF动态路由协议获得的，到达网络20.0.0.0/8需经接口地址为10.0.0.2的路由器转发，路由优先级（即管理距离）为110，度量值为128，本路由器的出接口为串口Serial2。其他两条新增路由表信息请读者自己分析。

同样可以看到Router2和Router3的路由信息，也增加了几条路由，由读者自己验证，此处略。

查询路由协议信息

分别在每台路由器的用户模式或特权模式下输入show ip protocol可以显示每台路由器的路由协议信息，Router1的路由协议信息如图3.9所示。

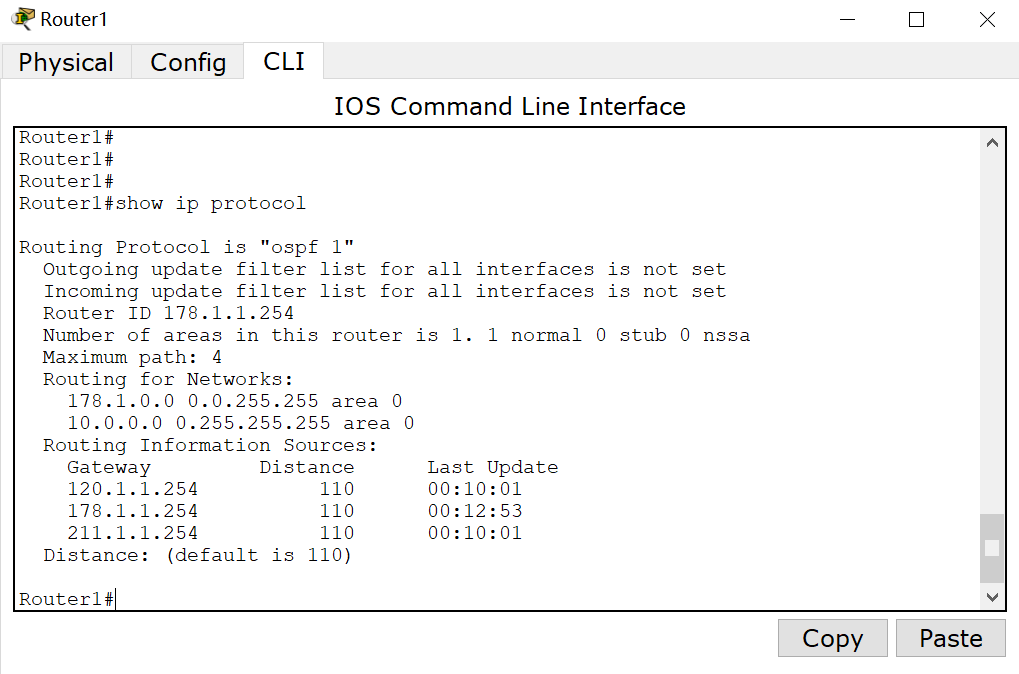


图3.9 查询Router1的路由协议信息

从图中可看出此路由器是采用OSPF作为动态路由协议的，路由进程号为1。路由器ID是178.1.1.254，是此路由器中IP地址的最大值。区域数为1，有1个标准区域（即骨干区域0），没有末梢区域（stub），没有nssa区域。在计算路由时，最多考虑 4 条等价路径。路由器将对 178.1.0.0/16 和 10.0.0.0/8 这两个网络进行路由，并且它们都属于 OSPF 区域 0。“Gateway” 列显示了邻居路由器的默认网关的IP 地址，分别为 120.1.1.254、178.1.1.254 和 211.1.1.254。

六、路由网络信息

另外两台路由器的路由信息读者可自行验证。

**8.** 验证网络的连通性

在主机PC1的命令行分别输入ping PC2和PC3的IP地址的命令，如图3.10所示，证明PC1与PC2、PC3已经连通，从而可以认为三台计算机所在的网络是相互连通的。读者可自行在PC2和PC3的命令行验证到其他计算机的连通性。

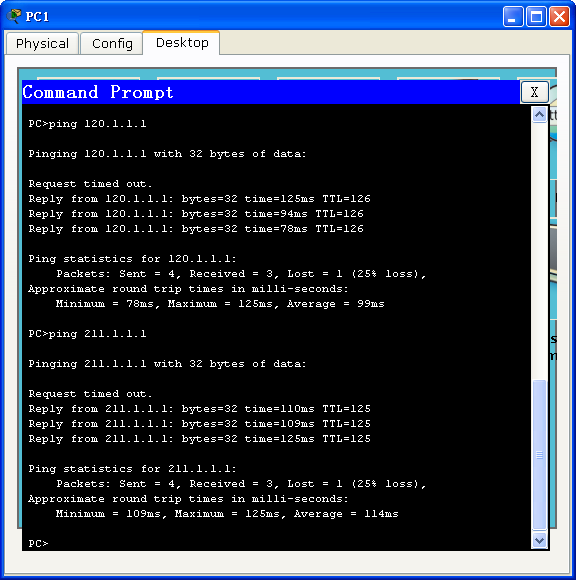


图3.10 用ping命令检测PC1至PC2和PC3的连通性

**六、实验注意事项**

1．路由器到计算机之间的连线必须使用交叉线（黑色虚线），不能使用直连线。

2．在配置路由器串口时，务必在DCE侧配置时钟信号频率并激活，否则路由器之间的链路不能连通。

3．配置完毕后如果ping不通，则要查看路由是否正确，查看路由器的各接口是否有正确地址并已激活，或者查看计算机的IP地址及默认网关是否正确。

**七、思考题**

1．此实验如改成用静态路由，如何配置？

2．动态路由与静态路由相比有何优点？

**八、实验考核要求**

1.撰写实验报告。

2.修改IP地址后，能正确配置OSPF路由协议，实现网络互联互通。

**实验项目四 典型三层网络规划与实现**

**一、实验目的**

掌握交换机VLAN、路由器静态路由和动态路由配置以及服务器配置，实现三层网络互联互通。

**二、实验内容**

此实验为综合实验，用来作为第2次阶段考核，通常采用全年级以赛代考方式进行。具体要求是，利用Packet Tracer网络仿真软件构建三层网络，给定IP地址、路由协议等参数，要求学生自行配置，实现网络互联互通。

**三、实验设备与环境**

运行Windows 7或Windows 10操作系统的计算机1台， Packet Tracer 6.2网络仿真软件1套，仿真设备路由器、交换机、PC机若干。

**四、实验原理**

交换机VLAN工作原理，路由器的静态路由和动态路由原理，以及服务器DNS、DHCP、HTTP和Email等工作原理，这些原理在其他实验项目中均有介绍，此处略。

**五、实验步骤**

由于此实验为综合实验，用于阶段考核，故略去详细步骤。学生可参考实验指导书其他部分完成此实验。

**六、实验注意事项**

1．全年级统一安排，要求在规定时间完成实验，通常为1小时。

2．学生可以自行参考任何资料，但必须完全由学生个人独立完成，不允许相互讨论。

**七、思考题**

无

**八、实验考核要求**

此实验通常作为第2次阶段考核来安排，所有学生统一时间完成。一般采用以赛代考方式进行。

**实验项目五 数据包捕获与分析**

**一、实验目的**

通过使用wireshark软件抓取TCP数据包，验证TCP数据格式和建立连接过程，加深对端口、TCP协议等网络基础知识的理解，掌握网络数据分析的基本技能。

**二、实验内容**

1. wireshark软件安装。
2. 使用wireshark软件捕获数据包，并阅读数据包内容。
3. 使用wireshark过滤器发现TCP建立连接的三次握手过程。
4. 使用netstat命令查看各端口状态，并读懂结果。

**三、实验设备与环境**

运行Windows 7或Windows 10操作系统的计算机1台，Wireshark软件。此实验也可在虚拟机上完成。

**四、实验原理**

传输控制协议（TCP，Transmission Control Protocol）是一种面向连接的、可靠的、基于字节流的传输层通信协议。有以下特点：

1.基于流的方式；

2.面向连接；（在通信之前要通过三次握手建立链接）

3.可靠通信方式；（确保数据不会丢失）

4.在网络状况不佳的时候尽量降低系统由于重传带来的带宽开销；（拥塞控制）

5.通信连接维护是面向通信的两个端点的，而不考虑中间网段和节点。因为有着拥塞控制和可靠数据传输的要求所以导致了TCP协议的传输效率相对于UDP要低，但是不会像UDP一样出现丢包现象。

TCP协议的报文格式如图4.1所示，各字段含义详见教材，此处略。截取TCP数据包后，需对照此图进行分析。



图4.1 TCP协议报文格式

**五、实验步骤**

1.安装Wireshark软件。如机器上未安装Wireshark软件，自行从网上下载，双节exe安装软件，直接点击下一步，按照提示继续下一步，重复多次即可安装成功。

2.启动软件。双击安装完毕的Wireshark，得到图4.2所示界面。



图4.2 Wireshark软件启动后的界面

3. 捕获数据包。鼠标单击红色线条标记的“开始捕获分组”，Wireshark开始抓包。然后打开浏览器，输入一个web网站地址，此处输入www.qq.com。捕获到TCP三次握手的数据包，如图4.3所示。

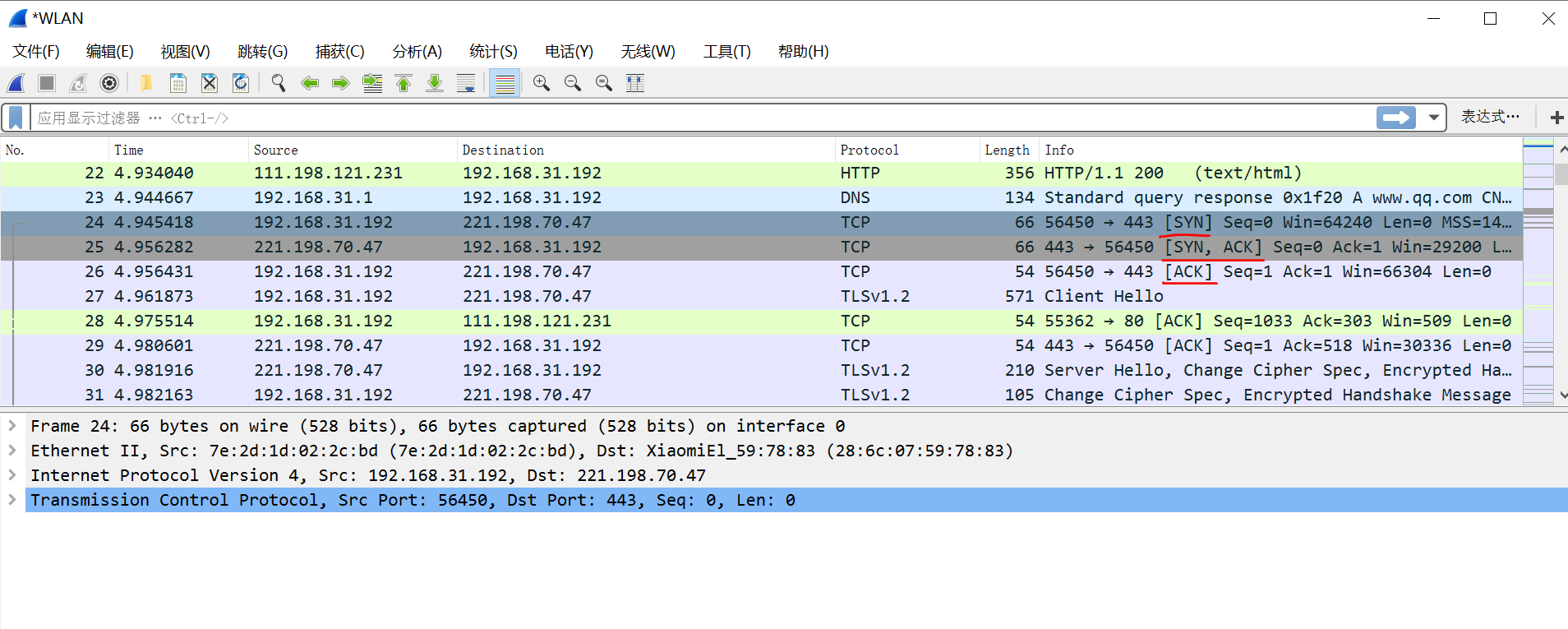


图4.3 TCP三次握手数据包

4.观察分析第一次握手的数据包。鼠标点击第一次握手的数据包，即第24个数据包，再展开TCP协议，可得到TCP报文各字段的数据详情，其16进制数据见最下面的阴影部分，如图4.4所示。

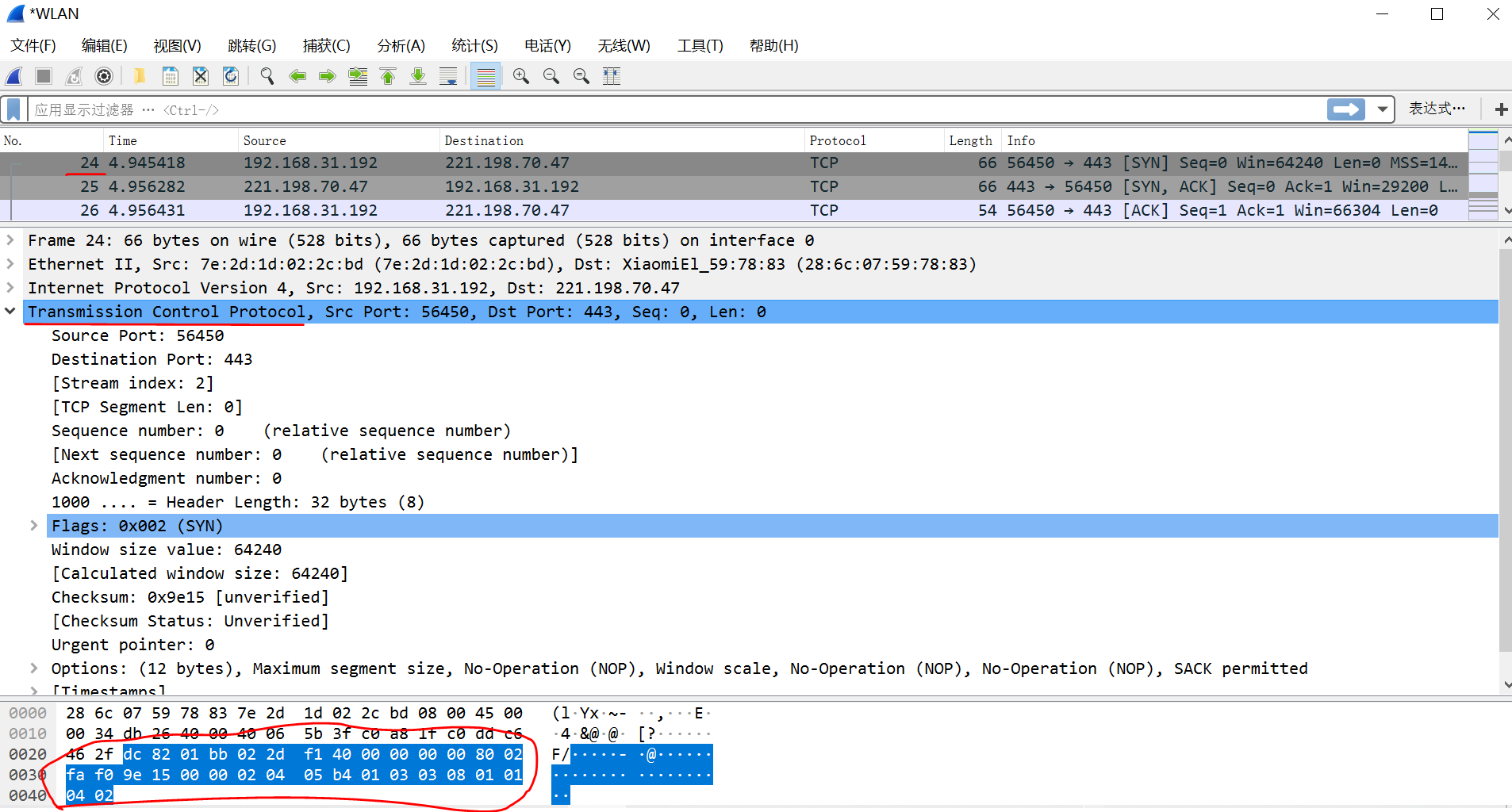


图4.4 TCP第一次握手数据包详情

5.填表对照分析第一次握手数据包，同学们也可分析第二次或第三次握手数据包。对照TCP报文格式，将各个字段数据填入表8.1。

表4.1 TCP报文字段分析

|  |  |
| --- | --- |
| 源端口 |  |
| 目的端口 |  |
| 序号 |  |
| 确认号 |  |
| 数据偏移  （即头部长度） |  |
| 紧急比特（URG) |  |
| 确认比特（ACK） |  |
| 推送比特（PSH） |  |
| 复位比特（RST） |  |
| 同步比特（SYN） |  |
| 结束比特（FIN） |  |
| 报文段的类型（服务类型） |  |
| 窗口值 |  |
| 检验和 |  |
| 紧急指针 |  |

**在实验报告中还需回答以下问题：**

这是第几次握手包？ 回答：

第2次握手包与第1次相比，增加了哪项？ 回答：

第2次握手包的序号：

第2次握手包的确认号：

第3次握手包的序号：

第3次握手包的确认号：

第3次握手包SYN比特为：

如果时间充裕，同学们还可以对照UDP、IP、ARP、ICMP等协议的报文字段，分别分析UDP、IP、ARP、ICMP等协议的数据包。

**六、实验注意事项**

如果“开始捕获分组”按钮是虚的，底下会提示找不到可用网卡或接口，是因为没有开启npf服务。则需用管理员权限启动命令行，用命令net start npf开启NetGroup Packet Filter Driver服务。

**七、思考题**

见实验步骤5要求在实验报告中回答的问题，此处略。

**八、实验考核要求**

1.按给定的专用的实验报告模板撰写本次实验报告。

2.能够截获TCP三次握手包，并进行分析。

3.TCP协议字段数据分析正确，表格填写正确。

**实验项目六 NAT技术**

**一、实验目的**

通过在网络仿真软件上完成NAT技术的实现和应用过程，加深对端口、公网IP和NAT等网络基础知识的理解，养成理论联系实际和勤于思考的态度和学风。

理解NAT网络地址转换的原理及功能，掌握静态 NAT 的配置，实现局域网访问互联网。在此基础上了解动态NAT和NAPT的配置过程。

1. **实验内容**

1.在百度网页上查看实验室计算机的外网地址，认识NAT在实际中的应用；

2.配置静态NAT或动态NAT，观察NAT路由器对数据包的处理方法，理解NAT工作原理。

**三、实验设备与环境**

运行Windows 7或Windows 10操作系统的计算机1台，Packet Tracer 6.2网络仿真软件1套，仿真设备路由器、交换机、PC机若干。

**四、实验原理**

网络地址转换 NAT（Network Address Translation），被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。原因很简单，NAT 不仅完美地解决了 IP 地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

默认情况下，内部 IP 地址是无法被路由到外网的，内部主机 10.1.1.1 要与外部 Internet 通信，IP 包到达 NAT路由器时，IP 包头的源地址 10.1.1.1 被替换成一个合法的外网 IP，并在 NAT 转发表中保存这条记录。当外部主机发送一个应答到内网时，NAT 路由器受到后，查看当前 NAT 转换表，用 10.1.1.1 替换掉这个外网地址。

NAT 将网络划分为内部网络和外部网络两部分，局域网主机利用 NAT 访问网络时，是将局域网内部的本地地址转换为全局地址（互联网合法的 IP 地址）后转发数据包；

NAT 分为两种类型：NAT（网络地址转换）和 NAPT（网络端口地址转换 IP 地址对应一个全局地址）。

静态 NAT：实现内部地址与外部地址一对一的映射。现实中，一般都用于服务器；

动态 NAT：定义一个地址池，自动映射，也是一对一的。现实中，用得比较少；

NAPT（也叫作PAT）：使用不同的端口来映射多个内网 IP 地址到一个指定的外网 IP 地址，多对一。

**五、实验步骤**

（一）在百度网页上查看NAT转换情况。

首先，在命令行用ipconfig查看本机IP地址，可以看到是一个私网地址。

其次，打开浏览器，输入百度网址后，在搜索框里输入“IP”两个字母，即可查到用于访问互联网的公网地址。

（二）在Packet Tracer软件上进行静态NAT配置

1.新建 Packet Tracer 拓扑图，如图6.1所示。

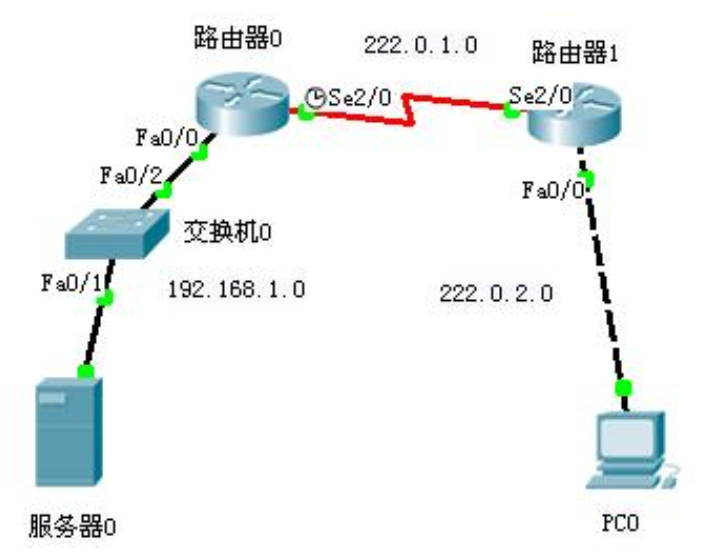


图6.1 静态NAT配置拓扑

**注意：**本实验指导书中Router0的Fa0/0的IP地址为192.168.1.1，Router1的Fa0/0的IP地址为222.0.2.1，实际配置时需将Router0的Fa0/0的IP地址改为192.168.1.本人学号后2位或后3位，Router1的Fa0/0的IP地址修改为222.0.2.本人学号后2位或后3位。

R1 为公司出口路由器，其与外部路由器之间通过 V.35 电缆串口连接，DCE 端连接在R1上，配置其时钟频率 64000；  
2.配置 PC 机、服务器及路由器接口 IP 地址，如下：

Server-PT的配置：

IP地址：192.168.1.2

子网掩码：255.255.255.0

默认网关：192.168.1.1，学生配置时要注意修改

PC0的配置：

IP地址：222.0.2.2

子网掩码：255.255.255.0

默认网关：222.0.2.1，学生配置时要注意修改  
3.在各路由器上配置接口的IP地址和静态路由协议，让PC间能相互Ping 通。

**Router0的配置：**

en //从用户配置模式切换到特权配置模式

conf t //从特权配置模式切换到全局配置模式

host R0 //为Router0命名为R0，学生需改成自己姓名全拼+0

int fa 0/0 //从全局配置模式切换到接口配置模式

ip address 192.168.1.1 255.255.255.0 //接口IP地址配置

no shutdown //激活接口

int s 2/0

ip address 222.0.1.1 255.255.255.0

no shutdown

clock rate 64000 //DCE侧设备配置时钟频率

exit //从接口配置模式返回上一层（全局）配置模式

ip route 222.0.2.0 255.255.255.0 222.0.1.2 //静态路由配置

**Router1的配置：**

en

conf t

host R1

int s 2/0

ip address 222.0.1.2 255.255.255.0

no shut

int fa 0/0

ip address 222.0.2.1 255.255.255.0

no shutdown

exit

ip route 192.168.1.0 255.255.255.0 222.0.1.1

end

show ip route //显示路由表

在PC0上验证网络连通性。

**PC0的配置：**

进入CMD命令行（即run），输入

ping 192.168.1.2 (有数据包回应，success)

打开Web 浏览器，输入

http://192.168.1.2 (可以打开网页，success)  
4.在R1上定义内外网络接口并配置静态NAT。

int fa 0/0

ip nat inside  //配置NAT转换的内部接口

int s 2/0

ip nat outside //配置NAT转换的外部接口

exit

ip nat inside source static 192.168.1.2 222.0.1.3 //配置静态NAT

end

show ip nat translations //显示NAT转换结果  
5.验证NAT配置完成后，主机之间的互通性。

**PC0的配置：**

打开Web 浏览器，输入

http://222.0.1.3 (success)

6.查看NAT转换结果。

**Router0的配置：**

show ip nat translations

可以看到一些内外网地址，这些就是NAT的转换结果。

**动态NAT和NAPT实验要求和步骤见教材，此处略。**

**六、实验注意事项**

此实验是采用静态路由实现互联互通，同学们也可采用OSPF动态路由协议完成此实验。鼓励同学们脱离指导书，采用OSPF协议实现。

**七、思考题**

1.静态NAT能否节约IPv4地址资源？如果不能节约地址资源，为什么还需要静态NAT？

2.在实验室电脑上通过百度网页查看到公网地址，它是采用哪种NAT技术实现的？

**八、实验考核要求**

1.撰写实验报告。

2.会配置静态NAT。

3.会查看NAT转换结果。

4.如能完成动态NAT和NAPT实验，可酌情加分。

**实验项目七 基于服务器的网络应用搭建**

**一、实验目的**

1．理解DNS原理，掌握DNS服务器的安装与配置。

2．理解DHCP原理，掌握DHCP服务器的安装与配置。

3. 掌握WWW、FTP、Email服务器的安装与配置。

**二、实验内容**

**说明：**由于在电脑上运行多台Win7、Win10或高版本的Windows Server虚拟机非常卡，经常无法正常实验，故此采用较早版本的Windows XP和Windows 2003 Server虚拟机进行组网实验。

利用VMware软件组建由三台计算机组成的局域网，其中两台为Windows Server 2003服务器，一台为Windows XP客户机，在一台Windows Server 2003上安装、配置DNS和DHCP服务，在一台Windows Server 2003上安装、配置WWW、FTP、Email服务，在Windows XP上对这些服务进行验证。此实验也可直接在Packet Tracer软件上完成，配置思路与此指导书相同，但步骤有所区别，学生可参考有关配置录屏。其中DHCP、Email以及FTP服务的配置过程也可参考网页：

https://blog.csdn.net/qq\_44223394/article/details/121107053

**三、实验设备与环境**

运行Windows 7或Windows 10操作系统的计算机1台，安装有 VMware虚拟机软件并新建了Windows 2003 Server和Windows XP操作系统，Windows 2003 Server安装光盘镜像文件。三台虚拟机组成的网络拓扑如图7.1所示：

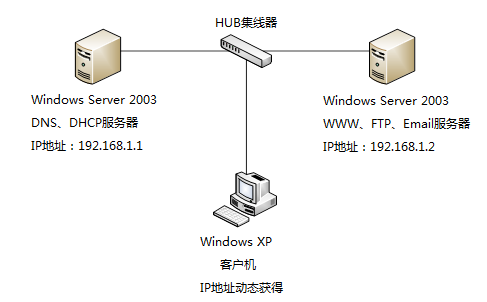


图7.1 虚拟机组网拓扑图

**四、实验原理**

Internet之所以能为人们提供各种各样的服务，就是因为在Internet上有无数的服务器。例如DNS是将域名地址解析成IP地址，DHCP是为网络内的计算机动态分配IP地址，WWW是提供web网页服务，FTP是为两台计算机之间提供文件传输服务，Email是为网络内的用户提供电子邮件服务。以访问搜狐网站为例，在客户机浏览器地址栏输入www.sohu.com的域名地址后，浏览器即向本机设置的DNS服务器发出域名解析请求，如果这台DNS服务器缓存或区域数据库里有www.sohu.com的IP地址信息，则将IP地址返回给客户机，然后客户机再通过此IP地址去访问搜狐网站。否则，这台DNS服务器必须通过递归或迭代查询其它DNS服务器才能获得www.sohu.com的IP地址信息。

在递归查询中，DNS域名服务器将代替提出请求的下级DNS服务器进行域名查询，若域名服务器不能直接回答，则域名服务器会在域树中的各分支的上下进行递归查询，最终将返回查询结果给客户机，在域名服务器查询期间，客户机将完全处于等待状态。DNS递归查询原理如图7.2所示：

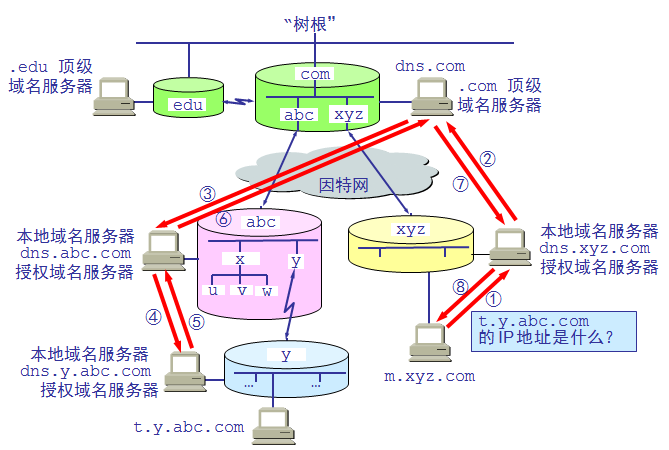


图7.2 DNS递归查询

DHCP叫做动态主机配置协议，作用是分配动态的IP地址。DHCP工作时客户机和服务器进行交互，由客户机通过广播向服务器发起申请IP地址的请求，然后由服务器分配一个IP地址以及其他的TCP/IP设置信息。整个过程可以分为以下步骤：

DHCP发现：DHCP客户机的TCP/IP首次启动时，使用广播方式发送DHCP请求信息包，广播信息中包括了客户机的网络界面的硬件地址和计算机名字，以提供DHCP服务器进行分配。

DHCP提供：当接收到DHCP客户机的广播信息之后，所有的DHCP服务器均为这个客户机分配一个合适的IP地址，将这些IP地址、网络 掩码、租用时间等信息，按照DHCP客户提供的硬件地址发送回DHCP客户机。此客户机能收到多个IP地址提供信息。

DHCP请求：由于客户机接收到多个服务器发送的多个IP地址提供信息，客户机将选择一个IP地址，拒绝其他提供的IP地址。

DHCP确认：服务器将收到客户的选择信息，如果也没有例外发生，将回应一个确认信息，将这个IP地址真正分配给这个客户机。客户机就能使用这个IP地址及相关的TCP/IP数据，来设置自己的TCP/IP堆栈。

DHCP工作的四个步骤如图7.3所示：

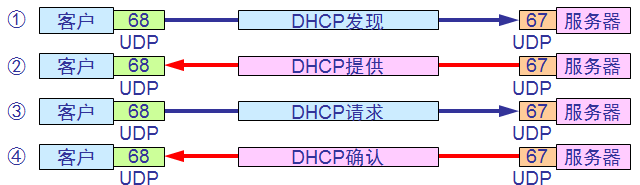


图7.3 DHCP工作过程

**五、实验步骤**

（一） 在虚拟机环境下组建局域网

1． 使用VMware Workstation组建由2台服务器和1台客户机组成的局域网，网络拓扑如图7.4所示。启动虚拟机软件WMware Workstation，选择1台XP虚拟机，2台Windows 2003 Server虚拟机。在每台虚拟机的网络适配器上单击鼠标，打开虚拟机设置，点击网络适配器，选择LAN区段，新建一个LAN1区段，将3台虚拟机同时加入到一个局域网，如图7.4所示。

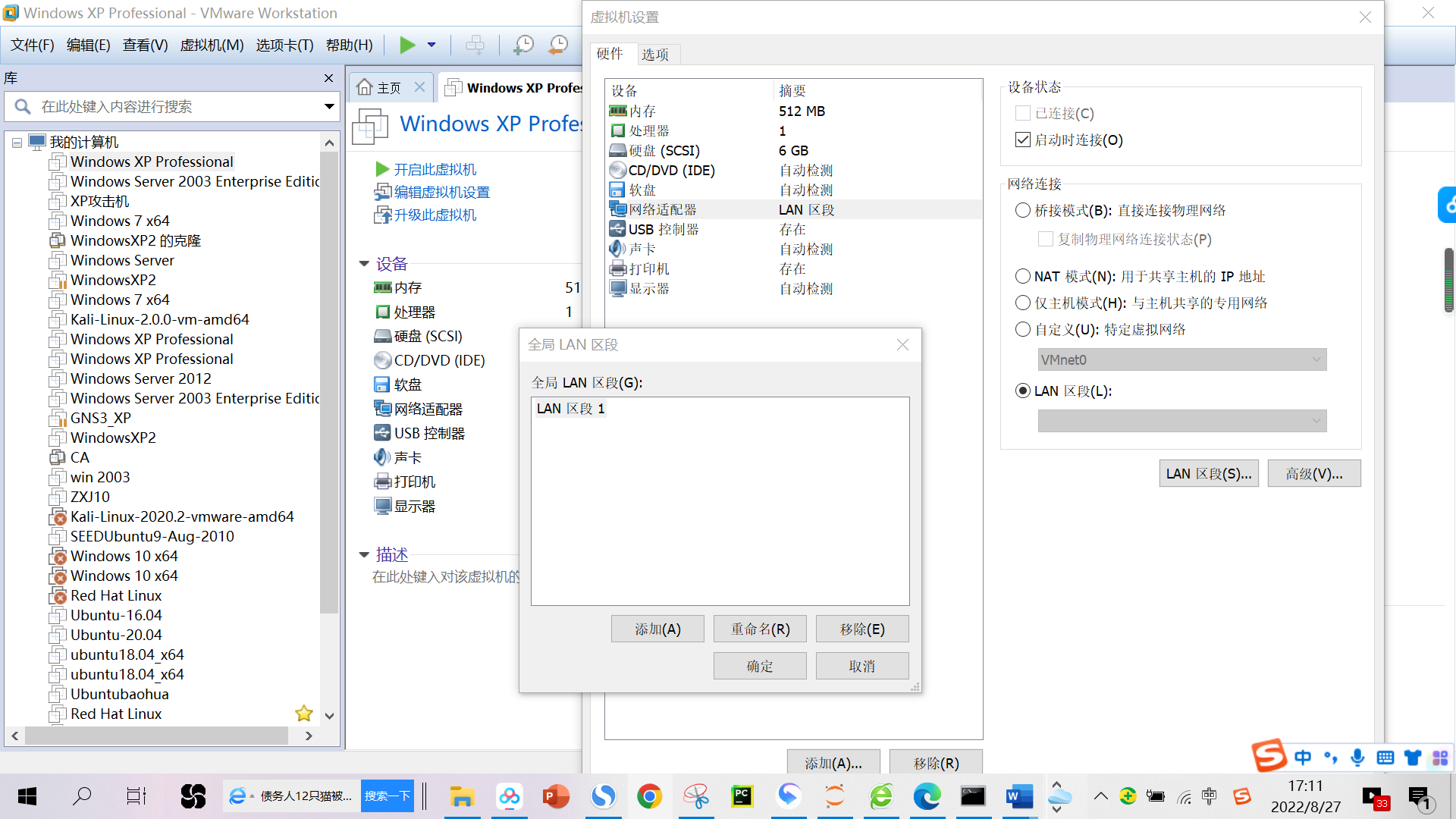


图7.4 将所有虚拟机添加到一个LAN区段

**2.** 启动Team，在Server虚拟机上通过“开始→控制面板→网络连接→本地连接”，打开本地连接状态对话框，点击“属性”打开本地连接属性对话框，选择“Internet协议(TCP/IP)”后点击“属性”，按照网络拓扑图的配置，将2台Server虚拟机的IP地址分别设置为：192.168.1.1和192.168.1.2（学生实验时，IP地址根据学生学号进行修改），子网掩码设置为默认，首选DNS服务器都设置为192.168.1.1。按照类似的步骤，设置XP虚拟机上的Internet协议(TCP/IP)属性，选择自动获得IP地址和自动获得DNS服务器地址。如图7.5和图7.6所示。

图7.5 选择本地连接

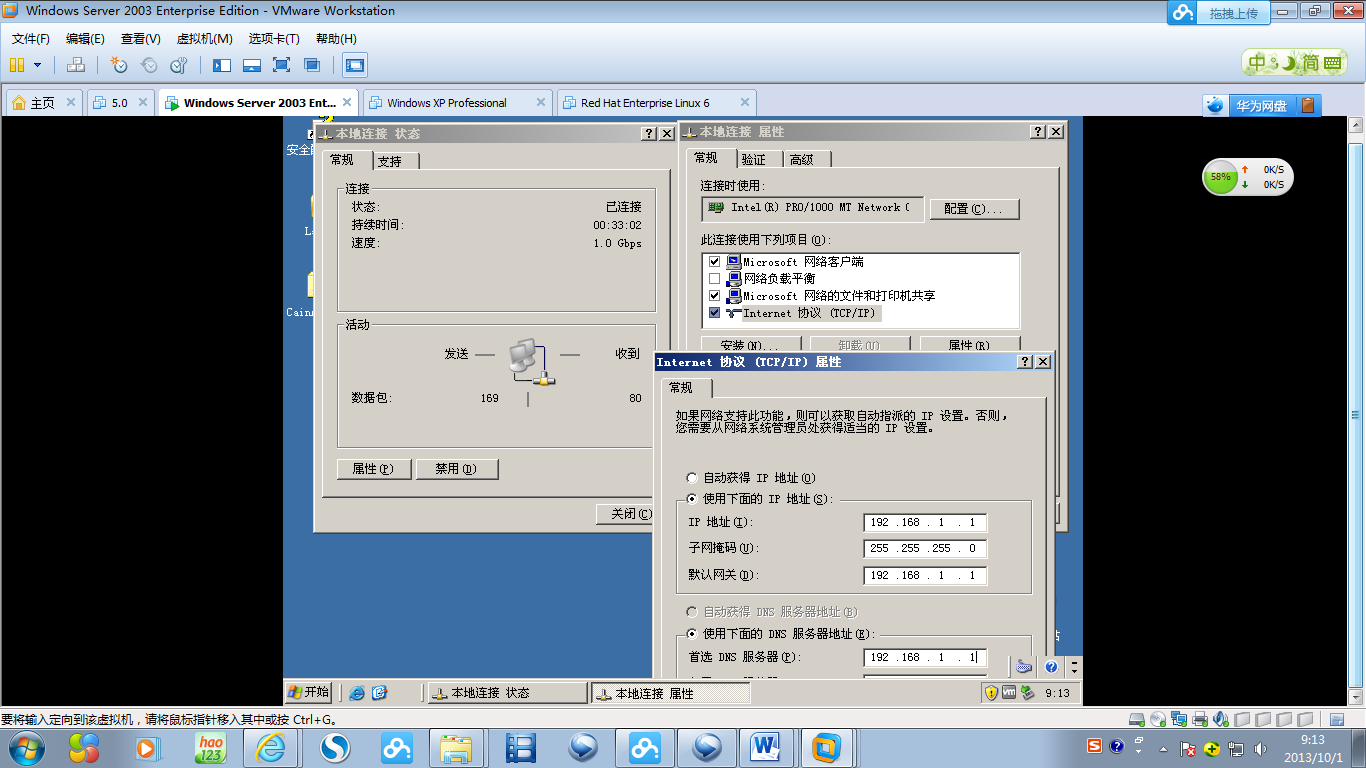


图 10.6 设置IP地址和DNS服务器地址

设置完IP地址后，在第1台Server计算机上打开命令行，输入ping 192.168.1.2 的命令，看是否有reply，如果有reply表明网络已连通，否则要查找原因，把网络连通起来。

（二）DNS服务器和DHCP服务器的安装与配置

1. DNS、DHCP服务器的安装

选择Team中的第1台Windows 2003 Server服务器，运行“控制面板”中的“添加/删除程序”选项，选择“添加/删除Windows组件”，出现如图7.7所示对话框，选择“网络服务”复选框，并单击“详细信息”按钮，在出现“网络服务”对话框中，选择”动态主机配置协议(DHCP)” 和“域名系统（DNS）”，单击“确定”按钮，系统开始自动安装相应服务程序。出现放入安装光盘文件的提示时，将 Windows Server 2003 CD-ROM 插入计算机的 CD-ROM 或者 DVD-ROM 驱动器，也可在虚拟机软件的VM菜单下点击Settings，在Hardware里点击CD-ROM，选中右侧的Use ISO Image，点击Browse找到Windows Server 2003光盘镜像文件，点击确认就可安装DNS和DHCP服务组件了。

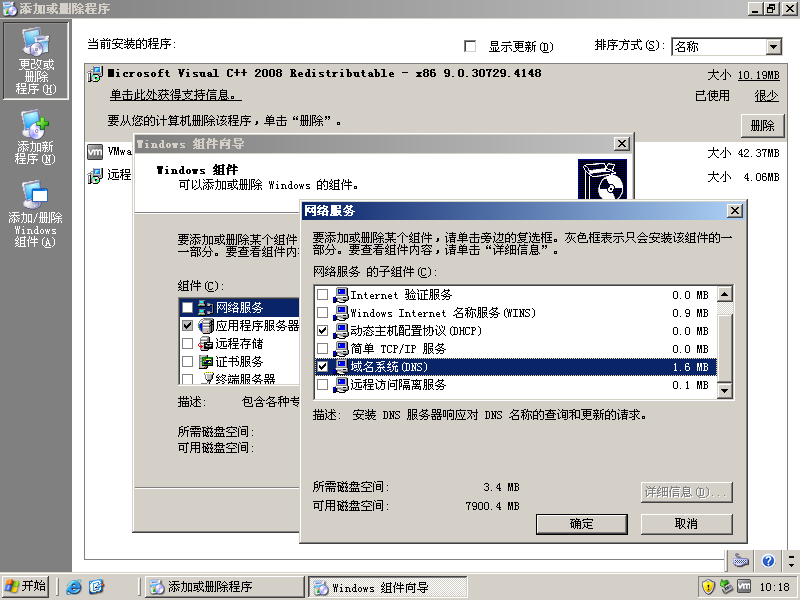


图7.7 安装网络服务组件

2．DNS服务器的配置

完成安装后，在“开始”→“所有程序”→“管理工具”，选择“DNS”选项，进行DNS服务器管理与设置。

**1）**添加正向查找区域

在创建新的区域之前，首先检查一下DNS服务器的设置，确认已将“IP地址”、“主机名”、“域”分配给了DNS服务器。检查完DNS的设置，按如下步骤创建新的区域：

* 1. 选择“开始”→“程序”→“管理工具”→“DNS”，打开DNS管理窗口。
  2. 选取要创建区域的DNS服务器，右键单击“正向查找区域”选择“新建区域”。
  3. Windows 2003的DNS服务器支持三种区域类型：主要区域，该区域存放此区域内所有主机数据的正本；辅助区域该区域存放区域内所有主机数据的副本；Active Directory集成的区域，该区域主机数据存放在域控制器的Active Directory内，这份数据会自动复制到其他的域控制器内。
  4. 在出现的对话框中选择要建立的区域类型，这里我们选择“主要区域”，单击“下一步”，注意只有在域控制器的DNS服务器才可以选择“Active Directory集成的区域”。
  5. 出现“区域名”对话框如图7.8，输入新建主区域的区域名，例如bcu.edu.cn，然后单击“下一步”，文本框中会自动显示默认的区域文件名。如果不想使用默认的文件名，也可以键入不同的名称。

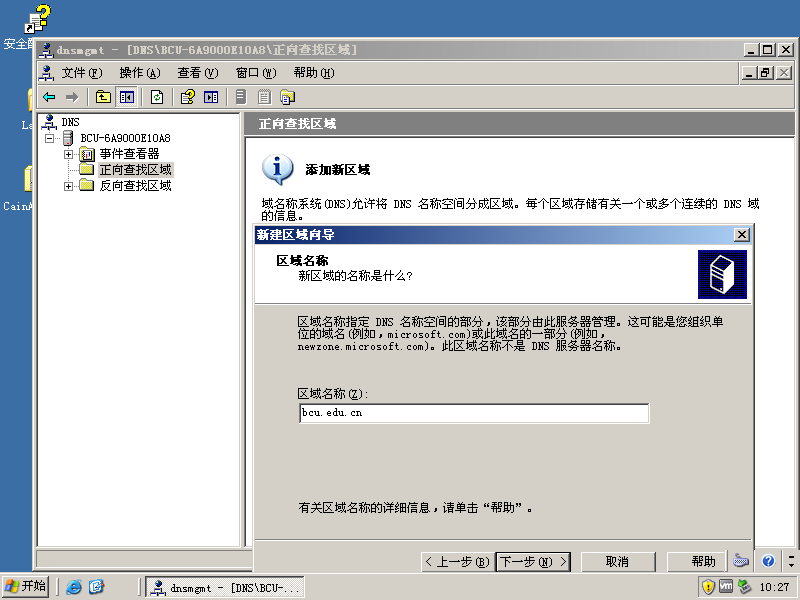


图7.8 新建正向查找区域

* 1. 在“正在完成新建区域向导”的对话框中单击“完成”按钮，结束区域添加。新创建的主区域bcu.edu.cn显示在所属DNS服务器的列表中，如图7.9所示。



图7.9 正向查找区域bcu.edu.cn

**2）**添加DNS记录

创建新的主区域后，“域服务管理器”会自动创建起始机构授权、名称服务器、主机等记录。在“bcu.edu.cn”区域名上右击鼠标，选择”添加主机”，输入”www”主机名，则完全合格的域名中显示”www.bcu.edu.cn”的完整域名，输入其对应的IP地址，点击“添加地址”如图7.10所示。按网络拓扑图中给定的数据，依次添加FTP、Email服务器的主机名和IP地址，如图7.11所示。



图7.10 添加www主机及其IP地址

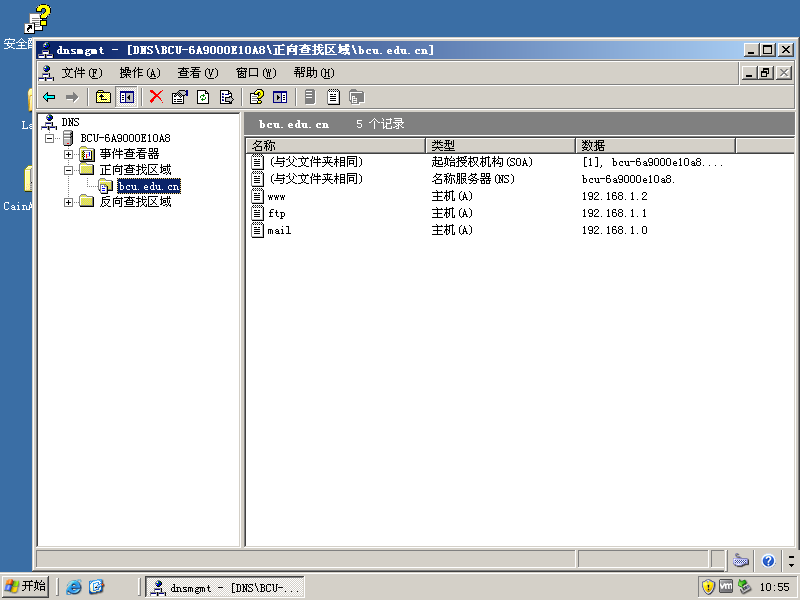


图7.11 正向查找区域主机列表

3）验证DNS服务器是否正常工作

在本服务器上或其他计算机上输入ping www.bcu.edu.cn，看DNS服务器是否能正常解析域名。

3．DHCP服务器的配置

1）新建作用域。选择Team中的第一台Windows 2003 Server的服务器，单击“开始”→“所有程序”→“管理工具”→“ DHCP”，可以对DHCP服务进行配置。 在控制台树中，右键单击要在其上创建新 DHCP 作用域的 DHCP 服务器，然后单击新作用域，如图7.12所示。

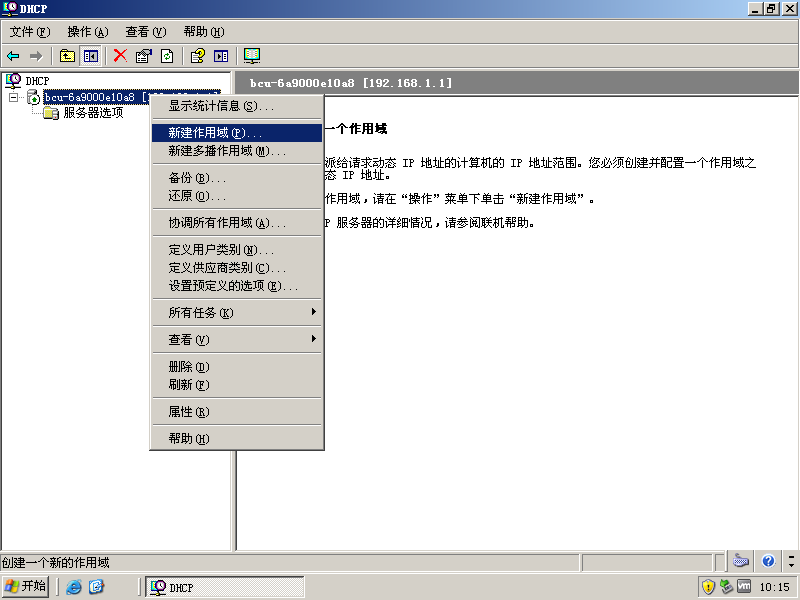


图7.12 新建作用域

2）在“新作用域向导”中，单击“下一步”，然后键入该作用域的名称及说明，如图7.13。

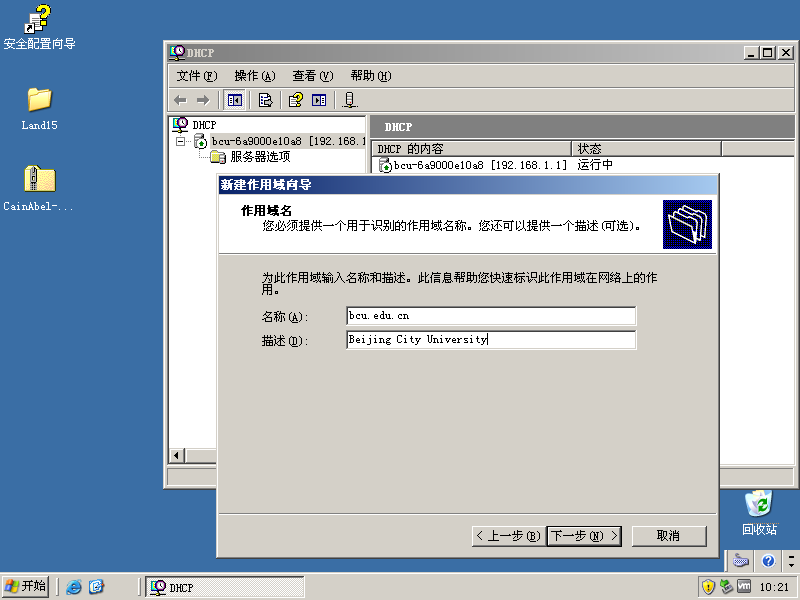


图7.13 输入作用域名称和描述

3）输入在该作用域可分配的IP地址范围。例如，起始 IP 地址为 192.168.1.1，结束地址为 192.168.1.254，如图7.14所示。

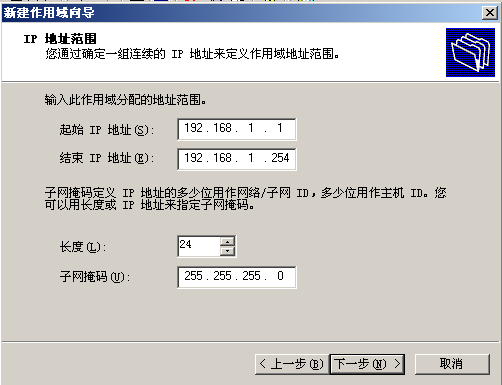


图7.14 输入可分配的IP地址范围

4）添加不分配的IP地址（即排除范围）。单击“下一步”，在弹出的对话框中键入要从所输入范围中排除的任何 IP 地址。如已静态分配给局域网中各个计算机的所有地址。通常情况下，默认网关、域控制器、Web 服务器、DHCP 服务器、域名系统 （DNS） 服务器和其他服务器均需静态分配IP 地址，如图7.15所示。单击“下一步”。

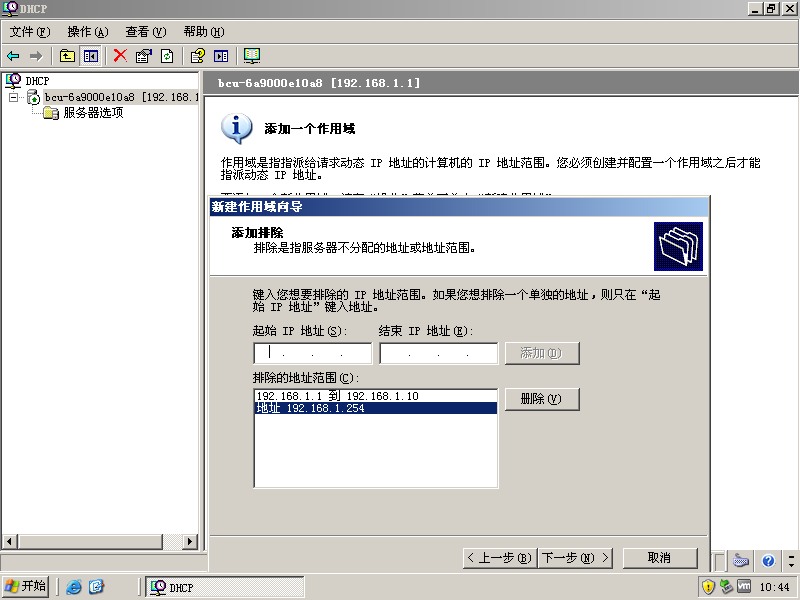


图7.15 添加IP地址排除范围

5）键入该作用域的IP地址租用到期之前的天数、小时数和分钟数，单击“下一步”后选择“是，我想现在配置这些选项（Y）”。单击“下一步”后输入路由器（默认网关）的 IP 地址，并点击“添加”，从作用域获得IP 地址的客户端将使用此IP 地址作为默认的转发路由器。如果在网络中使用 DNS 服务器，则在“父域”框中键入此DHCP服务器所在域的父域名称，此处可不输入。输入DNS 服务器的IP地址，服务器名可不输入，如图7.16所示。单击下一步后提示输入WINS服务器名和IP地址信息，此处可忽略，直接单击“下一步”，选择激活此作用域，完成DHCP服务器的配置。

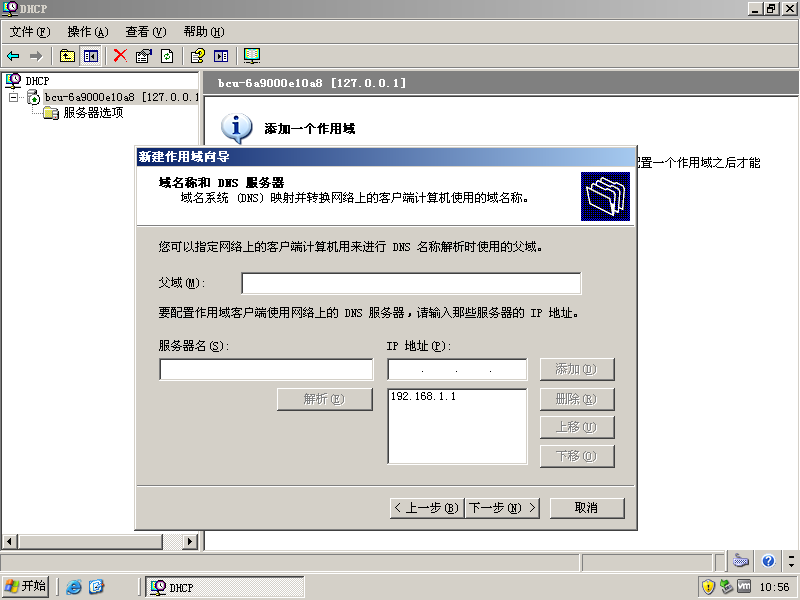


图7.16 输入DNS服务器地址

6）使XP计算机获得IP地址、默认网关等TCP/IP配置信息。在Team组里的XP计算机上找到“本地连接”图标，鼠标右击后选择“停用”，再次右键点击后选择“启用”，此台XP计算机就可从DHCP服务器获得一个IP地址。

7） 查询DHCP地址池和租约。单击DHCP配置对话框的“地址池”，可看到此作用域可供分配的IP地址范围以及被排除的范围，如图7.17所示。单击“地址租约”，看到有一个地址192.168.1.11被分配出去，如图7.18所示。在XP计算机上运行ipconfig /all命令，即可查到XP计算机的IP地址、默认网关和首选DNS服务器的地址信息，这些信息都是由DHCP服务器自动为XP计算机设置的，如图7.19所示。

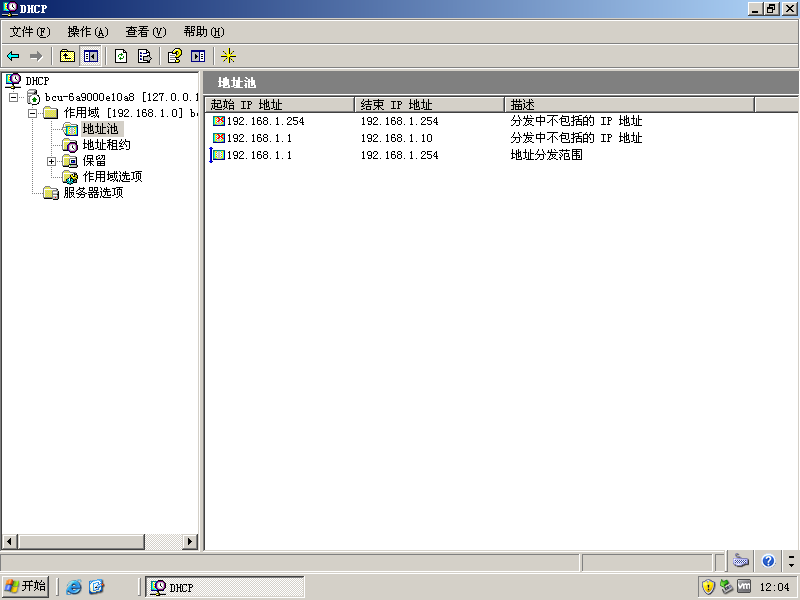


图7.17 可供分配的IP地址及排除范围

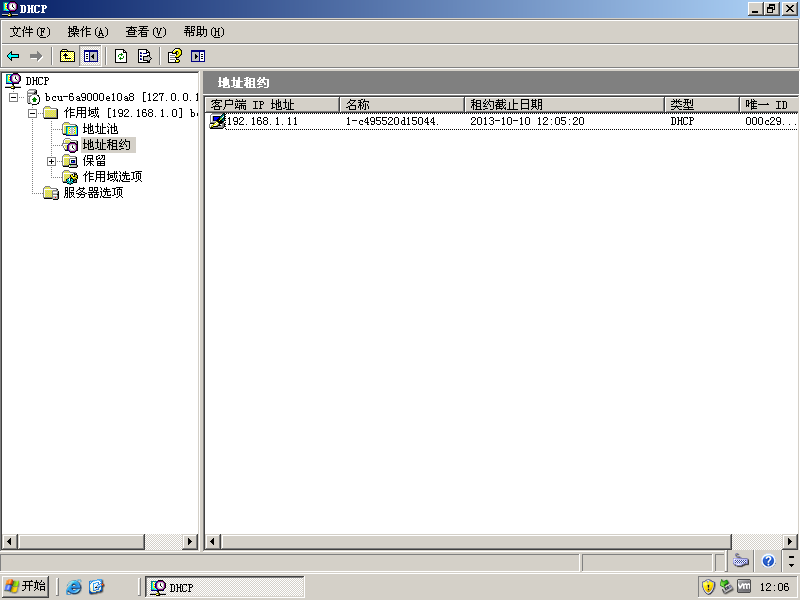


图7.18 已分配的IP地址（地址租约）

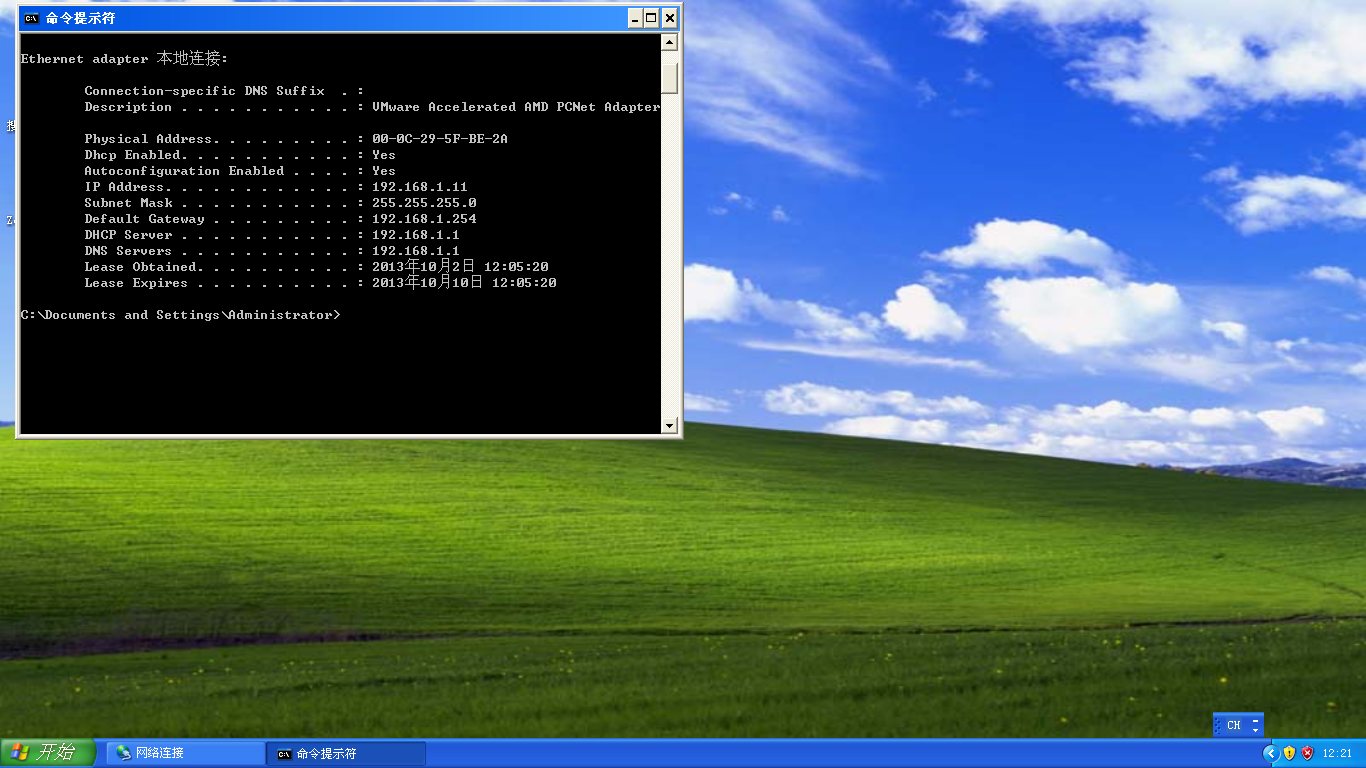


图7.19 使用ipconfig命令查询TCP/IP配置信息

（三）WWW、FTP、Email应用服务器的安装与配置

1**.** IIS Internet信息服务（IIS）及电子邮件服务的安装

在Team中的第二台Windows Server 2003服务器上，通过“开始→控制面板→添加/删除程序→添加/删除Windows组件”，打开Windows组件向导，勾选“电子邮件服务”，然后选中“应用程序服务”（不在前面方框处打勾）后单击“详细信息”选“Internet信息服务（IIS）”， 单击“详细信息”后勾选“SMTP Service”、“万维网服务”和“文件传输协议（FTP）服务”，如图7.20，单击两次“确定”后，单击“下一步”系统自动安装组件，出现放入安装光盘文件的提示时，可以使用Windows 2003光盘镜像文件，设置好镜像安装文件的位置，点击确认就可安装IIS服务组件了。完成安装后，系统在控制面板的管理工具中，添加一项“Internet服务管理器”。

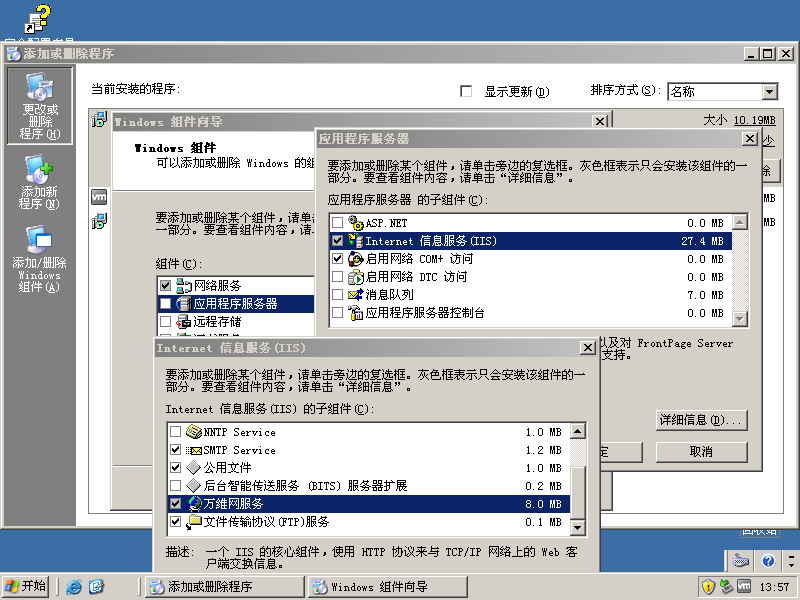


图7.20 添加IIS服务

2. WWW站点的配置

单击“开始”→“所有程序”→“管理工具”→“Internet信息服务（IIS）管理器”，打开“Internet信息服务窗口”，可看到有FTP站点、网站、默认SMTP虚拟服务。展开“网站”，在“默认站点”上右击鼠标，点击“属性”，打开默认站点的“属性”对话框，选择“主目录”，可看到默认网站文件存放的默认目录是c:\inetpub\wwwroot，默认权限为读取，如图7.21所示。

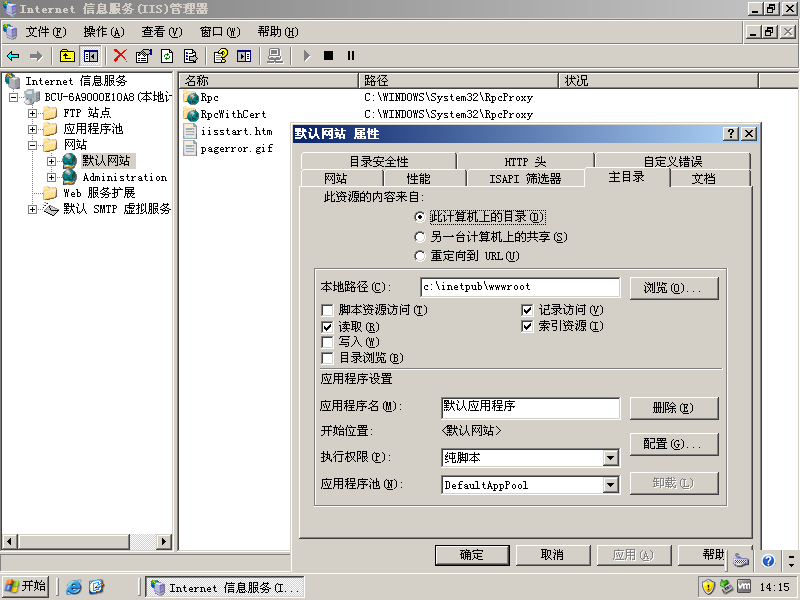


图7.21 默认网站的属性对话框

在“主目录”属性页，可设置WWW站点文件的存放主目录，内容的访问权限以及应用程序在此站点的执行许可等。 在“文档”属性页，可设置启动默认文档，默认文档可以是HTML文件或ASP文件，是站点的主页，如default.htm、default.asp和index.htm等。

将制作好的站点的所有文件复制到站点对应主目录，把网站首页文件取名为Default.htm，就可以发布此Web网站。此处实验用一个简单的网页进行验证。

在c:\inetpub\wwwroot目录下新建一个文本文档，并键入以下html语句：

<html>

<head>

<title>

简单网站示例

</title>

</head>

<body>

这是一个简单的网站，欢迎访问！

</body>

</html>

保存文件后将文件名改成Default.htm，打开本机或客户机浏览器，在地址栏中输入站点的IP地址或域名地址，即可浏览该站点，测试WWW服务是否运行正常。如图7.22所示。

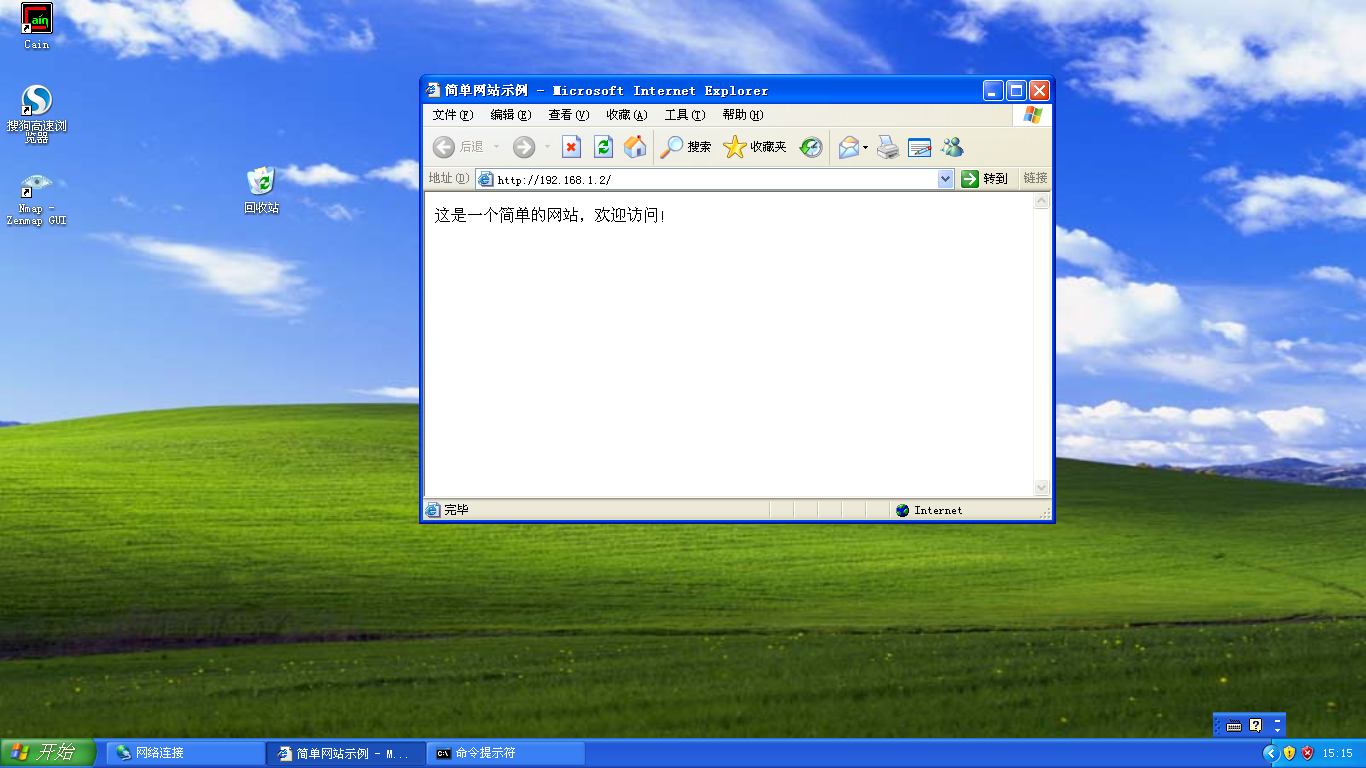


图7.22用浏览器访问一个简单的网站

站点开始运行后，如果要维护系统或更新网站数据，可以暂停或停止站点的运行，完成上述工作后，再重新启动站点。

3. FTP服务器的配置

1）查看FTP站点属性

依次单击“开始”→“控制面板”→“管理工具”→“Internet服务管理器”，在打开的窗口中单击“FTP站点”旁边“+”，显示“默认FTP站点”图标，右击鼠标查看其属性，可看到FTP站点的默认端口号是21，如图7.23所示。

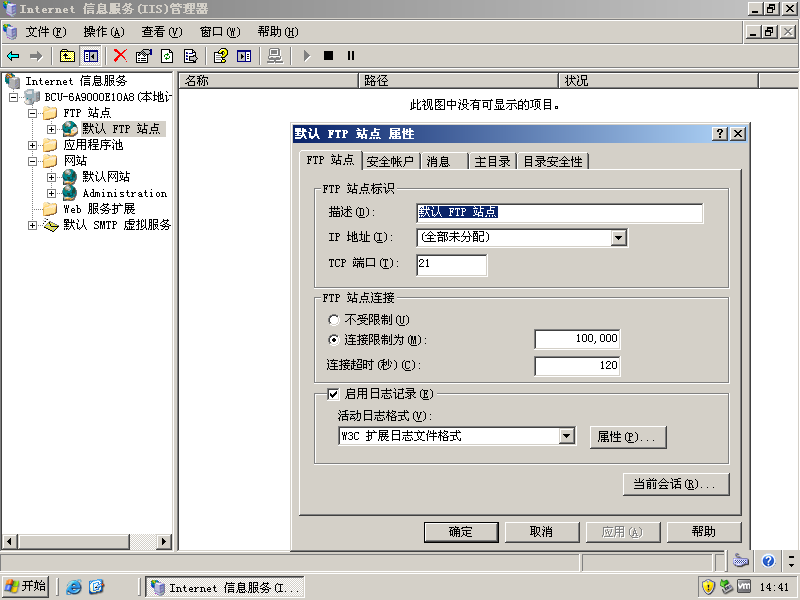


图7.23 默认FTP站点的属性

2）设置站点目录和访问权限

在属性对话框上点击“主目录”，可看到默认FTP站点的文件存放在c:\inetpub\ftproot

目录下，用户可以更改成另一个目录，并设置站点访问权限。默认情况下，FTP站点只允许用户下载，不许上传，如果需要将文件传给FTP站点，我们也可在“写入”前面打勾。此处实验仍采用默认目录，把需要供人下载的文件或文件夹拖放到此目录里，如电影、学习资料等。

3）选择“安全账号”选项卡后，可对匿名账号和FTP'站点操作员等属性进行配置。并可为FTP服务器建立一个安全的专用FTP帐号。此处实验采用匿名访问。

通常有3种方式访问FTP站点：一是命令；二是Web浏览器；三是FTP客户端软件。这3种方法都可以实现浏览、下载和上传文件，但是后两种、方式简单方便，最为常用。

4）验证FTP站点是否正常运行

打开本机或客户机浏览器，在地址栏中输入“ftp://FTP站点的IP地址或域名地址”，即可登录FTP站点，并下载所需文件。如图7.24所示。

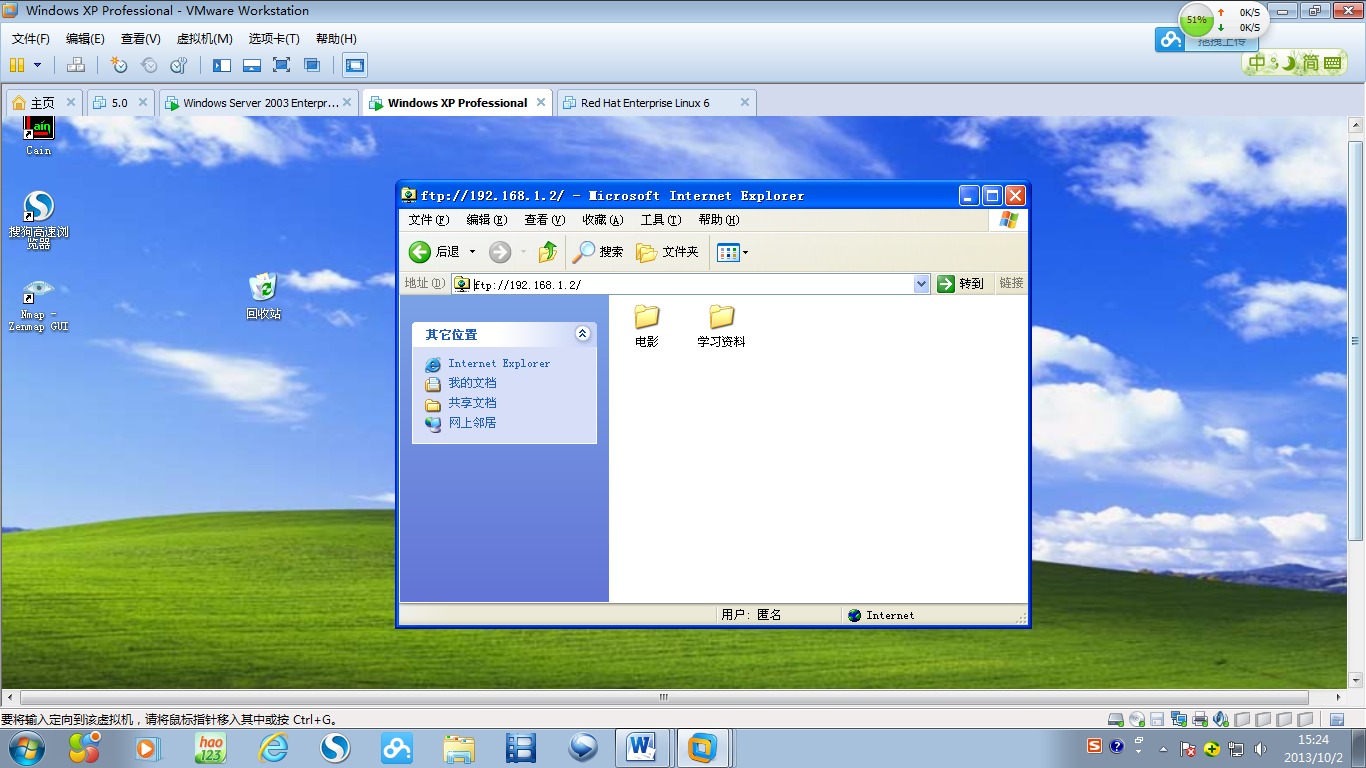


图7.24 用浏览器访问FTP站点

4．邮件服务器的配置

1）配置POP3服务器

创建邮件域：点击“开始”→“管理工具”→“POP3服务”，弹出POP3服务控制台窗口。选中左栏中的POP3服务后，点击右栏中的“新域”，弹出“添加域”对话框，接着在“域名”栏中输入邮件服务器的域名，也就是邮件地址“@”后面的部分，如“bcu.edu.cn”，最后点击“确定”按钮。

创建用户邮箱：选中刚才新建的“bcu.edu.cn”域，在右栏中点击“添加邮箱”，弹出添加邮箱对话框，在“邮箱名”栏中输入邮件用户名，然后设置用户密码，最后点击“确定”按钮，完成邮箱的创建，本例创建两个邮箱，分别是zhangsan@bcu.edu.cn和lisi@bcu.edu.cn。如图7.25所示。

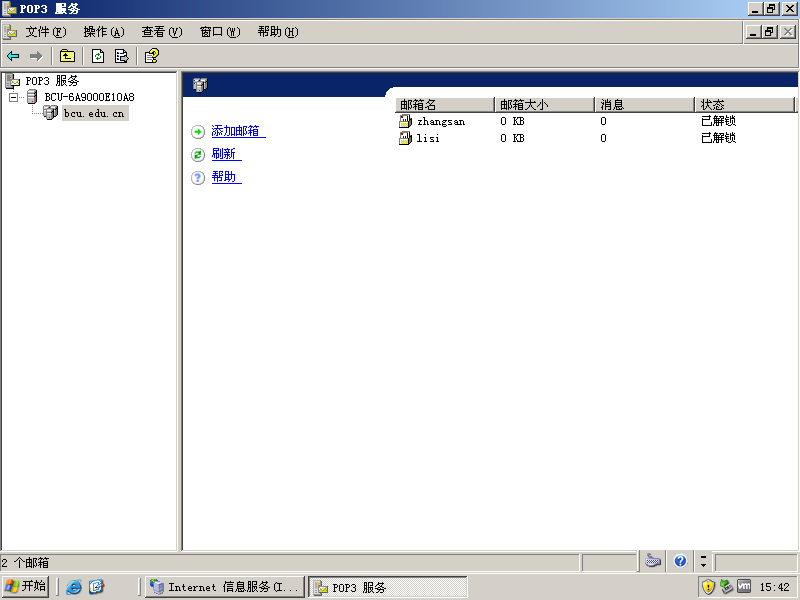


图7.25 创建邮箱域和邮箱账号

2）配置SMTP服务器

完成POP3服务器的配置后，就可开始配置SMTP服务器了。点击“开始”→“程序”→“管理工具”→ “Internet信息服务（IIS）管理器”，在“IIS管理器”窗口中右键点击“默认SMTP虚拟服务器”选项，在弹出的菜单中选中“属性”，进入“默认SMTP虚拟服务器”窗口，切换到“常规”标签页，在“IP地址”下拉列表框中选中邮件服务器的IP地址即可。点击“确定”按钮，这样一个简单的邮件服务器就架设完成了。

完成以上设置后，用户就可以使用邮件客户端软件连接邮件服务器进行邮件收发工作，只要在POP3和SMTP处输入邮件服务器的IP地址即可。

3）使用Outlook Express收发邮件

打开Outlook Express邮件客户程序，设置zhangsan@bcu.edu.cn的登录信息，在输入账户名和密码时，一定要勾选“使用安全密码验证（SPA）（S）”。如图7.26所示。

进入邮箱界面后，创建一封发送给lisi@bcu.edu.cn的邮件，主题为“hello”，输入邮件正文，如图7.27所示。点击发送，此邮件即被发送出去，在已发送邮件中可看到一封收件人为lisi@bcu.edu.cn，主题为“hello”的邮件，如图7.28所示。我们可在此局域网内的另一台计算机上用lisi@bcu.edu.cn登录到邮箱服务器，接收zhangsan@bcu.edu.cn发来的邮件，如图7.29所示。

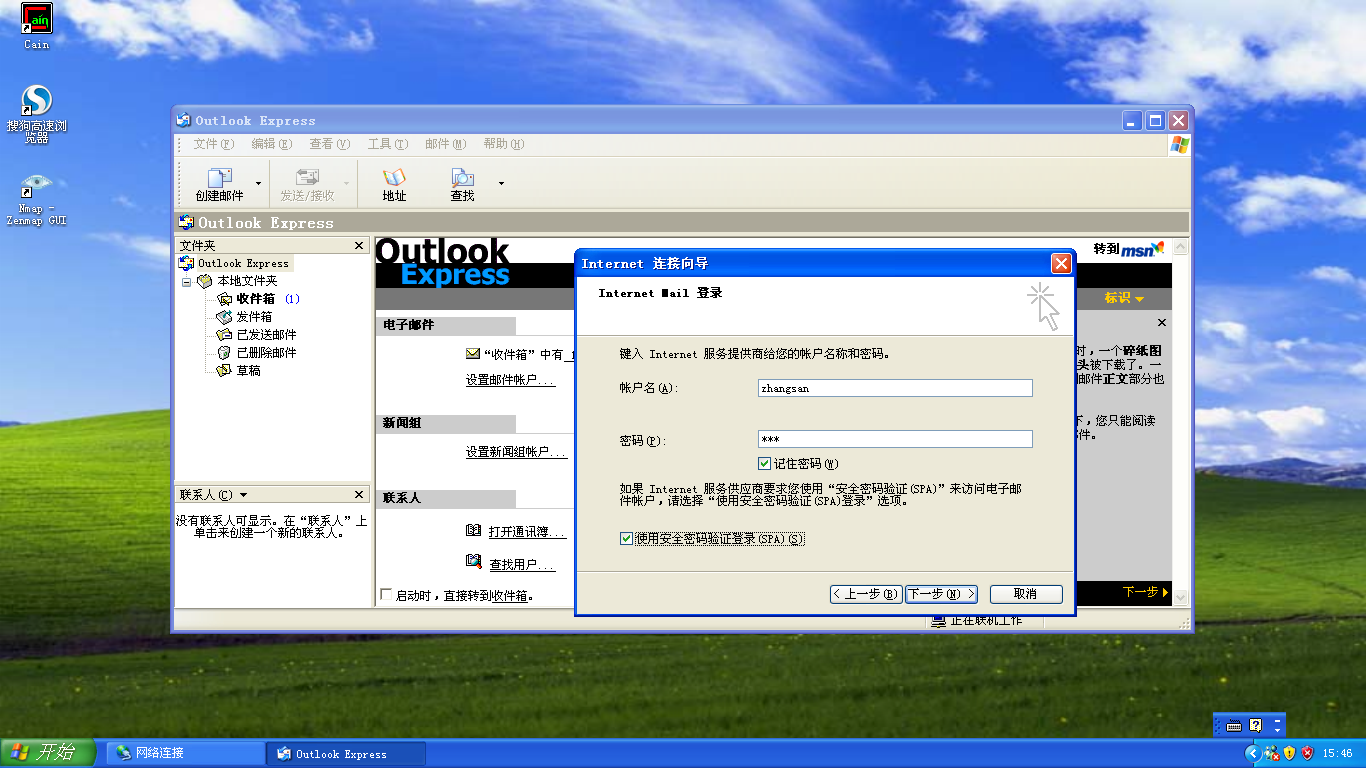


图7.26 使用Outlook Express设置邮箱登录

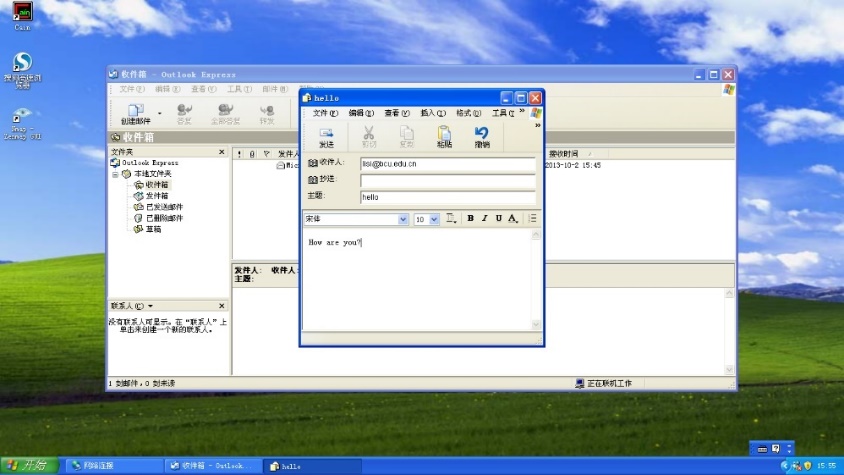


图7.27 创建发送给lisi@bcu.edu.cn的电子邮件

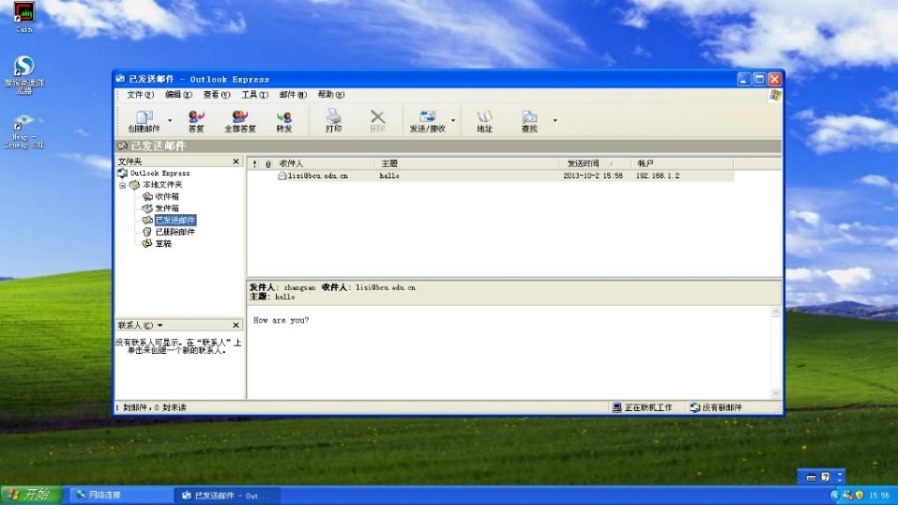


图7.28 zhangsan@bcu.edu.cn的已发送邮件

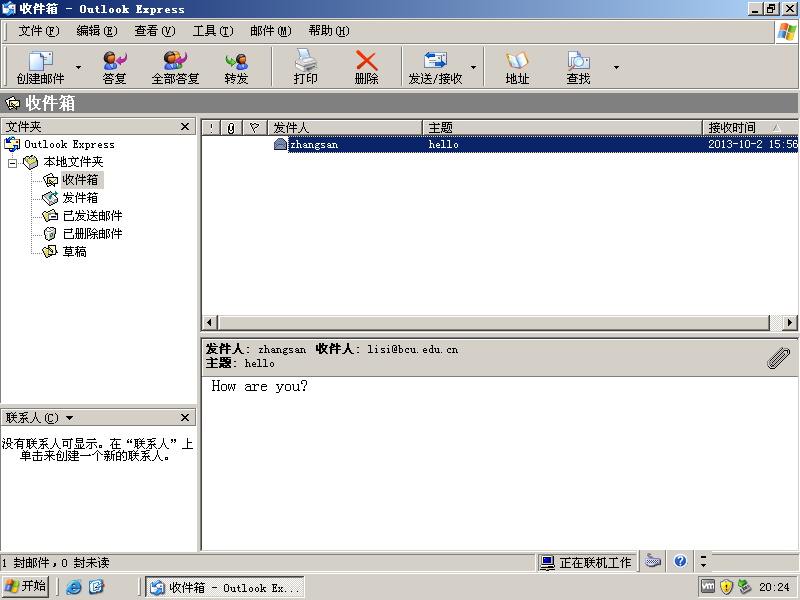


图7.29 lisi@bcu.edu.cn收到的电子邮件

**六、实验注意事项**

1． 本实验综合性较强，可分成2-3个小实验来做，如DNS、DHCP可作为一个实验，WWW、FTP、Email可作为一个或两个实验。

2. 虽然本实验是在虚拟机环境下实现的，读者也可在实际的计算机上按类似步骤完成以上实验。

**七、思考题**

1． 怎样在服务器上发布一个WWW网站？

2. 怎样取消匿名访问并设置访问FTP站点的用户账号？

**八、实验考核要求**

1.撰写实验报告。

2.课上完成DNS、DHCP实验。

3.课后完成WWW、FTP、EMAIL实验。