第3章

项目2 小型企业网络组建

3.1 项目背景

某小型企业内部共有40台左右的PC，共分为三个区域：领导区、商务区和技术服务区，为了保证信息安全，每个区域都希望按照一个独立的网段进行规划，各个区域之间不能相互访问，并且，各个区域的计算机能够上互联网。为此，企业购买了2台二层交换机，1台路由器，用来连接所有的PC。

为了提高上网速度，企业向电信局申请了一条10M的光纤接入Internet。并申请到一个全局地址段：100.1.1.0/30。为了信息安全和网络的正常运行，需要在交换机上做些限制，其中，领导区的PC机做MAC地址绑定，以保证网络的安全性。

为了实现企业品牌的宣传，企业建设了门户网站，并且向互联网用户提供Web服务。为此，企业购买了1台服务器。

3.2 需求分析

根据该企业提出的要求，进行需求分析可得出如下需求：

(1)为使该企业所有信息点都能上网，企业向电信局申请了一条10M的光纤接入Internet。并申请到2个全局地址，分别为：100.1.1.1/30，100.1.1.2/30(说明：100.1.1.1 /30用于局域网路由器与外部网络互连的端口；100.1.1.2/30用于局域网路由器所连互联网的对端地址，该地址由ISP设置)；

(2)企业内部共有40台左右的PC，共分为三个区域：领导区、商务区和技术服务区；

(3)针对领导区的PC机做MAC地址绑定；

(4)所需网络设备有：路由器1台、2层交换机多台、服务器1台。

网络拓扑图如图3-1所示：

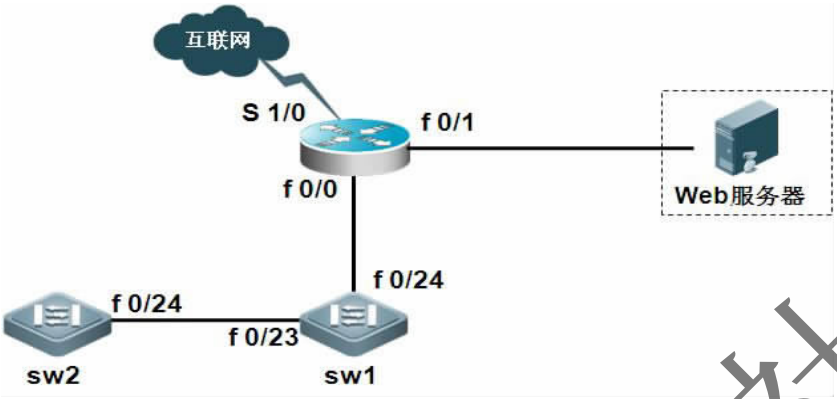

图 3-1　网络拓扑图

3.3　制定实施方案

1. 根据需求分析，列举网络设备上实现的功能及使用的技术

(1)交换机上主要功能是信息点的接入、VLAN 的划分(各部门之间的隔离)、MAC 地址绑定、端口流量控制，使用的技术有 VLAN 技术、MAC 绑定技术等。

(2)路由器上主要功能是确保全网进行互联网络的访问，对数据包的转发与过滤，使用的技术有 NAT 技术、默认路由技术等。

2. 设备选型

(1)交换机的选型，信息点 40 个，需要 24 端口交换机 2 台，具体功能见上述的接入层交换机的主要功能，综合多方面的因素接入层交换机选择思科 2950-24 交换机；

(2)路由器主要功能是确保全网进行互联网络的访问，对数据包的转发与过滤。需要支持的技术指标和完成的功能见上述路由器的主要功能。综合多方面的因素路由器选择思科 2811 路由器，如表 3-1 所示。

表 3-1　设备选型

设备	型号	厂商	数量(台)
接入层交换机	2950-24	思科	2
路由器	2811	思科	1
服务器		IBM	1

3. VLAN 规划及 IP 地址规划

VLAN 规划及 IP 地址规划如图 3-2 和表 3-2、表 3-3 所示。

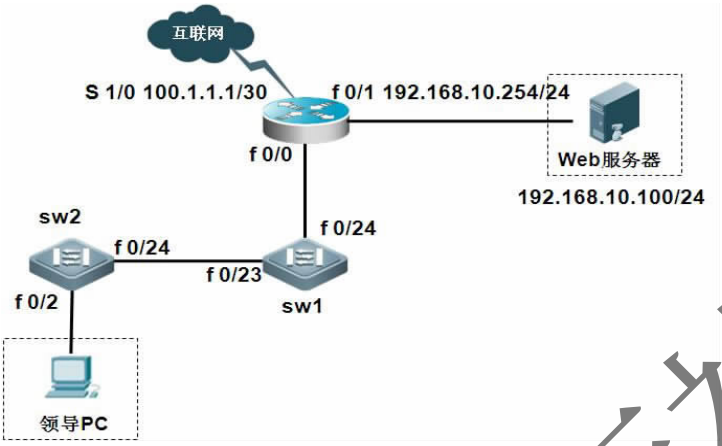

图 3-2 VLAN 及 IP 地址规划

表 3-2 IP 地址规划表

设备名称	端口	IP 地址/子网掩码	备注
Router 2811	S 1/0	100.1.1.1/30	与外网互连
	F 0/0.1	192.168.1.254/24	领导区(VLAN 10 的网关)
	F 0/0.2	192.168.2.254/24	商务区(VLAN 20 的网关)
	F 0/0.3	192.168.3.254/24	技术服务区(VLAN 30 的网关)
	F 0/1	192.168.10.254/24	与 Web 服务器区互连
Web 服务器	网卡 1	192.168.10.100/24	与路由器 f 0/1 口相连
领导 PC	网卡 1	192.168.1.100/24	与 SW2 的 f 0/2 口相连

表 3-3 VLAN 规划表

设备名称	VLAN	端口	备注
SW1	VLAN 10	F0/1-5	
	VLAN 20	F0/6-15	
	VLAN 30	F0/16-22	
SW2	VLAN 10	F0/1-5	
	VLAN 20	F0/6-15	
	VLAN 30	F0/16-22	

3.4 招投标

根据企业的需求进行招投标,详见第 1 章。

3.5　实施

1. 接入层交换机配置文档

SW1 配置文档：

```
SW1#show running-config
Building configuration...
Current configuration : 1728 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW1
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport access VLAN 10
switchport mode access
!
interface FastEthernet0/2
switchport access VLAN 10
switchport mode access
!
interface FastEthernet0/3
switchport access VLAN 10
switchport mode access
!
interface FastEthernet0/4
switchport access VLAN 10
switchport mode access
!
interface FastEthernet0/5
switchport access VLAN 10
switchport mode access
!
interface FastEthernet0/6
switchport access VLAN 20
!
```

```
interface FastEthernet0/7
switchport access VLAN 20
!
interface FastEthernet0/8
switchport access VLAN 20
!
interface FastEthernet0/9
switchport access VLAN 20
!
interface FastEthernet0/10
switchport access VLAN 20
!
interface FastEthernet0/11
switchport access VLAN 20
!
interface FastEthernet0/12
switchport access VLAN 20
!
interface FastEthernet0/13
switchport access VLAN 20
!
interface FastEthernet0/14
switchport access VLAN 20
!
interface FastEthernet0/15
switchport access VLAN 20
!
interface FastEthernet0/16
switchport access VLAN 30
!
interface FastEthernet0/17
switchport access VLAN 30
!
interface FastEthernet0/18
switchport access VLAN 30
!
interface FastEthernet0/19
switchport access VLAN 30
!
interface FastEthernet0/20
switchport access VLAN 30
!
```

```
interface FastEthernet0/21
switchport access VLAN 30
!
interface FastEthernet0/22
switchport access VLAN 30
!
interface FastEthernet0/23
switchport mode trunk
!
interface FastEthernet0/24
switchport mode trunk
!
interface VLAN1
no ip address
shutdown
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
end
```

SW2 配置文档：

```
SW2#show running-config
Building configuration...

Current configuration : 1954 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW2
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport access VLAN 10
!
```

```
interface FastEthernet0/2
switchport access VLAN 10
switchport mode access
switchport port-security
switchport port-security mac-address 0001.9641.080A
!
interface FastEthernet0/3
switchport access VLAN 10
!
interface FastEthernet0/4
switchport access VLAN 10
!
interface FastEthernet0/5
switchport access VLAN 10
!
interface FastEthernet0/6
switchport access VLAN 20
!
interface FastEthernet0/7
switchport access VLAN 20
!
interface FastEthernet0/8
switchport access VLAN 20
!
interface FastEthernet0/9
switchport access VLAN 20
!
interface FastEthernet0/10
switchport access VLAN 20
!
interface FastEthernet0/11
switchport access VLAN 20
!
interface FastEthernet0/12
switchport access VLAN 20
!
interface FastEthernet0/13
switchport access VLAN 20
!
interface FastEthernet0/14
switchport access VLAN 20
!
```

```
interface FastEthernet0/15
switchport access VLAN 20
!
interface FastEthernet0/16
switchport access VLAN 30
switchport mode access
!
interface FastEthernet0/17
switchport access VLAN 30
switchport mode access
!
interface FastEthernet0/18
switchport access VLAN 30
switchport mode access
!
interface FastEthernet0/19
switchport access VLAN 30
switchport mode access
!
interface FastEthernet0/20
switchport access VLAN 30
switchport mode access
!
interface FastEthernet0/21
switchport access VLAN 30
switchport mode access
!
interface FastEthernet0/22
switchport access VLAN 30
switchport mode access
!
interface FastEthernet0/23
!
interface FastEthernet0/24
switchport mode trunk
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface VLAN1
no ip address
```

```
shutdown
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
end
```

2. 路由器配置文档

```
2811 # show running-config
Building configuration...

Current configuration : 1057 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname 2811
!
spanning-tree mode pvst
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.1
encapsulation dot1Q 10
ip address 192.168.1.254 255.255.255.0
!
interface FastEthernet0/0.2
encapsulation dot1Q 20
ip address 192.168.2.254 255.255.255.0
!
interface FastEthernet0/0.3
encapsulation dot1Q 30
ip address 192.168.3.254 255.255.255.0
!
```

```
interface FastEthernet0/1
ip address 192.168.10.254 255.255.255.0
duplex auto
speed auto
!
interface Serial1/0
ip address 100.1.1.1 255.255.255.252
!
interface Serial1/1
no ip address
clock rate 2000000
shutdown
!
interface Serial1/2
no ip address
clock rate 2000000
shutdown
!
interface Serial1/3
no ip address
clock rate 2000000
shutdown
!
interface VLAN1
no ip address
shutdown
!
ip classless
ip route0.0.0.0 0.0.0.0 100.1.1.2
!
line con 0
line vty 0 4
login
!
end
```


3.6　验收

验收的基本单位是合同。验收以国家有关规范、网络系统工程项目合同、技术要求书、施工设计报告、经审核的合同变更补充协议为依据。

1. 设备验收

对不同的设备要根据不同的要求进行设备验收。主要检验以下几项：到货的品名与数量与订货清单的一致性；设备的外观完好性；设备通电自检是否正常。

2. 网络系统集成工程项目验收

(1)网络系统集成工程项目整个施工、调试过程结束后，网络系统继续试运行一个月，然后使用单位向项目负责单位提交系统运行测试报告。

(2)网络系统集成项目施工单位向项目负责单位提交完整的工程文档，至少包含以下内容，但不限于以下内容。文档一式三份，并提交电子文档。合同副本；系统结构图；网络拓扑图；设备配置表；设备配置资料；网络管理系统工具软件；项目验收申请报告。

(3)由项目责任单位会同有关部门组织系统集成项目验收，并出具验收报告。验收内容包括：

设备间验收(附件)；网络拓扑图：各个局域网之间通过 WAN 的连接拓朴、主干网的连接拓扑、主交换设备之间连接、交换机和交换机之间的连接、服务器及其他网络服务设备的连接、网络站点的连接。

网络的规划报告。指的是网络设置信息包括：网段，域，VLAN 等。

网络设备信息清单。包括：设备分类清单、网络互联设备清单、路由器的信息、路由器的路由表、交换机端口列表、服务器。

单机、网络测试验收。

正常运行时网络重点端口的流量(网络基准测试)、路由器或交换机端口流量趋势图、流量趋势。

正常运行时网络协议和繁忙用户的分布统计(网络基准测试)。包括：各种协议所占用带宽的比例、使用协议的最繁忙用户(按不同角度做统计)、数据包数量，大小，类型等、对话最繁忙用户、广播统计(广播，多播，单播)、协议分布记录。

网络的吞吐能力或加载测试(路由和交换能力)。互联网吞吐量测试、网络吞吐量测试。

3. 提交验收证明意见

项目负责单位在收到系统集成项目申请工程验收书后，应及时组织使用、审计、项目施工等单位人员先进行现场验收，再根据提交的系统测试数据及完整的工程文档，对照验收标准逐项逐条核实，确定合格后，提交验收证明意见。

3.7 完成项目所需知识点

3.7.1 任务 1 如何实现多台交换机通信并实现端口分组隔离

现有两台交换机，三台 PC。PC1(192.168.1.1)和 PC2(192.168.1.2)连接到同一台交换机上，但是处在不同的 VLAN 中，PC3(192.168.1.3)连接到另一台的交换机上，如图 3-3 所示。

要求：PC1 能与 PC3 互相通信，PC2 不能与 PC3 互相通信，并加以显示和验证。

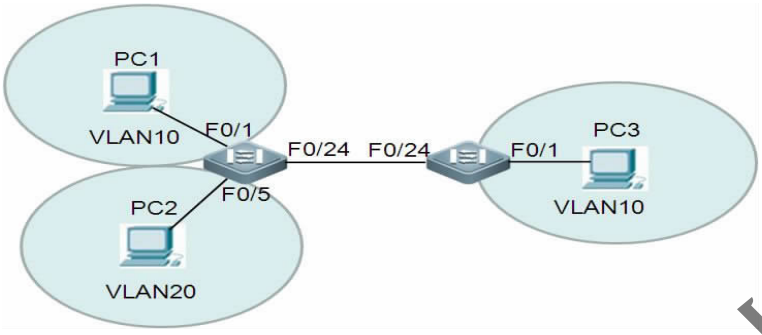

图 3-3　网络拓扑图

1. 跨交换机 VLAN 介绍

跨交换机 VLAN 的划分方法在很多领域中应用广泛，下面主要介绍怎样划分和配置跨交换机 VLAN 技术。

跨交换机 VLAN 也就是 802.1Q VLAN，它是跨交换机划分 VLAN、不同的交换机的端口属于同一 VLAN、满足 IEEE802.1Q 协议标准，而且是基于交换机的端口的划分方法。

跨交换机 VLAN 也称为 Tag VLAN。这种划分方法必须满足两个条件：传输多个 VLAN 的信息和实现同一 VLAN 跨越不同的交换机，如图 3-4 所示。

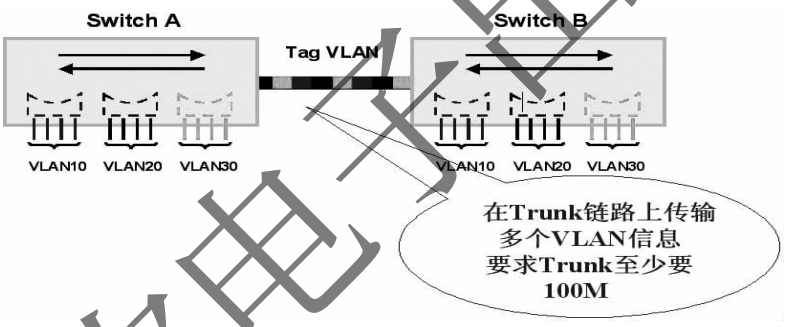

图 3-4　Tag VLAN

Tag VLAN 要求交换机与交换机相连的端口必须实现多个 VLAN 信息的传输，该端口的设置方法在菜单式中表现为 Tag 模式，命令行中表现为 Trunk 模式。

2. 跨交换机 VLAN 配置

以 CISCO 交换机为例。跨交换机 VLAN 配置的步骤如下：

```
Switch# configure terminal
Switch(config)# interface fastethernet0/1
! 进入端口配置模式
Switch(config-if)# switchport mode trunk
! 设置端口模式为“trunk”
Switch(config-if)# switchport  trunk allowed VLAN all
Switch(config-if)# end
```

配置过程中应注意：交换机与交换机相连的端口应设成 Trunk(干道)模式；Tag VLAN 的划分方法要满足 IEEE802.1Q 协议标准。

3. 任务 1 的实施

步骤 1：按照拓扑图连接计算机和交换机，在 Switch1 上创建 VLAN10 和 VLAN20，并将

端口 F0/1 加入到 VLAN10 中，端口 F0/5 加入到 VLAN20 中。具体操作如下：

```
Switch1# configure terminal
Switch1(config)# VLAN 10
Switch1(config-VLAN)#exit
Switch1(config)# VLAN 20
Switch1(config-VLAN)# exit
Switch1(config)#interface fastethernet 0/1
Switch1(config-if)#switchport port mode access
Switch1(config-if)#switch access VLAN 10
Switch1(config-if)#exit
Switch1(config)#interface fastEthernet 0/5
Switch1(config-if)#switch port mode access
Switch1(config-if)#switch access VLAN 20
Switch1(config-if)#exit
```

验证测试：(如图 3-5 所示)

```
Switch1#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
10   VLAN0010                          active    Fa0/1
20   VLAN0020                          active    Fa0/5
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

图 3-5　显示 Switch1 的 VLAN 配置情况

步骤 2：在 Switch1 上，将与 Switch2 相连的 F0/24 端口定义为 Tag VLAN 模式。具体操作如下：

```
Switch1(config)#interface fastEthernet 0/24
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#switchport trunk allowed VLAN all
Switch1(config-if)#exit
```

验证测试：(如图 3-6 所示)

```
Switch1#sh int f 0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

图 3-6　显示 Switch1 的 F0/24 端口的状态

步骤 3：在 Switch2 上创建 VLAN10，将端口 F0/1 加入到 VLAN10 中，并将与 Switch1 相连的 F0/24 端口定义为 Tag VLAN 模式。具体操作如下：

```
Switch2# configure terminal
Switch2(config)# VLAN 10
Switch2(config-VLAN)# exit
Switch2(config)# interface fastEthernet 0/1
Switch2(config-if)# switchport mode access
Switch2(config-if)# switch access VLAN 10
Switch2(config-if)# exit
Switch2(config)# interface fastEthernet 0/24
Switch2(config-if)# switchport mode trunk
Switch2(config-if)# switchport trunk allowed VLAN all
Switch2(config-if)# exit
```

验证测试：(如图 3-7 所示)

```
Switch2#  sh vl

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23
10   VLAN0010                         active    Fa0/1
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

图 3-7　显示 Switch2 的 VLAN 配置情况

步骤 4：验证 PC1 与 PC3 能互相通信，如图 3-8 所示。

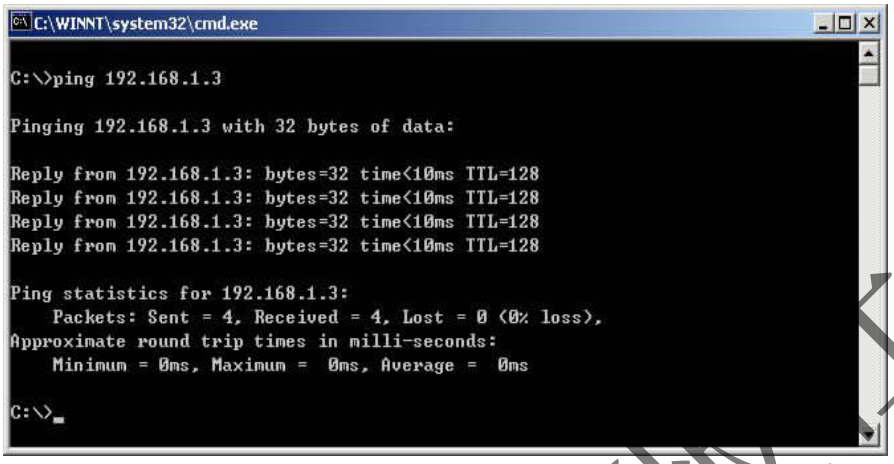

图 3-8　PC1 与 PC3 连通

验证 PC2 与 PC3 不能互相通信，如图 3-9 所示。

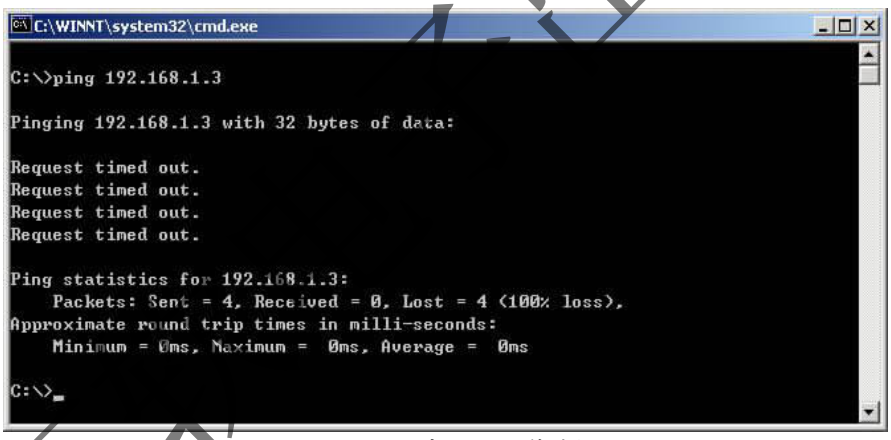

图 3-9　PC2 与 PC3 不能连通

3.7.2　任务 2 如何进行路由器的管理

假设某公司的网络管理员希望以后在办公室或出差时也可以对设备进行远程管理，现要在路由器上做适当配置，使它可以实现这一要求。

本实验以一台 Cisco 2811 路由器为例，路由器命名为 Router0。PC 机通过串口(Com)连接到路由器的控制(Console)端口，实现对交换机的初始配置；PC1 通过网卡(NIC)远程连接到路由器的 fastethernet0/0 端口，如图 3-10 所示。

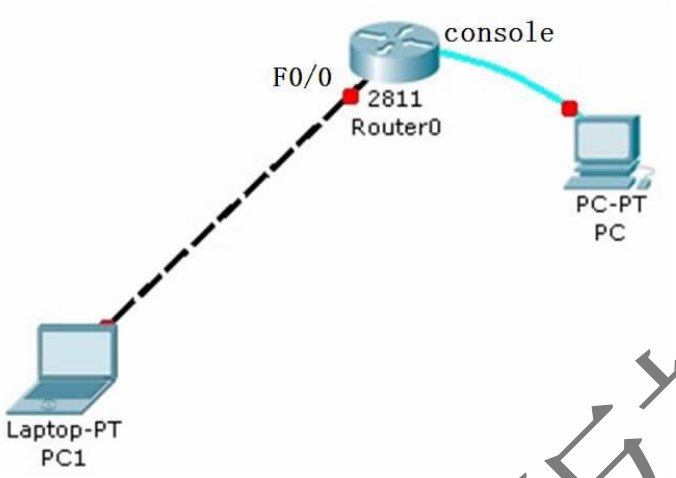

图 3-10　搭建路由器的 Telnet 管理环境

1. 路由器工作原理及应用

路由器工作在 OSI 模型中的第三层，即网络层。它利用网络层定义的“逻辑”上的网络地址（即 IP 地址）来区别不同的网络。

路由器的主要作用：

连通不同的网络。路由器支持多种协议，可连接不同协议的网络，并根据网络逻辑地址在互连的子网之间传递分组。

选择信息传送的线路并进行数据包转发。选择通畅快捷的近路，能大大提高通信速度。数据转发时，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，发送到本网络的数据将被丢弃。

路由器是互联网的主要节点设备，路由器系统构成了基于 TCP/IP 的 Internet 的主体脉络。因此，它的处理速度是网络通信的主要瓶颈之一，它的可靠性则直接影响着网络互连的质量。

2. 路由器的硬件组成、接口及连接线缆

路由器的硬件主要由中央处理器、内存、接口、控制端口等物理硬件和电路组成，如图 3-11 所示。

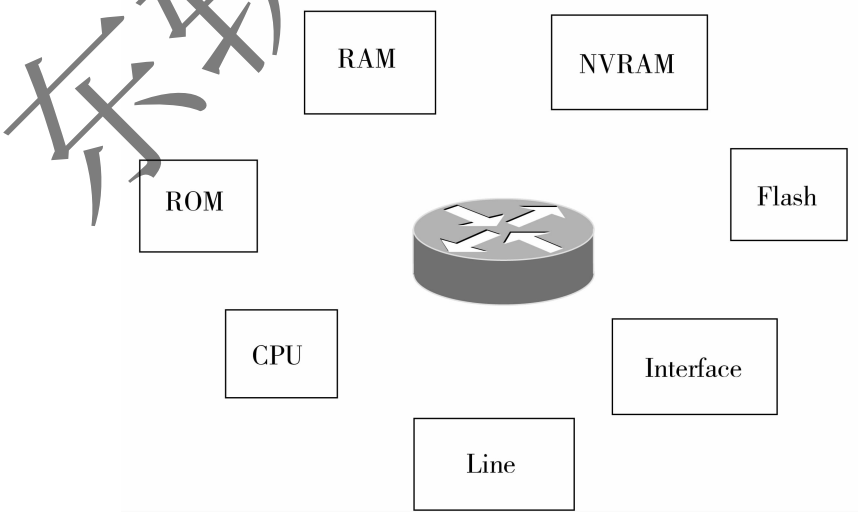

图 3-11　路由器硬件组成

(1)中央处理器。

与计算机一样,路由器也包含了一个中央处理器(CPU)。不同系列和型号的路由器,其CPU也不尽相同。

路由器的CPU负责路由器的配置管理和数据包的转发工作,如维护路由器所需的各种表格以及路由运算等。路由器对数据包的处理速度很大程度上取决于CPU的类型和性能。

(2)内存。

路由器采用了以下几种不同类型的内存,每种内存以不同方式协助路由器工作。

①只读内存(ROM)。

只读内存(ROM)在路由器中的功能与计算机中的ROM相似,主要用于系统初始化等功能。ROM中主要包含:

- 系统加电自检代码(POST),用于检测路由器中各硬件部分是否完好;
- 系统引导区代码(BootStrap),用于启动路由器并载入IOS操作系统;
- 备份的IOS操作系统,以便在原有IOS操作系统被删除或破坏时使用。通常,这个IOS比主用的IOS的版本低一些,但足以使路由器启动和工作。

顾名思义,ROM是只读存储器,不能修改其中存放的代码。如要进行升级,则要替换ROM芯片。

②闪存(Flash)。

闪存(Flash)是可读可写的存储器,在系统重新启动或关机之后仍能保存数据。Flash中存放着路由器主体软件IOS。事实上,如果Flash容量足够大,甚至可以存放多个IOS操作系统。

③非易失性RAM(NVRAM)。

非易失性RAM(Nonvolatile RAM)是可读可写的存储器,在系统重新启动或关机之后仍能保存数据。NVRAM仅用于保存启动配置文件(Startup-Config),故其容量较小,通常在路由器上只配置32KB~128KB大小的NVRAM。同时,NVRAM的速度较快,成本也比较高。

④随机存储器(RAM)。

RAM也是可读可写的存储器,但它存储的内容在系统重启或关机后将被清除。和计算机中的RAM一样,路由器中的RAM也是运行期间暂时存放操作系统和数据的存储器,让路由器能迅速访问这些信息。RAM的存取速度优于前面所提到的3种内存的存取速度。

运行期间,RAM中运行路由器主体软件IOS和现运行配置文件(running-config)。

(3)接口。

所有路由器都有接口(Interface),每个接口都有自己的名字和编号。一个接口的全名称由它的类型标志与数字编号构成,编号自0开始。

对于接口固定的路由器或采用模块化接口的路由器,在接口的全名称中,只采用一个数字,并根据它们在路由器的物理顺序进行编号,例如“Ethernet0”表示第1个以太网接口,“Serial1”表示第2个串口。

对于支持“在线插拔和删除”或具有动态更改物理接口配置的路由器,其接口全名称中至少包含两个数字,中间用斜杠“/”分割。其中,第1个数字代表插槽编号,第2个数字代表接口卡内的端口编号。如“serial3/0”代表位于3号插槽上的第1个串口。

对于支持“万用接口处理器(VIP)”的路由器,其接口编号形式为“插槽/端口适配器/端口

号”，如“Ethernet4/0/1”是指 4 号插槽上第 1 个端口适配器的第 2 个以太网接口。

(4)控制台端口。

所有路由器都安装了控制台端口，使用户或管理员能够利用终端与路由器进行通信，完成路由器配置。该端口提供了一个 EIA/TIA-232 异步串行接口，用于在本地对路由器进行配置。特别要注意的是，首次配置时必须通过控制台端口进行配置。

路由器的型号不同，与控制台进行连接的具体接口方式也不同，有些采用 DB25 连接器，有些采用 RJ45 连接器。

(5)辅助端口。

多数路由器均配备了一个辅助端口，它与控制台端口类似，提供了一个 EIA/TIA-232 异步串行接口，通常用于连接 Modem 以使用户或管理员对路由器进行远程管理。

(6)路由器加电启动过程。

①系统硬件加电自检。运行 ROM 中的硬件检测程序，检测各组件能否正常工作。完成硬件检测后，开始软件初始化工作。

②软件初始化过程。运行 ROM 中的 BootStrap 程序，进行初步引导工作。

③寻找并载入 IOS 系统文件。IOS 系统文件可以存放在多处，至于到底采用哪一个 IOS，是通过命令设置指定的。

④IOS 装载完毕，系统在 NVRAM 中搜索保存的 Startup-Config 文件，进行系统的配置。如果 NVRAM 中存在 Startup-Config 文件，则将该文件调入 RAM 中并逐条执行。否则，系统进入 Setup 模式，进行路由器初始配置。

3. 路由器管理方式

路由器一般情况下都可以支持多种方式进行管理，用户可以选择最合适的方式管理路由器，以下是路由器支持的四种配置方式：

(1)利用终端通过 Console 口进行本地管理。

(2)利用异步口连接 Modem 进行远程管理。

(3)通过 Telnet 方式进行本地或远程方式管理。

(4)预先编辑好配置文件，通过 TFTP 方式进行网络管理。

下面，我们就对其中三种常用的配置方法进行详细介绍。

(1)通过 Console 口搭建本地管理环境。

在路由器第一次使用的时候，必须采用通过 Console 口的方式对路由器进行配置，具体的操作步骤如下：

第一步：用标准的串口电缆将 PC 电脑的 COM 口和路由器的 Console 口(也叫配置口)相连起来。

第二步：在 PC 中运行超级终端软件，建立新连接，选择路由器的 Console 连接的串口，设置通讯参数：9600 波特率、8 位数据位、1 位停止位、无校验、无流控。

第三步：路由器上电，启动路由器，这时将在超级终端屏幕内显示自检信息，自检结束后，会提示“System Configuration Dialog”，键入【Ctrl + C】结束该对话框，直接进入用户模式“Route>”。

第四步：这时便可以在超级终端中对路由器进行配置，查看路由器的运行状态，如果需要帮

助，可以随时键入“?”，路由器便可以随时提供详细的在线帮助了，具体的各种命令我们在以后的章节会学到。

(2)搭建本地或者远程的 Telnet 配置环境。

如果用户对路由器已经配置好各接口的 IP 地址，同时可以正常的进行网络通讯了，则可以通过局域网或者广域网使用 Telnet 客户端登录到路由器上，对路由器进行本地或者远程的配置。下面详细介绍具体的配置步骤。

第一步：如果建立本地 Telnet 配置环境，则只需要将 PC 上的网卡接口通过局域网与路由器的以太网口连接；如果需要建立远程 Telnet 配置环境，则需要将 PC 和路由器的广域网口连接。

第二步：在 Windows 的 DOS 命令提示符下，直接输入“Telenet a. b. c. d”，这里的 a. b. c. d 为路由器的以太网口的 IP 地址(如果在远程 Telnet 配置模式下，为路由器的广域网口的 IP 地址)，与路由器建立连接，提示输入登录密码，如果没有配置密码，会出现“password required, but none set”的提示，正确输入密码后，出现“route>”。

第三步：这时便可以利用 PC 的 Telnet 客户端对路由器进行配置，查看路由器的运行状态，如果需要帮助，可以随时键入“?”，路由器便可以随时提供详细的在线帮助了，具体的各处命令我们也将在后面的章节学到。

(3)搭建 tftp 服务器的管理环境。

如果想一次性恢复以前的配置，或者一次性完成对路由器的配置，就可以使用 tftp 服务器方式来配置路由器。具体的操作如下：

第一步：将一台 PC 上的网卡接口通过局域网与路由器的以太网口连接，分别在 PC 机网卡和路由器以太网口上设置同一网段的 IP 地址，以 ping 命令验证两者网络是否接通。

第二步：在 PC 机上安装 tftp 服务器软件，并将已编辑好的或原导出的路由器配置文件(文件格式为文本文件)导入 tftp 服务器软件中，准备对路由器进行配置或恢复。

第三步：进入路由器命令行接口，键入：copy tftp startup-config，随后按提示键入 tftp 服务器 IP 地址和 tftp 中的路由器配置文件名，路由器便从 tftp 下载指定文件到路由器的 NVRAM 中，该文件将覆盖原有配置文件并成为初始配置文件(startup-config)。下载完成后，使用 copy startup-config running-config 或重启路由器，便可运行所下载的配置文件，从而完成对路由器的配置。

4. 命令行接口(CLI)

命令行接口(Command Line Interface，CLI)，是用户配置路由器的最主要的途径，通过命令行接口，可以简单的输入配置命令，达到配置、监控、维护路由器的目的。路由器提供了丰富的命令集，可以简单的通过控制口(Console)进行本地配置，也可以通过异步口进行远程配置，还可以通过 Telnet 客户端方便的在本地或者远程进行配置路由器。

(1)路由器命令行接口模式。

为了方便使用路由器，路由器提供了不同的命令模式，在不同的命令模式中，有各自完整的一套指令集，也有不同的系统提示符，在各自的系统提示符下，简单的键入“?”，便可以列出在各自命令模式下的所有可以使用的命令了。在不同的命令模式下，可以方便的相互转换。对于不同的命令模式，路由器提供了不同的分级保护方式，防止非法用户入侵路由器，提高网络的安全

性。比如普通用户模式只能查看简单的路由器运行状态和测试网络的连通性，无法对路由器的配置进行修改，而特权用户模式则有权对路由器配置进行修改。

关于几个常用的命令模式，汇总如表 3-4 所示。

表 3-4　　路由器常用命令模式

命令模式	提示符	进入命令	退出命令
普通用户模式	Route>	各路由器建立连接即可进入，如果为 Telnet 方式，需要输入登录密码	Exit 断开连接
特权用户模式	Route#	在普通用户模式下输入 enable，同时输入授权密码	Exit 退出到普通用户模式
全局配置模式	Route(config) #	在特权用户模式下，输入 configure terminal	Exit 退出到特权用户模式
路由协议配置模式	Route(config-router)#	在全局配置模式下，根据路由协议用 router 命令进入	Exit 退出到全局配置模式
接口配置模式	Route(config-if)#	在全局配置模式下，根据配置的接口用 interface 命令进入	Exit 退出到全局配置模式
子接口配置模式	Route(config-subif)#	在全局配置模式下，根据指定的子接口类型，用 interface 命令进入	Exit 退出到全局配置模式
线路配置模式	Route(config-line)#	在全局配置模式下，根据要配置的线路类型，用 line 命令进入	Exit 退出到全局配置模式

注：进入特权模式里，不管再进入何种模式下，键入“end”都会退回特权模式。

(2)查看命令行历史记录。

路由器提供了可以记录用户输入命令的功能，即命令行历史记录功能，这个功能在输入一些比较长、复杂的指令时特别有用，以前输入的所有的指令可以简单的通过上下光标键重新调出来。

要调出用户最近输入的命令行，可以使用下面的键盘输入或者命令(如表 3-5 所示)。

表 3-5　　查看历史记录

命令或者键盘输入	作用
【Ctrl+P】或者光标键向上键	访问上一条历史命令，如果没有则响铃警告
【Ctrl+N】或者光标键向下键	访问下一条历史命令，如果没有则响铃警告
Route# show history	查看命令历史记录

(3)命令行配置编辑功能。

路由器提供了强大的命令编辑功能，使用热键或者快捷键，可以方便的编辑命令行。

①在命令行移动光标键功能(如表 3-6 所示)。

表 3-6 命令行移动的光标键功能

键盘输入	作用
【Ctrl＋B】或者光标键向左键	向左移动光标，最多可以移动到系统提示符
【Ctrl＋F】或者光标键向右键	向右移动光标，最多可以移动到行末
【Ctrl＋A】	光标直接移动到命令行的最左端
【Ctrl＋E】	光标直接移动到命令行的末端

②命令行删除功能(如表 3-7 所示)。

表 3-7 命令行删除的光标键功能

键盘输入	作用
【Backspace】键	删除光标左边的一个字符，最多到系统提示符
【Ctrl＋U】	删除光标键以左的所有命令行字符

③命令行自动补齐功能。

如果您忘记了一个完整的命令，或者希望可以减少输入的字符的数量，可以采用路由器提供的命令行自动补齐功能，您只需要输入少量的字符，然后按【TAB】，或者按【Ctrl＋I】键，由路由器自动补齐成为完整的命令，当然必要条件是输入的少量字符，已经可以确定一个唯一的命令了。

比如特权用户层，您只需要输入 en ，然后按【TAB】或者【Ctrl＋I】，则由路由器自动为您补齐成为完整的 enable 命令。

```
Route＞en ＜TAB＞
Route＞enable
```

(4)命令行在线相关帮助。

路由器提供了丰富的在线帮助功能，可以使用如下的方法，如表 3-8 所示。

表 3-8 命令行在线帮助

命令或者键盘输入	作用
Route＃help	显示简短和系统帮助描述信息
Route＃？	列出当前命令模式下的所有的命令
Route＃abbreviate-command-entry? 如：Router＃c?	显示出当前命令模式下，以指定的字符开始的所有命令
Route＃command ？ 如：Router＃copy ？	列出这个命令开头的所有的参数或后续命令选项，及其简要说明

(5)命令行错误提示信息。

路由器对用户输入的命令、参数进行严格的检查判断，对于错误的命令，不合法的参数会作出相应的错误提示，方便用户找出问题，常见的错误提示，如表 3-9 所示。

表 3-9　　错误提示信息

错误提示信息	错误的原因
% Invalid input detected at '^' marker.	输入的命令有错误，错误的地方在'^'指明的位置
% Incomplete command	命令输入不完整
% Ambiguous command:"command"	以 command 开头的指令有多个，指令输入不够明确
Password required,but none set	以 Telnet 方式登录时，需要在对应的 line vty num 配置密码，该提示是由于没有配置对应的登录密码
% No password set	没有设置控制密码，对于非控制台口登录时，必须配置特权密码，否则无法进入特权用户模式

(6)setup 交互式配置命令。

路由器提供了 setup 交互式配置模式，在路由器首次上电使用时，在路由器内部没有任何配置，这时路由器自动进入 setup 交互式配置模式中，也可以在特权用户模式下，随时键入 setup 进入交互式配置模式。这时用户只需要简单的回答路由器的问题，便可以轻松的将路由器配置完成了。

但如果不希望在此模式下一步步地配置，可以直接按【Ctrl+C】，退出 Setup 配置模式，进入命令行配置模式。

```
Route# setup
```

5. 基本系统管理

(1)基本系统管理。

路由器的基本系统管理包括如下的配置，如表 3-10 所示。

表 3-10　　路由器基本系统配置

命令	作用
Route (config)# hostname hostname	设置路由器名称
Route # clock set hh : mm : ss date month year 或 route # clock set hh : mm : ss month date year	设置路由器的日期和系统时钟
Route # reload	重新启动路由器

①配置路由器的名称，如将路由器的名称改为 Gxzjy，命令如下：

```
Route # configure terminal
Router(config)#hostname Gxzjy
Gxzjy(config)#
```

②设置路由器的日期和系统时钟。如把系统时间改为 2005-05-25，08:00:00，命令如下：

```
Gxzjy # sh clock
*07:41:06.961 UTC Tue Mar 30 1993
Gxzjy # clock set 08:00:00 25 may 2005
Gxzjy # sh clock
08:00:02.961 UTC Tue 25 May 2005
```

③重新启动路由器。命令为：

```
Gxzjy# reload
Proceed with reload ? [confirm]
```

(2)配置文件管理。

①理解路由器配置文件。

配置文件在文件格式上是一个文本文件,路由器启动后,对配置文件中的命令解释执行,路由器的配置文件有以下的特点:

配置文件包含了一组路由器的命令。命令的组织以命令模式为基本框架,同一命令模式的命令组织在一起,形成一节,节与节之间通常用空行或注释行隔开(以!开始的为注释行)。配置文件仅仅保存非缺省参数的命令,对于已经是缺省值的命令不予保存。配置文件以“end”为结束符。

下面是一个简单的配置文件的例子:

```
Building configuration...
Current configuration : 532 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
spanning-tree mode pvst
!
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
duplex full
speed auto
!
interface FastEthernet0/1
ip address10.1.1.1 255.255.255.252
duplex auto
speed auto
!
interface VLAN1
no ip address
shutdown
!
ip classless
ip route0.0.0.0 0.0.0.0 10.1.1.2
!
line con 0
```

```
line vty 0 4
login
!
end
```

②显示路由器配置文件。

在路由器中，有两套配置文件，一套为当前正在使用的配置文件，也叫 running-config，还有一套是初始配置文件，也叫 startup-config，其中 running-config 是保存在 RAM 中，路由器关机后便丢失了，而 startup-config 是保存在 NVRAM，断电文件内容也不会丢失。

这两套配置文件的内容可以不一样，可以通过以下命令查看，如表 3-11 所示。

表 3-11　　显示路由器配置文件

命令	作用
Route # show running-config	显示当前配置文件的内容
Route # show startup-config	显示初始配置文件的内容

③路由器文件的管理。

路由器在系统启动时，对 startup-config 配置文件是逐条命令解释执行，并且在执行的同时把 startup-config 拷贝到 running-config 中，在系统运行期间，可以随时利用路由器提供的命令行接口，进行配置模式，对 running-config 进行修改。

startup-config 和 running-config 两套配置文件之间，可以相互拷贝，同时也可以通过网络，与 TFTP 服务器相互拷贝。命令如表 3-12 所示。

表 3-12　　配置文件拷贝命令

命令	作用
Route# write 或 route # write memory 或 route# copy running-config startup-config	保存当前配置，也就是将当前配置文件拷贝到初始配置文件中
Route # copy running-config tftp	将当前配置文件保存 TFTP 服务器上
Route# copy startup-config running-config	将初始配置文件拷贝到当前配置文件中，覆盖当前配置文件
Route# copy startup-config tftp	将初始配置文件拷贝到 TFTP 服务器上
Route# copy tftp startup-config	将 TFTP 服务器上保存的配置文件覆盖到初始配置文件上
Route# copy tftp running-config	将 TFTP 服务器上保存的配置文件覆盖到当前配置文件上
Route # write erase 或 Route# erase startup-config	擦除初始配置文件

6. 接口管理

(1)接口管理概述。

路由器支持两种类型接口：物理接口和逻辑接口。物理接口意味着该接口在路由器上有对应的、实际存在的硬件接口，如：以太网接口、同步串行接口、异步串行接口、ISDN 接口。逻辑

接口意味着该接口在路由器上没有对应的、实际存在的硬件接口，逻辑辑口可以与物理接口关联，也可以独立于物理接口存在。如：Dialer 接口、NULL 接口、Loopback 接口、Tunnel 接口、子接口等。实际上对于网络协议而言，无论是物理接口还是逻辑接口，都是一样对待的。

路由器支持的具体接口类型如表 3-13 所示。

表 3-13　　路由器接口类型

接口类型	接口配置名称	符合标准
异步串口	async	EIA/TIA RS-232
同步串口	serial	V.24、V.35、EIA/TIA-449、X.21、EIA-530
以太网口	Ethernet	IEEE802.3、RFC894
快速以太网口	FastEthernet	IEEE802.3、RFC894
Dialer 接口	dialer	—
Loopback 接口	Loopback	—
Tunnel 接口	Tunnel	—
NULL 接口	NULL	—
子接口	Serial0.1(例)	—
异步串口组	Group-Async	—

①接口共性配置。

● 进入指定的接口配置模式。

配置每个接口，首先必须进入这个接口的配置模式模式，首先进入全局配置模式，然后输入进入指定接口配置模式，命令格式如下：

```
Router(config)#interface interface-type interface-number
! 创建一个接口，并进入指定接口配置模式
Router(config)#no interface interface-type interface-number
! 删除指定接口
```

例如：进入快速以太网口的第 0 个端口，步骤是：

```
Router#config terminal
Router(config)#interface FastEthernet 0
```

● 配置 IP 地址。

除了 NULL 接口，每个接口都有其 IP 地址，IP 地址的配置是使用接口必须考虑的，命令如下：

```
Router(config-if)#ip address ip-address ip-mask
! 配置该接口的网络地址
Router(config-if)#no ip address
! 删除该接口的网络地址
```

②配置接口描述。

接口描述只是用以识别该接口的用途。要配置接口描述，在接口配置模式中执行以下命令：

```
Router(config-if)#description interface-description
```

```
! 描述指定接口的用途,最大支持 240 个字符的描述串
Router(config-if)# no description
! 删除该接口用途的描述
```

● 配置最大传输单元 MTU。

最大传输单元 MTU 是 IP 报文的特性,它的取值范围是 60～1600 字节,设定命令如下所示:

```
Router(config-if)# mtu bytes
! 配置 MTU 大小
Router(config-if)# no mtu
! 恢复 MTU 的缺省值
```

● 配置带宽 Bandwidth。

BandWidth 主要用于一些路由协议(如 OSPF 路由协议)计算路由量度和 RSVP 计算保留带宽。修改接口带宽不会影响物理接口的数据传输速率。带宽的取值范围是 1～10000000,要配置接口的带宽,在接口配置模式中执行以下命令:

```
Router(config-if)# bandwidth kilobits
! 配置 bandwidth
Router(config-if)# no bandwidth
! 取消 bandwidth 的设置
```

③接口监控和维护。

● 监控接口和控制器状态。

```
Router# Show interface [serial] | [Ethernet] | [FastEthernet]
! 显示接口的传输特性、协议特性的参数
Router# Show controllers [serial] | [Ethernet] | [FastEthernet]
! 显示接口的当前内部控制寄存器等信息,以及识别到的电缆线等特性。
```

封装不同链路层协议接口的状态显示有些内容是不同的,例如:接口封装帧中继时,show interace serial0 将显示帧中继的接口信息。

● 关闭和重启接口。

在需要的时候,接口必须被关闭,比如在接口上更换电缆,然后再重新启动接口。

```
Router(config-if)# shutdown
! 关闭端口
Router(config-if)# no shutdown
! 启动该接口
```

(2)LAN 接口管理。

LAN(Local Aare Network)局域网主要有以太网接口、令牌环接口等类型,而以太网口以其灵活简单、易于实现而被广泛应用,其中以太网口以 10M/100M 自适应的 100Base-T 和 10Base-T(RJ-45)接口最为广泛使用。

以太网接口配置如下:

①进入以太网网接口配置模式。

要进入以太网接口配置模式,在全局配置模式中执行以下命令:

```
Router(Config)# Interface ethernet number
```

```
! 进入以太网接口配置模式
Router(Config)# Interface Fastethernet number
! 进入快速以太网接口配置模式
```

②配置 IP 地址。

要配置以太网口接口 IP 地址，在接口配置模式中执行以下命令：

```
Router(Config-if)# ip address ip-address ip-mask [secondary]
! 配置 IP 地址以及其掩码
Router(Config-if)# no ip address ip-address
! 取消以太网口的 IP 地址的设定
```

以太网接口支持多个 IP 地址，用 Secondary 关键字来指出第一个 IP 地址之外的其他 IP 地址。

③配置 MAC 地址。

缺省情况下，每个以太网口都有一个全球唯一的 MAC 地址。如果需要，以太网接口的 MAC 地址可以修改，但必须保证同一局域网上 MAC 地址的唯一性。要配置以太网接口的 MAC 地址，在接口配置模式中执行以下命令：

```
Router(Config-if)# mac-address mac-address
! 配置 MAC 地址
Router(Config-if)# No mac-address
! 取消 MAC 地址的设定
```

MAC 地址的配置可能会影响了局域网内部的通讯，不是必要的情况下，建议用户不要自行配置 MAC 地址。

④配置 MTU。

MTU(Maxiumum Transmission Unit)最大传输单元，在 ETHERNET_II 的帧格式中 MTU 缺省值是 1500，在 ETHERNET_SNAP 帧格式中，缺省是 1492。MTU 的设置可能会影响网络的吞吐量和时延。要配置以太网接口的 MTU，在接口配置模式中执行以下命令：

```
Router(Config-if)# mtu bytes
! 配置 MTU 大小
Router(Config-if)# no mtu
! 恢复 MTU 到缺省值
```

MTU 的取值范围：64～1600。

(3)以太口监控和维护。

①监控以太网接口状态。

监控以太网口接口状态的命令如下：

```
Router# show interface Ethernet number
! 显示以太网接口的状态
Router# show interface FastEthernet number
! 显示快速以太网接口的状态
```

②监控以太网接口控制器状态。

监控以太网口接口状态的命令如下：

```
Router# show controllers Ethernet number
```

```
! 显示以太网接口的当前内部控制寄存器的状态
Router#show controllers FastEthernet number
! 显示快速以太网接口当前内部控制寄存器的状态
```

(4)WAN 接口管理。

WAN(Wide Area Network)就是广域网,按照线路类型来分广域网有 X.25 网、帧中继(Frame-Relay)网、ATM 网以及 ISDN 网等类型。路由器也相应的提供 WAN 接口。现在 RGNOS 支持的 WAN 接口有异步串口以及同步串口。本教材在这里只介绍同步串口的配置方法。

路由器支持的同步串口其接口名称为 Serial。

①同步串口的配置。

● 进入指定同步串口的配置模式的命令。

```
Router(config)#interface serial serial-number
! 进入指定同步串口的配置模式
```

● 设置链路封装协议。

封装协议是同步串口传输的链路层数据的帧格式,RGNOS 支持五种封装协议:PPP、帧中继(Frame-Relay)、LAPB、X.25 以及 HDLC。命令如下:

```
Router(config-if)#encapsulation{ frame-relay | hdlc | lapb | ppp | x25}
! 设置同步串口的链路封装协议
```

同步串口缺省的链路封装格式是 HDLC。

● 设置同步口时钟速率。

同步串口有两种工作方式:DTE 和 DCE,不同的工作方式则选择不同的时钟。如果同步串口作为 DCE 设备,需要向 DTE 设备提供时钟;如果同步串口作为 DTE 设备,需要接受 DCE 设备提供的时钟。

两个同步串口相连时,线路上的时钟速率由 DCE 端决定,因此当同步串口工作在 DCE 方式下,需要配置同步时钟速率,如果作为 DTE 设备使用,则不需配置,其时钟将由 DCE 端提供。要设置同步口时钟速率,在接口配置模式中执行以下命令:

```
Router(config-if)#clock rate clockrate
! 设置同步串口(DCE)的时钟速率
```

缺省情况下,同步口没有时钟的设置。如果同步串口作 DTE 设备,RGNOS 系统将禁止配置其时钟速率。

● 设置 MTU。

同步串口的最大传输单元(MTU)影响 IP 报文在该接口上传输拆包和组包。要设置 MTU,在接口配置模式中执行以下命令:

```
Router(config-if)#mtu mtu-size
! 配置 MTU
Router(config-if)#no mtu
! 取消 MTU 设置,恢复为默认值 1500
```

MTU 单位为字节,缺省值为 1500,取值范围 64～17940(各个型号不同的路由器有所不同)。

②同步串口监控和维护。

命令：

```
Router#show controllers serial [ serial-number ]
! 考察指定的同步串口硬件相关状态
Router#show interfaces serial serial-number
! 考察指定的同步串口软件相关状态
```

③同步串口的故障诊断。

下面给出在同步口与同步口相连，却无法连通的时候，首先必须了解的几个注意点：

- 确保物理接口以及线路连接良好；
- 必须确保 DTE 与 DCE 使用相同的链路层封装协议，且配置正确；
- 必须确保 DTE 与 DCE 同时使用或同时不使用链路层数据压缩传输。

(5)逻辑接口管理。

逻辑接口是相对物理接口而言的，它是指能够实现数据交换功能但在物理上不存在、需要通过配置来建立的接口。RGNOS 提供五类逻辑接口：Loopback(回环)接口，NULL(空)接口，Tunnel(隧道)接口，Dialer(拨号)接口以及子接口。

对于路由器来说，逻辑接口也是和物理接口一样对待的。

①Loopback 接口配置。

Loopback(回环)接口是完全软件模拟的路由器本地接口，它只在逻辑意义上存在，永远都处于 UP 状态。发往 Loopback 接口的数据包将会在路由器本地处理，包括路由信息。Loopback 接口的 IP 地址可以用来作为路由器的管理 IP 地址、OSPF 等动态路由协议的路由器标识等等。配置一个 Loopback 接口类似于配置一个以太网接口，可以把它看作一个虚拟的以太网接口。命令：

```
Router(config)#interface loopback loopback-interface-number
! 设置 loopback 接口
Router(config)#no interface loopback loopback-interface-number
! 删除 loopback 接口
```

使用命令 interface loopback loopback-interface-number 创建一个指定接口号的 loopback 后就可以象配置以太网口一样配置 loopback 接口的参数了。

```
Router(config)#no interface loopback loopback-interface-number
! 删除指定的 loopback 接口
Router#show interfaces loopback loopback-interface-number
! 显示 loopback 接口状态
```

②子接口概述。

路由器中的子接口的概念，是从单个物理接口上衍生出来并依附于该物理接口的逻辑接口，允许在单个物理接口上配置多个子接口，并为应用提供了高度灵活性。子接口是在一个物理接口上衍生出来的多个逻辑接口，即将多个逻辑接口与一个物理接口建立关联关系，同属于一个物理接口的若干个逻辑接口在工作时共用物理接口的物理配置参数，但又有各自的链路层与网络层配置参数。

路由器中支持子接口的物理接口有：

- 非交换式以太网接口；
- 封装帧中继的广域网接口；

● 封装 X.25 的广域网接口。

配置以太网口的子接口，命令如下：

```
Router(config)# interface fastethernet interface-number.subinterface-number
! 进入以太网子接口配置模式
Router(config)# no interface fastethernet interface-number.subinterface-number
! 删除已创建的以太网子接口
```

其中 interface-number 为物理接口序号，subinterface-number 为子接口在该物理接口上的序号，注意二者之间由标号“.”连接。

7. 任务 2 的实施

步骤 1：在路由器上配置 fastethernet 0/0 端口的 IP 地址。

```
Red-Giant>enable! 进入特权模式
Red-Giant # configure terminal
! 进入全局配置模式
Red-Giant (config)# hostname RouterA
! 配置路由器名称为“RouterA”
RouterA(config)# interface fastethernet 0/0
! 进入路由器接口配置模式
RouterA(config)# ip address 192.168.0.1 255.255.255.0
! 配置路由器管理接口 IP 地址
RouterA(config)# no shutdown
! 开启路由器 fastethernet 0/0 接口
```

验证测试：验证路由器接口 fastethernet 0/0 的 IP 地址已经配置和开启。

```
RouterA#show  ip  interface fastethernet 0/0
! 验证接口 fastethernet 0/0 的 IP 地址已经配置和开启
```

或

```
RouterA#show ip interface brief
! 验证接口 fastethernet 0/0 的 IP 地址已经配置和开启
```

显示结果如下：

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.0.1	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0	unassigned	YES	unset	administrativelydown	down
Serial1	unassigned	YES	unset	administratively down	down

步骤 2：配置路由器远程登录密码。

```
RouterA(config)# line vty 0 4
! 进入路由器线路配置模式
RouterA(config-line)# login
! 配置远程登录
RouterA(config-line)# password star
! 设置路由器远程登录密码为“star”
RouterA(config-line)#end
```

验证测试:验证从 PC 机可以通过网线远程登录到路由器上,但无法进入特权模式。

```
C:\>telnet 192.168.0.1
! 从 PC 机登录到路由器上
```

步骤 3:配置路由器特权模式密码。

```
RouterA(config)# enable secret star
! 设置路由器特权模式密码为“star”
```

或

```
RouterA(config)# enable password  star
```

验证测试:配置 PC 机的 IP 为 192.168.0.100/24,验证从 PC 机通过网线远程登录到路由器上后可以进入特权模式:

```
C:\>telnet 192.168.0.1
! 从 PC 机登录到路由器上
```

步骤 4:保存在路由器上所做的配置。

```
RouterA# copy  running-config startup-config
! 保存路由器配置
```

或

```
RouterA# write memory
```

验证测试:验证路由器配置已保存。

```
RouterA#show startup-config
! 验证路由器配置已保存
Building configuration...
Current configuration : 551 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname RouterA
!
enable secret 5 $1$mERr$xRzrjhbAt2e/bvmDgbmqQ1
!
spanning-tree mode pvst
!
interface FastEthernet0/0
ip address 192.168.0.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
```

```
duplex auto
speed auto
shutdown
!
interface VLAN1
no ip address
shutdown
!
ip classless
!
line con 0
line vty 0 4
password star
login
!
End
```

注意事项：

(1)一般通过本地管理环境来搭建 Telnet 环境。要实现 Telnet 必须设置远程登录密码和特权密码；

(2)路由器接口缺省是关闭的(shutdown)，因此必须在配置接口 fastethernet 0/0 的 IP 地址后用“no shutdown”命令开启该接口。

3.7.3　任务 3 开启路由器的缺省路由

1. 缺省路由简介

不是所有的路由器都有一张完整的全网路由表，为了使每台路由器能够处理所有包的路由转发，通常的做法是功能强大的网络核心路由器具有完整的路由表，其余的路由器将缺省路由指向核心路由器。缺省路由可以通过动态路由协议进行传播，也可以在每台路由器上进行手工配置。

2. 缺省路由的配置

(1)手工配置缺省静态路由。

```
Router(config)# ip route0.0.0.0 0.0.0.0 {ip-address | interface-type interface-number }
[distance][tag tag][permanent]
! 配置静态路由
Router(config)#no ip route0.0.0.0 0.0.0.0
! 删除静态路由
```

其中“0.0.0.0 0.0.0.0”表示网络号和子网掩码均为“0.0.0.0”，指所有网络。

(2)手工配置缺省网络。

多数的内部网关路由协议，都有一个将缺省路由传播到整个路由域的机制。要传播缺省路由的路由器必须具有缺省路由。

要配置缺省网络，在全局命令配置模式中执行以下命令：

```
Router(config)# ip default-network network
! 配置缺省网络
Router(config)# no ip default-network network
! 删除缺省网络
```

当路由器有缺省路由时，不管是动态路由协议学习的还是手工配置产生的，show ip route 时，路由表中的“gateway of last resort”会显示该最后网关的信息。一个路由表可能会有多条网络路由为候选缺省路由，但只有最好的缺省路由才能成为“gateway of last resort”。

3.7.4 任务4 使用1个公网地址如何满足多人上网

假如你是某公司的网络管理员，公司只向 ISP 申请了一个公网 IP 地址段 100.1.1.0/24，希望全公司的主机都能访问外网，请你在路由器 R1 上作 NAPT 配置加以实现，如图 3-12 所示。

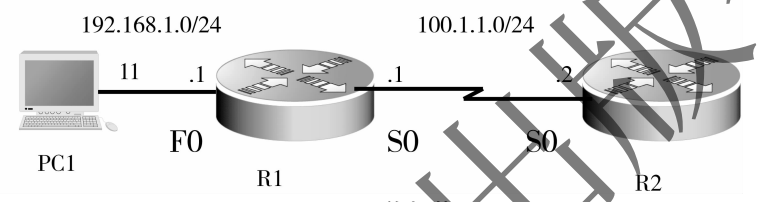

图 3-12 网络拓扑图

1. NAT 简介

(1)NAT 的基本概念。

随着接入 Internet 的计算机数量的不断猛增，公有 IP 地址资源也就愈加显得捉襟见肘，公有 IP 地址根本无法满足网络用户的需求，因此 NAT 技术应运而生。

NAT 的英文全称是“Network Address Translation”，中文意思是“网络地址转换”，它是一个 IETF 标准，广义的概念，它是一种把内部私有网络地址(IP 地址)翻译成合法网络 IP 地址的技术。

狭义的 NAT 是指一对一的地址映射，即一个私有 IP 地址转换成一个合法 IP，能实现内部网络主机轮流与外部通讯，但不能同时满足所有的内部网络主机与外部网络通讯的需要，因此又产生了 NAPT。使用 NAPT，可以将多个内部本地地址映射到一个内部全局地址，路由器用“内部全局地址＋TCP/UDP 端口号”来对应“一个内部主机地址＋TCP/UDP 端口号”，即多个私有 IP 地址通过占用同一个合法 IP 的不同端口，实现多对一的地址映射。

一般我们讲 NAT，是指广义上的概念。NAT 不仅完美地解决了 IP 地址不足的问题，让一个局域网只需使用少量 IP 地址(甚至是 1 个)即可实现私有地址网络内所有计算机与 Internet 的通信需求，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。

NAT 的用途和特点：

当出现如下情况时，我们可以考虑使用 NAT：

①连接到 Internet，但却没有足够的合法地址分配给内部主机。

②更改到一个需要重新分配地址的 ISP。

③有相同的 IP 地址的两个 Intranet 合并。

④需要做 TCP 流量的负载均衡(主机)。

在决定应用 NAT 时,我们需要知道 NAT 同时也会带来一些限制:

①影响网络速度,NAT 的应用可能会使 NAT 设备成为网络的瓶颈,随着软、硬件技术的发展,该问题已经逐渐得到改善。

②NAT 将无法对内嵌 IP 地址进行地址转换,造成这些应用不能正常运行。

③地址转换不能处理 IP 报头加密的报文。

④无法实现对 IP 端到端的路径跟踪,经过 NAT 地址转换之后,你不能再经过 NAT 使用 ping 和 traceroute。

(2)NAT 的一些常用术语。

Inside 表示内部网络,一般指需要 NAT 的局域网。在内部网络,每台主机都分配一个内部私配的 IP 地址,但与外部网络互连时,必须转换为另外一个合法公有地址才能正常通信。每台主机的前一个地址又称为内部本地地址,后一个地址又称为内部全局地址。

Outside 表示外部网络,是相对内部网而言的,指内部网络需要连接的网络,一般指互联网,也可以是另外一个局域网。外部网的地址也可以被转换,外部主机也同时具有本地地址和全局地址。

综上所述,NAT 做了以下定义:

①内部本地地址(Inside Local IP Address):指定于内部网络的主机地址,在内部网络唯一,但为私有地址或未注册地址。

②内部全局地址(Inside Global IP Address):代表一个或更多内部本地 IP 到外部网络的合法 IP。

③外部本地地址(Outside Local IP Address):外部网络分配给外部主机的 IP 地址,在外部网络唯一,但为私有地址或未注册地址。

④外部全局地址(Outside Global IP Address):外部网络主机的合法 IP。

2. NAT 配置

在 NAT 配置之前,我们首先需要了解 NAT 的分类、特点及适用条件,以便我们能根据实际情况有选择的进行适当的 NAT 配置,如表 3-14 所示。

表 3-14　　NAT 分类表

类别	转换对象	方式	特点	适用条件
NAT(网络地址转换)	网络地址	静态	内部本地地址和内部全局地址的一对一永久映射	外部网络需要通过固定的全局可路由地址访问内部主机时
		动态	内部本地地址和内部全局地址池的一对一临时映射关系,过一段时间没有用就会删除映射关系	同时与外网通信的内部主机数量≤可用内部全局地址数量

（续表）

类别	转换对象	方式	特点	适用条件
NAPT（网络地址端口转换）	网络地址＋TCP/UDP端口号	静态	1.（内部本地地址＋端口号）和（内部全局地址＋端口号）的一对一永久映射 2.内部本地地址和内部全局地址的多对一永久映射	全局地址极缺时，外部网络需要通过固定的全局可路由地址和固定端口号访问内部主机，如WWW服务器等
		动态	1.（内部本地地址＋端口号）和（内部全局地址＋端口号）的一对一临时映射关系，过一段时间没有用就会删除映射关系 2.内部本地地址和内部全局地址的多对一临时映射	同时与外网通信的内部主机数量≥可用内部全局地址数量 （特别适用于内部全局地址数量极少甚至只有一个外部接口地址是合法的情况）

（1）内部源地址NAT配置。

内部源地址转换，就是当内部网络需要与外部网络通讯时，需要将内部私有IP地址转换成全局唯一IP地址。

当一个唯一的内部本地地址要转换成一个唯一的内部全局地址时，我们可以配置静态或动态的NAT来实现互联互通的目的，或者需要同时配置静态和动态的NAT。如图3-13所示反映了内部源地址NAT的整个过程。

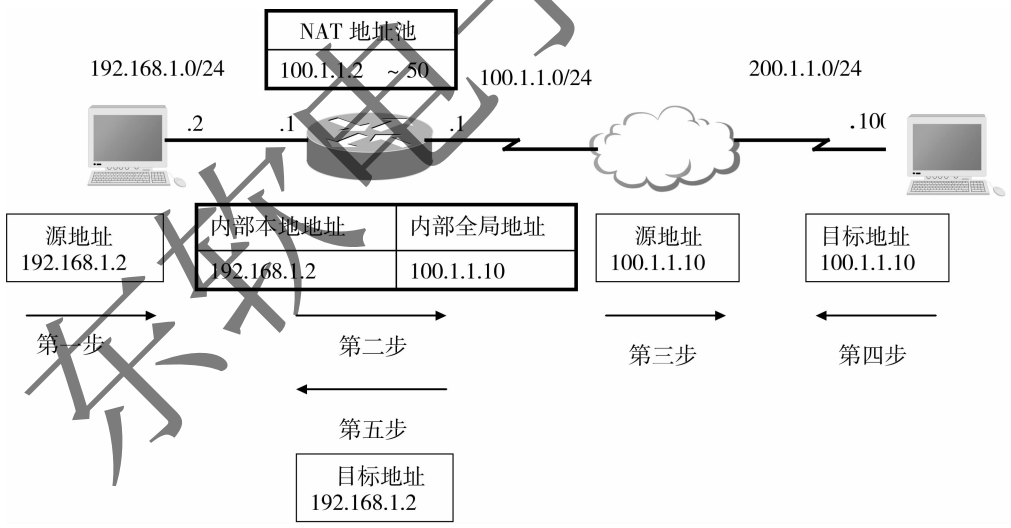

图3-13 内部源地址NAT

当内部网络一台主机访问外部网络资源时，详细过程描述如下：

①内部主机192.168.1.2发起一个到外部主机200.1.1.100的连接。

②当路由器接收到以192.168.1.2为源地址的第一个数据包时，引起路由器检查NAT映射表。

③该地址有配置静态映射，就执行第三步。

④如果没有静态映射，就进行动态映射，路由器就从内部全局地址池中随机选择一个有效

的地址，并在 NAT 映射表中创建 NAT 转换记录，这种记录叫基本记录。

⑤路由器用 192.168.1.2 对应的 NAT 转换记录中全局地址，替换数据包源地址，经过转换后，数据包的源地址变为 100.1.1.10，然后转发该数据包。

⑥200.1.1.100 主机接收到数据包后，将向 100.1.1.10 发送响应包。

⑦当路由器接收到内部全局地址的数据包时，将以内部全局地址 100.1.1.10 为关键字查找 NAT 记录表，将数据包的目的地址转换成内部本地地址 192.168.1.2 并转发给主机 192.168.1.2。

⑧192.168.1.2 接收到应答包，并继续保持会话。第 1 步到第 5 步将一直重复，直到会话结束。

● 静态 NAT 配置。

要配置静态 NAT，在全局配置模式中执行以下命令：

```
Router(config)# ip nat inside source static local-address global-address
! 定义内部源地址静态转换关系
Router(config)# interface interface-type interface-number
! 进入接口配置模式
Router(config-if)# ip nat inside
! 定义该接口连接内部网络
Router(config)# interface interface-type interface-number
! 进入接口配置模式
Router(config-if)# ip nat outside
! 定义接口连接外部网络
```

以上配置为最简单配置，你可以配置多个 Inside 和 Outside 接口。

● 动态 NAT 配置。

要配置动态 NAT，在全局配置模式中执行以下命令：

```
Router(config)# ip nat pool address-pool start-address end-address netmask [netmask]
! 定义全局 IP 地址池
Router(config)# access-list access-list-number permit ip-address wildcard
! 定义访问列表，只有匹配该列表的地址才转换
Router(config)# ip nat inside source access-list-number pool address-pool
! 定义内部源地址动态转换关系
Router(config)# interface interface-type interfacenumber
! 进入接口配置模式 interface-number
Router(config-if)# ip nat inside
! 定义接口连接内部网络
Router(config)# interface interface-type interface-number
! 进入接口配置模式
Router(config-if)# ip nat outside
! 定义接口连接外部网络
```

(2)内部源地址 NAPT 配置。

当需要多个内部本地地址映射到一个内部全局地址室，我们需要进行 NAPT 转换。当进行 NAPT 转换时，路由器需要维护足够的信息(比如 IP 地址、TCP/UDP 端口号)才能将全局

地址转换为内部本地地址。如图 3-14 所示反映了内部源地址 NAPT 的整个过程。

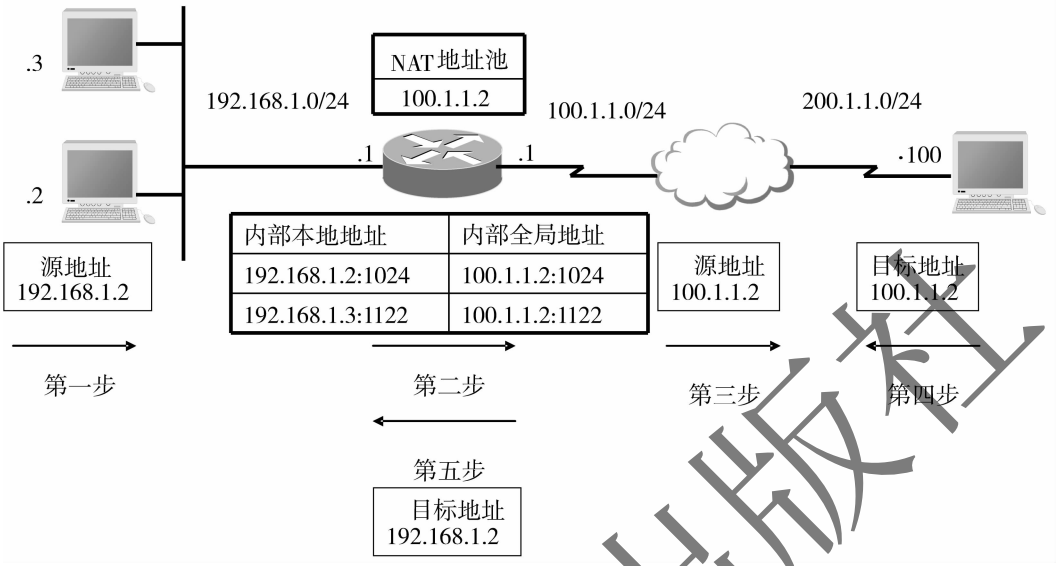

图 3-14　内部源地址 NAPT

如图 3-14 所示，主机 200.1.1.100 以为是在跟同一台设备通信，实际上是分别与内部网络两台地址不同的主机通信。以下详细描述了内部网络 NAPT 的整个过程：

①内部主机 192.168.1.2 发起一个到外部主机 200.1.1.100 的连接。

②当路由器接收到以 192.168.1.2 为源地址的第一个数据包时，引起路由器检查 NAT 映射表。

③如果 NAT 没有转换记录，路由器就为 192.168.1.2 作地址转换，并创建一条转换记录。

④如果启用了 NAPT，就进行另外一次转换，路由器将用不同端口号复用全局地址并保存足够的信息以便能够将全局地址转换回本地地址。NAPT 的地址转换记录称为扩展记录。

⑤路由器用 192.168.1.2 对应的 NAT 转换记录中全局地址，替换数据包源地址，经过转换后，数据包的源地址变为 100.1.1.2，然后转发该数据包。

⑥200.1.1.100 主机接收到数据包后，将向 100.1.1.2 发送响应包。

⑦当路由器接收到内部全局地址的数据包时，将以内部全局地址 100.1.1.2 及其端口号、外部全局地址及其端口号为关键字查找 NAT 记录表，将数据包的目的地址转换成 192.168.1.2 并转发给主机 192.168.1.2。

⑧192.168.1.2 接收到应答包，并继续保持会话。第一步到第五步将一直重复，直到会话结束。

● 静态 NAPT 配置。

要配置静态 NAPT，在全局配置模式中执行以下命令：

```
Router(config)# ip nat inside source static{UDP | TCP} local-address port global-address port
! 定义内部源地址静态转换关系
Router(config)# interface interface-type interface-number
! 进入接口配置模式
Router(config-if)# ip nat inside
```

```
! 定义该接口连接内部网络
Router(config)# interface interface-type interface-number
! 进入接口配置模式
Router(config-if)# ip nat outside
! 定义接口连接外部网络
```

● 动态 NAPT 配置。

要配置内部源地址动态 NAPT,在全局配置模式中执行以下命令:

```
Router(config)# ip nat pool address-pool start-address end-address{netmask mask | prefix-length prefix-length}
! 定义全局 IP 地址池,对于 NAPT,一般就定义一个 IP 地址
Router(config)#access-list access-list-number permit ip-address wildcard
! 定义访问列表,只有匹配该列表的地址才转换
Router(config)# ip nat inside source list access-list-number{[ pool address-pool]|[interface interface-type interface-number]} overload
! 定义源地址动态转换关系
Router(config)# interface interface-type interface-number
! 进入接口配置模式
Router(config-if)# ip nat inside
! 定义接口连接内部网络
Router(config)# interface interface-type interface-number
! 进入接口配置模式
Router(config-if)# ip nat outside
! 定义接口连接外部网络
```

NAPT 可以使用地址池中的 IP 地址,也可以直接使用接口的 IP 地址。一般来说一个地址就可以满足一个网络的地址转换需要。如果地址不够,地址池可以将多定义几个地址。

3. 维护和监控 NAT

虽然动态 NAT 转换记录在一定空闲时间后会被清除,但也可以通过命令强制清除 NAT 映射表。要清除 NAT 的状态以及 NAT 转换记录表,在命令执行模式中执行以下命令:

```
Router#clear ip nat translation *
! 清除 NAT 所有转换记录
```

要显示 NAT 转换的统计状态,在命令执行模式中执行以下命令:

```
Router#show ip nat statistics
显示 NAT 统计状态
```

4. 任务 4 的实施

步骤 1:基本配置。

```
Red-Giant (config)#hostname R1
R1(config)#interface serial 0
R1(config-if)#ip address 100.1.1.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
```

```
R1(config)#interface fastEthernet 0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown

Red-Giant(config)#hostname R2
R2(config)#interface serial 0
R2(config-if)#ip add 100.1.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#end
```

验证测试：

```
R2#ping 100.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 100.1.1.1, timeout is 2 seconds:
!!!!!
```

步骤 2：配置动态 NAPT 映射。

```
R1(config)#ip nat pool to-internet 100.1.1.1 100.1.1.1 netmask 255.255.255.0
! 定义地址池
R1(config)#access-list 1 permit 192.168.1.00.0.0.255
! 定义允许转换的地址
R1(config)#ip nat inside source list 1 pool to-internet overload
! 为内部本地调用转换地址池
R1(config)#int fastEthernet 0
R1(config-if)#ip nat inside
! 定义内部接口
R1(config)#interface serial 0
R1(config-if)#ip nat outside
! 定义外部接口
```

验证测试：

```
R1#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 100.1.1.1:3000     192.168.1.11       ---                ---
```

注意事项：

(1)不要把 inside 和 outside 应用的接口弄错；

(2)要加上能使数据包向外转发的路由，比如默认路由；

(3)尽量不要用广域网接口地址作为映射的全局地址，本例子中特定仅有一个公网地址，实际工作中不推荐。

3.7.5 任务 5 在交换机端口上实现 MAC 地址绑定

MAC 地址绑定是指在交换机的端口设置固定的 MAC 地址，只有绑定在该端口上的 MAC 地址才能通过交换机进行数据交换，其他 MAC 地址无法通过该端口进行数据交换。从而实现端口安全管理。

命令：

```
Switch(config-if)# switchport mode access
! 设置端口为 access 模式。
Switch(config-if)#switchport port-security
! 设置端口为端口安全模式。
Switch(config-if)#switchport port-security mac-address [H.H.H]
! 设置 MAC 地址绑定。H.H.H 表示要绑定的 MAC 地址。
Switch(config-if)#switchport port-security maximum [1-132]
! 设置最大连接数。
```