锐捷 NBR 系列路由器
用户手册

V1.1

版权声明

前言

版本说明

本手册适用于锐捷 NBR 系列 NBR100 路由器。

内容介绍

这份手册主要介绍了锐捷 NBR 系列路由器的硬件特性、安装配置维护以及常见故障的排除。

在安装路由器之前及安装过程中为避免可能出现的设备损坏和人身伤害，请仔细阅读本手册。

建议：

建议由熟悉电气环境、线缆连接以及有实际安装和配置路由器经验的专业技术人员进行安装和配置。

这份手册包括以下章节：

第一章 产品介绍

介绍了锐捷 NBR 系列路由器的外观图以及系统特性；

第二章 安装路由器前的准备

描述了安装路由器的环境要求、安装前和安装过程中需要注意的事项、安装所需工具。

第三章 路由器的安装

介绍路由器的机械安装方法、电源连接方法、备份口电缆连接方法以及配置口电缆连接方法；

第四章 快速配置指导

介绍如何启动并对路由器、搭建路由器的配置环境以及针对网吧的不同应用模式如何进行快速配置；

第五章 高级配置指导

介绍如何进行路由器的 IP 地址配置、静态路由配置、防火墙配置、PPPoE 配置、DHCP 配置以及 NAT 配置；

第六章 安装故障处理

介绍了如何处理安装过程中可能出现的问题以及各种 LED 的含义；

第七章 路由器的维护

介绍了如何对路由器进行主体软件、BOOTROM 软件进行升级。

感谢您选择锐捷 NBR 系列路由器！

说明：

该安装手册只介绍如何安装锐捷 NBR 系列路由器，要使用路由器还需要进行具体的配置，关于如何配置路由器的详细信息，请参考相关部分的配置参考。

在本手册中，锐捷 RG-NBRxxx 系列路由器简称为锐捷 NBRxxx 系列路由器。

详细的说明和配置以随机附带的光盘为准，如果因为时间而有改变，恕不另行通知。

读者对象

本书适合下列人员阅读

网络工程师

技术推广人员

网络管理员

本书约定

1、通用格式约定

宋体：正文采用 5 号宋体。

楷体：

目 录

外型尺寸(高×长×宽)	44.4mm×444.5mm×268.2mm
电压	AC: 170~264V 47/63Hz
功率	小于 30W
	温度：0~40

图 1-3 NBR 路由器的典型应用

其中 NBR 通过光纤转换器使用光纤与 Internet 连接。

第二章 路由器安装前的准备

2.1 安全注意事项

路由器承担着网络连接的中转站的重要作用，其正常使用关系到整个网络是否能正常运作。

在路由器的安装和使用过程中特提出如下的安全建议

请不要将路由器放置在有水的地方，也不要让液体进入路由器。

请将路由器放置在远离热源的地方。

请确认路由器的正常接地。

请用户在安装维护过程中佩戴防静电手腕。

不要穿着松散的服装以防勾住器件造成损坏，为此请系紧衣带、围巾，扎好衣袖。

将工具、器件放在远离人员行走的地方以防碰。

建议用户使用 UPS 不间断

15℃~30℃	0℃~40℃	40%~65%	10%~90%

说明：

工作环境温度湿度是指在路由器机架前后没有保护板时距地板以上 1.5m 和距路由器架前方 0.4m 处测量所得的数值。

短期工作条件指路由器连续工作不超过 48 小时或每年累醋 l e V V P v {

因此，为防止静电的破坏应做到：

设备及地板良好接地

室内防尘

保持适当的温度湿度

接触路由器电路板时，应戴防静电手腕穿防静电工作服。

将拆卸下的路由器电路板面朝上放置在抗静电的工作台上或放入电磁屏蔽袋中。

观察或转移拆卸的路由器电路板时，请用手接触电路板的外边缘避免用手直接触摸电路板上的元器件。

2.2.4 抗干扰要求

这里抗干扰只要是指电磁、电流等干扰，下面是抗干扰的一些要求：

对供电系统采取有效的防电网干扰措施。

路由器工作地最好不要与电力设备的接地装置或防雷接地装置合用并尽可能相距远一些。

远离强功率无线电发射台、雷达发射台等高频大电流设备。

必要时笳榛 3 有薪雷设备。

2.3 安装工具和设备

为了您的安装顺利，请准备：

安装工具
连接电缆
相关设备

安装工具包括：

十字螺丝刀
一字螺丝刀
防静电手腕

连接电缆包括：

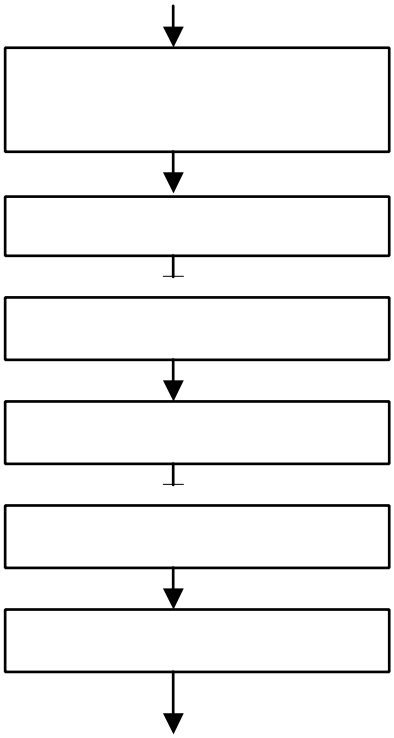
电源线
配置线
以太网线

说明：

锐捷系列路由器随机附电源线、配置线、以太网线以及相关接头。如果还需要其它电缆，需要用户自己另外采购。

相关设备包括：

HUB 或交换机
配置终端(传统字符终端、Windows 终端或者是终端仿真软件的 PC)
电源插座



3.2.2 安装在工作台上

由于经济等各种原因，很多情况下用户并不具备 19 英寸标准机柜，更经常是将路由器放置在干净的工作台上，此种操作比较简单，操作中需要注意如下事项：

保证工作台的平稳性与良好接地。

使用随机带的塑料垫粘到路由器底部的小孔上，同时在路由器周围留出 10cm 的散热空间。

不要在路由器上面放置重物。

3.3. 安装电源线及地线

锐捷系列路由器支持以下交流电源：

AC: 170~264V 47/63Hz

请确认您的电源满足要求。

	3.当作一个异步接口，提供终端接入服务。

您可以通过以下步骤连接路由器控制台口：

第一步，使用随机附带的 DB-9 或 DB-25 孔式插头接到要对路由器进行配置的微机或终端的串口上。如果是微机，请确认微机上有终端仿真软件如超级终端。

第二步，使用随机附带配置线，一端连到路由器的控制台口，另一端连接 DB-9

第四章 快速配置指导

这一章将给出 NBR 功能快速配置说明，其中通过几个典型应用示例的配置过程来说明，用户可以对照自己的应用模式进行类比配置。如果用户需要更进一步的配置，请参考 NBR 功能高级配置部分的说明。无论是 NBR 功能的快速配置还是 NBR 功能的高级配置，都必须首先启动路由器并搭建配置环境。

4.1 启动路由器

4.1.1 搭建配置环境

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

第一步：如图 4-1 所示，将一字符终端或者微机的串口通过标准的 RS232 电缆和路由器的 Console 口（也叫配置口或控制台口）连接。

图 4-1 通过 Console 口搭建本地配置环境

第二步：配置终端的通讯设置参数，如果采用微机，则需要运行终端仿真程序，如 Windows 操作系统提供的 Hyperterm(超级终端)等，以下以超级终端为例，说明具体的操作过程。运行超级终端软件，建立新连接，选择和路由器的 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，并且选择终端仿真类型位 VT100，如下图的 Windows 的超级终端的设置界面。

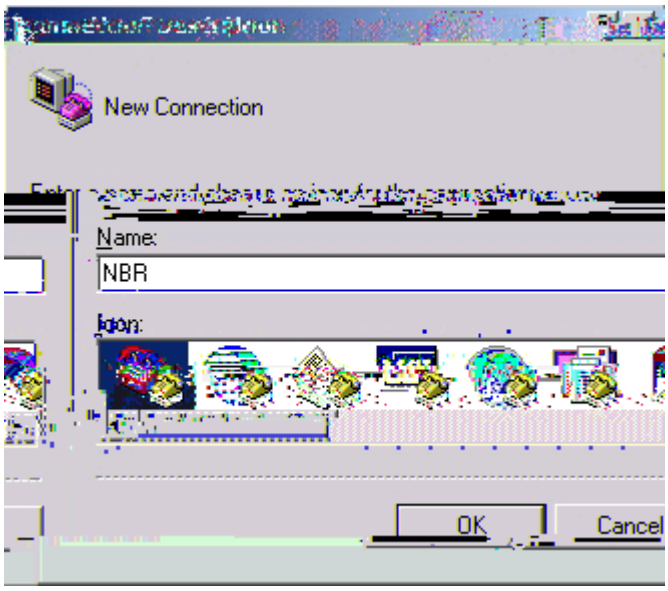


图 4-2 建立新连接

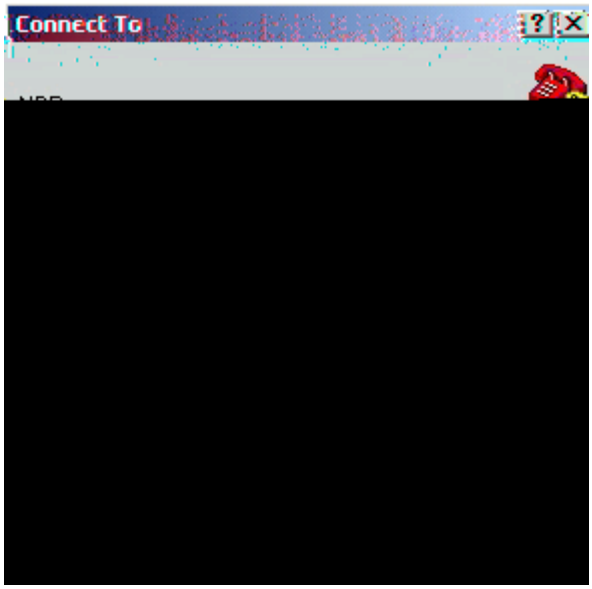


图 4-3 选择和路由器的 Console 连接的微机串口

图 4-4 设置串口的通讯参数

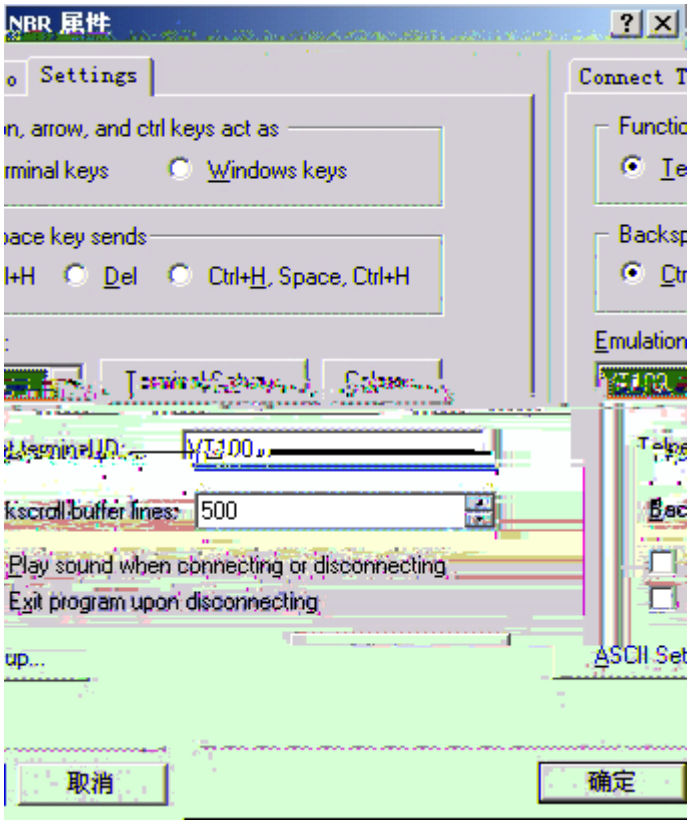


图 4-5 选择终端仿真类型

搭建完配置环境，即可对路由器进行上电。

4.1.2 路由器上电

4.1.2.1 上电前检查

在上电之前，请对路由器进行如下检查：

电源线和地线连接是否正确

供电电压与路由器的要求是否一致

配置电缆连接是否正确配置用微机或终端是否已经打开并设置完毕

警告：

请在路由器上电之前，确认路由器供电开关的位置，以便在发生事故时能够及时切断供电电源。

4.1.2.2 路由器上电

打开路由器供电电源开关

打开路由器电源开关，将路由器电源开关置于“开”位置

4.1.2.3 上电后检查

路由器上电后，请进行如下检查：

通风系统是否正常

检查方法：路由器上电后应该可以听到风扇旋转的声音，把手放在路由器的通风孔附近应该可以感觉到空气的流动。

路由器前面板上的指示灯显示是否正常

检查方法：路由器上电后，前面板上的 POWER 指示灯常亮。

配置终端是否显示正常

检查方法：路由器上电后终端上会显示路由器软件自解压等信息，同时提示是否接入 *setup* 配置过程。

4.1.3 启动过程

路由器第一次启动，会出现如下信息：

```
Start BOOTROM V1.9 build 1 for NBR
Verifying
checksum ......############################################################
#################################################################[0x91e
2][OK!
```

```
Now Loading Image......
################################################################################
######
##########################################
Image load complete! Please wait ...

Uncompress begin...
Uncompressing the image : ======================================== [OK]

Red-Giant Operating System Software
```

是否允许 ping 广域网接口? [yes]: <=*允许应答来自广域网上的针对广域网口的 Ping*

配置局域网口 FastEthernet1: <=*在当前模式下配置本地局域网的地址*
请输入 IP 地址: **192.168.0.1**
请输入地址掩码 [255.255.255.0]:

是否对内部局域网启用 DHCP SERVER 功能? [no]: **no** <=*关闭 DHCP Server 功能*

配置完毕，生成的配置脚本文件如下: <=*预览配置脚本*

```
hostname NBR
ip routing
enable secret 5 $1$aBgm$QujUHlPDifkjVHBfX21hE1
line vty 0 4
password remoteuser
!
!
interface FastEthernet0
no shutdown
ip address 218.6.92.21 255.255.255.0
ip nat outside
!
!
interface FastEthernet1
no shutdown
ip address 192.168.0.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0  218.6.92.1
!
ip nat inside source list 1 interface FastEthernet 0 overload
ip nat optimize
!
access-list 1 permit any
!
end
```

是否应用此配置? [yes/no]: **yes** **<=***保存并应用当前设置*
Building configuration...
在 enabled 模式下使用'configure'命令可修改这些配置。

Press RETURN to get started!

NBR>
NBR>enable <=*进入特权用户层*
Password: <=输入设定的特权用户口令
NBR#

建议：

Setup 配置模式通常用于路由器首次上电时，对路由器进行引导配置，也可以在特权用户模式下随时执行特权用户模式命令 *setup* 命令进入 *setup* 配置模式。

以上说明了 NBR 系列路由器的 Setup 参数的含义，下面将结合三个典型应用示例来说明如何使用 NBR 的 Setup 进行快速配置。

说明：

您在 NBR 上的 *Setup* 快速配置流程中看到的提示信息或者配置步骤或许与本文档中略有出入，这种情况下请以 NBR 上的 RGNOS 当前版本以及随机附带的 CD-ROM 为准。

RGNOS 功能的后续更新恕不另行通知，由此带来的任何可能损失本公司概不负责。如欲了解 RGNOS 功能的最新更新请联系设备供应商或者访问锐捷公司网站 *http://www.red-giant.com.cn/*的相关链接。

4.2 配置路由器

要使用路由器，必须根据需要对路由器进行具体的配置，下面将结合典型的应用使用具体的示例来将描述如何在 NBR 上配置 IP 地址、静态路由、防火墙、PPPoE、DHCP 以及 NAT，其中使用*'!"*开头的斜体是注释说明部分，不是用户输入也不是路由器输出的信息。如果用户需要了解更详细的高级功能配置，可以参考下一章相关的功能配置说明部分。

说明：

下面的典型配置示例均是基于以下这种情况，即不进入初始配置流程，而是借助自动配置命令 *setup* 来实现。

4.2.1 固定 IP 地址接入典型配置

如图 4-6，用户使用电信的光纤线路接入 Interne ，用户将电信提供的光纤接头通过光纤转换器与路由器的 WAN 口连接。用户在 WAN 口上使用电信分配的广域网地址 218.5.19.2，在 LAN 口上使用内部网地址 192.168.0.1，该地址即内部网关地址。用户在 LAN 和 WAN 口上配置了 NAT 以使内部网用户可以共享光纤线路来访问 Internet。

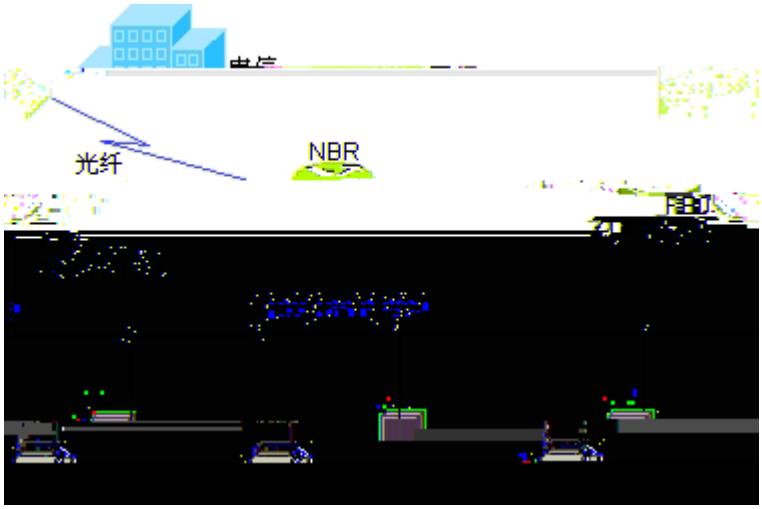


图 4-6 固定 IP 地址接入典型配置示例

在这种情况下，就可以在 NBR 上如下配置即可：

```
Red-Giant>enable
!启动快速配置功能
Red-Giant#setup
        ------------ 交互式系统配置 ----------------
输入 ctrl-c 中止配置流程；默认配置参数在'[]'中。
!选择是否进入快速配置流程
确定进入交互式系统配置? [yes]: yes
配置全局参数:
  请输入路由器名称（只能用字母数字组合） [Red-Giant]: NBR
!配置进入特权用户层的口令
  请输入特权用户密码: private
!配置允许远程 Telnet 登陆的用户密码
  请输入 telnet 远程登陆密码: remoteuser
!启动防止冲击波病毒的功能
启动防止冲击波病毒功能会降低性能，如果确认没有病毒，请不要启动!
  是否启动此功能? [no]: yes
!选择广域网接入方式。这个示例中由于是通过电信的光纤接入，广域网使用的是电信分配的固定 IP 地址，故这里选择模式 1
请选择上网模式:
        1. 固定 IP 地址
        2. PPPOE 连接
        3. DHCP 分配 IP

请输入数字 1---3: 1
!这里为广域网接口 FastEthernet 0 设置电信分配的固定 IP 地址以及掩码。
配置广域网口 FastEthernet0:
  请输入 IP 地址: 218.5.19.2
  请输入地址掩码 [255.255.255.0]:

!禁止广域网上其他用户 ping 广域网口以防止来自广域网上的 Ping 攻击。
是否允许 ping 广域网接口? [yes]: no
!配置本地局域网口 FastEthernet 1 的地址和掩码，这也是内部网关的地址
配置局域网口 FastEthernet1:
```

```
!确定保存当前配置
是否应用此配置? [yes/no]: yes
Building configuration...
[OK]
在 enabled 模式下使用'configure'命令可修改这些配置。

NBR#
%UPDOWN: Line protocol on Interface FastEthernet0, changed state to up
%UPDOWN: Line protocol on Interface FastEthernet1, changed state to up
%CHANGED: Interface Dialer0, changed state to administratively down
%UPDOWN: Interface FastEthernet0, changed state to up
%UPDOWN: Interface FastEthernet1, changed state to up
!再次检查配置.
NBR#show running-config
Building configuration...

Current configuration:
!
!
hostname "NBR"
!
enable secret 5 $1$I3u0$.RIU6kH0S.fil.ivOe9td1
!
!
!
ip subnet-zero
!
interface FastEthernet0
 ip address 218.5.19.2 255.255.255.0
 ip access-group 100 in
 no ip unreachables
 ip nat outside
!
interface FastEthernet1
 ip address 192.168.0.1 255.255.255.0
 ip access-group 100 in
 ip nat inside
!
ip nat inside source list 1 interface FastEthernet0 overload
ip nat optimize
ip classless
ip route 0.0.0.0 0.0.0.0 218.5.19.1
access-list 1 permit any
access-list 100 deny   icmp any any echo
access-list 100 deny   icmp any any echo-reply
access-list 100 deny   tcp any any eq 135
access-list 100 deny   tcp any any eq 136
access-list 100 deny   tcp any any eq 137
access-list 100 deny   tcp any any eq 138
access-list 100 deny   tcp any any eq 139
access-list 100 deny   tcp any any eq 445
access-list 100 deny   udp any any eq 135
```

```
access-list 100 deny   udp any any eq tftp
access-list 100 permit ip any any
!
line con 0
line vty 0 4
 password remoteuser
 login
!
end
```

请输入 telnet 远程登陆密码：**remoteuser**

!启动冲击波病毒防护功能。如果确认内部网没有感染冲击波病毒，建议不要启动该防护功能以免降低系统性能。

启动防止冲击波病毒功能会降低性能，如果确认没有病毒，请不要启动!

是否启动此功能? [no]：**yes**

!选择上网模式即 WAN 口接入 Internet 的模式,这里使用的是 PPPoE 模式。

请选择上网模式:

1．固定 IP 地址

2．PPPOE 连接

3．DHCP 分配 IP

请输入数字 1---3：**2**

!设置局域网口地址即本地网关地址以及 IP MTU

配置局域网口 FastEthernet1:

请输入 IP 地址：**192.168.0.1**

请输入地址掩码 [255.255.255.0]:

!设置 PPPoE 工作参数

配置 PPPOE 参数:

请输入用户名：**pppoeusername**

请输入密码：**pppoepassword**

配置接口 MTU，确切取值和您连接的 ISP 有关(64－1492)。

请输入 MTU [1488]:

!由于内部网主机的 IP 地址是静态配置的，这里就无需启用 DHCP Server 功能

是否对内部局域网启用 DHCP SERVER 功能? [no]:

!预览通过快速配置生产的配置脚本文件

配置完毕，生成的配置脚本文件如下:

```
hostname NBR
ip route 2800 4 5 Tc 8.528C-client dial-pool-numb/MC1 dial-on-demanMCID 18 >>BDCBT/TT9 1
enable secret 5 $1$U8e1$ai/JCzDmSJwi9dwu/z9fr0
line vty 0 4
password remoteuser
!
!
interface FastEthernet0
no shutdown
no ip address
```

```
ppp pap sent-username pppoeusername password 0 pppoepassword
mtu 1488
ip access-group 100 in
ip nat outside
!
ip route 0.0.0.0 0.0.0.0 Dialer 0
!
ip nat inside source list 1 interface Dialer 0 overload
ip nat optimize
!
access-list 1 permit any
access-list 100 deny tcp any any eq 135
access-list 100 deny tcp any any eq 136
access-list 100 deny tcp any any eq 137
access-list 100 deny tcp any any eq 138
access-list 100 deny tcp any any eq 139
access-list 100 deny tcp any any eq 445
access-list 100 deny udp any any eq 135
access-list 100 deny udp any any eq 136
access-list 100 deny udp any any eq netbios-ns
access-list 100 deny udp any any eq netbios-dgm
access-list 100 deny udp any any eq 139
access-list 100 deny udp any any eq 445
access-list 100 deny tcp any any eq 4444
access-list 100 deny udp any any eq tftp
access-list 100 permit ip any any
dialer-list 1 protocol ip permit
!
```

```
 pppoe enable
 pppoe-client dial-pool-number 1 dial-on-demand
!
interface FastEthernet1
 ip address 192.168.0.1 255.255.255.0
 ip access-group 100 in
 ip mtu 1488
 ip nat inside
!
interface Dialer0
 mtu 1488
 ip address negotiate
 ip access-group 100 in
 encapsulation ppp
 ip nat outside
 dialer pool 1
 dialer idle-timeout 200
 dialer-group
 ppp chap hostname pppoeusername
 ppp chap password 7 0508162E0C2A0513341605451F25
 ppp pap sent-username pppoeusername password 7 123715024508311338 3F124A132D
!
ip nat inside source list 1 interface Dialer0 overload
ip nat optimize
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer0
access-list 1 permit any
access-list 100 deny   tcp any any eq 135
access-list 100 deny   tcp any any eq 136
access-list 100 deny   tcp any any eq 137
access-list 100 deny   tcp any any eq 138
access-list 100 deny   tcp any any eq 139
access-list 100 deny   tcp any any eq 445
access-list 100 deny   udp any any eq 135
access-list 100 deny   udp any any eq 136
access-list 100 deny   udp any any eq netbios-ns
access-list 100 deny   udp any any eq netbios-dgm
access-list 100 deny   udp any any eq 139
access-list 100 deny   udp any any eq 445
access-list 100 deny   tcp any any eq 4444
access-list 100 deny   udp any any eq tftp
access-list 100 permit ip any any
dialer-list 1 protocol ip permit
!
line con 0
line vty 0 4
 password remoteuser
 login
!
end

NBR#
```

4.2.3 DHCP

!设置局域网口地址即本地网关地址
配置局域网口 FastEthernet1:
  请输入 IP 地址: **192.168.0.1**
  请输入地址掩码 [255.255.255.0]:
!由于内部网主机的 IP 地址是静态配置的，这里就无需启用 DHCP Server 功能
是否对内部局域网启用 DHCP SERVER 功能? [no]: **no**
!预览通过快速配置生产的配置脚本文件
配置完毕，生成的配置脚本文件如下:

```
hostname NBR
ip routing
enable secret 5 $1$4S/W$f498W8ZBcrVhvX7Bg/vOL.
line vty 0 4
password remoteuser
!
!
interface FastEthernet0
no shutdown
ip address dhcp
ip nat outside
!
!
interface FastEthernet1
no shutdown
ip address 192.168.0.1 255.255.255.0
ip nat inside
!
ip nat inside source list 1 interface FastEthernet 0 overload
ip nat optimize
!
access-list 1 permit any
!
end
```

!选择保存并应用这份配置

```
是否应用此配置? [yes/no]: yes
Building configuration...
[OK]
%UPDOWN: Line protocol on Interface FastEthernet0, changed state to up
%UPDOWN: Line protocol on Interface FastEthernet1, changed state to up
%CHANGED: Interface Dialer0, changed state to administratively down
在 enabled 模式下使用'configure'命令可修改这些配置。
NBR#
%UPDOWN: Interface FastEthernet0, changed state to up
%UPDOWN: Interface FastEthernet1, changed state to up
```

!再次确认配置

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

Current configuration:
!
!
hostname "NBR"
!
enable secret 5 $1$4S/W$f498W8ZBcrVhvX7Bg/vOL.
!
!
!
```

```
ip subnet-zero
!
interface FastEthernet0
 ip address dhcp
 ip nat outside
!
interface FastEthernet1
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
!
ip nat inside source list 1 interface FastEthernet0 overload
ip nat optimize
ip classless
access-list 1 permit any
!
line con 0
line vty 0 4
 password remoteuser
 login
!
end

NBR#
```

第五章 高级配置指导

这部分的内容将介绍如何在 NBR 路由器上配置高级功能，它将描述如何在合适的工作模式下配置或者调整某一单项功能，在描述如何进行 IP 地址配置、静态路由配置、防火墙配置、PPPoE 配置、DHCP 配置以及 NAT 配置之后，将给出一个使用固定 IP 地址接入 Internet 模式下构建多个本地服务器以供广域网用户访问的典型应用示例完整配置流程以供参考。建议一般用户选用 NBR 为网吧用户特意定制的快速配置功能 *Setup* 来进行配置。

5.1 配置 IP 地址

IP 地址配置任务包括以下各项：

接口 IP 地址配置(必须)
地址解析协议(ARP)配置(可选)
主机名到 IP 地址映射配置(可选)
关闭 IP 路由(可选)
广播包处理配置(可选)

5.1.1 接口 IP 地址配置

一个设甭塾行配至离　地郑　趴纫绞蘸椭⑺沤

命令	作用
Red-Giant(config-if)# **ip proxy-arp**	启用代理 ARP 功能
Red-Giant(config-if)# **no ip proxy-arp**	关闭代理 ARP 功能

5.1.3 主机名到 IP 地址映射配置

主机名到 IP 地址的映射有两种方式：1).静态映射，每台设备上都配

Red-Giant(config)#**ip domain-list** *domain-name*	增加域名到域名列表中
Red-Giant(config)#**no ip domain-name** *domain-name*	取消缺省域名
Red-Giant(config)#**no ip domain-list** *domain-name*	删除域名列表中的某个域名

你可以通过域名列表定义多个域名。对于不完整的主机名，路由器将按顺序查找域名列表中定义的后缀域名，DNS 会请求解析完整主机名的 IP 地址，如果所有的后缀域名与不完整主机名的组合都不能解析到 IP 地址，RGNOS 软件就会提示不存在该主机。配置了后缀域名列表，通过命令 **ip domain-name** 定义的缺省域名将失效。

说明：

配置 *ip domain-list* 命令，使用 **Connec***t* 和 **Telnet** 命令跟主机名时，如果主机名的后缀域名不在域名列表中，必须写全主机域名并以点做结尾。

5.1.4 关闭 IP 路由

IP 路由功能缺省情况

广播地址，这就是定向广播，这要求使用广播包的 IP 协议尽可能应用定向广播而不是淹没广播进行数据传播。RGNOS 提供三种途径来控制广播：1).定向网络广播到物理广播转换；2).UDP 广播包和协议转发；3).创建 IP 广播地址。

IP 定向广播报文是指目标地址为某个 IP 子网广播地址的 IP 报文，如目标地址为 172.16.16.255 的报文就称为定向广播报文。但是产生该广播报文的节点又不是目标子网的成员。没有与目标子网直连的路由器接收到 IP 定向广播报文，跟转发单播报文一样处理定向广播报文。你可以在指定的接口上，启动定向广播到物理广播转换的功能，这样该接口就可以转发到直连网络的定向广播了。该命令只影响已到最终目标子网的定向广播报文的最后传输。在接口配置模式中执行以下命令来配置定向广播到物理广播的转换：

命令	作用
Red-Giant(config-if)#**ip directed-broadcast** [*access-list-number*]	在接口上，启动定向广播到物理广播的转换

Red-Giant(config-if)#**no ip directed-broadcast**

5.1.6 IP 地址配置示例

下面给出一个 IP 地址配置示例：

```
Red-Giant#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Red-Giant(config)#interface fastethernet 0
Red-Giant(config-if)#ip add 192.168.20.3 255.255.255.0
Red-Giant(config)#end
Red-Giant#
```

5.2 配置静态路由

5.2.1 配置静态路由

静态路由就是手工配置的路由，使得到指定目标网络的数据包的传送，按照预定的路径进行。要配置静态路由，需在全局配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**ip route** *network mask* {ip-address | *interface-type interface-number* } [*distance*] [**tag** *tag*] [**permanent**]	配置静态路由
Router(config)#**no ip route** *network mask*	删除静态路由

and/or **periodic** *days-of-the-week hh:mm* **to** [*days-of-the- week*] *hh:mm*	配置一个 absolute 规则,但允许多个 periodic 规则并存
Red-Giant(config-time-range)#**exit**	退出 time-range 配置层

关联 ACL 与 Time-range 接口。RGNOS 只允许扩展的 ACL 关联 Time- range 接口。该项功能的典型设置如下：

命令	目的

Red-Giant#

5.3.3 快速访问列表比较功能

启用快速访问列表比较功能会提高访问列表判断速度 ，在全局配置模式下执行以下命令：

命令	作用
Red-Giant(config)# fastaccess	启用快速访问列表比较功能
Red-Giant(config)#no fastaccess	取消快速访问列表比较功能

注意：启用快速访问列表比较功能适合对 access-list 粗粒度的控制以达到提高访问列表判断速度的目的，如果用户熟悉 access-list 的配置方法，不要配置全局 fastaccess 命令 ，这样可以达到更精确判断访问列表的目的。 如果用户需要利用

5.4.1 配置以太网口

以太网口配置任务包括以下部分：使能拨号池和绑定以太网口到指定的拨号池。当然，以太网口的其它一些基本配置是必须的，如接口激活(no shutdown)等。要使能以太网口的

以上配置命令除了第四步命令为可选命令以外，其他命令均必须配。特别是第六步 MTU 的值最大设置为 1492(建议设置为 1488，可以小于 1488，但是不能大于 1492)，否则无法正常通信。

另外建议联系 ISP 以确认合适的 MTU，有的 ISP(如某些地方的典型局端)要求将 MTU 必须设置为 1488，而有的 ISP 要求将 MTU 必须设置为 1492。

5.4.3 配置必要的全局参数

配置必要的全局参数。PPPoE 必要的全局参数，

```
 ip nat inside
!
```

5.5.1 启用 DHCP 服务器与中继代理

缺省情况下，RGNOS 启用了 DHCP 服务器同时关闭了 DHCP 中继代理，这两者不能并存。全局配置模式中执行以下命令来控制启用何种功能：

命令	作用
Red-Giant(config)#**service dhcp**	启用 DHCP 服务器,关闉ＶＢ８９６Ｃｖ 器

务器认为该地址已经在使用，就试图分配另外一个地址给 DHCP 客户端。要配置 Ping 包次数，在全局配置模式中执行以下命令：

命令	作用
Red-Giant(config)#**ip dhcp ping packets** *number*	配置 Ping 包次数

5.5.7 配置

5.5.10 DHCP Client 配置示例

以下配置中，路由器接口 FastEthernet0 配置了 DHCP 自动分配地址。

```
interface FastEthernet0
ip address dhcp
```

5.6 配置 NAT

在配置 NAT(网络地址转换)之前，你首先需要了解内部本地地址和内部全局地址的分配情况。根据你对 NAT 不同的需要，可以执行以下不同的任务来达到目的。

内部源地址 NAT 配置
内部源地址 NAPT 配置
重叠地址 NAT 配置
TCP 负载均衡
配置特殊应用 NAT
配置 NAT 快速优化
调整 NAT 超时时间

5.6.1 配置内部源地址 NAT

当内部网络需要与外部网络通讯时，需要配置 NAT，将内部私有 IP 地址转换成全局唯一 IP 地址。你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。

静态 NAT，是建立内部本地地址和内部全局地址的一对一永久映射。当外部网络需要通过固定的全局可路由地址访问内部主机，静态 NAT 就显得十分重要。要配置静态 NAT，在全局配置模式中执行以下命令：

命令	作用

命令	作用
Red-Giant(config)#**ip nat pool** *address-pool start-address end-address* {**netmask** *mask* | **prefix-length** *prefix-length*}	定义全局 IP 地址池
Red-Giant(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
Red-Giant(config)#**ip nat inside source list** *access-list-number* **pool** *address-pool*	定义内部源地址动态转换关系

Red-Giante

Red-Giant(config)#**ip nat pool** *address-pool start-address end-address*

Red-Giant(config)#**ip nat pool** *address-pool start-address end-address* {**netmask** *mask* | **prefix-length** *prefix-length*}

缺省情况下支持 FTP、DNS 应用,这些应用兼容在 RFC3027 中有规定，另外还支持腾讯 QQ 应用加速、帝国时代游戏以及 NetMeeting 等应用。

如果是内部网络主机做帝国时代游戏的服务器，为了方便配置，

默认是不控制内网的 ip 申请的 nat 会话数.

5.6.8 调整地址转换超时时间

静态 NAT 转换是永[illegible]，但动态 NA[illegible]闲一段时间后就会超时。要调整 NAT 地址转换超时[illegible]在全局配置模式[illegible]以下命令：

命令	
Red-Giant(config)#**ip n[illegible]ation timeout** *seconds*	[illegible]单动态 NAT 转换超时时间，[illegible]00 秒
Red-Giant(config)#**ip n[illegible]ation dns-timeout** *seconds*	[illegible]NS 转换记录的超时时间，缺[illegible]
Red-Giant(config)#**ip n[illegible]ation finrst-timeout** *second[illegible]*	[illegible]P 连接 FIN 以及 RESET 后[illegible]的超时时间，缺省 60 秒
Red-Giant(config)#**ip n[illegible]ation icmp-timeout** *seconds*	定[illegible]换记录的超时[illegible]缺省[illegible]
Red-Giant(config)#**ip n[illegible]ation tcp-timeout** *seconds*	

```
!
ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0
ip nat inside source list 1 pool net200
ip nat optimize
access-list 1 permit 192.168.12.0 0.0.0.255
```

通过显示 NAT 映射表，可以看到是否能够正确建立转换记录：

```
Red-Giant#sh ip nat translations verbose
Pro Inside global     Inside local      Outside local     Outside global
--- 200.168.12.2      192.168.12.2      ---               ---
create 00:00:42, use 00:00:33, left 00:09:26, flags: none
```

5.6.9.2 内部全局地址复用示例

内部全局地址复用，其实就是 NAPT。在定义地址池时写上“ overload ”参数就可以复用地址池中的全局地址了。在以下配置中，本地全局地址从 NAT 地址池 net200 中分配，该地址池只定义 200.168.12.200 一个 IP 地址，但允许复用。只有内部源地址匹配访问列表 1 的数据包才会建立该类型 NAT 转换记录。

```
!
interface FastEthernet0
 ip address 192.168.12.1 255.255.255.0
 ip nat inside
!
interface FastEthernet1
 ip address 200.168.12.1 255.255.255.0
 ip nat outside
!
ip nat pool net200 200.168.12.200 200.168.12.200 netmask 255.255.255.0
ip nat inside source list 1 pool net200
ip nat optimize
access-list 1 permit 192.168.12.0 0.0.0.255
```

通过显示 NAT 映射表，可以看到是否能够正确建立转换记录：

```
Red-Giant#show ip nat translations verbose
Pro Inside global     Inside local      Outside local     Outside global
tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23
   create 00:00:19, use 00:00:10, left 00:09:49, flags: extended
Red-Giant#
```

5.6.9.3 重叠地址转换示例

当内部网络地址与外部网络地址重叠时，外部重叠地址在内部网络上应该表现为不同的私有网络地址。在以下配置中，内部网络分配了非注册的 192.198.12.0/24 网络地址，外部网络已经分配了该地址，因此当内部网络通过域名方式访问外部重叠地址主机时，NAT 会将重叠地址转换为地址池 net172 中的地址，这样重叠地址的问题就解决了。以下配置，访问外部重叠地址主机时，只能通过主机域名，如果需要通过 IP 地址直接访问，就要配置外部源地址静态 NAT 映射。内部主机访问外部主机的映射方式采用动态 NAPT 方式。

```
!
```

```
!
interface FastEthernet1
 ip address 200.198.12.1 255.255.255.0
 ip nat outside
!
!
ip nat pool net200 200.198.12.2 200.198.12.100 netmask 255.255.255.0
ip nat pool net172 172.16.198.2 172.16.198.100 netmask 255.255.255.0
ip nat inside source list 1 pool net200 overload
ip nat outside source list 1 pool net172
ip nat optimize
ip route 172.16.198.0 255.255.255.0 200.16.23.2
access-list 1 permit 192.198.12.0 0.0.0.255
!
```

通过显示 NAT 映射表，可以看到是否能够正确建立转换记录：

```
Red-Giant#sh ip nat translations
Pro Inside global     Inside local      Outside local     Outside global
udp 200.168.12.2:1256 192.168.12.91:1256 200.168.168.11:53 200.168.168.11:53
tcp 200.168.12.2:1257 192.168.12.91:1257 172.16.198.2:23  192.168.12.91:23
--- ---               ---               172.16.198.2       192.168.12.91
Red-Giant#
```

在以上配置中，如果没有配置到 172.16.198.0/24 的静态路由，从内部接口接收到目标地址为该网络的数据包，路由器不能判断出来该数据将往哪个接口转发，导致通讯失败。所以当配置重叠地址时，必须配置静态路由或者在 outside 接口配置次 IP 地址，使得路由器知道地址转换以后该往哪个接口转发数据包。

5.6.9.4 TCP 负载均衡示例

在以下配置中，定义了一个虚拟主机地址，所有来自外部网络访问该虚拟主机的 TCP 连接，将被路由器分配到多台实际主机上，从而实现负载分流的目标。Realhosts 定义了实际主机地址池，访问列表

这里的本地服务器是指利用 NBR 将一个或者多个内部主机映射成网络服务器，从而使得广域网上的网络用户可以获得对应的服务。如图 5-1，用户在内部网内设置了三台服务器(FTP 服务器、WEB 服务器以及 E-MAIL 服务器)，他希望广域网上的网络主机能够访问这三个服务器。RGNOS 提供静态 NAT 映射功能来实现这些需求。

图 5-1 构建本地服务器的典型配置示例

为了实现这些功能，需要配置 NAT 静态映射功能。快速配置功能中不包含该功能的设置，因此需要在第一次启动路由器后使用“ *no* ”放弃快速配置然后进入特权用户模式进行高级设置：

```
!进入特权用户层
Red-Giant>enable
!进入全局配置层
Red-Giant#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
!进入 WAN 口配置层
Red-Giant(config)#interface fastethernet 0
!配置 WAN 口地址
Red-Giant(config-if)#ip address 218.5.19.2 255.255.255.0
!设置 WAN 口为共享连接的 Internet 接入口
Red-Giant(config-if)#ip nat outside
!启用 WAN 口
Red-Giant(config-if)#no shut
!返回普通用户层
Red-Giant(config-if)#end
Red-Giant#
!这些是系统提示信息，系统提示 WAN 口链路处于 UP 状态( 可通讯状态).
%UPDOWN: Line protocol on Interface FastEthernet0, changed state to up
%UPDOWN: Interface FastEthernet0, changed state to up
Red-Giant#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
!进入 LAN 口配置层
Red-Giant(config)#interface fastethernet 1
!配置 LAN 口地址
Red-Giant(config-if)#ip address 192.168.0.1 255.255.255.0
!设置 LAN 口为共享连接的 Intranet 接入口
Red-Giant(config-if)#ip nat inside
```

```
!
!
!
!
ip subnet-zero
!
interface FastEthernet0
 ip address 218.5.19.2 255.255.255.0
 ip nat outside
!
interface FastEthernet1
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
!
ip nat inside source list 1 interface FastEthernet0 overload
ip nat inside source static tcp 192.168.0.4 110 218.5.19.2 110
ip nat inside source static tcp 192.168.0.4 25 218.5.19.2 25
ip nat inside source static tcp 192.168.0.3 80 218.5.19.2 80
ip nat inside source static tcp 192.168.0.2 21 218.5.19.2 21
ip nat inside source static tcp 192.168.0.2 20 218.5.19.2 20
ip nat optimize
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0 218.5.19.1
access-list 1 permit any
!
line con 0
line vty 0 4
 password     remoteuser
 login
!
end

NBR#
```

5.8 VRRP 配置

5.8.1 VRRP 概述

VRRP 设计用来实现 IP 传输失败情况下的不中断服务，具体地说，就是用于在局域网内源主机无法动态地学习到首跳路由器 IP 地址的情况下防止首跳路由的失败。VRRP 组内多个路由器都映射为一个虚拟的路由器。VRRP 保证同时有且只有一个路由器在代表虚拟路由器进行包的发送。而主机则是把数据包发向该虚拟路由器。这个转发数据包的路由器被成为主路由器。如果这个主路由器在某个时候由于某种原因而无法工作的话，则处于备份状态的路由器将被选择来代替原来的主路由器。VRRP 使得局域网内的主机看上去只使用了一个路由器，并且即使在它当前所使用的首跳路由器失败的情况下仍能够保持路由的连通性。

RFC 2338 中定义了 VRRP 类型的 IP 报文格式及其运作机制，VRRP 报文是一类指定目的地址的组播报文，该报文由主路由器定时发出来标志其运行正常同时该报文也用于选举主路由器。VRRP 允许为 IP 局域网承担路由转发功能的路由器失效后，局域网中另外一个路由器将自动接管失效的路由器，从而实现 IP 路由的热备份

与容错，同时也保证了局域网内主机通讯的连续性和可靠性。一个 VRRP 应用组通过多台路由器来实现冗余，但是任何时候只有一台路由器作为主路由器来承担路由转发功能，其他的为备份路由器，VRRP 应用组中不同路由器间的切换对局域网内的主机则是完全透明的。RFC 2338 规定了路由器的切换规则：

1). VRRP 协议采用简单竞选的方法选择主路由器。首先比较同一个 VRRP 组内的各台路由器对应接口上设置的 VRRP 优先级的大小，优先级最大的为主路由器，它的状态变为 Master。若路由器的优先级相同，则比较对应网络接口的主 IP 地址，主 IP 地址大的就成为主路由器，由它提供实际的路由转发服务。

2). 主路由器选出后，其它路由器作为备份路由器(状态变为 Backup)，并通过主路由器定时发出的 VRRP 报文监测主路由器的状态。当主路由器正常工作时，它会每隔一段时间发送一个 VRRP 组播报文，称为广告报文，以通知备份路由器：主路由器处于正常工作状态。如果组内的备份路由器在设定的时间段没有接收到来自主路由器的报文，则将自己状态转为 Master。当组内有多台备份路由器时，重复 01)的竞选过程。通过这样一个过程就会将优先级最大的路由器选成新的主路由器，从而实现 VRRP 的备份功能。

图 5-2 VRRP 工作原理图

一旦在一个 VRRP 备份组选举出它的主路由器，局域网内的主机将通过主路由器进行路由转发。通讯过程可以由图 5-2 来说明。在图 5-2 中，路由器 R1 和 R2 均通过以太网口 E0 与局域网 192.168.12.0/24 连接，路由器 R1 与 R2 的 E0 接口上设置了 VRRP，局域网内的主机都以该 VRRP 组的虚拟路由器 IP 地址作为默认网关。对于局域网内的主机而言，它们只能感受到由 VRRP 组的虚拟路由器，而实际承担路由转发功能的 VRRP 组的主路由器对它们而言则是透明的。譬如，局域网内的主机 PC 1 如果要与其它网络内的主机 PC 2 通讯，PC 1 会以虚拟路由器为默认网关来发送通向 PC 2 的网络数据包，VRRP 组中的主路由器在接收到该数据包后会将该数据包转发给 PC 2。在这个通讯过程中，PC 1 只能感受到虚拟路由器而不知道扮演虚拟路由器角色的主路由器究竟是 R1 还是 R2，在这个 VRRP 组中的主路由器是在 R1 与 R2 之间选举产生的，一旦主路由器失效

5.8.2 VRRP 的应用

VRRP 有两种应用模式：基本应用与高级应用。其中基本应用是使用单备份组实现简单路由冗余，高级应用是使用多备份组同时实现路由冗余与负载均衡。

5.8.2.1 路由冗余

VRRP 的基本应用可以通过图 5-3 示例来说明。

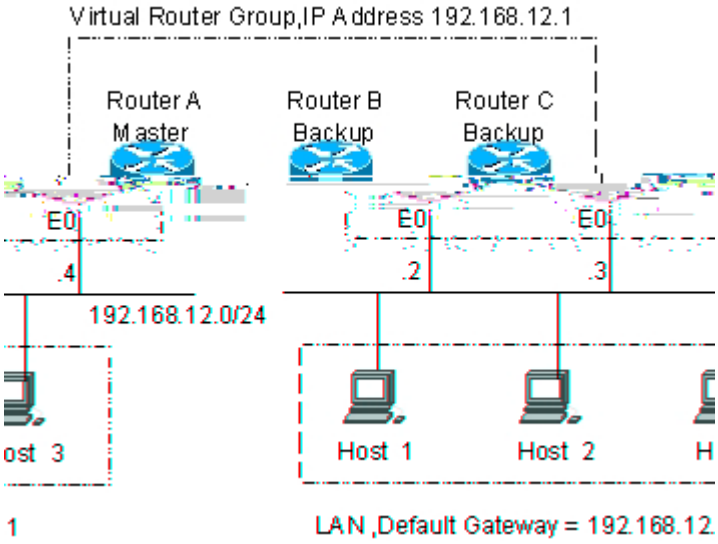


图 5-3 VRRP 基本应用示意图

如图 5-3，路由器 A

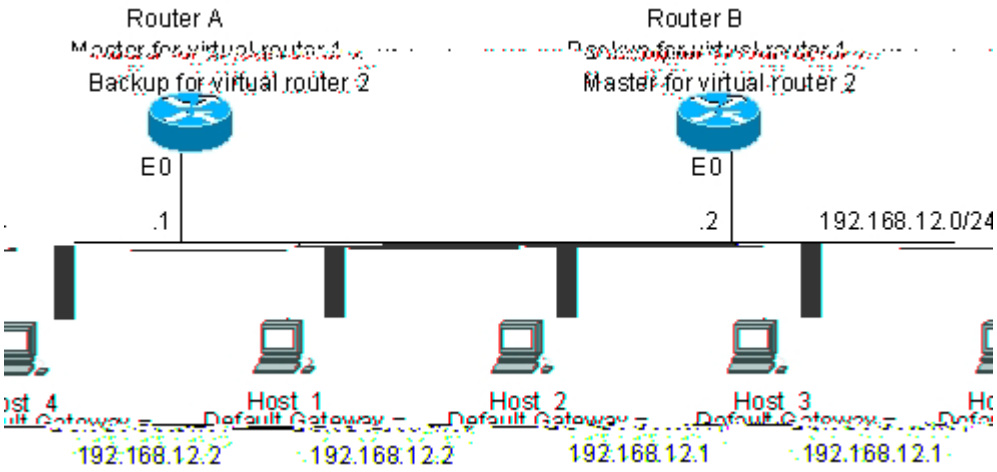


图 5-4 VRRP 高级应用示意图

如图 5-4，设置了两个虚拟路由器。对于虚拟路由器 1，路由器 A 使用以太网口 E0 的 IP 地址 192.168.12.1 作为虚拟路由器的 IP 地址,这样路由器 A 就成为主路由器，而路由器 B 成为备份路由器。对于虚拟路由器 2，路由器 B 使用以太网口 E0 的 IP 地址 192.168.12.2 作为虚拟路由器的 IP 地址，这样路由器 B 就成为主路由器，而路由器 A 成为备份路由器。在局域网内，主机 1 和主机 2 使用虚拟路由器 1 的 IP 地址 192.168.12.1 作为默认网关，主机 3 和主机 4 使用虚拟路由器 2 的 IP 地址 192.168.12.2 作为默认网关。在 VRRP 这个应用中，路由器 A 和路由器 B 实现了路由冗余，并同时分担了来自局域网的流量即实现了负载平衡。

5.8.3 VRRP V R R P

5.8.3.2 启动 VRRP 备份功能

通过设置备份组号和虚拟 IP 地址可以在指定的局域网段上添加一个备份组从而启动对应的以太网接口的 VRRP 备份功能。

命令	目的

说明：

在没有设置 VRRP 定时器学习功能的时候，同一个 VRRP 备份组要设置相同的 VRRP 广告发送间隔，否则处于备份状态的路由器将会丢弃接收到的 VRRP 广告。

5.8.3.5 设置路由器在 VRRP 备份组中的抢占模式

如果 VRRP 组工作在抢占模式下，一旦它发现自己的优先级高于当前 Master 的优先级，它将抢占成为该 VRRP 组的主路由器。如果 VRRP 组工作在非抢占模式下，即便它发现自己的优先级高于当前 Master 的优先级，它也不会抢占成为该 VRRP 组的主路由器。VRRP 组使用以太网接口 IP 地址情况下，抢占模式是否设置意义不大，因为此时该 VRRP 组具有最大优先级，它自动成为该 VRRP 组中的主路由器。

命令	目的
Router(config-if)# **vrrp** *group* **preempt [delay** *seconds*]	设置 VRRP 备份组处于抢占模式

Router(config-if)# **no vrrp** *group* **preempt**

	接口
Router(config-if)# **no vrrp** *group* **track** *interface-type number*	取消VRRP备份组监视接口设置

缺省状态下，系统没有设置 VRRP 备份组监视的接口。参数 *interface -priority* 取值范围为 1~255。如果参数 *interface -priority* 缺省，系统会取默认值即 10。

5.8.3.8 设置 VRRP 广播定时器学习功能

一旦启用了定时器学习功能，如果当前路由器是 VRRP 备份路由器，在设置了定时器学习功能后，它会从主路由器的 VRRP 广告中学习 VRRP 广告发送间隔　间隔

5.8.4.1 show vrrp

RGNOS 提供以下的 **show vrrp** 命令来考察本地路由器的 VRRP 状态。

命令	目的
Router# **show vrrp [brief |** *group*]	查看当前的 VRRP 状态
Router# **show vrrp interface** *type number* **[brief]**	显示指定网络接口上 VRRP 状态

下面给出使用这些命令的示例。

1.show vrrp 命令

```
Router#show vrrp
FastEthernet0 - Group 1
  State is Backup
  Virtual IP address is 192.168.201.1 configured
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is 192.168.201.213 , pritority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 9 sec
FastEthernet0 - Group 2
  State is Master
  Virtual IP address is 192.168.201.2 configured
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is 192.168.201.217 (local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 9 sec
Router#
```

上面的显示信息包括以太网口名称、接口上设置的 VRRP 备份组号、状态、优先级、抢占方式、VRRP 广告间隔、虚拟 IP 地址、虚拟 MAC 地址、Master 路由器 IP 地址、Master 路由器优先级、Master 路由器广告间隔、Master 路由器失效判断间隔、当前 VRRP 备份组监视的接口以及对应的优先级改变尺度。

2.show vrrp brief 命令

```
    Router#show vrrp brief
 Interface     Grp Pri Time  Own Pre State   Master addr     Group addr
 FastEthernet0  1   100   -    -   P  Backup  192.168.201.213 192.168.201.1
 FastEthernet0  2   120   -    -   P  Master  192.168.201.217 192.168.201.2
 Router#
```

上面的显示信息包括以太网口名称、接口上设置的 VRRP 备份组号、状态、优先级、抢占方式、虚拟 IP 地址、Master 路由器 IP 地址。

3.show vrrp interface 命令

```
Router#show vrrp interface fastethernet 0
FastEthernet0 - Group 1
  State is Backup
```

```
  Virtual IP address is 192.168.201.1 configured
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is 192.168.201.213 , pritority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 9 sec
FastEthernet0 - Group 2
  State is Master
  Virtual IP address is 192.168.201.2 configured
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 3 sec
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is 192.168.201.217 (local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 9 sec
Router#
```

上面的显示信息包括指定的以太网口名称、接口上设置的 VRRP 备份组号、状态、优先级、抢占方式、VRRP 广告间隔、虚拟 IP 地址、虚拟 MAC 地址、Master 路由器 IP 地址、Master 路由器优先级、Master 路由器广告间隔、Master 路由器失效判断间隔、当前 VRRP 备份组监视的接口以及对应的优先级改变尺度。

5.8.4.2 debug vrrp

RGNOS 提供以下的 **debug vrrp** 命令来提供本地路由器的 VRRP 状态调试信息。

命令	目的
Router# **debug vrrp error**	打开 VRRP 出错提示调试开关
Router# **no debug vrrp error**	关闭 VRRP 出错提示调试开关
Router# **debug vrrp events**	打开 VRRP 事件调试开关
Router# **no debug vrrp events**	关闭 VRRP 事件调试开关
Router# **debug vrrp packets**	打开 VRRP 报文调试开关
Router# **no debug vrrp packets**	关闭 VRRP 报文调试开关
Router# **debug vrrp state**	打开 VRRP 状态调试开关
Router# **no debug vrrp state**	关闭 VRRP 状态调试开关
Router# **debug vrrp all**	打开 VRRP 调试开关
Router# **no debug vrrp all**	关闭 VRRP 调试开关

下面给出使用这些命令的示例。

1.debug vrrp all 命令

```
Router#debug vrrp all
VRRP debugging is on
Router#
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
```

```
    %VRRP-6-STATECHANGE: Fa0 Grp 1 state Master -> Backup
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address
192.168.1.1
%VRRP-6-STATECHANGE: Fa0 Grp 1 state Backup -> Master
    Router#
```

debug vrrp all

```
%VRRP-6-STATECHANGE: Fa0 Grp 2 state Master -> Backup
%VRRP-6-STATECHANGE: Fa0 Grp 2 state Backup -> Master
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastethernet0
Router(config-if)#no shutdown
Router(config-if)#end
Router#
%VRRP-6-STATECHANGE: Fa0 Grp 2 state Master -> Init
 Router#
```

上面的显示信息表明 Fastethernet 0 上的 VRRP 组状态在 Master，Backup 以及 Init 之间转换。

5.8.5 VRRP 的典型配置示例

在图 5-5 所示的连接中，在路由器 R1 与 R2 上配置了 VRRP 备份组来为内部网段 192.168.201.0 /24 提供 VRRP 服务，而在路由器 R3 上没有配置 VRRP 而只是配置了普通路由功能。下面的配置中将只给出路由器 R1 与 R2 的 VRRP 相关配置。

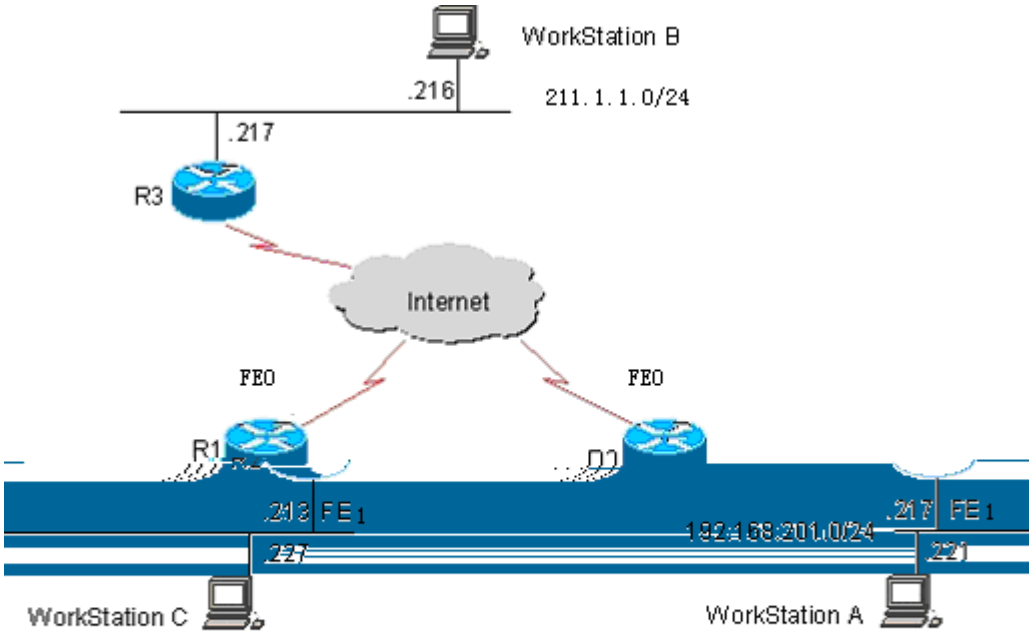


图 5-5 建立 VRRP 环境的网络连接示意图

在下面的配置示例中，路由器 R3 的配置是不变的。下面给出路由器 R3 的配置:

```
R3#show running-config
Building configuration..

Current configuration:
!
!
hostname "R3"
!
```

```
!
ip subnet-zero
no ip domain-lookup
!
interface FastEthernet0
 ip address 211.1.1.217 255.255.255.0
 !
interface FastEthernet1
 ip address 202.1.1.5 255.255.255.0

!
ip classless
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 privilege level 15
 no login
!
end
```

5.8.5.1 VRRP 单备份组配置示例

按照图 5-5 建立连接。在这个配置示例中，用户工作站群(192.168.201.0/24)使用路由器 R1 与 R2 组成的备份组，并将其网关指向该备份组设置的虚拟路由器的 IP 地址 192.168.201.1，经由虚拟路由器 192.168.201.1 访问远程用户工作站群。在这里 R1 被设置成 VRRP 的 Master！檯梔

(歟氖： 011205.592Ovrrp6 1ip (192(1682(011 2)TjET EMC /Artifact <</

```
!

 no ip address

!
ip nat inside source list 1 interface Fastethernet 0 overload
ip nat optimize
access-list 1 permit any
ip route 0.0.0.0 0.0.0.0 202.1.1.5
ip classless
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 privilege level 15
 no login
!
end
```

路由器 R2 的配置：

```
R2#show running-config
Building configuration...

!
hostname "R2"
!
ip subnet-zero
!
no ip domain lookup
!
interface FastEthernet0
 ip address 202.1.1.8 255.255.255.0
 ip nat outside
 keepalive 10 auto-detect
!
!
interface FastEthernet1
 ip address 192.168.201.213 255.255.255.0
 ip nat inside
  vrrp 1 ip 192.168.201.1
  vrrp 1 timers advertise 3
!
ip nat inside source list 1 interface Fastethernet 0 overload
ip nat optimize
access-list 1 permit any
ip classless
ip route 0.0.0.0 0.0.0.0 202.1.1.5
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 no login
!
```

```
end
```

可见，路由器 R1 与 R2 同处于 VRRP 备份组 1 中，指向相同的虚拟路由器的 IP 地址(192.168.201.1)并且均处于 VRRP 的抢占模式下。由于路由器 R1 的 VRRP 备份组优先级为 120，而路由器 R2 的 VRRP 备份组优先级取默认值 100，所以路由器 R1 在正常情况下充当 VRRP 的 Master 路由器。

5.8.5.2 使用 VRRP 监视接口配置示例

按照图 5-5 建立连接。在这个配置示例中，用户工作站群(192.168.201.0/24)使用路由器 R1 与 R2 组成的备份组，并将其网关指向该备份组设置的虚拟路由器的 IP 地址 192.168.201.1，经由虚拟路由器 192.168.201.1 访问远程用户工作站群(其工作网络为 192.168.12.0/24)。在这里 R1 被设置成 VRRP 的 Master 路由器。与单备份组配置示例不同的是，在这个配置示例中，路由器 R1 中设置了 VRRP 监视接口 f0(即 Fastethernet0，下文有相同用法处将不再说明)。正常情况下，路由器 R1 作为活动路由器提供虚拟网关(192.168.201.1)的功能，当路由器 R1 由于关机或者出现故障而不可到达时，路由器 R2 将替代它来提供虚拟网关(也就是虚拟路由器的地址 192.168.201.1)的功能。特别的是在路由器 R1 的与广域网的接口 f0 不可用的时候，路由器 R1 将会按照设置降低自己的 VRRP 备份组的优先级，从而使得路由器 R2 有机会成为主动路由器并提供虚拟网关(192.168.201.1)的功能；如果此后路由器 R1 与广域网的接口 f0 恢复正常，那么路由器 R1 将恢复自己的 VRRP 备份组优先级再次成为主动路由器并提供虚拟网关的功能。下面分别给出路由器 R1 与 R2 的相关配置。

路由器 R1 的配置：

```
R1#show running-config
Building configuration...

Current configuration:
!
!
hostname "R1"
!
!
ip subnet-zero
no ip domain-lookup
!
interface FastEthernet 0
 ip address 202.1.1.6 255.255.255.0
 ip nat outside
 keepalive 10 auto-detect
!
interface FastEthernet 1
 ip address 192.168.201.217 255.255.255.0
 ip nat inside
 vrrp 1 priority 120
 vrrp 1 timers advertise 3
 vrrp 1 ip 192.168.201.1
 vrrp 1 track Fathernet0 30
!
ip nat inside source list 1 interface Fastethernet 0 overload
ip nat optimize
access-list 1 permit any
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 202.1.1.5
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 privilege level 15
 no login
!
end
```

路由器 R2 的配置：

```
R2#show running-config
Building configuration...
!
hostname "R2"
!
ip subnet-zero
!
no ip domain lookup
!
interface FastEthernet 0
 ip address 202.1.1.8 255.255.255.0
 ip nat outside
 keepalive 10 auto-detect
!
interface FastEthernet 1
 ip address 192.168.201.213 255.255.255.0
 ip nat inside
 vrrp 1 ip 192.168.201.1
 vrrp 1 timers advertise 3
!
ip nat inside source list 1 interface Fastethernet 0 overload
ip nat optimize
access-list 1 permit any
!
ip classless
ip route 0.0.0.0 0.0.0.0 202.1.1.5
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4

 no login
!
end
```

可见，路由器 R1 与 R2 同处于 VRRP 备份组 1 中，使用相同的 VRRP 备份组验证模式(无验证模式)、指向相同的虚拟 IP 地址(192.168.201.1)并且均处于 VRRP 的抢占模式下。路由器 R2 与路由器 R2 的 VRRP 的广告(Advertisement)间隔均为 3 秒。正常情况下，由于路由器 R1 的 VRRP 备份组优先级为 120，而路由器 R2 的 VRRP 备份组优先级取默认值 100，所以路由器 R1 在正常情况下充当 Master 路由器。如果路由器 R1 在作为 Master 路由器状态下发现与广域网的接口 f0 不可用，路由器 R1 将降低自己的 VRRP 备份组优先级 30 而成为 90，这样路由器 R2 就会成为 Master 路由器。如果在此后，路由器 R1 发现自己的与广域网的接口 f0 恢复可用，

就增加自己的 VRRP 备份组优先级 30 而恢复到 120，这样路由器 R1 将再次成为主路由器。

5.8.5.3 VRRP 多备份组配置示例

除了单备份组，RGNOS 还允许在同一个以太网接口上配置多个 VRRP 备份组。使用多备份组，有着显而易见的好处：可以实现负载均衡同时通过互 ` 8 盼 口上娥 D

```
line aux 0
line vty 0 4
 no login
!
end
```

路由器 R2 的配置：

```
R2#show running-config
Building configuration...


!
!
hostname "R2"
!
ip subnet-zero
!
no ip domain lookup
!
!
interface FastEthernet 0
 ip address 202.1.1.8 255.255.255.0
 ip nat outside
 keepalive 10 auto-detect
!
interface FastEthernet 1
 ip address 192.168.201.213 255.255.255.0
 ip nat inside
 vrrp 1 ip 192.168.201.1
 vrrp 1 timers advertise 3
 vrrp 1 priority 120
 vrrp 2 ip 192.168.201.2
 vrrp 2 timers advertise 3
!
!
ip nat inside source list 1 FastEthernet 0 overload
ip nat optimize
access-list 1 permit any
ip classless
ip route 0.0.0.0 0.0.0.0 202.1.1.5
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
no login
!
end
```

可见路由器 R2 与 R1 相互备份，而且二者分别在 VRRP 备份组 1 与 2 中成为主路由器提供不同的虚拟网关功能。

```
  mtu 1488
  ip nat outside
  encapsulation ppp
  dialer pool 1
  dialer-group 1
  dialer idle-timeout 300
  ppp chap hostname xxxx
  ppp chap password 0 xxxxx
  ppp pap sent-username xxxx password 0 xxxx

!
ip nat inside source list 1 Dialer 0 overload
ip nat optimize
access-list 1 permit any
dialer-list 1 protocol ip permit
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer0 permanent
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
no login
!
end
```

可见路由器 R2 与 R1 相互备份，而且二者分别在 VRRP 备份组 1 与 2 中成为主路由器提供不同的虚拟网关功能。

同一 VRRP 备份组内存在路由器的以太网口电缆断开，但是路由器未能检测到以太网口电缆已经断开；

同一个 VRRP 备份组内路由器上 VRRP 的广告发送间隔不一致，并且未设置定时器学习功能；

同一个 VRRP 备份组内路由器上 VRRP 的虚拟 IP 地址不一致。

第六章 安装故障处理

6.1 电源故障排除

锐捷系列路由器可以根据前面板上的 POWER 指示灯来判断路由器电源系统是否出现故障。电源系统工作正常时，POWER 指示灯应保持常亮。如果电源指示灯 POWER 不亮时，请进行如下检查：

路由器电源开关是否打开
路由器供电电源开关是否打开
路由器电源线是否连接正确
路由器供电电源与路由器所要求的电源是否匹配

警告：

请不要带电插拔电源线，如果检查确认一切没有问题，电源 POWER 指示灯还是不亮，请与当地分销商或技术支持人员联系。

6.2 配置系统故障排除

路由器上电后，如果系统正常，在终端上将显示在第四章启动过程中所描述的信息。如果配置系统出现故障，终端上可能无显示或者显示乱码。

如果终端没有显示信息，请进行如下检查：

电源系统是否正常。
控制台口电缆是否正确连接

如果以上检查确认没有问题后，还是无法显示，很可能是配置电缆错误或者终端参数的设置错误，请调整终端的参数。

如果终端上出现乱码，可能是因为终端参数配置不匹配导致，请确认终端参数：波特率为 9600；数据位为 8；奇偶校验为无；停止位为 1； 流量控制为无；终端仿真为 VT100。

说明：

如果您的路由器控制台口参数已经被修改，则也可能导致终端不显示。

第七章 路由器的维护

7.1 ROM 监控模式维护与升级

7.1.1 ROM 监控模式简介

路由器软件包括 BootROM 启动软件和 RGNOS 路由器主体软件，它们运行在不同的模式下。BootROM 软件在路由器开机时，负责启动路由器，同时将路由器主体软件从 FLASH(闪速存储器)中读入到内存，启动完毕后，路由器便退出了 BootROM 软件，进入到正常运行模式。在正常运行模式下，便是 RGNOS 路由器主体软件在工作了。BootROM 软件也有自己的提示符和命令行接口，进入到 BootROM 提示符状态时，便称为 ROM 监控模式。在 ROM 监控模式下，可以完成路由器的 BootROM 升级，RGNOS 主体软件的升级，以及一些路由器的其他维护工作。

7.1.2 如何进入 ROM 监控模式

如果在 BootROM 软件启动时，无法在 FLASH 内找到合法的 RGNOS 主体软件映像时，便直接进入到 ROM 监控模式了。也可以采用手工进入，首先在路由器的 Console 口用标准 RS-232 线缆连接一台微机，并且在微机上运行终端仿真程序，在开机后的 5 秒内按**<Ctrl+Break>**，便进入了 ROM 监控模式了。

启动路由器，当出现

Start BOOTROM V1.9 build 1 (该提示随版本不同，可能有所不同)

的时候，在 5 秒钟内连续按下 CTRL＋Break，出现以下提示：

boot:提示符

即进入 ROM 模式，在 boot:提示符下输入‘**?**’回车，便看到在 ROM 模式下可以执行的指令：

```
boot: ?
boot            boot up an external process
help            monitor builtin command help
reset           system reset
show-env        display the boot env-variables
show-log        display the log of factory test
save            write boot-rom env variable to FLASH
env-delete      unset a boot env-variable
xmodem          x/y modem download
tftp            tftpdown
boot:
```

说明：

要进入 ROM 监控模式，只能在 Console 口上连接终端的方式才可以，不支持其他异步口配置方式和 Telnet 客户端配置方式进入。

锐捷

```
boot: show-env                                    确认修改后环境变量正确
boot: save                                        保存修改后环境变量
PM=boot:
TFTP_SERVER=192.168.12.181
IP_ADDRESS=192.168.12.182
TFTP_FILE=router.rom
boot: tftp –c                                     开始升级路由器主体软件
 %Now Begin Download File router.bin From 192.168.12.181
     !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
 %Mission Completion. FILELEN = 1796468
Now Init Flash...
Now Erase Flash ......
EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE
EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE
EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE
EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE
EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE
EEEEEEEEEENow Copy Image To Flash (FileLen == 1796468)......
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK!]
You Must Reset or Power Cycle for New Config to Take Effect !
boot: reset                                       升级成功，重启动路由器
```

注意：

使用 tftp –c 升级主体软件，请确保你所用软件为 rom 格式的文件，否则路由器无法启动。

如果你手上只有 bin 格式的升级软件，请先使用 tftp –r 下载软件，进入路由器后，在正常模式下升级主体软件。关于 tftp –r 下载软件的详细信息请参考“ ROM 监控模式网络下载执行功能 ”。

7.1.3.2 ROM 监控模式下升级路由器 BootROM 软件

在 ROM 监控模式下，升级路由器的 BootROM 监控软件的步骤和升级路由器主体软件的步骤基本相似，只是最后用于升级的指令的参数不同而已，**一定注意，升级文件不能弄错，否则路由器将彻底无法启动**，具体的升级步骤如下：

选择用于升级的以太网口

锐捷系列路由器支持通过特定的以太网口对路由器的 BootROM 软件进行升级，对于 NBR 系列路由器，选择 WAN 口。确定好以太口后，将该接口和一台有 TFTP 服务功能的微机（假定 IP 地址为 192.168.12.181）通过以太口连接，同时将路由器的配置口通过控制台线缆连接到一台微机的串口上（可以是同一台微机）。

在与以太口连接的微机上运行 TFTP Server 程序，同时将升级路径指向放置 BootRom 升级文件（bootrom.bin）的目录。

设置路由器的环境变量。

用 show-env 查看当前的路由器的环境变量，比如如下提示：

```
boot: show-env
PM=boot:
IP_ADDRESS=192.168.12.3
TFTP_SERVER=192.168.12.98
TFTP_FILE=router.bin
boot:
```

以上环境变量中，IP_ADDRESS 为路由器用于升级的以太口的 IP 地址，TFTP_SERVER 为运行 TFTP Server 的微机的 IP 地址，TFTP_FILE 为用于升级的文件名称，这些环境变量根据具体的升级环境，需要进行重新设定，这些变量全部都为大写，同时在输入新值时，中间不能有空格。

运行 **tftp -b** 对路由器的 BootROM 监控软件进行升级

在 ROM 监控模式下升级路由器 BootROM 监控软件的操作实例如下：

```
boot:
```

对于 NBR 系列路由器，选择 WAN 口。确定好以太口后，将该接口和一台有 TFTP 服务功能的微机(假定 IP 地址为 192.168.12.181)通过以太口连

.

可以在路由器方先用 Ping 测试网络的连通性，

7.3 应对密码遗失

用户忘记[illegible]

configuration running-configuration 来完成这项任务，然后执行 ***config terminal*** 命令进入全局配置模式，运行 ***enabl***

在这里输入'y'，然后回车，接下去的全部直接回车，采用缺省的应答。最后路由器会提示：

```
You must reset or power cycle for new config to take effect
```

5).在 boot:下运行 ***reset*** 重启路由器 ,等待路由器正常启动。

7.5 删除配置

有时用户需要删除配置,恢复出厂配置,方法是:

在特权模式下执行

Red-Giant#**erase startup-config** ,

然后关机重启路由器